DIP: Una solución descentralizada para la gestión de proyectos y pagos

M.Joan Perelló Autor.

***Resumen*—En este documento, se introduce DIP, un sistema descentralizado basado en la tecnología blockchain que facilita la creación de contratos inteligentes entre compradores y proveedores de servicios. Su propósito es gestionar los pagos de manera transparente, confiable y justa entre ambas partes, sin necesidad de confiar en una autoridad central. El White Paper explora el contexto en el que surge DIP, detallando cómo la tecnología blockchain y el protocolo DIP pueden solventar la problemática de pagos entre compradores y proveedores.**

I. Problemática Actual

En la actualidad, numerosos autónomos y empresas, desde pequeñas y medianas hasta incluso grandes corporativos, enfrentan la problemática de recibir los pagos por sus servicios con retraso, e incluso en algunos casos, el trabajo puede quedar sin recompensa. Según el último informe de “Informa DyB” , los retrasos en el pago de facturas están generando pérdidas significativas, ascendiendo a 2.970 millones de euros para autónomos y pymes, según las cifras del primer trimestre de 2023.

Este análisis evidencia que solo el 28% de las facturas se abonan dentro del plazo legal establecido, mientras que el 68% experimenta demoras considerables. Incluso la Administración pública, en el primer trimestre de 2023, superó los plazos legales, marcados en 30 días máximos, con una demora media de 28.50 días por encima de lo estipulado para el sector público.

Estos retrasos tienen un impacto significativo en la economía de las empresas afectadas, llegando en algunos casos al cierre total del negocio.

La respuesta adoptada por muchas empresas es trasladar el riesgo al cliente mediante la solicitud de un pago por adelantado. Sin embargo, esta alternativa dista de ser la solución ideal, ya que pasa de un modelo en el que el contratista debe confiar en el cliente a otro en el que el cliente debe confiar en la buena fe del contratista.

La solución óptima sería aquella en la que no sea necesario depositar la confianza en una de las partes y donde ninguna de ellas tenga un control predominante. Imaginemos un árbitro imparcial, justo y transparente que, una vez definidas las reglas acordadas por ambas partes, custodie los fondos del proyecto y realice el pago de manera automática una vez completado, sin necesidad de confiar en ninguna de las partes ni en una autoridad central. Esto es posible gracias a la tecnología blockchain.

Una solución basada en la tecnología blockchain no sólo resolvería el problema de los impagos y retrasos en los cobros de los proyectos, sino que, gracias a su naturaleza, posibilitará la colaboración entre empresas de todo el mundo.

II. DIP

A. Web3 y Blockchain

En esta sección, explicaremos las razones por las cuales optamos por la tecnología blockchain para implementar el sistema.

Una red blockchain es esencialmente una red descentralizada de tipo peer-to-peer, donde cada nodo mantiene una copia exacta de todas las transacciones realizadas desde la creación de la red hasta el momento actual. Estas transacciones se agrupan en bloques, y cada bloque está enlazado criptográficamente al bloque anterior, formando así una cadena de bloques.

La gobernanza de la red se realiza a través de un protocolo de consenso cuyo objetivo es lograr que todos los nodos estén de acuerdo sobre el estado actual de la red.

Otro elemento fundamental de la tecnología blockchain, especialmente en las blockchains de segunda generación, son los contratos inteligentes. Estos, son un programa informático que se ejecuta en una blockchain. Establece condiciones específicas que, cuando se cumplen, activan automáticamente la ejecución de un acuerdo. Al estar en una cadena de bloques, es seguro, transparente y elimina la necesidad de intermediarios. Puede usarse en una variedad de situaciones, desde transacciones financieras hasta acuerdos legales, simplificando y asegurando procesos.

Las características de transparencia, inmutabilidad y trazabilidad que ofrece la tecnología blockchain, junto con los contratos inteligentes, la convierten en una base atractiva para nuestro sistema. Nos permite definir contratos entre compradores y vendedores, almacenarlos de manera inmutable en la cadena de bloques, lo que significa que ni siquiera las partes involucradas pueden modificar el contrato. Además, al

ser autoejecutables, el pago se realiza automáticamente cuando se cumplen las condiciones definidas, sin intermediarios y sin necesidad de confiar en ninguna de las partes.Para agregar una capa adicional de seguridad tanto a los compradores como a los vendedores, se establece el protocolo DIP. Este protocolo es responsable de supervisar cada uno de los contratos creados en el sistema. Su objetivo principal es actuar como mediador en caso de que surjan conflictos entre las partes involucradas durante el desarrollo del proyecto.

