VIABILIDAD DE LA MEDIACIÓN FAMILIAR SOBRE BLOCKCHAIN
VIABILITY OF FAMILY MEDIATION ON BLOCKCHAIN

TRABAJO FIN DE MÁSTER
CURSO 2019-2020

AUTOR
EDGAR ESCOBAR ROJO

DIRECTOR
ANTONIO A. SÁNCHEZ RUIZ-GRANADOS

MÁSTER EN INGENIERÍA INFORMÁTICA
FACULTAD DE INFORMÁTICA
UNIVERSIDAD COMPLUTENSE DE MADRID

VIABILIDAD DE LA MEDIACIÓN FAMILIAR SOBRE BLOCKCHAIN

VIABILITY OF FAMILY MEDIATION ON BLOCKCHAIN

TRABAJO DE FIN DE MÁSTER EN INGENIERÍA INFORMÁTICA
DEPARTAMENTO DE INGENIERÍA DEL SOFTWARE E INTELIGENCIA ARTIFICIAL

AUTOR
EDGAR ESCOBAR ROJO

DIRECTOR
ANTONIO A. SÁNCHEZ RUIZ-GRANADOS

CONVOCATORIA: SEPTIEMBRE 2020
CALIFICACIÓN:
9

MÁSTER EN INGENIERÍA INFORMÁTICA
FACULTAD DE INFORMÁTICA
UNIVERSIDAD COMPLUTENSE DE MADRID

7 DE SEPTIEMBRE DE 2020

DEDICATORIA

A mi novia, por haberme animado en los momentos en los que solo veía oscuridad, y haber aguantado esos días junto a mí, que he estado ausente centrado en el trabajo, sin dejar de apoyarme.

A mi madre, que siempre me ayuda a relajarme en los momentos de agobio, permitiéndome tomar de vez en cuando.

A mi padre, por la fuerza de voluntad que me ha transferido, durante toda mi vida, y durante el proyecto.

Y a los tres en conjunto porque sin ellos es muy posible que hubiera tardado otros dos años en acabar este trabajo.

Gracias por no dejar de creer en mí.

AGRADECIMIENTOS

También me gustaría agradecer el apoyo de mis compañeros de trabajo, así como la flexibilidad que me han concedido cuando la he necesitado.

A mi casero, que siendo abogado entendido en los procesos de mediación, fue el que me abrió camino para enfocar el trabajo en este aspecto, resolviéndome diferentes dudas y aclarándome el proceso para poder trasladarlo lo mejor posible a la aplicación.

Y sobre todo a mi tutor Antonio A. Sanchez Ruiz-Granados, que siempre ha sido paciente conmigo durante el largo tiempo que ha durado el desarrollo del trabajo, y que me ha motivado y ayudado a continuar en diferentes momentos.

RESUMEN

Viabilidad de la mediación familiar sobre Blockchain

La tecnología de cadenas de bloques o *Blockchain* es conocida por su potencial al ser una base de datos totalmente descentralizada, pública y con una seguridad muy robusta. Sin embargo, su uso está poco enfocado a las personas individuales, siendo las empresas sus principales beneficiarias, a pesar de sus posibilidades en entornos sociales.

La mediación familiar es una vía alternativa a la judicial para llevar a cabo un proceso de divorcio de forma pacífica y de mutuo acuerdo entre los divorciados, la cual se apoya en una figura mediadora y otra legal.

El objetivo de este trabajo es mostrar la viabilidad del uso de la tecnología en procesos cotidianos entre dos personas, concretamente en la mediación familiar.

Para ello, a partir de una investigación sobre las limitaciones legales y tecnológicas de la cadena de bloques, y sobre el proceso tradicional de mediación, así como de otros casos de uso similares, se ha diseñado y construido una aplicación basada en tecnologías distribuidas (*dApp*) para abogados, mediadores, y personas que se van a separar, sobre la que realizar el proceso de mediación.

Entre otros beneficios de esta aplicación se puede destacar la descongestión en la justicia al simplificar y minimizar la gestión de los procesos judiciales, la mejora del proceso de mediación en la forma de participación de los mediadores y los abogados intentando asegurar su imparcialidad, facilitar el proceso para los separados y aumentar la transparencia del proceso y por lo tanto su fiabilidad.

También se expone la falta de regulación legal sobre estas aplicaciones, que aún necesita tiempo para que se normalice completamente, y permita llevar el potencial del *Blockchain* al máximo.

Palabras clave

Mediación familiar, dApp, Contrato inteligente, Cadena de bloques, Separación, Divorcio, Ethereum

ABSTRACT

Viability of family mediation Blockchain

Blockchain technology is a fully decentralized and public database with very robust security. However, despite its possibilities in social settings, it is focused on companies rather than individuals.

In a divorce process, family mediation is an alternative way to carry out a peaceful agreement between the divorced. Family mediation avoids the judicial players and is supported by a mediator and a legal figure.

This work is focused on the use of the blockchain technology in daily processes between two people, with an especial interest in family mediation.

Accordingly, an application based on distributed technologies (dApp) for people involved in a divorce has been designed. This application is based on the legal and technological limitations of the blockchain, the traditional mediation process, as well as other similar cases.

One of the main advance of this application is the simplification of the judicial processes. It leads to an improvement of the mediation process, facilitates the participation of mediators and lawyers and ensures their impartiality. Altogether, the application facilitates the divorce and increase the transparency of the process, and therefore its reliability.

The lack of legal regulation on these applications is also exposed. They should be normalized and legally regulated to maximize their potential.

Keywords

Family Mediation, Blockchain, dApp, Smart Contract, Divorced, Ethereum, Separation

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Capítulo 1 - Introducción

Desde que apareció la tecnología de cadena de bloques en el año 2008, el mundo empezó a experimentar un gran cambio, que junto con el *IoT* y otras tecnologías se denominó Revolución Industrial 4.0 [1]. Entonces se especulaban muchas posibles aplicaciones de esta tecnología que se han cumplido a lo largo de su evolución, así como han aparecido nuevas posibilidades.

En su comienzo, con el conocido *Bitcoin* su función era únicamente el traspaso de capital de forma segura y sin intermediarios, lo cual era de gran utilidad en muchos escenarios [2]. Pero fue con la aparición de los contratos inteligentes o *Smart Contracts* cuando las posibilidades de la tecnología *Blockhain* se dispararon, y siguen aumentando de manera exponencial, con aplicación en gran cantidad de sectores, permitiendo ejecutar contratos entre dos partes de manera automática, segura y con validez legal [3].

Aunque la tecnología ha tenido una buena aceptación y ya es utilizada en diferentes sectores, aún tiene un largo camino por recorrer hasta que se consigan explotar sus beneficios al máximo.

En la actualidad la realidad es que los principales beneficiarios de esta tecnología están siendo las empresas y sectores industriales en general, utilizándola por ejemplo para realizar contratos entre empresas colaboradoras, para la trazabilidad de sus productos, o seguridad en las transferencias de capital, aportando beneficios empresariales y aumentando la confianza de los clientes en las empresas [4]. En el siguiente texto se muestran las conclusiones de un trabajo de análisis del *Blockchain*. Por un lado, hace visible la inmadurez de la tecnología, y por otro, el enfoque de la misma, el cual se está dirigiendo, principalmente, a modelos de negocio de grandes empresas, en vez de utilizar su verdadero potencial, la descentralización y su uso púbico en el ámbito social.

"*Existen una variedad de industrias en el ámbito privado que ven a la tecnología Blockchain como una forma de mejorar sus procesos reduciendo*

tiempos de procesos, reducción de costos, aumento de la seguridad, transparencia y estabilidad del sistema. Sin embargo, el verdadero potencial de la tecnología se puede apreciar en una red mayor mediante una rápida adopción general, con la generación de nuevos modelos de negocio mediante aplicaciones públicas descentralizadas apoyando el desarrollo de la infraestructura en un aspecto económico, empresarial y social. Pero esta adopción requiere de la articulación tanto del ámbito tecnológico como político, social y económico para llegar a una fase de maduración, si hoy existe un ecosistema robusto aún falta el desarrollo en temas relacionados a la regulación y al conocimiento por parte del macro-entorno." [4].

En la siguiente figura 1.1 se muestra un gráfico del uso del *Blockchain* por sectores, donde es visible su baja aplicación en sectores públicos o en aplicaciones enfocadas a las personas individuales. Es curioso que su mayor uso sea en la banca, cuando el *Bitcoin* nació como un posible sustituto de ella.

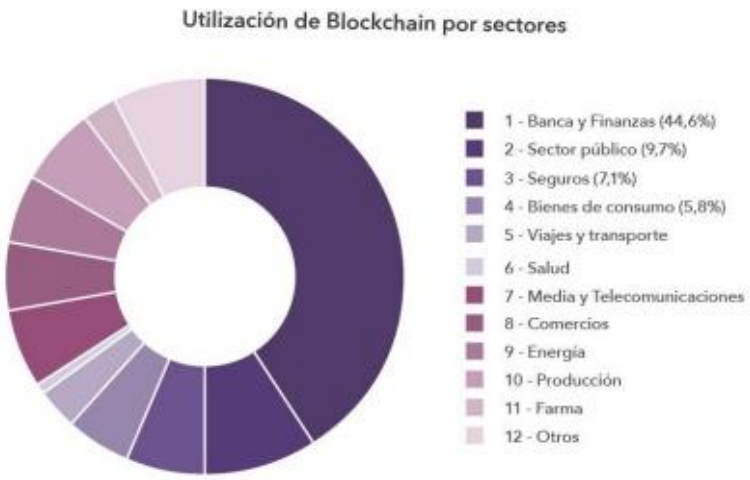

Figura 1.1 Gráfico utilización de *Blockchain* por sectores [5].

1.1 Mediación familiar en el divorcio

Como se ha dicho en el apartado anterior, la aplicación de los contratos inteligentes está poco orientada a los acuerdos entre personas individuales, y como se detalla en los objetivos, este trabajo pretende fortalecer este enfoque. Para ello se ha elegido abordar el proceso de mediación familiar, que intenta sustituir la vía judicial de los procesos comunes de divorcio, como caso de uso en el que aplicar la tecnología tratada.

El proceso de mediación familiar surge de la necesidad de humanizar y facilitar el proceso de divorcio. Por lo general, un divorcio es un suceso triste para las partes, que suele ir unido a otras emociones como la ira, el disgusto, depresiones, etc [15]. Si a las emociones se le suma un entorno judicial, con abogados y jueces, estas emociones pueden aumentar fácilmente debido al ambiente serio y hostil existente. Además, en muchas ocasiones, los abogados no toman conciencia del estado anímico de las personas o de la situación que rodea a cada una (hijos, entorno familiar de cada uno, etc.), llegando incluso a intensificar el odio hacia la otra parte, aunque sea de manera no intencionada, o alentando a una de las partes a pedir unas condiciones en el divorcio desproporcionadas o muy dañinas para la otra parte [16].

Por lo tanto, la mediación pretende sustituir todo este proceso por uno más amistoso, en la medida de lo posible, y para ello se basa en los siguientes puntos:

- Las condiciones de divorcio o separación nacen del consenso de las dos partes, sin tener participación de terceros, como abogados, posicionados hacia alguna de las partes.
- La existencia de una figura mediadora. La misión de esta persona es ayudar a que las partes resuelvan los conflictos que van surgiendo durante el procedimiento de forma pacífica y consensuada. Esta persona debe ser totalmente imparcial y tener conocimientos de psicología y sociología para conseguir su objetivo.

- La existencia de una figura con conocimientos legales que ayude a redactar las cláusulas (dictadas por las partes) del contrato de forma legal y valida ante un jurado. Esta figura también debe ser totalmente imparcial.
- Un juez que valide el acuerdo una vez finalizado el proceso.

Durante el proceso se producen varias iteraciones con reuniones en las que se va llegando a consenso entre las partes y redactando las diferentes cláusulas.

Puede darse que la figura legal y mediadora sea la misma si tiene los conocimientos requeridos tanto legales como psicosociológicos.

Si una vez el contrato está vigente, por haber sido validado por la autoridad judicial, se da un incumplimiento del acuerdo, o existen factores que hacen que alguna de las partes esté en desacuerdo, se debería volver a iniciar el proceso hasta volver a alcanzar un consenso [17].

Es importante mencionar que no se pretende validar la posibilidad de sustituir completamente el proceso actual de mediación familiar por un proceso únicamente tecnológico, ya que como veremos en detalle a continuación, existen diferentes factores y componentes sociológicos y psicológicos del proceso que deben seguir siendo humanos y no son sustituibles. Pero es posible que la tecnología pueda ayudar a complementar ciertas partes del proceso, o incluso conseguir hacerlo viable en escenarios que serían imposibles.

Capítulo 2 - Motivación

La motivación de este trabajo surge de la falta de acercamiento de la tecnología *Blockchain* a las personas, que podría facilitar y mejorar muchos ámbitos de la vida cotidiana. Mostrando la viabilidad y el potencial de aplicaciones descentralizadas, se espera que las personas tomen conciencia, y se redirija el enfoque de las aplicaciones *Blockchain* a una verdadera descentralización útil para todo el mundo.

La idea principal comienza con buscar cómo la tecnología del *Blockchain* se puede utilizar en interacciones entre dos personas de forma que les ayude en situaciones o procesos del día a día, de alguna manera similar a como está ayudando a las empresas al aportar fiabilidad a la trazabilidad de sus productos, por ejemplo, o a funciones de la administración pública como el conteo de voto.

Para encontrar una aplicación concreta de la tecnología se ha buscado un proceso público que pueda aprovechar las ventajas de la cadena de bloques:

- Transparencia.
- Anonimato.
- Descentralización.
- Confianza.

Debido a conocer la problemática que conlleva un divorcio o separación y gracias a la cercanía de un abogado conocedor de los procesos de mediación familiar, los cuales, al igual que la tecnología *Blockchain*, están en una etapa temprana de maduración, se escoge este caso de uso para elaborar una aplicación, ya que se basa en puntos similares, al requerir confianza en el proceso, los abogados, y el mediador, así como el respeto de la privacidad de los participantes. Otro punto de motivación es la saturación de la justicia, la cual puede disminuir con el uso de aplicaciones de este tipo.

Aunque se detalle más adelante, en resumen, la mediación intenta evitar la confrontación entre las partes, eliminando tanto a los abogados personales de cada parte, que pueden llegar a ser avivadores del enfrentamiento, como el entorno de un juzgado presencial, que suele hacer que la situación tome un carácter o enfoque deprimente y belicoso.

Por lo tanto, en el siguiente trabajo se va a desarrollar una aplicación que permita mantener las premisas de un proceso de mediación (privacidad, imparcialidad y legalidad), agilizar y facilitar el proceso de mediación, y acercar tanto el proceso como la tecnología a un mayor número de personas de cualquier clase social al hacer visibles los procesos y aumentar la confianza de los posibles usuarios.

Capítulo 3 - Objetivos y plan de trabajo

3.1 Objetivo general

El principal objetivo de este trabajo es, por lo tanto, mejorar un proceso concreto, la mediación familiar, mediante una aplicación basada en la cadena de bloques.

En segundo lugar, se pretende visibilizar las posibles aplicaciones de la tecnología en diferentes procesos cotidianos de las personas, mostrando el valor de esta a un nivel más bajo y personal que el empresarial y promoviendo su uso a todos los niveles y para todo el mundo, ayudando por lo tanto a que la misma crezca de manera más rápida aportando su valor real.

3.2 Objetivos específicos

Se intenta mejorar los procesos de mediación familiar entre dos personas utilizando la tecnología *Blockchain* con estos fines:

- Abaratar costes:
    - En desplazamientos, tanto para los separados como para los abogados o mediadores que deben participar en el proceso.
    - En tiempo de intervención de los abogados y los mediadores.
    - El coste del proceso en general para las partes, reduciendo papeleo, tiempos de gestión, etc.
- Aumentar la confianza en la imparcialidad de abogados y mediadores.
- Facilitar el dialogo y el arbitraje sin necesidad de tener reuniones presenciales, pero sin perder el seguimiento del proceso por parte de los abogados o los mediadores, minimizando así el impacto psicológico del divorcio en los separados.

- Empoderar a las partes separadas en cuanto a la gestión y la decisión, haciéndolas propietarias de su proceso de separación a la vez que se asegura la equidad de responsabilidades, derechos y obligaciones de cada parte.
- Tener un registro público del proceso completo, validado por autoridades legales y posibilitando la revisión del mismo por un juez, en caso de necesidad una vez resuelto el acuerdo, pero manteniendo el anonimato de las personas que actúan en el contrato para todo el mundo, excepto para cualquier autoridad legal que requiera conocer a las partes, como podría ser un juez.
- Agilizar los procesos judiciales al necesitar menos participación de jueces y abogados, así como descongestionar los juzgados, dejándolos libres para situaciones que de verdad lo requieran.

3.3 Plan de trabajo

Para conseguir estos objetivos, en primer lugar, se investigarán diferentes casos de uso de la tecnología *Blockchain* para conocer sus aplicaciones y extrapolar ideas al contexto del trabajo.

El segundo paso será investigar el proceso de mediación en divorcios, viendo las ventajas que aporta, el estado actual del proceso, y el camino que está llevando ya que es un proceso joven, que está en crecimiento, y aún se está regulando.

Llegados a este punto, se revisarán los casos de uso de la tecnología, investigados en un primer momento, con más detalle, buscando aplicaciones concretas que puedan servir o ayudar en el caso concreto que aborda el trabajo. También se investigarán nuevos casos de uso, más focalizados en el contexto del trabajo para resolver puntos específicos del proceso.

Una vez se haya recabado suficiente información del contexto y las posibilidades de la tecnología, se extrapolará todo lo investigado a una aplicación que resuelva los objetivos para el caso de la mediación en divorcios. Primero se realizará un primer diseño con la funcionalidad básica de la aplicación para a posteriori diseñar la parte técnica (arquitectura, interacciones necesarias, etc.). Después se comenzará a configurar la plataforma y a desarrollar la base de la aplicación. En este punto se hará una valoración de lo desarrollado, extrayendo los puntos no resueltos y buscando posibles soluciones.

Capítulo 4 - Conceptos previos sobre contratos inteligentes en el ámbito de la mediación

4.1 Cadena de bloques y contratos inteligentes

Aunque en este trabajo no se van a detallar las bases teóricas que sustentan la tecnología de cadena de bloques o de los contratos inteligentes, es necesario indicar ciertos puntos básicos que permiten entender como esta tecnología puede servir para cumplir los objetivos de este trabajo.