Para lograr este objetivo, se va a desarrollar una aplicación web3, que tiene por objetivo facilitar la interacción entre los usuarios del sistema y los contratos almacenados en la red

A primera vista, una aplicación web3 se asemeja visualmente a una aplicación convencional. Sin embargo, la distinción radica en su núcleo, donde la aplicación web3 se basa en la tecnología blockchain. En la siguiente imagen, vemos la arquitectura general de una aplicación web3, no es objetivo de este documento, explicarlo detalladamente

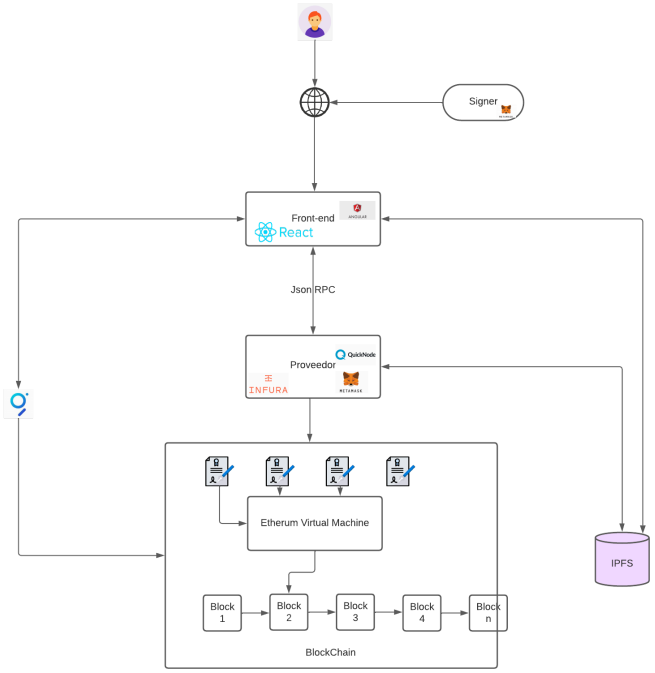

Fig. 1 Arquitectura aplicación web3

Hay que tener en cuenta que cada operación que realizamos sobre una cadena de bloques que implique un cambio en el estado de la misma, tiene un coste económico, por lo tanto sería extremadamente caro e ineficiente usar como backend exclusivamente una cadena de bloques, es por ello que vamos a contar con un enfoque híbrido, una parte de las funcionalidades se realizarán on-chain, directamente sobre la cadena de bloques, mientras que el resto de las funcionalidades se gestionan off-chain mediante una api rest, en la base de datos entre otras cosas, se gestiona la comunicación entre las partes interesadas, así como la evolución del proyecto

B. El Sistema : Roles de la aplicación

Organización: Una organización es cualquier persona o empresa que ha contratado un servicio. Puede estar controlada por una única persona o por un grupo de individuos. Dentro de una misma organización, se pueden añadir diferentes usuarios con distintos niveles de privilegios:

- **Administradores**: Son aquellos que tienen la capacidad de añadir o eliminar empleados de la cuenta de la organización, y son los únicos autorizados para depositar dinero en un contrato inteligente (smart contract).
- **Empleados**: Son cuentas que tienen permisos para hacer seguimiento de los proyectos. No pueden retirar ni añadir fondos en un contrato inteligente. Sin embargo, podrán aportar pruebas en caso de conflicto.

Freelance: Un freelance es una persona que presta un servicio a cambio de una compensación económica. Puede tener uno o más socios, cada uno con una billetera (wallet) independiente y gestionados como cuentas independientes que pueden colaborar.

Árbitros: Los árbitros serán personas anónimas que intervendrán en caso de disputa entre una organización y un freelance. Entre sus funciones están:

- Desempatar en caso de impago: Cuando la organización y el freelance notifican que el proyecto se ha terminado, se realiza automáticamente la transferencia de fondos. En caso de que el freelance notifique que el proyecto se ha terminado, pero la otra parte no lo notifica o indica que aún no considera que se ha finalizado, 5 árbitros intervendrán. Ambas partes dispondrán de un plazo para presentar pruebas/alegaciones a los árbitros, quienes decidirán si se realiza el pago o no. La decisión de la mayoría prevalecerá.
- Aprobar una retirada de fondos: Si una organización decide retirar los fondos, notifica al freelance su intención. Si el freelance acepta, se retiran los fondos. En caso de que no acepte, se produce una disputa y los fondos quedan bloqueados en el contrato inteligente. Los árbitros decidirán si autorizan la retirada de fondos por mayoría.

B.2. Smart Contracts

Un smart contract, o contrato inteligente, es un programa informático autoejecutable y autónomo que se ejecuta en una blockchain. Es un código que define y aplica automáticamente los términos y condiciones de un contrato, sin necesidad de intermediarios.