Una cadena de bloques es una base de datos, con unas características específicas:

- **Control de usuario**: son los usuarios de la aplicación los que controlan totalmente las acciones (transacciones de información) entre ellos y la cadena de bloques.
- **Transparencia**: los datos contenidos están disponibles públicamente y son verificables.
- **Anonimidad y confiabilidad**: los usuarios pueden interactuar con la cadena de bloques de forma anónima y segura, sin existir conflicto con el principio de transparencia. Aunque se conozcan los datos enviados a la cadena de bloques, y se asegure que proceden de una cuenta verificada, no se tiene por qué saber quién es el propietario de esa cuenta de manera pública si el usuario no lo desea.
- **Inmutabilidad**: Los datos añadidos a la base de datos *Blockchain* son inmutables. Un dato no se puede sobre-escribir borrando el anterior. Esto significa que la cadena siempre contendrá el histórico de cambios, similar a un libro de cuentas.

Una vez conocidas esas características que serán importantes para lograr cubrir los objetivos propuestos también es necesario hablar de *Blockchain* como

red. Dependiendo de la permisividad de acceso, existen dos tipos principales de redes:

- **Redes públicas o no permisionadas.**
  En estas, todo el mundo puede acceder y operar, y sus datos son totalmente públicos, aunque sean anónimos. Un ejemplo podría ser *Bitcoin* o *Ethereum*.
- **Redes privadas o permisionadas.**
  Los usuarios deben ser invitados para poder acceder y se pueden establecer permisos para operar. Hyperledger es una de estas redes. En estas no se asegura el anonimato, ya que, como mínimo, el propietario de la red conoce la identidad del resto. [6]

Por otro lado, y ya que este trabajo gira en torno a los contratos inteligentes, se debe explicar de forma breve lo que son los contratos inteligentes. Para ello, primero describimos lo que es un contrato tradicional:

"Un contrato es un acuerdo entre dos o más partes, en el que se define lo que se puede hacer, cómo se puede hacer, y que pasa si no se hace, y que las dos partes se comprometen a cumplir y respetar." [7].

De forma resumida un contrato inteligente es como un contrato tradicional cuyas cláusulas se encuentran definidas en código sobre la cadena de bloques, y que puede contener scripts que hagan que ciertas acciones se ejecuten automáticamente.

Con estas premisas ya se puede ver gran parte del potencial que tienen, ya que implica que utilizando esta tecnología:

- Las cláusulas del contrato no podrán modificarse de forma unilateral de ninguna manera, ya que necesitarían el consentimiento de las dos partes.
- Siempre se tendrá el historial de modificaciones de las cláusulas, siempre aceptadas por las dos partes, permitiendo revisar si esas modificaciones son válidas y se hicieron en la forma correcta, ante cualquier problema que pueda suceder entre las partes.

- En caso de que el contrato implique acciones de las partes automatizables, se podrán programar automáticamente, asegurando su cumplimiento.

Con todo esto los contratos inteligentes pueden facilitar la realización de un acuerdo entre dos partes, ahorrándose ambas, en algunos casos, la necesidad de contratar a terceros que verifiquen ese acuerdo o el coste de llevar el proceso por una vía judicial. En caso de necesitar participación de terceros la ventaja que puede ofrecer la tecnología es la confianza en estos [8].

4.2 Aplicaciones actuales de los *Smart Contracts*

Dadas las características de la tecnología, esta puede aportar valor en cualquier sector en el que:

- Se requiera almacenar datos de forma segura e inmutable.
- Se precise que el acceso a estos datos sea compartido por varias partes.
- Las partes no se conozcan entre ellas o no exista confianza mutua por algún motivo.

Ya son muchos los sectores que utilizan la tecnología para su beneficio o para aportar confianza de sus clientes.

Por ejemplo, la inmutabilidad de los datos es esencial para mantener la trazabilidad de un producto desde su creación hasta su utilización. Asegurando que ha pasado por todas las etapas necesarias, que no se pierden productos, o que no llegan a manos indeseadas. Cualquier producto, ya sea un bien material como un fármaco o uno inmaterial como una aplicación con licencia, puede estar conectado (mediante *IoT* o *software*) con la cadena de bloques, e ir registrando en ella datos tanto de su uso, como de su posición, o de los controles de calidad que ha pasado [10].

Un caso de uso de las transacciones o cláusulas programadas automáticamente se da en el sector asegurador. Un contrato de siniestro con una aseguradora en el que se acuerda un pago ante un acontecimiento constatable

por la cadena de bloques, por ejemplo, un agricultor que contrata un seguro por sequía, en el que si no llueve cierta cantidad en los meses anteriores a la cosecha el contrato inteligente transferirá el pago del seguro a su cuenta automáticamente, es una posible utilidad. También puede valer de ejemplo la garantía de un electrodoméstico, en la que combinando *IoT* e inteligencia artificial, si el aparato se rompe por alguna razón expuesta en la garantía durante el tiempo valido de la misma, se hará el reembolso al cliente automáticamente [11].

En cuanto a la confianza entre las partes existen también infinidad de ejemplos, por ejemplo, en votaciones, en las que evitaría que se manipularan los recuentos ya que todo el mundo vería el sistema o la forma en la que se realiza el conteo, pero nadie podría alterarlo [12]. Otro ejemplo curioso podría ser una cadena televisiva que cobra los anuncios dependiendo del número de personas que lo esté viendo [13]. Un contrato sujeto a esta cláusula realizaría el cobro evitando que la cadena pudiera manipular el dato de la cantidad de personas que estaban viendo el canal en el momento del anuncio.

Existen gran cantidad de aplicaciones, pero el resumen y la conclusión de investigar sobre las posibilidades, es que casi todas están enfocadas al uso para grandes instituciones o empresas, que, aunque beneficien a las personas individuales, no se puede decir que estas sean los usuarios finales principales. Se enfocan en interacciones institución-persona o institución-institución [14].

4.3 Validez legal de los contratos inteligentes

4.3.1 La firma del contrato

Para dar validez a un contrato, una de las premisas principales es que el contrato esté firmado, de forma valida, por ambas partes contratantes. Debido a la evolución tecnológica existen diversos modos de firmar un contrato electrónicamente y en el artículo 3.1 de la Ley 59/2003 de 19 de diciembre se define a la firma electrónica como:

"El conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante." [18].

Dicha firma tiene validez jurídica en los procedimientos judiciales como recoge el artículo 25 del Reglamento eIDAS 910/2014:

"No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada." [18].

Dicho esto, una aceptación de un contrato inteligente en *Blockchain*, mediante una acción del usuario sobre el contrato, y cuya acción esté regulada y por código a que solo el usuario poseedor de la cuenta contenida en el contrato pueda ejecutarla, es suficiente ante un juez para demostrar que el usuario firmó ese contrato. Además, partiendo de las premisas de la tecnología nadie podría sustituir ese código o la cuenta contenida en el contrato con el fin de falsificar la firma.

Aunque de esta manera, ya conseguiríamos suficiente base legal, se podría llegar a dar una mayor validez utilizando lo que se conoce como firma cualificada. La misma se define como:

"Aquella que permite identificar a la persona que firma y detectar cualquier cambio posterior en los datos" [18].

Respecto a utilizar esta firma, en *Blockchain* sería posible mediante el modelo de identidad respaldado por autoridades. Una autoridad externa a la red será la que acredite la validez de la identidad, asociando su clave pública a dicha persona. Incluso podría hacerse todavía más seguro obligando al usuario a que varias autoridades legítimas, validen su identidad, disminuyendo así la posibilidad de suplantación.

Tecnológicamente el requisito para que las claves sean válidas en *Blockchain* es que sean ECDSA [21], lo cual antes podía ser un impedimento, ya que casi todas las autoridades expedían únicamente certificados RSA [21], pero

cada vez existen más que utilizan ECDSA. Por otro lado, es necesario que se pueda comprobar el certificado por otras partes dentro de la red. Aunque en *Ethereum* [19] es necesario implementar operaciones de Validación de Autoridades (VA) de forma manual, otros sistemas como *HyperLedger* [19] ofrecen facilidades de integración para realizar estas operaciones.

Por otro lado, tenemos la importancia, para nuestro caso de estudio, del momento en que se ha firmado el contrato por ambas partes y ha sido validado, y por lo tanto es vigente. La cadena de bloques simplifica estipular el momento en el que el contrato toma vigencia, ya que automáticamente tendremos en la cadena de bloques el dato de la hora en que hubo un cambio y se validó ese bloque, pudiendo tener un pequeño desfase de tiempo. También se pueden utilizar sellos de tiempo (TSA) sellando la información antes de que se transcriba a la cadena de bloques.

- Verificación ECDSA (Algoritmo de firma digital de curva elíptica)

  Se basa en la conocida clave pública-privada, que ya usan muchos algoritmos, y permite añadir a los bloques de la cadena una firma con la clave privada. De esta forma, si una persona valida su identidad ante alguna autoridad legal y esta guarda la clave pública asociada a él, sería posible contrastarla en el futuro con la clave privada con la que se ha firmado un bloque.

  La razón de usar este algoritmo es que permite, crear claves publicas más pequeñas que las RSA, igual de seguras y con bajo coste computacional, lo que las hace perfectas para la tecnología *Blockchain*. Esto se debe a su diferencia con las claves RSA, las cuales se calculaban multiplicandos números primos bastantes grandes, mientras que, para el caso de las ECDSA, la operación radica en calcular los puntos en los que una recta corta con una curva elíptica usando la aritmética modular. Esto es mucho más rentable a nivel computacional [19] [20].

$$k * G = K$$

Clave privada * Punto base = Clave pública

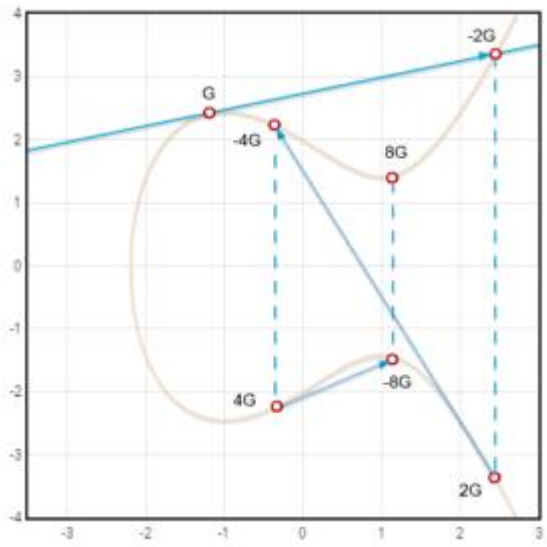

Figura 2.1 Ejemplo visual del cálculo de la clave pública.

Explicando el proceso de la imagen para generar la clave, G será el mismo punto para todas las claves

1. La tangente de G corta la curva en el punto -2G en el eje X.
2. Al reflejarlo se llega al punto 2G y se vuelve a trazar una tangente que corte la curva.
3. Al repetir varias veces los pasos (1) y (2) se llegará al punto kG que será igual a nuestra clave pública [21].

Es importante anotar que para que el proceso sea totalmente seguro la clave privada se debe generar de manera aleatoria.

En el caso de *Bitcoin* y *Ethereum* por ejemplo, la clave pública correspondería con la dirección de tu cuenta que todo el mundo puede conocer, y es generada a partir de la dirección privada que se mantiene en secreto.

4.3.2 Legalidad de las cláusulas

Según las cláusulas o el contenido de un contrato inteligente, junto con la manera de auto ejecutarse, se puede hacer distinción de dos tipos de contratos inteligentes:

- ***Smart Legal Contract***

  Se trata de los más básicos, que funcionarán como scripts autoejecutables mediante cláusulas del tipo *if-then-else*. Otra característica importante de estos contratos es que no necesitan de la intervención de las partes contratantes o de terceros para ejecutarse. Estos contratos pueden ser puramente código ejecutable.

  Debido a estas características, estos contratos inteligentes tienen algunas limitaciones legales, como por ejemplo que las cláusulas del contrato deberían ser objetivables, lo que suele ser muy difícil en la vida real. De ahí que muchos abogados coinciden en que este tipo de tecnología podría ser útil para garantizar el cumplimiento de algunas de las cláusulas de un contrato normal pero no para sustituirlo.

- **Contratos Ricardianos**

  El concepto es creado por Ian Grigg en 1995, y ahora es utilizado en el contexto de los contratos inteligentes. Ian Grigg los denomina como:

  "Contratos digitales que definen los términos y condiciones de una interacción entre dos o más partes, firmados criptográficamente y verificados. Estos deben ser legibles tanto para los humanos como para las maquinas". La principal diferencia con los anteriores es el hecho de que sea

legible para las personas, lo cual borra muchas de las limitaciones que tenían los *Smart Legal Contract* [22].

Aunque en *Blockchain*, generalmente, los que dan validez a un contrato inteligente son los usuarios de la red mediante consenso, para nuestros objetivos esto no sería suficiente. Estos usuarios pueden dar fiabilidad a las transacciones monetarias de las partes, pero no servirían para legitimar el contrato. Por lo tanto, los contratos a los que queremos llegar con este trabajo deberán estar validados por una o varias entidades facultadas con arreglo a Derecho, las cuales podrían ser usuarios de la red, legitimados por dicha autoridad [23].

Otro problema que expone la ley para los contratos inteligentes, es la imposibilidad en la tecnología de cambiar las reglas y consecuencias de las cláusulas una vez se ha creado el contrato. Como veremos en este trabajo esto no será así para algunos casos de uso de aplicación de los contratos inteligentes, en los que son las partes las que ingresan y acuerdan las reglas sobre el mismo contrato inteligente que ofrece una plantilla con cláusulas a completar, con supervisión de una entidad legal [24].

Por otra parte, la Ley expone que cualquier persona está en su derecho de no ser objeto de una decisión basada en el tratamiento de forma automática de datos. Por lo tanto, cualquier persona podría invalidar un contrato preexistente en una red *Blockchain*.

Sin embargo, si en la creación del contrato, en la toma de decisiones que se haga sobre este, en la validación del mismo o el consentimiento de las partes, existiese intervención humana, como es el caso que se investigará en este trabajo, la legalidad del contrato está sujeta a la ley común que rige los contratos, salvo excepciones no contempladas [25].

Para hacer posible el objetivo de la aplicación, se debe permitir a las personas crear sus propios acuerdos de manera autónoma, y sin necesidad de conocer o entender el lenguaje de programación. Para ello, hay que ofrecer una interfaz simple, con las plantillas de cláusulas descritas de manera legal de forma que el usuario solo tenga que seleccionar las posibles variables de la cláusula. El

conjunto, de la cláusula prescrita y de la variable escogida, debe transcribirse literalmente a la *Blockchain* o quedar vinculado a este literal mediante un hash de forma que lo haga inmutable. Como ejemplo *Confideal* [26], en *Ethereum*, ofrece una interfaz para escribir de esta forma los contratos inteligentes, como se puede ver en la figura 2.2.

Figura 2.2: Interfaz *Confideal* [27].

4.4 Arbitraje en contratos inteligentes

Dado que el enfoque del trabajo es sobre la mediación, y en esta existirán dos personas que formularán un contrato, se tiene que partir de la base de que, muy probablemente haya controversia entre las partes, por lo que se necesitará de

terceros que ayuden a resolver esos conflictos. Por otro lado, también es muy posible que las cláusulas formuladas por las partes no sean correctas, y necesitarán reformularse de forma legal, como ya hablamos en la sección anterior.

Aquí entra la posibilidad de acercar el arbitraje a los contratos inteligentes. Existen ya varias aplicaciones de la tecnología en este contexto. Son ejemplos *Kleros* [28], SAMBA o *Confideal* [29], este último, propiedad de *Ethereum*.

En resumen, su funcionamiento es enviar un contrato inteligente a un jurado descentralizado antes de que se ejecuten sus cláusulas. El contrato entre las partes tendrá unos honorarios guardados en él, que habrían sido depositados por ambas partes en la creación del contrato, y que serán distribuidos entre los jueces o árbitros en la resolución del arbitraje. En el contrato enviado a los árbitros, deberán figurar las posibles decisiones o resultados del arbitraje que se pueden dar, que dependerán del contexto del contrato y de las cláusulas que contenga, y podrán ser descritas por las partes contratantes o ser fijas de una plantilla. Los jurados que quieran participar en el arbitraje, y que son reconocidos como autoridades en la materia del contrato, depositaran una fianza en forma de *tokens*. El contrato elegirá, según el número de árbitros pactado en el contrato por las partes interesadas, a los que más *tokens* hayan depositado. En este punto comienza el arbitraje descentralizado, y cada juez vota la resolución que cree conveniente, de las que se propusieron en un principio, de forma privada sin que los demás conozcan su voto. Una vez han decidido todos, se publica el resultado y se resuelve. Los jueces que hayan votado de acuerdo a la decisión mayoritaria, recuperarán sus *tokens* depositados y los honorarios, mientras los que hayan emitido un voto dispar respecto a la mayoría perderán sus *tokens*. Este sistema de incentivos permite la confianza en el jurado, ya que tendrán perdidas si no se implican en dar una resolución correcta [26] [28] [30] [31].

4.5 Legalidad de los oráculos

Como ya hemos hablado anteriormente, la legalidad de las cláusulas de un contrato es un aspecto muy importante y por ello tienen que ser objetivables. Además de esto, si el contrato debe ejecutar alguna acción automáticamente, en base al cumplimiento o incumplimiento de alguna de las cláusulas, el criterio que dicte el cumplimiento o incumplimiento debe ser fiable y no corruptible. Quizás es aquí donde aún se necesita un mayor avance de la inteligencia artificial y adaptación de las leyes.

Esta misión de introducir información en la cadena de bloques es la de los oráculos, ya que los contratos inteligentes no pueden leer información de fuera de la cadena de bloques. De ahí su problema legal, ya que, aunque ya se ha hablado de la seguridad de la cadena de bloques, es en estos sistemas externos en los que hay que mejorar y asegurar su fiabilidad.

Una de las técnicas existentes es utilizar oráculos que recogen la información de múltiples sitios diferentes y la contrastan para luego introducir la información más veraz en la cadena de bloques. De esta forma evitan el problema de la centralización en ellos en cuanto al origen de la información, pero siguen siendo un cuello de botella en el flujo, lo que los hace susceptibles de hackeos, ya que son el único punto de entrada de información externa en la cadena de bloques. [22]

Por otro lado, existe la posibilidad de que sean varios oráculos humanos, los cuales podrían validar cláusulas más subjetivas del contrato. Volvemos a tener el problema de la centralización en esta persona, y la necesidad de confianza en él, por lo que de alguna manera habría que resolver estos dos puntos. Una posibilidad sería mediante identificación y validación de estos oráculos por una autoridad legal, junto a la obligación de que sean varios oráculos humanos, que no se conocerán entre ellos, los que tienen que validar el contrato, evitando la centralización de la decisión en una sola persona [25].

4.6 Flujo de creación de un *Smart Contract*

Hasta ahora, casi toda la ley y la tecnología gira en torno a que los contratos inteligentes son códigos auto-ejecutables y predefinidos de cláusulas de un contrato, y por lo tanto su flujo de creación de forma resumida es:

1. Las partes establecen los términos y condiciones (cláusulas) del contrato de forma legal y fuera de la tecnología *Blockchain*.
2. Se desarrolla el código del contrato inteligente que efectuará el cumplimiento de esas cláusulas automáticamente y se incorpora a la cadena de bloques.
3. Cuando se dan las condiciones pactadas el código se ejecuta automáticamente cumplimentando lo pactado [24].

Con este trabajo se pretende cambiar un poco este paradigma, teniendo plantillas de contratos generales de cada contexto precargados en la red *Blockchain*, y permitiendo que sean los usuarios (partes contratantes) de esos acuerdos los que especificaran de forma autónoma las condiciones particulares del contrato, siempre con supervisión y validación legal. Pudiendo ir cambiando dichas condiciones siempre y cuando los dos estén de acuerdo y el contrato siga siendo legítimo, y figurando en la red la trazabilidad de todos estos cambios, que sería válida en un juicio en caso de llegar a un punto de desacuerdo.

4.7 Conferencias de chat sobre *Blockchain*

Para que el proceso de mediación sobre la tecnología sea completo es necesario que puedan darse reuniones de voz en las que participarán los mediados y un mediador, y dado que estas reuniones no pueden ser sustituidas por un sistema tecnológico, debido a su alto contexto psicosociológico y por lo tanto a la necesidad de presencia humana directa, se debe ofrecer una forma de llevar a cabo estas charlas, manteniendo la seguridad de los datos (lo que se hable) y la anonimidad de los hablantes.

Esto es posible en *Blockchain*. Un ejemplo es la red *Crypviser* [32], de origen alemán, que ha lanzado una plataforma de mensajería instantánea sobre la tecnología que permite, entre otras cosas, el chat de voz.

No recopila datos en la red y estos viajan encriptados, mediante clave pública-privada, por lo que se evita el robo de información y mantiene el anonimato de los participantes dado que la autenticación se realiza a través de *Blockchain*. Ni siquiera la red sabe quién está detrás del nombre de usuario que crea el cliente [32].

Capítulo 5 - Diseño de la aplicación

5.1 Introducción

En base a lo investigado es factible crear una aplicación sustentada en la tecnología *Blockchain* que permita y facilite realizar acuerdos de separación legales bajo las bases del proceso de medicación, con todo lo que ello supone, como el ahorro de recursos tanto para el sistema judicial como para las partes contratantes, o la confianza de la resolución de los hechos pactados, llegando a esta resolución de mutuo acuerdo entre las partes y minimizando la posibilidad de confrontación "violenta", además de tener la seguridad de estar amparados por terceras partes fiables y descentralizadas, que interactuaran en el acuerdo a petición de las partes contratantes y siempre de forma imparcial.

A continuación, se explicará el funcionamiento básico de la aplicación para después detallarlo proceso por proceso. En el siguiente esquema se muestra el conjunto de actores (personas, entidades jurídicas y entidades técnicas) que participan o son necesarias en esta aplicación junto con sus interacciones básicas:

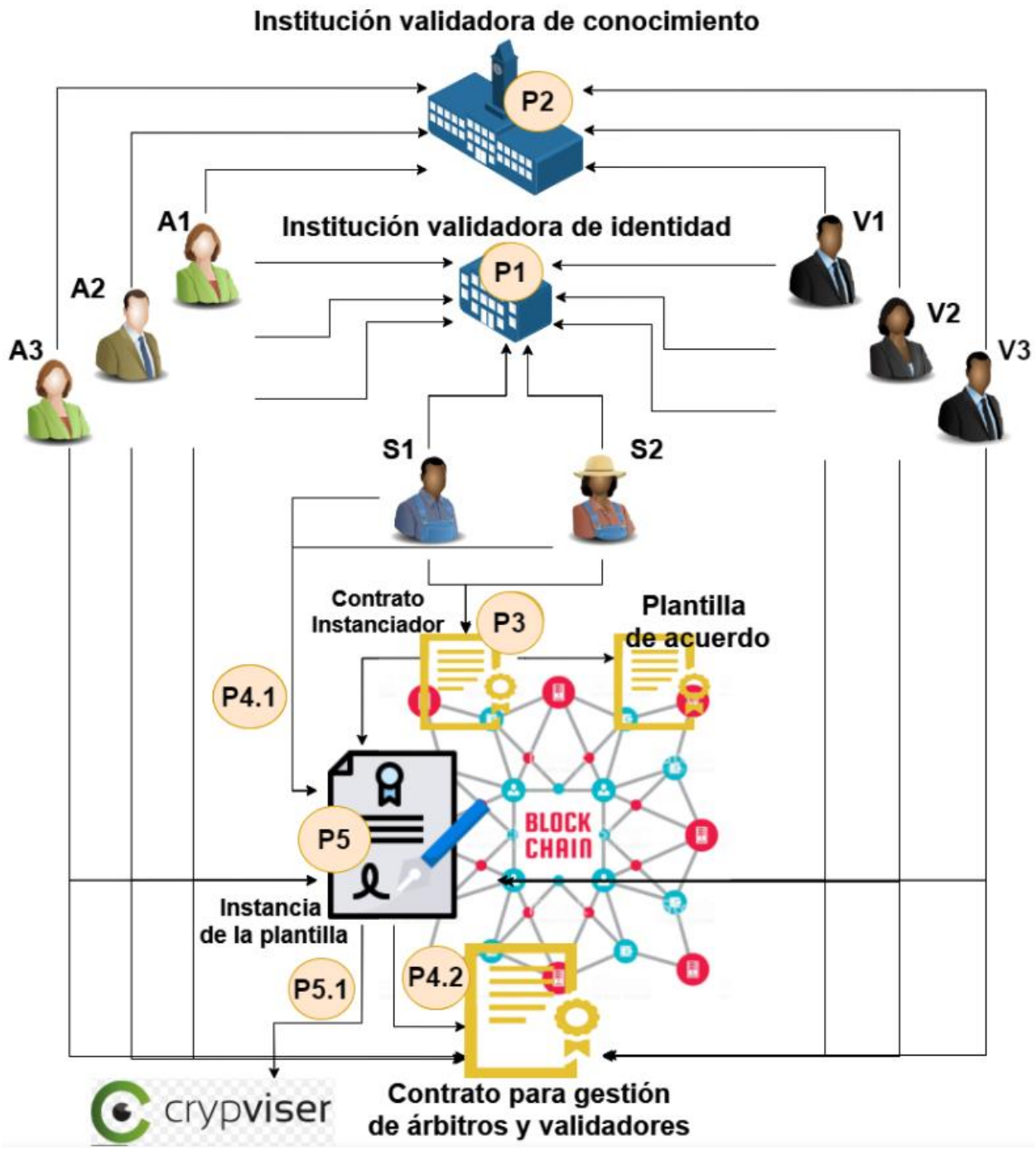

Figura 3.1: Esquema de actores e interacciones básicas.

5.2 Actores

Dentro de la aplicación interactuarán distintas partes que podremos identificar en la figura 3.1 diferenciadas en tres tipos, dependiendo de sus características:

- **Actores humanos**: Serán personas físicas e individuales que interactuarán en los procesos de la aplicación.
    - Partes contratantes (S1 y S2): Serán los principales usuarios de la aplicación. En el caso de este trabajo, dos personas que se quieren separar de mutuo acuerdo.
    - Validadores legales [V1…Vn]: Son los abogados o jueces que se encargarán de validar que cada cláusula, y el contrato en su globalidad, sean válidos legítimamente y estén redactados de forma correcta, ajustado a la legalidad. Pueden ser uno o varios y son elegidos de forma automática por la aplicación.
    - Árbitros de mediación [A1…An]: Su misión es aconsejar y ayudar a que las dos partes contratantes (S1 y S2) lleguen a un acuerdo mutuo justo de forma pacífica, aconsejando sobre la redacción de las cláusulas o apoyando el diálogo en caso de disputa de manera imparcial. Deben tener conocimientos de mediación (psicología, sociología, experiencia en casos, etc) y sería beneficioso si además tienen nociones de legislación. Pueden ser uno o varios y son elegidos de forma automática por la aplicación.
- **Actores Institucionales**: Son las entidades legales que se encargaran de validar a los actores humanos, en identidad y conocimiento. Deben ser instituciones de carácter público, de reconocido prestigio, ya que son un punto de centralización y por lo tanto se requiere la confianza total en su licita actividad. Más adelante se explicarán opciones para generar y validar esta confianza.

- Institución validadora de identidad (Ii): Su misión es posibilitar la identificación de todas las personas que interactúan en la aplicación, de forma que estas puedan ser anónimas dentro del proceso y la cadena de bloques, pero en caso de disputa que necesite llegar juicio, y por lo tanto pueda haber consecuencias para alguno de los inter-actores, se pueda establecer quien es cada uno y en que parte del acuerdo participó.
- Institución validadora de conocimiento (Ic): Se encarga de autentificar los conocimientos y la legalidad de los validadores y los árbitros, certificando que tienen los títulos y la experiencia necesaria para participar en la aplicación.

En ambos casos se ha apostado por instituciones que requieren confianza, en vez de apoyarnos en un sistema de reputación basado en *Blockchain*, ya que, debido a la legislación actual, es necesario para conseguir la legitimidad del contrato.

Para el caso de la identidad, un contrato legal de este tipo requiere, por un lado, que se pueda identificar a las partes contratantes ante un jurado, y por otro, se debe mantener la privacidad de los datos de las partes. Si la identificación dependiera de usuarios de la red, estos necesitarían algún dato que les permitiera verificar la identidad de las partes, rompiendo por tanto el compromiso de privacidad.

De la misma forma, para el caso de la validación de conocimiento, un sistema de reputación requeriría que los usuarios que dan esa reputación tuvieran acceso a documentación o certificados, por ejemplo, de los abogados, rompiendo con su anonimato. Esto provocaría la posibilidad de que una de las partes pudiera identificar a un mediador, perdiendo el beneficio que da la aplicación para confiar en la imparcialidad de estos.

- **Actores tecnológicos**: Se trata de toda la parte técnica que interactúa en la aplicación, como los diferentes contratos inteligentes y otras aplicaciones basadas en *Blockchain* en la que se apoya la nuestra.
    - Plantilla de acuerdo (C): Es un contrato inteligente que contiene la funcionalidad de los procesos y las variables que se usaran durante la mediación y como cláusulas del contrato. La plantilla del proyecto contendrá únicamente tres cláusulas. Una para la custodia de un hijo, otra para la manutención a pagar, y otra para el reparto de la propiedad. También tendrá una sección para pactar tanto el número de abogados y mediadores como el coste que están dispuestos a asumir los separados.
    - Contrato Instanciador (CC): Este contrato será el encargado de crear instancias de la plantilla por cada par (S1, S2) que quieran iniciar un proceso de separación mediante la aplicación. A partir de su interfaz los usuarios pueden crear el contrato.
    - Instancia de la plantilla (Ci): Será el acuerdo en sí, siendo una instancia de la plantilla, y, por lo tanto, conteniendo también la interfaz que permite a los usuarios ejecutar los procesos. Esté será el acuerdo que tendrá validez legal una vez ejecutado y contendrá toda la información referida al contrato.
    - Selección de árbitros y validadores (G_V&A): Este contrato se encarga de gestionar la elección de los validadores y árbitros que van a participar en la instancia. Contendrá la información necesaria de los mismos para gestionar su participación.
    - *Crypviser*: Es la aplicación (*dApp*) encargada de gestionar las reuniones de chat de voz entre las partes y los mediadores.
    - *IoT* Puertas Inteligentes: Es la aplicación (*dApp*) encargada de gestionar el uso de la propiedad. Mediante una puerta inteligente

con *IoT* el contrato indicara qué código tiene acceso, dependiendo de lo definido en la cláusula del contrato.

5.3 Definición funcional

En los siguientes puntos se explican los procesos de interacción entre los actores desde un punto de vista funcional. Durante la explicación se podrán identificar las interacciones de la figura 3.1, representadas en esta con (PN) donde "N" indicará el orden de interacción.

5.3.1 Identificación de actores humanos

Para poder usar la aplicación, tiene que ser posible identificar a la persona que ha participado, pero por otro lado hay que mantener el anonimato de la persona en la red *Blockchain*.

Para ello cada actor humano tendrá una clave privada con la que firmará sus acciones sobre el proceso. Esta clave debe ser conocida únicamente por el actor, ya que será la encargada de mantener la seguridad, evitando que nadie pueda actuar en su nombre.

A partir de esta clave privada se crea una clave pública a la que quedará vinculada. Y será a partir de esta vinculación la manera de determinar, en caso necesario, quien es la persona que actuó sobre el contrato. Por lo tanto, para conseguir su clave privada debe acudir a una entidad legal (Ii), en la que pueda acreditar su identidad, para que le proporcione su clave privada, y esta entidad guarde la pública de la que se originó (P1).

Un caso de ejemplo sería (P1):

1. Carlos entra en la página Web de la entidad (Ii) indicando su DNI, Nombre, Apellidos, Dirección, Fecha de nacimiento.

2. La entidad contrasta la información en su base de datos y envía un código a Carlos. Por mayor seguridad se podría fraccionar y enviar una parte del código como SMS a su teléfono, otra parte a su email, y otra por correo postal.
3. Una vez Carlos ha recibido ese código lo introduce en la página Web, en la que pasara a registrarse en la cadena de bloques.
4. El sistema generará una clave pública conocida para la entidad y Carlos tendrá su clave privada conocida solo por él, con la que podrá actuar dentro de la aplicación.
5. Al añadirse esa clave pública a una lista accesible por el contrato encargado de crear el acuerdo (Ci), estos ya pueden saber si esa persona es identificable sin necesidad de tener ningún dato personal en la cadena de bloques, y, por lo tanto, permitirles usar la aplicación.

En este punto de la aplicación, es necesario confiar en esta entidad, para legitimar el contrato y poder llegar a los usuarios reales en caso de que fuera necesario por un jurado. Partimos de la base de que estas entidades deben ser siempre de carácter público. Para aumentar la confianza en estas entidades, se podría utilizar un sistema sobre *Blockchain* que permita a los usuarios votar o puntuarlas. A mayores, se pueden utilizar oráculos que se encarguen de buscar noticias, en webs oficiales de confianza, sobre corrupción o ilegalidades en estas entidades, de forma que, si encuentra alguna, la invalide en la aplicación.

Al igual que para identificar a la persona como individuo, se debe realizar el mismo proceso para identificar a la persona como autoridad legal (V) o como árbitro preparado (A). Sería un segundo proceso (P2).

Una vez hecho esto tanto "A's" como "V's" pueden registrarse en la aplicación, a través de la interfaz del contrato de selección de árbitros y validadores (G_V&A) para poder participar en acuerdos. En este punto ya tendremos a todos los actores identificados y por lo tanto será posible participar legalmente en el acuerdo.

En la red, la clave privada sería la dirección privada de la red y la clave pública la dirección pública de la red.

5.3.2 Creación de acuerdo entre S1 y S2

S1 o S2, una vez identificados, pueden entrar en la aplicación y crear una instancia de la plantilla de acuerdo, que será donde se desarrolle su contrato. Esta interacción se reconoce en la figura 3.1 como (P3).

Para ello solo tienen que acceder a la aplicación con su cuenta e ingresar sus direcciones públicas (parte superior de la figura 3.2) de cuenta de *Blockchain*, y seleccionar la plantilla de contrato que quieren utilizar, que dependerá de los puntos en los que quieren llegar a un acuerdo. Para la aplicación de este trabajo solo se contempla una plantilla con cláusulas referidas a manutención, custodia y propiedades.

Figura 3.2: *Mockup* de la interfaz de creación del contrato.

La aplicación les devolverá la dirección de *Blockchain*, en el recuadro visible en la parte inferior de la figura 3.2, en la que se ha guardado su contrato para que puedan acceder a él y comenzar su proceso, redactando las cláusulas y operando sobre ellas.

5.3.3 Selección de validadores y árbitros

Una vez creada la instancia las dos partes deberán llegar a un primer acuerdo para conseguir a los terceros actores (validadores y árbitros). En este primer acuerdo se escogen:

- El número de abogados (Vn) que van a querer que den como válida la cláusula de custodia, la cual va a ser una cláusula de tipo texto plano que no tendrá ninguna auto-ejecución, sencillamente será útil para presentar ante un juez, y, por lo tanto, debe tener un formato legal para que no pueda ser impugnada. También tendrán la responsabilidad final sobre la resolución y legalidad del contrato. Tendrán que ser más de tres y un número impar para permitir el sistema de incentivos y votaciones, comparando sus veredictos sin que exista posibilidad de empate.
- El número de árbitros (An) que van a ayudar en el proceso, de los cuales uno será el que actuará como mediador principal interactuando con ambas partes y los demás supervisaran el proceso con el fin de validar su integridad y buena práctica. Este será un número par mayor que cuatro, para permitir el sistema de incentivos y votaciones. La razón de ser pares es que, en este caso, existirá uno principal, y por lo tanto tiene que existir un número impar de personas que evalúe su participación en la mediación.
- La suma de honorarios que las partes (S1 y S2) van a ofrecer a los abogados. Este número tendrá un mínimo y un máximo en función del número de abogados y se repartirá de manera equitativa entre Vn.
- La suma de honorarios que las partes (S1 y S2)) van a ofrecer a los mediadores. Este número tendrá un mínimo y un máximo en función del número de mediadores y se repartirá en función del número de mediadores, llevándose siempre una cantidad mayor el mediador principal que el resto de participantes.

Para llegar a acuerdo entre S1 y S2, estos indicarán sus propuestas en varias iteraciones hasta que los dos estén de acuerdo, en cuyo momento la instancia

llamará al contrato encargado de seleccionar a estos validadores (Vn) y árbitros (An) (P4.1 en la figura 3.1) e incluir sus direcciones en el contrato. En la siguiente figura 3.3 se muestra la interfaz que utilizan S1 y S2 para este fin. En la parte inferior se puede ver y aceptar la propuesta de la parte contraria y en la superior proponer una nueva. En la casilla a la derecha de "Honorarios" se muestra el rango de honorarios en función del número de validadores.

Figura 3.3: *Mockup* de la interfaz de selección de árbitros y validadores para S1 y S2.

Las direcciones públicas de los validadores (Vn) y los árbitros (An) estarán en un contrato, asociados con un mínimo de honorarios que esperan ganar en la participación, elegido por ellos. Al registrarse, depositaran una cantidad de capital (*Ether*), que recuperaran cuando finalice un contrato en el que participen

correctamente, o perderán ante una mala actuación. Esta cantidad dependerá del rango de ganancias que desean ganar, como se muestra en la interfaz que utilizaran en la siguiente figura. Las ganancias esperadas a su vez estarán limitadas por el porcentaje de decisiones acertadas en los diferentes acuerdos que ha participado el árbitro o validador.

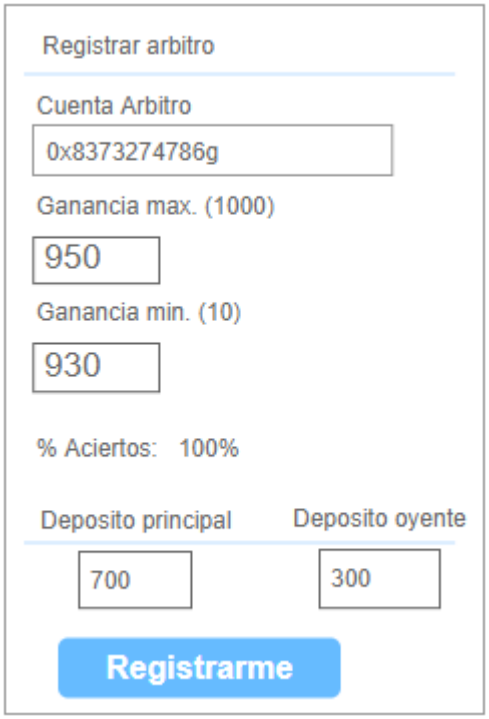

Figura 3.4: *Mockup* de la interfaz de registro para árbitros y validadores.

El contrato inteligente seleccionará a los validadores (Vn) y los árbitros (An), de forma que el reparto de la cantidad ofrecida en el contrato por S1 y S2 para cada participante este dentro de su rango de ganancia esperada, y de esta lista escogerá a los que menos han participado en otros contratos. En caso de que haya empate se compararán las fechas en las que se registraron los árbitros o validadores, eligiendo los que mayor tiempo lleven utilizando el sistema.

Una vez seleccionadas estas cuentas ganadoras, se añaden a la instancia del contrato entre S1 y S2 para que puedan participar en ella (P4.2 en la figura 3.1).

Sistema de reputación y fiabilidad

La ganancia esperada, tanto para validadores (Vn) como para los árbitros (An), deberá estar entre un rango permitido para evitar los precios abusivos, y el depósito de fianza, se escogerá en función de este rango. De esta forma, se consigue que los que tengan mayor coste por su servicio pierdan más en caso de emitir resoluciones incorrectas, consiguiendo así un equilibrio entre el precio pagado y la experiencia del actor en el tema. El rango de ganancia de estos actores tampoco será totalmente libre dentro de ese máximo y mínimo, ya que dependerá del porcentaje de aciertos en participaciones en otros contratos, de forma que cuantas más evaluaciones negativas se tengan en relación a las participaciones en otros contratos se irá disminuyendo la posibilidad de pedir una ganancia en rangos altos.

Porcentaje de aciertos	Rango de ganancias	Deposito Principal (V)	Deposito Principal (A)	Deposito oyentes (Solo árbitros)
>95%	<(900-1000) €	1000 €	700 €	300 €
>85%	<(800-900) €	900 €	630 €	270 €
>75%	<(700-800) €	800 €	560 €	240 €
>65%	<(600-700) €	700 €	490 €	210 €
>55%	<(500-600) €	600 €	420 €	180 €
<55%	Libre	Ganancia max.	70% ganancia max.	30% ganancia max.
0% (1ª participación)	<(600- 700 €)			
>50% (2ª participación)	<(700-800 €)			
>66% (3ª Participación)	<(800-900 €)			

Tabla 3.1: Tabla de ejemplo de ganancias y pérdidas en la aplicación

Aunque en la tabla se muestran valores en euros, estos se pagarán en la aplicación mediante *Ether*, que es la moneda virtual o *tokens* de la red *Ethereum* sobre la que corre nuestra *dApp*. Un *Ether* equivale en torno a 300 euros.

Como se puede ver en la tabla 3.1 un validador o arbitro que no suele acertar no podrá pedir un alto beneficio por sus servicios. De esta forma se asegura una relación oferta-demanda honesta. Como en las primeras participaciones no se puede estimar correctamente la reputación de un actor solo se le permitirán ciertas cantidades, aunque su rango de aciertos le permita elegir cantidades superiores.

Una vez ya se han elegido estos actores, es decir, que ya pueden participar en el contrato, interactuarán de acuerdo al flujo de proceso establecido, siendo estas interactuaciones evaluadas y contrastadas entre ellos con el fin de establecer sus nuevas posibilidades en siguientes participaciones, ajustando su oferta y su demanda.

Como se explicaba en el apartado anterior los validadores y árbitros tienen misiones un poco diferentes, y, por lo tanto, su forma de evaluarse, aunque semejantes, tienen algunas diferencias de unos a otros.

Para los validadores (Vn), que se encargan de validar cláusulas y el contrato global, tanto en una validación u otra, tendrán que emitir su voto de forma privada. Cada actor no puede ver el voto de los demás participantes hasta que todos lo hayan emitido, para evitar que se influyan unos a otros y asegurar que cada uno sea honesto con su evaluación.

Una vez que se hayan emitido, se comparará con la mayoría, de forma que los que sean minoría perderán la cantidad depositada, y perderán su participación en el contrato, siendo sustituidos por otros nuevos actores mediante el mismo proceso explicado anteriormente.

En cuanto al *Ether* que los participantes pierdan por malas actuación, se repartirá entre la pareja (S1 y S2) y la aplicación, en primer lugar, cubriendo parte de los gastos de los interesados (S1 y S2), y el resto destinado a la aplicación. Se ha propuesto este sistema con el fin, por un lado, de conseguir fondos y poder

continuar mejorando la aplicación, y por otro, para devolver a los usuarios S1 y S2 parte de lo gastado, al haberse retrasado el proceso por una causa ajena a ellos. La tecnología podría admitir otra configuración de reparto.

Para los árbitros (An), de forma similar, valorarán la interacción del mediador principal, y los árbitros cuyo voto pertenece a la minoría perderán la cantidad designada (última columna de la tabla 3.1). La diferencia en estos es respecto a la sustitución del mediador principal, el cual perderá su cantidad designada si la mayoría de votos van en su contra, siendo sustituido por uno de los mediadores que participó en el contrato desde su inicio para no perder el contexto del proceso de mediación hasta el momento.

Ya que para el principal (An) la ganancia es mayor que para el resto de mediadores, la perdida designada de este también es mayor que la del resto. No obstante, este tipo de actores tendrán indicadas las dos cantidades posibles a perder, para el caso en que actúen como oyentes y para cuando actúan como mediador principal. Esto es así ya que, si el actor principal es sustituido, un oyente pasará a ser el principal y, por tanto, su cantidad invertida como depósito de fiabilidad deberá cambiar (ultima y penúltima columna de la tabla 3.1).

Todo este sistema intenta evitar la posibilidad de "abusar del sistema", como que varias personas que se conocen intenten participar en el mismo contrato, ingresando a la vez en la aplicación y poniendo un precio alto. Por un lado, no van a poder solicitar altas remuneraciones en sus primeras participaciones, y por otro, será muy difícil que varias personas consigan entrar en el mismo contrato, al tener en cuenta, su número de participaciones y la fecha en la que ingresaron.

Por otro lado, también se consigue la equidad en la participación, es decir, que no siempre sean los mismos los que participan en los contratos, ya que se evaluará el número de participaciones en otros acuerdos, eligiendo al que menos haya participado y cumpla con las especificaciones solicitadas.

Otras opciones que se han estudiado para el sistema de reputación y confianza es que las dos partes contratantes valoren la actuación de los árbitros y los validadores, la cual se ha desechado ya que para evaluar se debería tener unos

mínimos conocimientos, tanto de leyes para los validadores, como psico-sociales para los árbitros. También se decidió no permitir que sean las dos partes contratantes las que eligen al validador en base a su reputación. Esto se debe a que, es muy importante que estos participantes sean totalmente imparciales, y por lo tanto no debe existir la posibilidad, por ejemplo, de que una de las partes conozca la dirección pública con la que actúa un amigo en esta aplicación, pudiendo decantar el proceso de mediación a su favor.

Para esta aplicación no se ha contemplado una forma de evitar que los validadores y árbitros se compartan sus direcciones públicas, para conocerse entre sí. Esto se podría evitar con la encriptación de las direcciones públicas contenidas en los contratos, lo que implicaría un desencriptado cada vez que se tuviera que utilizar.

5.3.4 Desarrollo de la mediación

Para el ejemplo de este trabajo tendremos tres cláusulas (manutención, custodia, propiedad compartida) como se explicaba en el punto 3.2.

Sobre estas cláusulas es importante diferenciarlas en dos tipos:

- **Cláusulas auto-ejecutables**: Son las cláusulas que, una vez acordadas por las partes, el contrato inteligente puede ejecutar de manera automática.
- **Cláusulas verbales**: Estas serán texto plano y definirán un acuerdo verbal entre las dos partes. Ya que son de tipo texto y no se pueden transcribir a código no es posible que la tecnología la ejecute. Servirán como prueba legal de lo pactado ante un juez en caso de incumplimiento por alguna de las partes, ya que contendrán la fecha en la que se acordó y la firma de las dos partes. Este es el caso de la cláusula de custodia.

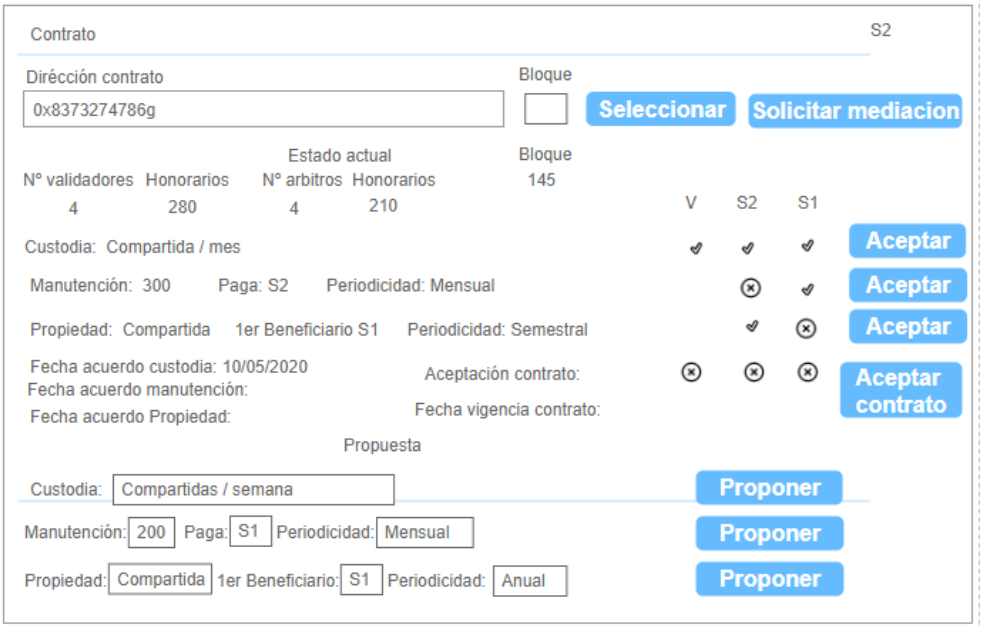

Figura 3.5: *Mockup* de la interfaz de mediación.

En este punto, en el que todos los participantes ya están contenidos en el contrato, se desarrolla la fase de mediación, que consistirá en una iteración, a través de la interfaz mostrada en la figura 3.5, sobre el siguiente proceso (P5 en la figura 3.1):

1. S1 o S2 propone valores para las distintas cláusulas del contrato como se muestra en la parte inferior de la figura 3.5. Las cláusulas que sean de tipo texto plano, como la de custodia, deberán ser validadas o corregidas, en cuanto a la legalidad y sin cambiar la finalidad de la cláusula descrita por S1 o S2, por los validadores (Vn). En caso de ser corregidas, tanto S1 como S2 deberán aceptar esa corrección de nuevo.
2. El otro participante puede aprobar las cláusulas propuestas por la otra parte, o proponer nuevas cláusulas que las reemplacen. Ante un cambio, cualquier cláusula debe volver a ser aceptada por los participantes. La aceptación y estado de las cláusulas tanto para S1, S2, validadores o árbitros, se ve en la línea central de la figura 3.5.

3. Se va iterando hasta que, tanto S1 como S2, estén de acuerdo con todas las cláusulas.
4. Los validadores (Vn) validan el contrato (botón "Aceptar contrato" en la figura 3.5), y este por lo tanto ya tendrá validez legal, y se podrá comenzar a ejecutar las cláusulas automáticas (manutención, propiedades compartidas) sobre el mismo contrato.

En cualquier momento de la iteración entre los puntos (1) y (3) cualquiera de las partes, S1 o S2, puede solicitar la participación del mediador principal mediante el botón "Solicitar mediación", situado en la parte superior derecha de la imagen. En este caso se concreta una reunión de voz, amparada con la tecnología *Blockchain*, entre las dos partes, S1 y S2, y el mediador principal, con el resto de mediadores (An) como oyentes, con el fin de ayudar a resolver el punto en desacuerdo de las partes. Este proceso es reconocible como (P5.1) en la figura 3.1.

Una vez acabada la reunión, se emite la votación de los oyentes, mediante el proceso explicado en el apartado anterior, y se continúa con la iteración.

Los participantes en el contrato también podrán consultar estados anteriores del contrato, indicando el bloque que desean consultar. De forma que puedan revisar el histórico de cambios si lo necesitan.

5.3.5 Ejecución de las cláusulas

Como hemos dicho anteriormente, la ejecución de la cláusula de custodia no se dará dentro del contexto *Blockchain*, por lo que solo figurará como prueba de su acuerdo entre las partes.

Figura 3.6: *Mockup* de la interfaz de ejecución de cláusulas.

Para la cláusula de manutención, se habrá llegado a un acuerdo de cantidad y periodicidad. Por lo que desde que el contrato ha sido aceptado por todos los actores, el que se acordó que fuera el pagador, podrá realizar los pagos a través del contrato, quedando así un registro de ello. El beneficiario podrá indicar si ha habido algún incumplimiento, para que quede constancia, pudiendo el pagador resolverlo también mediante el contrato como se explicará más adelante. En la parte inferior izquierda de la figura 3.6 se muestran los botones para este fin.

Para la cláusula de "propiedad compartida", en la que se habrá llegado a un acuerdo de disfrute de la propiedad por temporadas, el contrato se encargará del cambio de la propiedad, y mediante *IoT*, de permitir la entrada a la propiedad con la llave que posea S1 o con la de S2, que estarán vinculada a la cuenta de cada uno. Para realizar ese cambio, el usuario al que le toque lo solicitará en el contrato (parte inferior izquierda en la figura 3.6), y si ha finalizado el plazo de uso

de la propiedad para la otra parte cambiará la cuenta que figura como beneficiario.

5.4 Materiales y métodos

5.4.1 *Introducción*

Dado que qué el objetivo de este proyecto es hacer llegar la utilización de aplicaciones sobre *Blockchain* a todo el mundo, y más concretamente el proceso de mediación, se ha escogido una red pública que sostendrá nuestra *dApp*, que es *Ethereum*.

Para entender la arquitectura de una *dApp* sobre *Blockchain* se va a comparar con el típico modelo Cliente-Servidor, que se vería como sigue en la imagen.

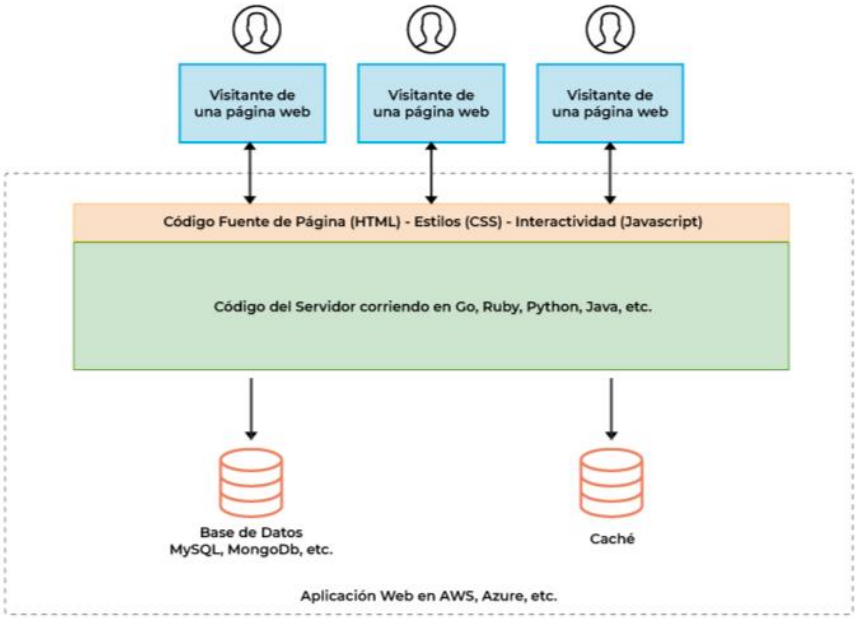

Figura 3.7: Modelo Cliente-Servidor tradicional.

En este modelo la información es accesible en la nube y está contenida en un servidor central, como puede ser *Amazon WS*, el cual puede tener varías copias en distintos servidores.

En cambio, en *Ethereum*, los datos no están centralizados en un servidor concreto, si no que se sostiene al ser respaldada y verificada por todos los mineros de la red.

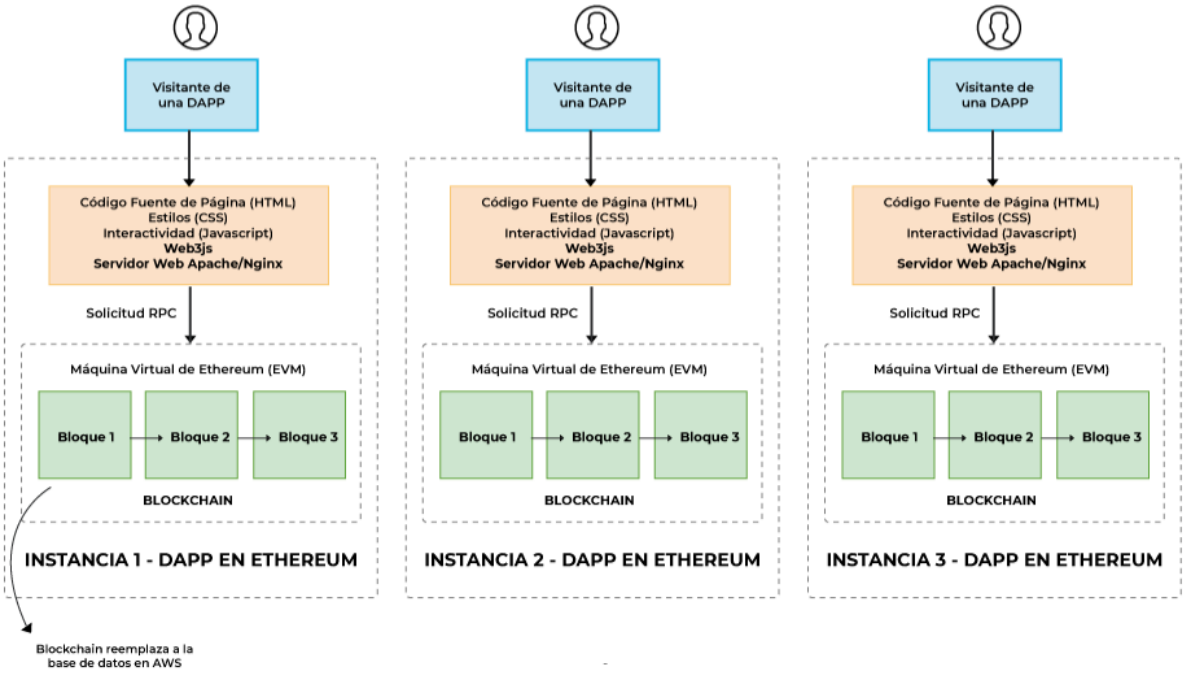

Figura 3.8: Modelo Cliente-Servidor en *Blockchain*.

En este modelo, cada nodo contendrá una copia completa del *Blockchain* desde su creación, lo que hace casi imposible su perdida. Para que un usuario pueda utilizar la *dApp*, bastaría conectarse a uno de esos nodos [33].

5.4.2 Arquitectura base y herramientas

En la siguiente imagen se puede ver el conjunto de herramientas y su interacción utilizadas en el proyecto para construir la aplicación:

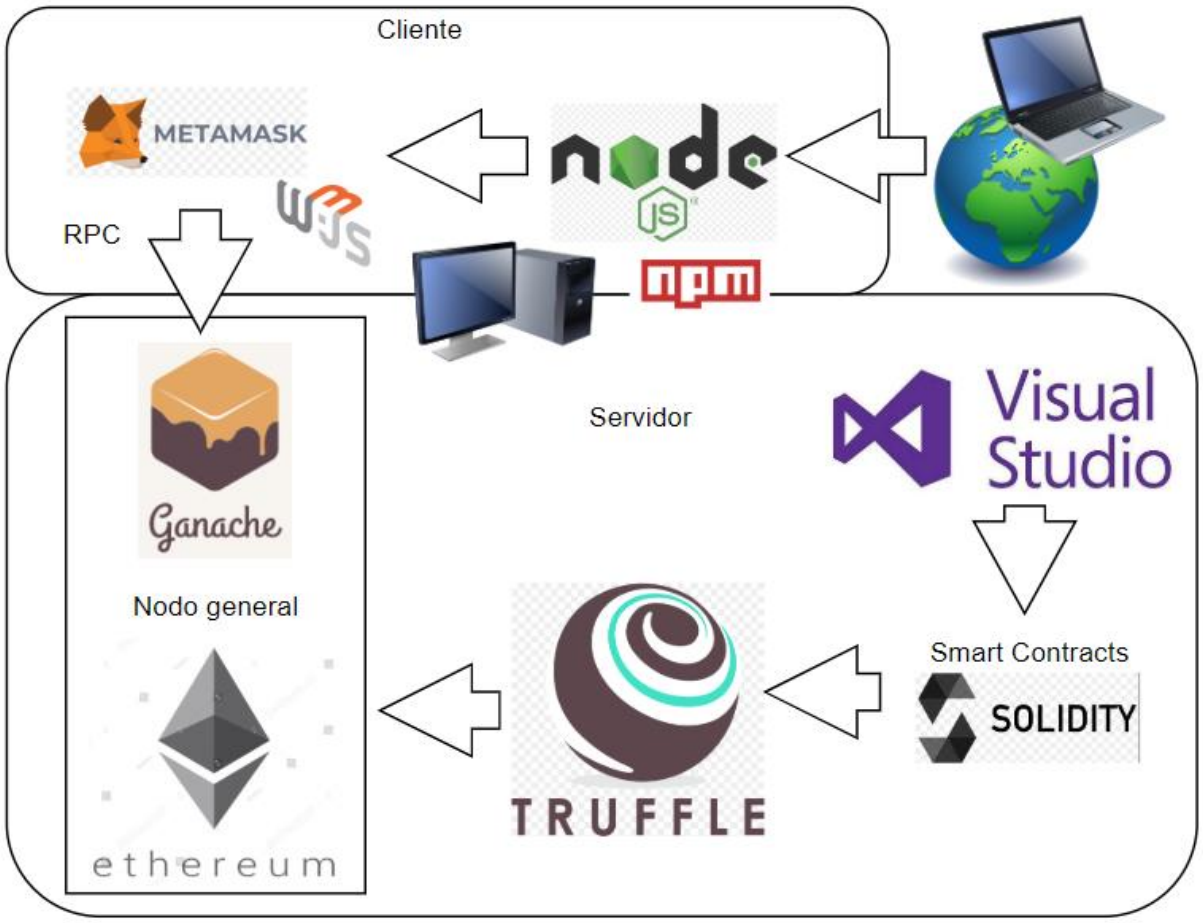

Figura 3.9: Diagrama de tecnologías empleadas.

Una vez la *dApp* es útil correría en la red pública de *Ethereum*, pero para este trabajo hemos utilizado el *framework Truffle* como cliente, junto con *Ganache CLI*, que es un emulador de red *Blockchain* local que ofrece *Truffle*. Además, permite ver, de forma visual, el estado de la *Blockchain* completo (cuentas, contratos, transacciones, etc). Nos permitirá desplegar los contratos y ejecutarlos desde su consola de comandos *Truffle Console*, al indicarle en un archivo *truffle-config.js* la red y el puerto en la que debe desplegar los contratos, que deben ser los mismos parámetros con los que hemos configurado *Ganache CLI*.

También nos apoyaremos en *Node.js* como entorno *JavaScript* en el lado del servidor, y *npm* para facilitar la gestión de paquetes.

Para permitir la interacción de los usuarios con los contratos inteligentes se ha utilizado *Metamask*, que es una extensión para *Chrome* o *Mozilla* que permite gestionar las cuentas de usuario y las transacciones, junto con la librería *Web3js* que actúa como conector.

El código de los contratos está hecho en *Solidity* v0.6.0 que es el lenguaje de programación de *Ethereum* y se ha utilizado *Visual Studio Code* para el desarrollo de los mismos [34] [35] [36].

5.4.3 Tipos de funciones y variables utilizadas

- ***Calls*** [function.call()]: Para leer datos de la cadena de bloques se utilizará este tipo de instrucción. Estas, por un lado, no consumen recursos (gas), y por otro, nos permiten consultar el estado del contrato en bloques anteriores indicándole el número del bloque [.call(145)]. Cuando no se le indica un bloque por defecto consulta el estado del contrato en el último bloque. Junto con la función [getBlockNumber()] que se lanzará en cada transacción que cambie el estado de la cadena de bloques para informar al usuario en que bloque se guardó su última actualización permitirá, que posteriormente, se pueda consultar el histórico evolutivo del contrato [37] [38].
- **Variables globales:** Son una serie de variables globales, muy útiles que podremos utilizar en nuestro contrato.
    - [msg.sender]: Devuelve la dirección de la cuenta que inicio la transacción.
    - [msg.value]: Devuelve el *Ether* enviado en la transacción.
    - [now/blocktimestamp]: Devuelve la hora en la que se hizo la transacción. Puede variar algunos segundos con la realidad, ya que depende, por un lado, de la sincronización del reloj en la máquina que mina la transacción, y por otro lado el momento de minarla.

- **Expresiones de control** [require(exp,msg)]: Esta expresión evalúa condiciones en el momento en el que se llama a una función. Se utilizara para controlar el *Ether* enviado [require(msg.value == 2, "*Ether* insuficiente")], o quien es el que llama a la función [require(msg.sender == dirS1 || dirS2, "No autorizado")], que permitirá controlar que solo las personas adecuadas interactúen con el contrato.
- **Concatenación de *String*** [abi.encodePacked(String1,String2,..,StringN)]: Permite la concatenación de *Strings* dentro de *Solidity*. Concatena los *bytes* de los diferentes *Strings* para formar una sola cadena de *bytes*, que será el *String* resultante.

5.5 Diseño técnico

5.5.1 Arquitectura

En la aplicación cada contrato tendrá una función diferente y, por tanto, ofrecerá una interfaz o API distinta que los usuarios podrán utilizar para llevar acabo las operaciones necesarias.

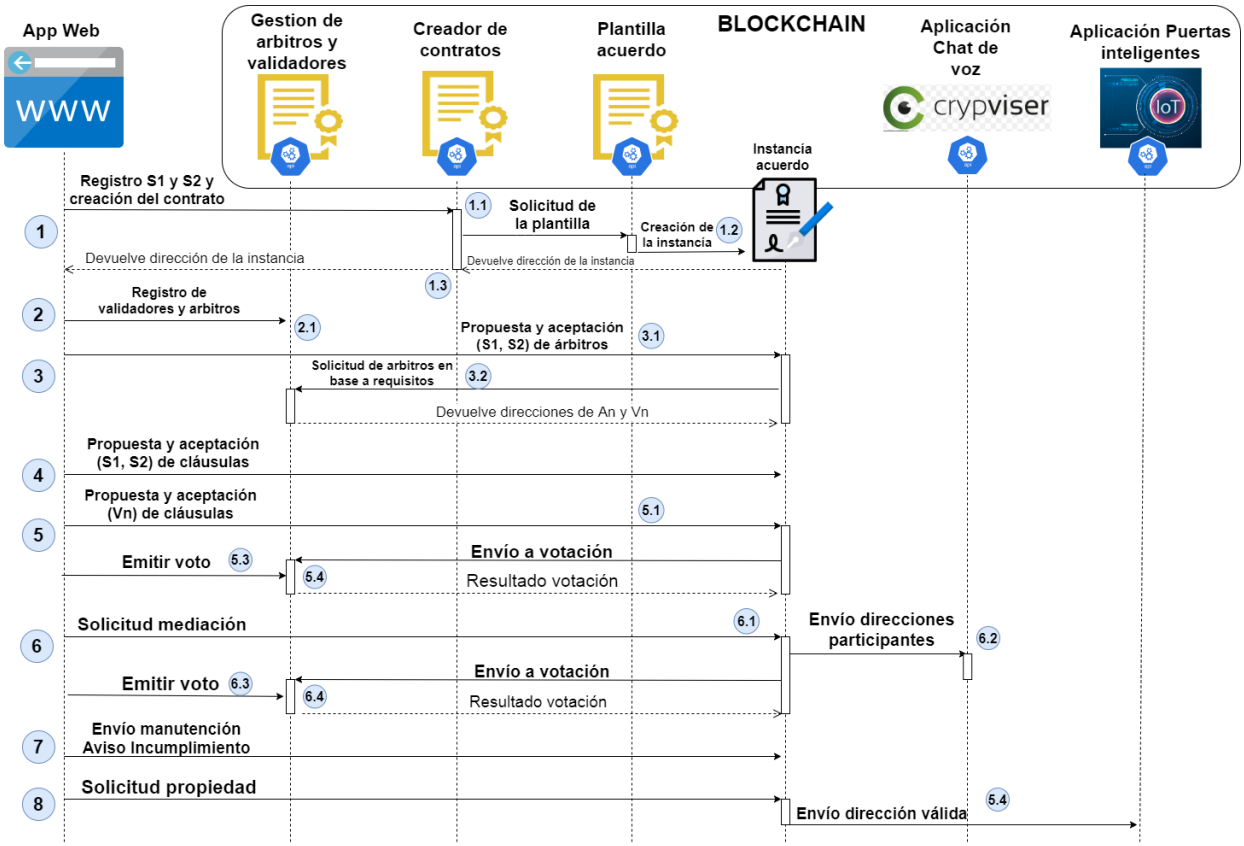

Figura 3.10: Interacción y arquitectura de la aplicación.

A continuación, se detalla la funcionalidad de cada contrato con referencias a la figura 3.10 (números entre paréntesis):

- **Gestión de árbitros y validadores**: Contiene una lista con todas las direcciones públicas de los usuarios (Vn y An) que han sido validados, en identidad y conocimientos, por alguna entidad como se habló en anteriores capítulos, y que por tanto pueden jugar algún papel en un proceso de mediación. Sus únicas funciones públicas vía API serán, por un lado, la encargada de permitir el registro de estos validadores o árbitros indicando sus requisitos (2), y por otro, la que les permitirá realizar las votaciones (5.3 y 6.3). También tendrá funciones privadas encargadas de la comprobación de direcciones (2.1), gestión de la votación (5.4 y 6.4) y elección de los

candidatos a participar en un contrato en base a las especificaciones de las partes solicitadoras (3.2). Estas se explican más adelante con mayor detalle.

- **Creador de contratos**: Contendrá otra lista con las direcciones de usuarios validados, solo en identidad, que pueden solicitar crear un contrato privado. Contendrá un listado de las direcciones de las instancias creadas (1.3), con el fin de permitir el acceso en el futuro a los usuarios del contrato. Mediante este, los usuarios S1 o S2 pueden crear su contrato y acceder a él (1.1).
- **Plantilla de acuerdo**: Es el modelo sobre el que se crea la instancia, heredando esta toda su funcionalidad (1.2). En esta funcionalidad están comprendidas las interacciones de los usuarios como enviar y aceptar propuestas (3.1 y 5.1), solicitud de mediación (6.1) antes de cerrar el contrato, y las de solicitar el uso de la propiedad (8), ingresar la manutención pactada o avisar de que no se ha recibido dicha manutención (7). También contiene la información de las direcciones de los participantes del contrato y del estado de aceptación de las cláusulas por cada parte (S1, S2 y validadores), el registro de las fechas en las que se ha cambiado la propiedad y se ha enviado la manutención, así como un contador de pagos incumplidos. Esta información junto con otras funciones privadas que detallaremos más adelante permiten llevar a cabo el proceso de mediación completo de forma segura y dinámica dentro de la aplicación.
- ***Crypviser***: Es una aplicación externa, también basada en *Blockchain*, que recibirá las direcciones públicas de los participantes cuando se solicite una reunión con los mediadores (6.2). para este proyecto no se explica su funcionamiento interno y actuará como una "caja negra".
- ***IoT* Puertas inteligentes**: Igual que la anterior funcionará como una "caja negra" que recibirá la dirección de la cuenta indicada en el contrato como beneficiaria de la propiedad cuando esta cambié (8.1), y en base a esta dirección permitirá el acceso, mediante *IoT*, a la llave vinculada con dicha cuenta.

En los siguientes apartados se explicará con más detalle cada proceso, profundizando un poco más en ellos.

5.5.2 *Comprobaciones de identidad y creación del contrato*

Tanto para S1 como para S2, en el momento de solicitar crear un contrato deben ingresar sus direcciones públicas de cuenta (1). El contrato inteligente comprobará si sus direcciones públicas existen en una lista (2), en la que se habrían añadido en el momento de identificarse ante la entidad legal. Si existen, y por lo tanto son personas identificables, se crearía su acuerdo (Ci) con sus direcciones (3a). El contrato creador (CC) recibe la dirección de ese acuerdo (4a) vinculándola a una clave (5a), de lectura más simple que la dirección hash. La interfaz solicita esta clave y se la informa al usuario (6a) para que pueda acceder a su contrato de forma sencilla en el futuro. Si el usuario no existe, se notifica un error al usuario y se le indica que debe acudir a alguna entidad de confianza para identificarse (3b). Todo este flujo se muestra en la siguiente figura 3.11.

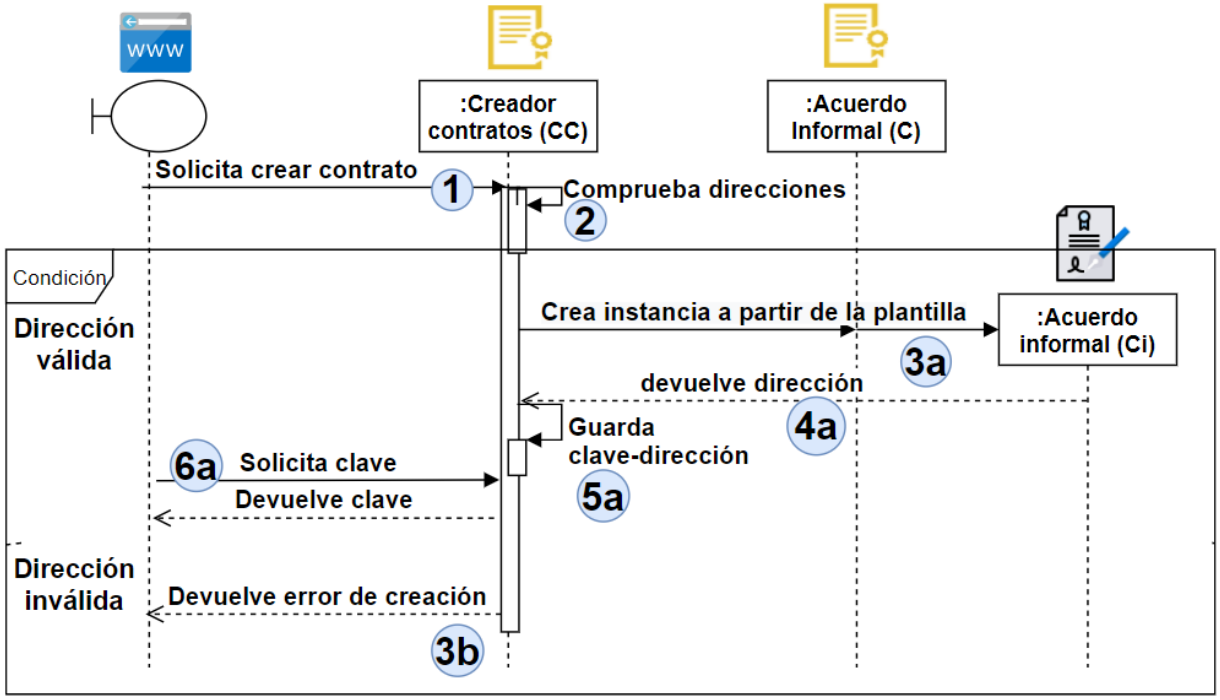

Figura 3.11: Creación del contrato.

De forma similar, como se explica en la siguiente figura 3.12, cuando un validador o arbitro se quiere dar de alta para participar en la aplicación, debe ingresar el rango de beneficios que desea ganar, en base a lo permitido por su experiencia como se indica en la Tabla 3.1. La aplicación en base a este rango calcula el *Ether* que el usuario debe depositar como fianza para el registro y se lo informa (1). Si está conforme, acepta el coste, enviando su dirección, rango de ganancia y el *Ether* que se le indicó (2). Entonces se comprueba si existe su dirección en la lista, y en caso de que exista, se retendrá la cantidad de *Ether* indicada (3). En caso de que su dirección no haya sido validada por una entidad, se le devuelve el *Ether* invertido y queda sin registrar (4). Ese *Ether* le será devuelto si actúa correctamente en la participación del contrato, o lo perderá en caso contrario, repartiéndose entre S1 y S2 o para la aplicación.

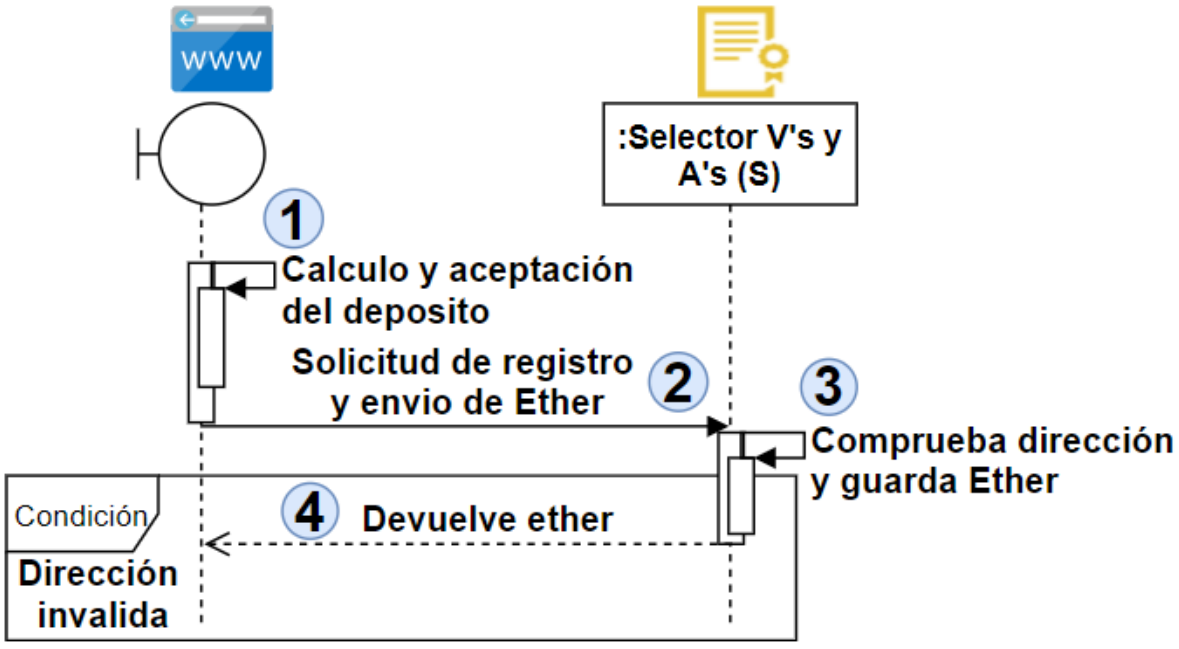

Figura 3.12: Registro y actualización para validadores y árbitros.

Tanto si es su primer registro, como si ya se había registrado se utilizará el mismo flujo, comprobando siempre que la dirección está identificada. Si es nuevo

se creará un registro con la dirección de la cuenta y las especificaciones de honorarios, aciertos, etc. Y para el caso de que ya existiera, pero se deseé cambiar su rango de ganancias, se actualizaría la información relacionada con la dirección existente.

5.5.3 Selección de participantes

Cada parte en el contrato (S1 y S2) podrá acceder al mismo mediante la clave obtenida en la creación y ver su estado (1). A partir de aquí las interacciones se hacen directamente con la instancia. Viendo el estado puede aceptar el actual (propuesto por la otra parte) (2b), o proponer nuevos valores y esperar a que los acepte el otro (2a). Al proponer los nuevos valores (nº de validadores y de árbitros, y honorarios a percibir por cada grupo) se enviará al contrato la mitad de la suma de honorarios como *Ether*, y se devolverá a la otra parte la cantidad que había depositado cuando hizo su propuesta (3a). En caso de aceptar la proposición se guarda el *Ether* (la mitad faltante) y la fecha (3b).

En este punto, que ya se haya llegado a un acuerdo, la instancia llama al gestor de participantes (4b), enviándole las especificaciones para elegirlos (nº de participantes y honorarios). Este gestor escoge a los candidatos de su lista en base a sus características (% de aciertos, participaciones, rango de ganancias) (5b), añadiéndoles la dirección de la instancia en la que actuarán, e ingresa en la instancia sus direcciones de cuenta, para que puedan participar (6b).

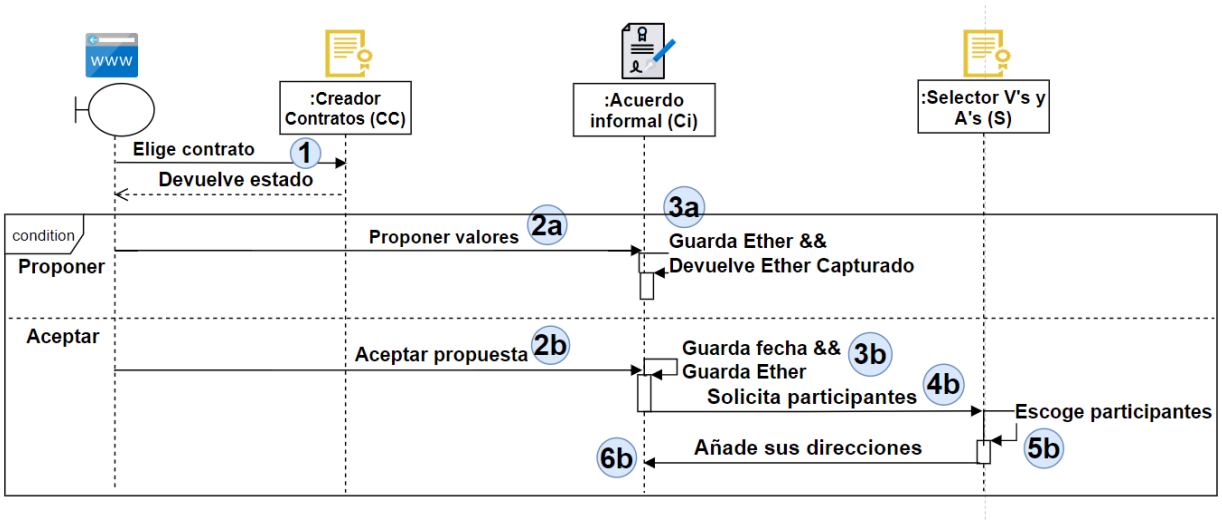

Figura 3.13: Elección de candidatos (validadores y árbitros).

5.5.4 Desarrollo de la mediación

A continuación, se explica el proceso de mediación con apoyo de diagramas de secuencia como los que se han usado hasta ahora. Con el fin de no sobrecargarlos innecesariamente, se han excluido algunas funciones repetitivas. Para todos se habrá realizado el paso (1) expuesto en la figura 3.13 del apartado anterior, y en cualquier interacción de los usuarios con la instancia (Ci) en la que se cambia el estado del contrato, implica guardar la fecha de modificación, similar al punto (3b) de la misma figura del apartado anterior.

5.5.4.1 Propuestas

Aunque en el contrato existen tres cláusulas diferentes el funcionamiento es muy similar, salvo para la cláusula de tipo texto que implica una validación por parte de los validadores. Por lo que es esta la que se va a explicar en la figura 3.14. Para el resto el flujo acabaría en el punto (2).

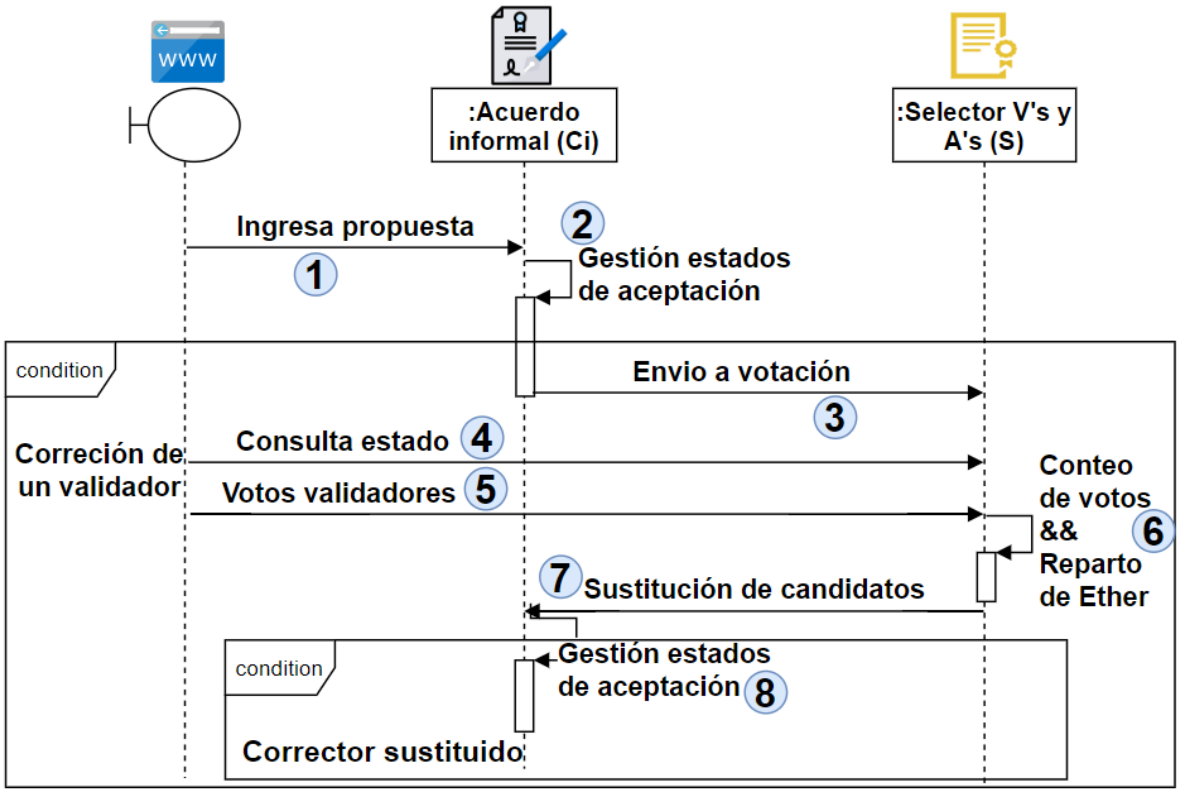

Figura 3.14: Propuesta / Corrección de cláusulas.

En cualquiera de las cláusulas, S1 o S2 ingresarían su propuesta rellenando las variables de esa cláusula en la interfaz mostrada anteriormente en la figura 3.5 y pulsando el botón "Proponer" (1). En cuanto un usuario introduce una nueva propuesta, cambiando el estado del contrato, el estado de aceptación de esa cláusula se modificará como aceptado para el usuario que comenzó la interacción y al contrario para el resto de usuarios (la otra parte mediada y los validadores) (2). Hasta aquí el proceso es idéntico para todas las cláusulas.

En caso de que el actor que ha hecho la propuesta sea uno de los validadores (solo posible para la cláusula de custodia), se notificará al contrato encargado de Gestionar las votaciones (3), actualizando la información de las direcciones de los validadores implicados, para que puedan identificar en dicho contrato que tienen una votación pendiente (4). Cada validador enviará su votó,

aprobando o desaprobando dicha corrección (5), el cuál no se hará público hasta que todos hayan votado. Una vez todos han emitido un veredicto se cuentan los votos (6), y se sustituyen los pertenecientes a la minoría (7) repartiendo su *Ether* depositado entre S1, S2 y la cuenta de la aplicación. Si el validador que realizó la propuesta, pertenece a la minoría, los estados de aceptación de la cláusula de todos los participantes quedarán como "no aceptada", a la espera de una nueva propuesta. En caso contrario, el estado de aceptación de los validadores será "aceptada".

5.5.4.2 Aceptaciones

El flujo para la cláusula de custodia es muy similar al anterior exceptuando el punto (2). En las aceptaciones por parte de S1 o S2, lo que se va a comprobar es si no está aceptada por los validadores, en cuyo caso se iniciará el flujo de votación desde el punto (3).

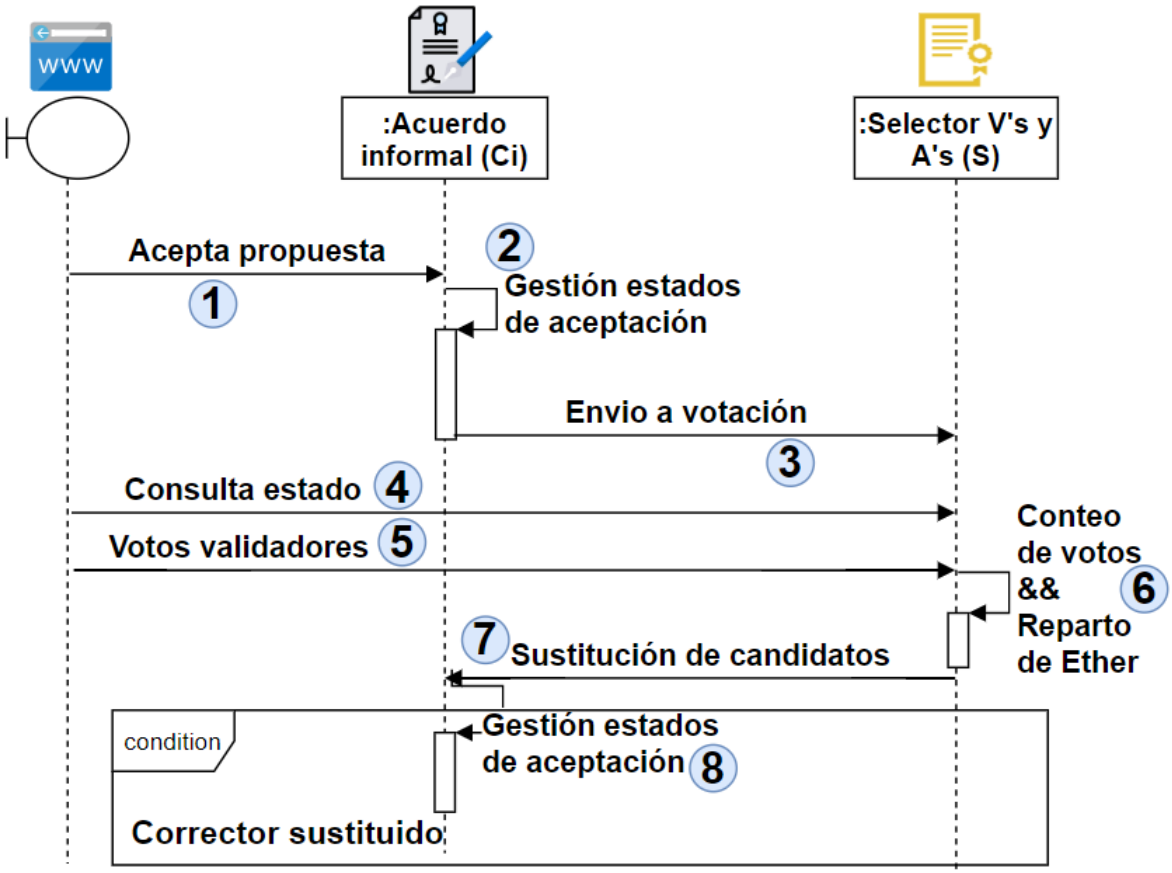

Figura 3.15: Aceptación de cláusulas.

Si el que está aceptando es uno de los validadores, el estado de aceptación de estos no se modificará y directamente se inicia el proceso de votaciones desde el punto (3). En caso de que se acepte por la mayoría se guarda su aceptación para los validadores. En caso de que la votación resulte negativa se elimina el texto de la cláusula volviendo a empezar el proceso, con todos los estados en "no aceptada".

Para el resto de las cláusulas solo participarán S1 y S2 por lo que el flujo acabaría en el punto (2).

5.5.4.3 *Solicitud de mediación*

Si las partes, S1 ó S2, solicitan una reunión con el mediador (1), se les conecta con la aplicación indicada para ello *Crypviser* [39] enviando la información necesaria para que esta pueda llevar a cabo la reunión (2). Una vez la reunión ha acabado se habilita la votación para los árbitros oyentes (3). Estos emites sus votos (4) y, al igual que en la votación para los validadores, se realiza el recuento (5) y los pertenecientes a la minoría son sustituidos (6). Como los árbitros siempre votan a un participante principal, si la mayoría ha emitido un voto negativo contra este, también es sustituido, pero en este casó por uno de los árbitros, pertenecientes a la mayoría, que lleve participando en el acuerdo desde el principio. En caso de que todos los iniciales hayan sido sustituidos se escogerá al que más tiempo lleve.

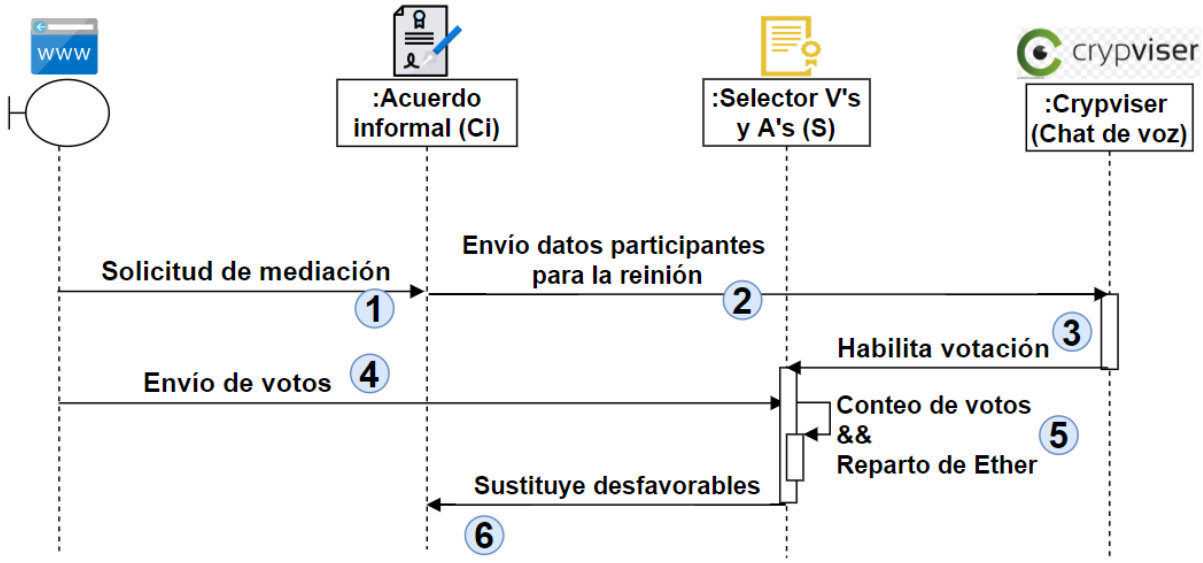

Figura 3.16: Solicitud de mediación.

5.5.5 *Resolución del contrato*

Una vez todas las cláusulas han sido aceptadas por las dos partes, y las de texto validadas por los validadores, se acepta el contrato global. En este momento el contrato inteligente (Ci) envía el *Ether*, que habían depositado al comienzo las

dos partes (S1 y S2), a los validadores y los árbitros. Desde este momento el contrato toma vigencia legal, y se cumplirán las cláusulas de manutención y propiedad sobre el mismo como muestra la figura 3.17.

Como se puede ver en la figura 3.6, la cláusula de manutención el contrato contendrá la cantidad a pagar, la dirección de cuenta del pagador y la periodicidad, además de seguir conteniendo la dirección de la otra parte y de los validadores y árbitros. Internamente el contrato también llevará un registro de las fechas en las que se hacen las transferencias en los diferentes bloques de la cadena, guardando la última como estado actual (2), y un contador, incrementado cada vez que se incumple la fecha de un pago (6) y decrementado cuando se resuelve (4), mostrando así en todo momento el grado de cumplimiento de la otra parte con el contrato.

El usuario que figure como pagador, podrá ingresar en la aplicación solicitando realizar el pago (1). En esta acción el contrato toma de su cuenta la cantidad de *Ether* acordada como "Manutención" y se la transfiere a la cuenta beneficiaria (la otra parte), guardando la fecha (2). En caso de que el contador de incumplimientos sea positivo, porque el pagador se ha saltado algún pago, comprueba la fecha del último pago (3), de forma que si es del día actual significa que ha realizado dos pagos seguidos, resolviendo un incumplimiento y decrementando el contador (4). Acto seguido al comprobar la fecha del último pago, la sobrescribe por la fecha actual (de la última transferencia) (3).

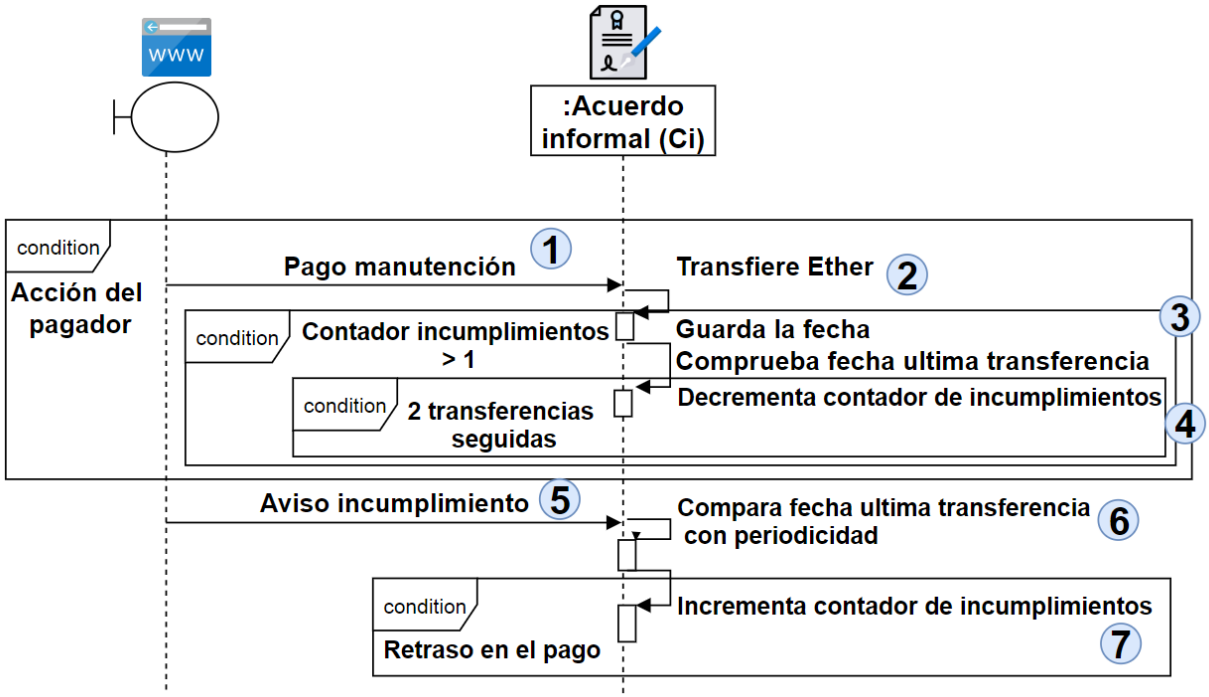

Figura 3.17: Pago manutención y notificación de incumplimiento.

Por otro lado, el beneficiario de la manutención podrá indicar si ha habido un incumplimiento, y el contrato se encargará de verificarlo. Para ello, pulsa el botón "Incumplimiento" (5), visible también en la figura 3.6. En este caso el contrato compara la fecha de la última transferencia que se hizo con la periodicidad acordada (6) de forma que, si el tiempo transcurrido entre ese último pago y la fecha actual es mayor que la periodicidad, se incrementa el contador de incumplimientos (7).

En la interfaz de la figura 3.6 se puede visualizar que la cláusula de propiedad contendrá la información de "Periodicidad" (tiempo de disfrute de la vivienda), "Beneficiario" (dirección de la cuenta que tiene acceso a la propiedad actualmente) y el reparto que se ha hecho de esta propiedad (Indefinida para una parte, o compartida por periodos). Adicionalmente también se dispondrá de la

fecha en la que se hizo el último cambio del beneficiario, en caso de que haya cambiado.

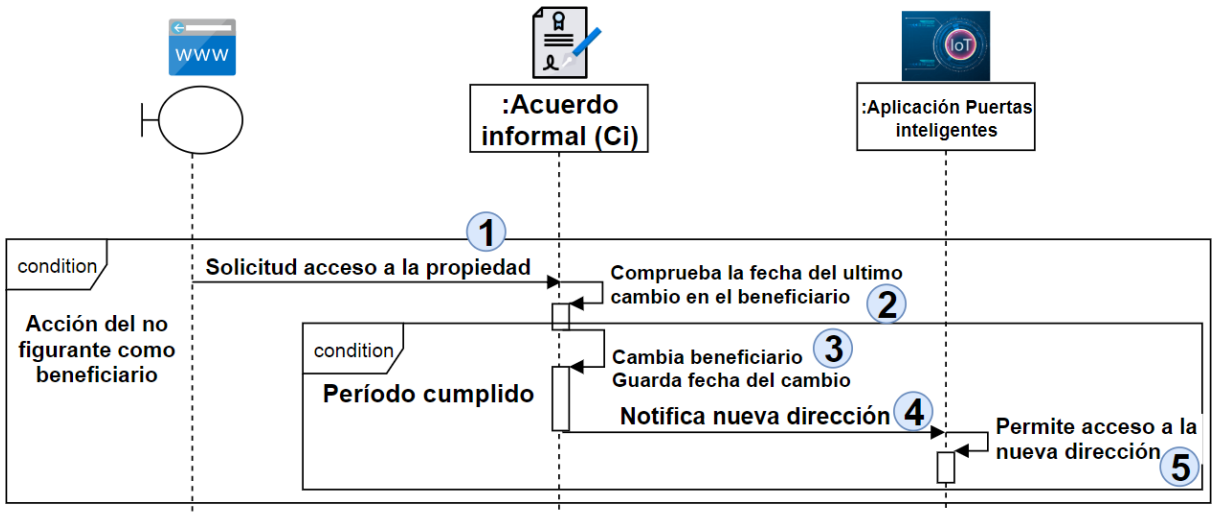

Figura 3.18: Solicitud de acceso a la propiedad.

Si se ha escogido la propiedad compartida por periodos, el usuario que no tenga acceso a la propiedad, podrá solicitarlo en cualquier momento (1), de forma que se le concederá el acceso o no dependiendo de si es su turno. Para ello el sistema compara la fecha del último cambio con la actual (2), de forma que, si el tiempo transcurrido es mayor a la periodicidad pactada, se intercambia la dirección del beneficiario guardando la fecha (3) y se le notifica la misma a la aplicación *IoT* (4) para que permitirle acceder con su llave y denegar la del anterior beneficiario (5).

5.6 Resultado

En el siguiente link de *GitHub* se puede encontrar el código completo y la estructura de carpetas de la aplicación junto con una explicación de los requisitos y los pasos para instalarla:

https://github.com/edesco/FMBEdgar

También se puede visualizar en este link de *Youtube* un video-tutorial básico de ejemplo de uso de la aplicación:

https://www.youtube.com/watch?v=02JAhtOdNBo&feature=youtu.be&ab_channel=EdgarEscobarRojo

5.6.1 Objetivos conseguidos

Aunque por falta de tiempo no se han implementado todas las funciones descritas en el trabajo, se ha conseguido mostrar su viabilidad y explicado cómo sería su desarrollo.

Como aplicación funcional se puede crear el contrato con un validador y un mediador, en el que estos se elegirán en base al rango de ganancias especificado por los separados, llevar a cabo el proceso de aceptación y proposición de cláusulas y del contrato general, así como ejecutar los pagos y los cambios de propiedad sobre el contrato o notificar los incumplimientos.

No se ha implementado un sistema de votaciones debido a que ya existen *dApps* que cubren esta funcionalidad, por lo que simplemente se ha indicado el punto en el que la aplicación del proyecto ejecutaría esa funcionalidad. Por las mismas razones no se ha implementado el contrato gestión de puertas inteligentes y el de chat, y se ha indicado el punto en el que se integraría a estas aplicaciones.

5.6.2 Objetivos no conseguidos

Se ha escogido utilizar solo un mediador y un validador para el ejemplo del trabajo ya que de esta forma se simplificaba el desarrollo, y seguía mostrando la finalidad y la viabilidad del proceso.

Por las mismas razones la elección del validador y el árbitro se hace solo en función del rango de ganancia esperado, sin tener en cuenta el porcentaje de

aciertos del participante, su número de participaciones o su fecha de registro en la aplicación.

Aunque estas implementaciones no se hayan llevado a cabo, o se hayan hecho de forma parcial, en el código se han definido el momento de ejecución y un pequeño pseudocódigo que define su funcionamiento básico, con el fin de poder hacer visible el comportamiento de la aplicación completa.

Capítulo 6 - Conclusiones y trabajo futuro

6.1 Conclusiones

Con las investigaciones realizadas durante el proyecto, tanto en el ámbito tecnológico como en los procesos de mediación, se ha implementado una aplicación básica que puede soportar un proceso de separación sencillo mediante la mediación familiar.

Se ha conseguido cubrir la mayoría de las fases de una mediación manteniendo sus principios de imparcialidad, privacidad y seguridad, además de aumentar la confianza en el proceso. Por otro lado, en la memoria se explica, de manera técnica y funcional, como se podrían cubrir las funcionalidades no desarrolladas, ya sea mediante integración con aplicaciones existentes o definiendo la implementación necesaria en los diferentes contratos inteligentes que utiliza la aplicación (*dApp*) de este proyecto. Por lo que, pese a no haber desarrollado todas las funcionalidades especificadas en la memoria, se cumple el objetivo de hacer visible la viabilidad de este proyecto.

Respecto a los objetivos secundarios propuestos en el proyecto, se han logrado alcanzar todos en mayor o menor medida, como se explica a continuación.

Los costes del proceso se reducen por la disminución de los desplazamientos necesarios y el tiempo de intervención de los actores involucrados en el proceso. Gracias a que se puede llevar todo el proceso desde cualquier sitio y al no ser necesario que todos los usuarios se coordinen para reunirse, excepto para las reuniones entre los separados y los mediadores, se agiliza el desarrollo de la mediación al facilitar la coordinación de los participantes. Por otro lado, también se da un ahorro en recursos materiales (papel, infraestructura, etc) y humanos al no necesitar el mismo personal administrativo, ya que casi toda la gestión del proceso es responsabilidad de la aplicación.

También se puede extrapolar un aumento de confianza en el proceso por parte de los separados. Aunque por ética de los participantes (abogados y mediadores) esta imparcialidad ya se daba por sentada, gracias a la aplicación es visible y regulable. Esto se consigue debido a que la aplicación designa, de manera imparcial y en base a los requisitos de los participantes, quienes serán los abogados y mediadores que llevarán el proceso, asegurando que ninguna de las partes separadas conoce a ninguno de estos actores y que estos actores tampoco se conocen entre sí. A mayores tienen la fiabilidad de que las decisiones de los abogados y mediadores son evaluadas por otros, minimizando la posibilidad de veredictos o arbitrajes incorrectos.

Otra ventaja de la aplicación para los separados es que, al poder llevar todas las fases de la mediación desde un lugar conocido como su casa, y de manera no presencial, pueden estar más relajados, disminuyendo las posibilidades de confrontación y facilitando el diálogo.

Por otro lado, el proceso de mediación se hace más dinámico para las diferentes situaciones en las que se puede dar un divorcio o separación. Aquellas parejas que se encuentren en una separación más pacífica podrán tener más independencia para llevar el proceso por sí mismos, sin perder la seguridad de que existe un seguimiento del mismo por parte de abogados y mediadores. De esta manera se podría disminuir el sentimiento de haber sido influido por el abogado o el mediador.

Para las partes separadas, estos beneficios pueden significar un aumento de uso de la medicación, consiguiendo así que mayor número de divorcios puedan acabar de forma pacífica. Esto supone ventajas como un mejor clima familiar pos-divorcio para los hijos, educación conjunta de los dos padres después del divorcio, menos secuelas psicológicas y económicas para las partes, etc.

Para los abogados y los mediadores los beneficios también están claros. Con una mayor facilidad para participar y gestionar el proceso, se dispondrá de mucho más tiempo para llevar más procesos de mediación familiar u otros procesos de

mayor importancia, aportando una liberación y descongestión tanto del sistema judicial como médico.

Para los mediadores y los jueces, la aplicación también puede suponer una mejora en la toma de decisiones, durante el arbitraje para los mediadores, o ante un incumplimiento de las cláusulas una vez vigente el contrato para los jueces. Además, podrán ver claramente en qué momento se incumplió una cláusula, sin necesidad de testigos o valoración de pruebas, pudiendo dar un veredicto de resolución mucho más rápido que en la forma tradicional. Ya que se dispone de una trazabilidad incorruptible del proceso, los mediadores pueden revisar las reuniones, ver el tiempo que ha costado llegar a un acuerdo en una cláusula concreta, visualizar comentarios, y tener un *feedback* en general que puede ayudarles a mejorar su participación en cada nueva reunión que tengan con las partes.

De forma menos explícita, de todos estos beneficios para este caso de uso concreto se puede extrapolar la utilidad y viabilidad de la tecnología *Blockchain* en otros sectores con procesos similares en los que existen usuarios individuales, los cuales obtendrían beneficios sociales de utilizar estas aplicaciones. Muchas instituciones públicas conseguirían liberarse de una gran carga de trabajo innecesaria, pudiendo centrarse en lo importante para mejorar más rápidamente. El uso de la tecnología también facilitaría la colaboración entre partes al ser descentralizado, sin perder la confianza y la seguridad en los procesos.

En conclusión, es posible llegar a tener una aplicación completa con más tiempo de trabajo y más recursos, como abogados y mediadores que participen en el diseño funcional de todos esos subprocesos que completarían la aplicación.

Con este trabajo se espera que cada vez más personas se enfoquen en utilizar la tecnología con fines sociales, mejorando la vida de la gente cotidiana y la forma de trabajar de las instituciones públicas al servicio de las personas, en vez de enfocarse en los beneficios para las empresas o entidades privadas.

6.2 Trabajo futuro

Como se ha explicado en el apartado de conclusiones, para lograr aumentar la funcionalidad de la aplicación sería necesaria la colaboración de entidades legales (abogados y mediadores) conocedoras del proceso de mediación, así como de personas técnicas implicadas en la tecnología *Blockchain*.

En los siguientes puntos se hablará de algunas funcionalidades viables que mejorarían la aplicación.

6.2.1 IoT para la propiedad

Para ejecutar de forma automática la cláusula de la propiedad, un contrato inteligente podría comprobar la cuenta que se encuentra ubicada en la cláusula del contrato como pagador, y a su vez esta cuenta, tener una llave con un RFID relacionado. Un lector de códigos RFID instalado en la puerta y conectado directamente con la aplicación, concretamente con el contrato de esa pareja en separación, podría comprobar si el RFID con el que se intenta entrar es el que aparece en el contrato, de forma que solo tendría acceso a la vivienda la persona que el contrato indica que es su período de estancia.

Por otro lado, también se podría hacer la transferencia de la propiedad a nivel legal sobre el contrato inteligente. Aunque aún está evolucionando este uso de la tecnología, falta una regulación legal total dentro de la tecnología. Fuera de España ya se han hecho compra-ventas de inmuebles sin ningún tipo de intermediario físico a través de contratos inteligentes. Aunque en España también se han realizado compras mediante criptomonedas, aquí sigue siendo necesaria la figura de un notario. Al igual que ya existen algunas aplicaciones como *Shelterzoom* o *Propy* para la venta legal de inmuebles, se podría utilizar está base tecnológica para transferir la propiedad de S1 a S2 automáticamente en base a la periodicidad de la cláusula de propiedad [40], siendo un oráculo el que calcula el tiempo y solicita el cambio en el contrato.

6.2.2 *Cambios sobre el contrato vigente*

En la aplicación del proyecto, una vez se ha aceptado y validado el acuerdo total, la finalidad del contrato inteligente es albergar la trazabilidad del acuerdo, pudiendo ver el histórico de cambios, así como la fiabilidad de las firmas ante un jurado y ejecutar las cláusulas pactadas (manutención y propiedad). En caso de que las partes S1 o S2 quieran cambiar alguna cláusula tendrían que crear un contrato nuevo.

Un siguiente paso para la aplicación es permitir a los usuarios modificar o rescindir cláusulas una vez el contrato está vigente, manteniendo la vigencia de las cláusulas anteriores que ya se han pactado y cerrado, y siguiendo un proceso de validación legal de las nuevas. De esta forma el mismo contrato serviría a las personas durante mucho más tiempo, sin tener que volver a iniciar el proceso completo. Ya que las circunstancias de las personas pueden variar fácilmente durante la vigencia del contrato, esto permitiría mucha más flexibilidad ante estos cambios.

Por otro lado, se podría establecer cláusulas dinámicas, por ejemplo, una manutención sujeta a un contrato de trabajo. Mientras el pagador tenga un contrato, se debe pagar la manutención, y en caso de que no lo tenga, no será necesario. En este punto el problema sería establecer un oráculo de confianza que sea el que indique al contrato si el pagador tiene un contrato de trabajo o no.

6.2.3 *Automatización del pago*

Facilitar la carga de *Ether* en el contrato por parte del pagador de la manutención sería otro punto posible de mejora. De esta forma el pagador podría ingresar varios pagos de una sola vez, dejando al contrato encargado de gestionar los pagos a la otra parte en base a la periodicidad y la cantidad de manutención especificadas en el contrato inteligente.

6.2.4 *Feedback y calendario*

Completar el proceso de mediación permitiendo mayor interacción de las partes separadas y los mediadores en el contrato almacenando el *feedback* y los comentarios, podría ayudar a los mediadores a mejorar su participación.

También sería muy útil tener la posibilidad de agendar las reuniones en la aplicación de forma similar a *Google Calendar*.

6.2.5 *Mejores oráculos*

Investigar en colaboración con mediadores, abogados y técnicos de *Blockchain*, con el fin de poder añadir más cláusulas al contrato y automatizar la verificación de las mismas, facilitando aún más el trabajo de los jueces ante incumplimientos.

6.2.6 *Plantillas dinámicas*

Una posibilidad es aumentar el número de plantillas de contratos, con diferentes cláusulas y para diferentes tipos de separación según la situación de las parejas.

Otra posibilidad es tener una plantilla de contrato global con todas las posibles cláusulas que se pueden dar en una separación y permitir a la pareja elegir cuales son las que quieren pactar en el contrato, desechando las demás.

6.2.7 *Otras aplicaciones*

Como se ha visto en el proyecto, la viabilidad de este uso de los contratos inteligentes se podría extrapolar a contratos entre dos personas en otros campos, en los que podrían beneficiarse igualmente del arbitraje y la validación

descentralizada, así como de la posibilidad de llegar a un acuerdo sin necesidad de pasar por ambientes judiciales y papeleos innecesarios.

Apéndice A - Introduction

The Blockchain technology appeared in 2008. Since then, the world experimented a great change. The Blockchain technology and the IoT, along with other technologies, triggered what was called The Industrial Revolution 4.0 [1]. These technologies opened new possibilities that have been assessed during these years and they have brought new approaches under development.

At the beginning, with the well-known Bitcoin, its function was only to safely transfer the money [2]. However, the appearance of smart contracts soared possibilities of the Blockchain technology. Now, it continues exponentially increasing. The Blockchain applications allows the execution of contracts between two parties automatically, safely and with legal validity, in a large number of environments [3].

Although the technology has had a good acceptance and is already used in different sectors, it still has a long way to go before its benefits are fully exploited.

Currently, the Industry is the main beneficiary of this technology, which is used to make contracts to trace the products, or to safely transfermoney. In sum, it increases business benefits and makes customers trust in companies [4]. The following text shows the conclusions of a Blockchain analysis work: On the one hand, this analysis highlights the immaturity of technology. On the other hand, it shows an approach focused on business models of large companies, instead of using its real potential, the decentralization and public use in the social spheres.

"*There are a variety of industries in the private sphere that see Blockchain technology as a way to improve their processes by reducing process times, reducing costs, increasing security, transparency and system stability. However, the real potential of the technology can be appreciated in a larger network through rapid general adoption, with the generation of new business models through decentralized public applications supporting the development of infrastructure in an economic, business and social aspect. But that requires the collaboration between technological, political, social and economic fields to reach a mature*

phase. Even though today the ecosystem is robust, there is not development on regulation and knowledge by the macro- environment." [4]

Figure 1.1 shows the use of Blockchain by sectors, where its low application in public sectors or individuals is visible. Curiously, its greatest use is in banking, where Bitcoin was born as a possible substitute for it.

7.1. Family mediation in divorce

As mentioned in the previous section, the application of smart contracts is not oriented to individual agreements. As detailed in the objectives, this work aims to strengthen this approach. For this reason, the family mediation process has been chosen. Here, this process would be used to replace the judicial way of common divorces.

The family mediation process appears to humanize and facilitate the divorce process. In general, a divorced is a sad event, which is usually associated with other emotions such as anger, disgust, depression, etc [15]. When a complicate judicial environment is added to the emotions, with lawyers and judges, these emotions can easily magnify due to the hostile environment. In addition, lawyers are often increasing the tension since they are not aware of the personal situation that surrounds each one (children, family environment, etc.) [16].

Therefore, the family mediation process is focused on moderating divorce process following the next points:

- The conditions of divorce or separation comes from the consensus of the two parties, without the participation of third parties, such as lawyers, positioned towards either of the parties.
- The existence of a mediating figure. The mission of this person is to help the parties resolve the conflicts that arise during the procedure in a peaceful and consensual manner. This person must be totally impartial

and have a background in psychology and sociology to achieve their goal.

- The existence of a figure with legal knowledge that helps to write the contract clauses (dictated by the parties) in a valid legal way. This figure must also be totally unbiased.
- A judge to validate the agreement once the process is finished.

During the process there are several meetings where the parties agree in a common consensus and the clauses are written.

The legal and mediating figure could be is the same if they have the required legal and psychosociological background.

Once the contract is validated, by the judicial authority, if there is a breach of the agreement, or there are factors that cause any of the parties to disagree, the process should be started again until a new agreement is reached [17].

It is important to mention that it is not intended to totally replace the current family mediation process with an entire technological process. As we will see in detail below, there are many sociological and psychological factors that are human, so they cannot be replaced. However, this technology can help complement parts of the process, or even make it viable in scenarios that would be impossible.

Apéndice B - Conclusions and future work

6.3 Conclusions

This project, focused on the use of technologic in a mediation process, has implemented a basic application that can support a separation process through family mediation.

Most of the phases of a mediation has been covered while maintaining its principles of impartiality, privacy and security. In addition, it has increased confidence in the process. The memory also explains, how the undeveloped functionalities could be covered, either through integration with existing applications or by defining the implementation in the different smart contracts used by the application (*dApp*) of this project. In spite of all functionalities specified in the document were not developed, the viability of this project has been exposed. Moreover, the secondary objectives proposed have been achieved.

On one hand, this study shows how the costs of the process are reduced by the reduction of the trips and the intervention time of the people involved. Due to the fact that the entire process can be done from anywhere and the users to coordinate do not need to meet, except for meetings between the separated and the mediators, the mediation is expedited. On the other hand, there is also a saving in material resources (paper, infrastructure, etc.) and human resources, since the application manages almost of the process.

Additionally, the technology increases the reliability of the process. Although the ethics of the participants grants their impartiality, human factors are often making the process bias. The application makes this fact visible and quantitative. The application impartially designates, who will be the lawyers and mediators, ensuring a double-blinded process. Thus, the decisions of lawyers and mediators are

evaluated by others, increasing the confidence and minimizing the risk of incorrect verdicts.

Another advantage of the application is that, by being able to carry out all the phases of the mediation from a place known as home, participants can be more relaxed, reducing the possibilities of confrontation and facilitating dialogue.

Moreover, the mediation process becomes more dynamic for the different situations in which a divorce or separation may occur. Those couples who are in a more peaceful separation will be able to have more independence to carry out the process by themselves, without losing the security that there is a follow-up of it by lawyers and mediators. In this way the feeling of having been influenced by the lawyer or the mediator could be diminished.

For the separated parties, these benefits could suppose a peaceful agreement. This would also translate into a better post-divorce family climate for the children education and psychology.

For lawyers and mediators, the benefits are also clear. Being easier to participate and manage the process, there would be much more time for mediation or other important processes, which would provide a release of the judicial and medical systems.

During arbitration, the application leads to an improvement in decision-making for mediators and judges, also in the event of a clause breach once the contract is in force for judges. In addition, participants would be able detect when a clause is breached, without witnesses or evidence assessment. This would solve the cases faster than in the traditional way. Since there is an incorruptible traceability of the process, mediators can review the meetings, see the time it took to reach an agreement on a specific clause, view comments, etc. Altogether, the application allows to have a feedback that can help mediators and judges improve their participation in the following meetings they have with the parties.

Generally, all the benefits mentioned before could be extend to other sectors s in which individual users, would obtain social benefits from using these applications. Many public institutions would be able to get rid of unnecessary work, being able to focus on the important things. The use of technology would also facilitate collaboration between parties since it is decentralized, which avoid losing trust and security in the processes.

In conclusion, it would be possible to have a complete application. However, it needs more time and resources, such as lawyers and mediators who could participate in the functional design to get the full process covered.

This work expects that progressively more people focus on the use of the technology for social purposes, improving the public institutions function and people lives, instead of focusing on the industry benefits.

6.4 Future work

As explained in the conclusions section, in order to increase the functionality of the application, the collaboration of legal entities (lawyers and mediators) who are familiar with the mediation process, as well as technical people involved in Blockchain technology, would be necessary.

In the following points, we will talk about some viable functionalities that would improve the application.

6.4.1 IoT for property

On one hand, a smart contract could automatically execute the property clause. It could verify the account that is located in the contract clause as a payer. This account would have a key with a related RFID. An RFID code reader would be installed on th door to check if the RFID is the one that appears in the contract. Thus, only the person who is allowed by the contract have access to the house.

On the other hand, a smart contract could also legally transfer of ownership. Although this use of technology is still evolving and there is not full legal regulation. Outside of Spain, real estate sales have already been totally made by smart contracts. In Spain, some purchases have also been made through cryptocurrencies, but the notary is still necessary. As there are already some applications such as "Shelterzoom" or "Propy" for the legal sale of real estate, this technological base could be used to automatically transfer ownership from S1 to S2 based on the periodicity of the ownership clause [40], being an oracle which calculates the changes in the contract.

6.4.2 Changes to the current contract

Once the total agreement has been accepted and validated, the smart contract would allow to store the traceability of the agreement. Thus, the history of changes, the signatures and the agreements in maintenance and property could be consulted at any time. In case the parties S1 or S2 want to change any clause, they would have to create a new contract.

The next step is to allow users to modify or terminate clauses once the contract is in force, while it maintains the validity of the previous clauses, and following a legal process of validation of the new clauses. In this way, the same contract would work for longer, avoiding starting the whole process all over again. This would allow more flexibility, since during the term of the contract.

Moreover, dynamic clauses could be established. For example, the maintenance could depend on an employment contract. Which means, as long as the payer has a contract, maintenance must be paid, but if the payer loose his or her job, the payment would not be mandatory. At this point, the problem would be to establish an oracle of trust, which would be who indicates to the smart contract whether the payer has an employement contract or not.

6.4.3 *Payment automation*

Another point of improvement would be to facilite the loading of Ether in the contract by the maintenance payer. In this way, the payer could enter several payments at once, allowing the contract to manage the payments. The decisions would be made based on the periodicity and the amount of maintenance specified in the smart contract.

6.4.4 *Feedback and calendar*

As mention before, one of the advantages of the application is the store of the information. Feedback and comments could increase the interaction of the parties and mediators, which improve the engagement of the people involved.

Also, the application could schedule meetings, in a similar way to Google Calendar, which would be very helpful.

6.4.5 *Better oracles*

To get better results, it is needed the collaboration with mediators, lawyers and Blockchain technicians to add more clauses to the contract, to automate their verification and to facilitate the work of judges in the event of non-compliance.

6.4.6 *Dynamic templates*

One possibility could be to increase the number of contract templates. These would have clauses that would adjust to different situations depending on the couples.

Another option could be a global contract template with all the possible clauses that could occur in a separation. In this one, the couple would choose the optimal one, discarding the others.

6.4.7 Other apps

As seen in the project, the smart contracts could be used not only in the Industry, but also in physical people contracts. The smart contracts guarantee equity in arbitration and decentralized validation, as well as the possibility of reaching an agreement without the need to go through judicial environments and unnecessary paperwork.

BIBLIOGRAFÍA

[1] M. C. Planas, «El Blockchain y la industria 4.0,» [En línea]. Available: https://forocapitalpymes.com/el-blockchain-y-la-industria-4-0/.

[2] S. Nakamoto, «Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario».

[3] «Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?,» bit2me Academy, [En línea]. Available: https://academy.bit2me.com/que-son-los-smart-contracts/.

[4] L. R. A. ROJAS, «ANÁLISIS DE LA TECNOLOGÍA,» 2018.

[5] E. D. Zúñiga, «La tecnología Blockchain en las instituciones financieras,» 27 Diciembre 2018. [En línea]. Available: https://www.ig.com/es/estrategias-de-trading/la-tecnologia-blockchain-en-las-instituciones-financieras-181224. [Último acceso: 10 Febrero 2020].

[6] bit2meAcademy, «bit2meAcademy,» [En línea]. Available: https://academy.bit2me.com/cuantos-tipos-de-blockchain-hay/.

[7] R. A. d. l. Lengua, «Definicion de contrato».

[8] «https://academy.bit2me.com/que-son-los-smart-contracts/,» [En línea]. Available: https://academy.bit2me.com/que-son-los-smart-contracts/.

[9] V. Christophe, «SUPPLY CHAIN: La blockchain garantiza la trazabilidad,» generix group, 8 Agosto 2018. [En línea]. Available: https://www.generixgroup.com/es/blog/supply-chain-la-blockchain-garantiza-la-trazabilidad.

[10] J. Maldonado, «Las aseguradoras buscan en blockchain y los smart contracts simplificar su relación con los usuarios,» ObservatorioBlockchain, 4 Septiembre 2019. [En línea]. Available: https://observatorioblockchain.com/las-aseguradoras-buscan-en-blockchain-y-los-smart-contracts-simplificar-su-relacion-con-los-usuarios/.

[11] S. JAGATI, «Sistemas de votación en la Blockchain - ¿Puede la Democracia confiar en ellos?,» Cripto Intercambio, 3 Noviembre 2019. [En línea]. Available: https://es.cointelegraph.com/news/blockchain-voting-systems-can-democracy-rely-on-them.

[12] «Tecnología Blockchain en marketing y publicidad,» 30 Abril 2019. [En línea]. Available: https://aunmasdificiltodavia.es/tecnologia-blockchain/.

[13] N. P. y. M. Conejero, «Tecnología blockchain: funcionamiento, aplicaciones,» 2018.

[14] I. Bolaños, «Mediación familiar en contextos judiciales.,» 2003.

[15] L. G. V. I. B. C. M. H. R. S. G. T. P. d. H. A.-M. A. D. B. y C. M. O. , «La familia dialoga y llega a acuerdos: La mediación familiar,» Dirección General de Familia, Madrid, 2010.

[16] I. Bolaños, «Mediación familiar en contextos judiciales,» Valencia, 2003.

[17] L. C. Galdón, «"Informe jurídico sobre la realización de un smart contract a una empresa de renting de vehiculos eléctricos,» Madrid, 2019.

[18] I. Molero, «Libroblochain - ECDSA,» Libro Blockchain, 31 Mayo 2017. [En línea]. Available: https://libroblockchain.com/ecdsa/.

[19] A. M. Bermúdez, «Estudio de la utilización de protocolos blockchain en sistemas de votación electrónica,» Barcelona, 2016.

[20] A. Muñoz Cuña, «Sistema de verificación de documentos usando árboles de Merkle,» Madrid, 2019.

[21] I. O. Moreiras, «Análisis jurídico de los smart contract,» LegalToday, 23 Mayo 2019. [En línea]. Available: http://www.legaltoday.com/firmas/legaltech/analisis-juridico-de-los-smart-contract.

[22] M. A. Blanco Pérez, E. López-Román, E. Montalván Calderón, E. Suárez Otero, P. Farran Castellà y F. F. Espinoza Valencia, «Abogacía Española - Consejo General Contratos inteligentes: los "smart contract",» Abogacía Española - Consejo General,

[En línea]. Available: https://www.abogacia.es/publicaciones/blogs/blog-nuevas-tecnologias/contratos-inteligentes-los-smart-contract/.

[23] K. G. L. CRUZ, «ANÁLISIS JURÍDICO DE LOS SMART CONTRACTS BASADOS EN LA TECNOLOGÍA BLOCKCHAIN EN EL COMERCIO ELECTRÓNICO EMPRESA – CONSUMIDOR (B2C),» 2019.

[24] P. d. R. Castillo, «PROBLEMAS CON LA EJECUCIÓN DE LOS LEGAL SMART CONTRACTS,» Madrid, 2019.

[25] Criptonoticias, «Criptonoticias,» 29 Septiembre 2017. [En línea]. Available: https://www.criptonoticias.com/aplicaciones/confideal-plataforma-hacer-tratos-arbitraje-descentralizado-anuncia-ico/.

[26] «CryptoNinjas,» 2018. [En línea]. Available: https://www.cryptoninjas.net/2017/09/22/confideal-end-complicated-processes-forming-signing-managing-smart-contracts/.

[27] «keros.io,» Kleros, [En línea]. Available: https://kleros.io/es/curated-list/.

[28] M. Duarte, «Ciar Global - El futuro del arbitraje radica en el uso del Blockchain,» Ciar Global, 16 Abril 2019. [En línea]. Available: https://ciarglobal.com/el-futuro-del-arbitraje-radica-en-el-uso-del-blockchain/.

[29] D. N. Baquero, «Agromercatorum,» 20 Marzo 2018. [En línea]. Available: https://agoramercatorum.uexternado.edu.co/los-smart-contracts-un-medio-para-el-desarrollo-del-arbitraje-virtual/.

[30] F. C. MÍNGUEZ, «BLOCKCHAIN: APLICACIONES A LA ADMINISTRACIÓN PÚBLICA,» Valencia, 2019.

[31] «Llegó Crypviser, el Whatsapp cripto imposible de hackear,» cripto247, 12 Febrero 2019. [En línea]. Available: https://www.cripto247.com/emprendimientos/llego-crypviser-el-whatsapp-cripto-imposible-de-hackear-180402.

[32] E. Garcia, «Medium - Aprende Blockchain: Tu primera DAPP en Ethereum - Parte I,» 5 Marzo 2018. [En línea]. Available: https://medium.com/@ernestognw/aprende-blockchain-tu-primera-dapp-en-ethereum-parte-1-a86773d44ca0.

[33] C. Vazquez, «IslaBit - 4 pasos para diseñar una arquitectura para tu app Ethereum,» 24 Mayo 2018. [En línea]. Available: https://www.islabit.com/81042/ethereum-disenar-aplicacion.html.

[34] M. P. H. Bas, «Implementacion y despliegue de una solución de gamificación en la empresa sobre redes públicas y privadas,» Madrid, 2018.

[35] «Aprende blockchain,» [En línea]. Available: https://aprendeblockchain.wordpress.com/desarrollo-en-ethereum/desarrollo-con-truffle-i/.

[36] «StackExchange Ethereum,» 2018. [En línea]. Available: https://ethereum.stackexchange.com/questions/47215/how-can-we-obtain-the-state-value-of-a-variable-from-previous-block-number-using.

[37] «web3.js Documentation,» [En línea]. Available: https://web3js.readthedocs.io/en/v1.2.7/web3-eth.html#id52.

[38] «crypviser,» [En línea]. Available: https://crypviser.com/es/index.html.

[39] «BBVA - ¿Puede "blockchain" cambiar la forma en que compramos casas?,» 1 Agosto 2019. [En línea]. Available: https://www.bbva.com/es/puede-blockchain-cambiar-la-forma-en-que-compramos-casas/.

[40] L. A. Bucki, Word 2013 Bible, John Wiley & Sons, 2013.

[41] J. P. V. Ramírez, «CONTRATOS INTELIGENTES,» Antioquía, 2019.

[42] «DAPPS,» [En línea]. Available: https://www.miethereum.com/smart-contracts/dapps/.