Nuestra solución se basa en el diseño de 3 smart contract :

Platform Management: En este smart contract se llevan a cabo las siguientes funciones

- Gestión de los árbitros : El smart contract tendrá un listado con todos los árbitros de la aplicación, junto con información acerca de si están activos o no, el smart contract se encargará de :
  - Añadir un nuevo árbitro
  - Eliminar un árbitro cuando este deja de estar activo
  - Marcar a un árbitro como activo cuando sea asignado a un proyecto.
- Registro de managers : El smart contract mantiene un listado con todas las direcciones que se han registrado como manager, entiéndase manager como administrador de una de las organizaciones.
- Creación de un nuevo Proyecto : El smart contract permite que un manager, pueda crear un smart contract,con los parámetros que previamente ha acordado con el freelancer, para ello será necesario que llamemos a la fábrica para que cree el smart contract.
- Reparto de comisiones : Cuando en un proyecto se realiza una transferencia de dinero y se da por finalizado, un % de dicha transacción es para la plataforma, este dinero se va acumulando en el smart contract de la plataforma, este balance es visible para cualquier usuario. Una vez a la semana, el propietario de la plataforma procede a repartir los fondos, para ello destina el 70% de los fondos recaudados para los árbitros y el 30% para el owner de la plataforma, de está manera el árbitro no cobra directamente del proyecto en el que trabaja por lo tanto sus decisiones no se ven condicionadas por intereses económicos.

Factory Contract : Este contrato inteligente, es llamado por el manager cuando desea crear un contrato para un proyecto. Se encarga de recibir los parámetros especificados por el manager y crear un contrato inteligente que gestione los pagos de dicho proyecto. Existe un contrato para generar contratos que reciban pagos con tokens ERC 20 nativos de DIP o con otra stablecoin definida en la red de polygon.

ModelContract : Este smart contract será responsable de :

- Gestionar Fondos : Una vez desplegado, el manager mandará fondos al smart contract, en ese momento el contrato será válido.Otras operaciones que también se podrán realizar son:
  - Incrementar los fondos mandados al smart contract.
  - Retirar fondos del smart contract : Esta operación necesitará del consenso de ambas partes o en su defecto que la mayoría de los árbitros voten a favor de realizar dicha operación .
  - Transferir Fondos al freelancer : Cuando el proyecto ha finalizado, el smart contract mandará los fondos al freelancer, para esta operación se necesita también la aprobación de ambas partes o en su defecto el voto mayoritario de los árbitros.
- Gestión de incidencias : Como hemos comentado, las operaciones de retirar y transferir los fondos del smart contract implicarán que haya consenso entre ambas partes, en caso contrario se emitirá una incidencia para indicar a los árbitros que necesitan su intervención.

B.3. DIP Protocol

En este apartado, explicaremos en qué consiste el protocolo implementado en la aplicación, en concreto este protocolo está programado en el contrato Model Contract,y tiene por objetivo garantizar una gestión transparente, segura y confiable de los fondos del proyecto, asegurando que estos se entreguen al freelancer únicamente cuando el proyecto ha sido terminado.

En el protocolo de consenso de DIP, encontramos 3 actores principales: el/los manager del proyecto, el freelancer y los árbitros asignados al proyecto. Ahora, profundicemos un poco más en qué consiste un árbitro.

En nuestro contexto, un árbitro será un usuario del cual únicamente tenemos su wallet, y que una vez depositado un aval, va a intervenir en las diferentes incidencias que ocurran en el proyecto. Recordemos que en nuestro contexto, una incidencia puede ser:

- Una retirada de fondos en la cual el freelancer no está de acuerdo.
- Una transferencia de fondos por fin de proyecto en la que el manager no está de acuerdo.

Los árbitros son asignados a un proyecto de manera totalmente aleatoria y no pueden estar inactivos más de 4 días. Al cuarto día, el árbitro es eliminado de todos los proyectos donde estaba activo y es reemplazado por otro. Si no tiene ninguna amonestación por mal comportamiento, recupera su aval; en caso contrario, lo pierde.

Cuando se registra una incidencia, todos los usuarios del proyecto reciben una notificación y se abre una vía de comunicación entre el freelancer y el manager con los árbitros para que puedan presentar las pruebas necesarias que ayuden a los árbitros a tomar una decisión sobre el voto que van a emitir. Si 3 de los 5 árbitros votan a favor, entonces se realiza la transferencia o retirada de fondos; de lo contrario, el bloqueo

continúa hasta que las partes se pongan de acuerdo o los árbitros desbloqueen.

Un árbitro nunca se puede comunicar con otro árbitro. Nunca tendrán un chat abierto que les permita dicha comunicación. El objetivo es que puedan tomar decisiones de manera totalmente independiente.

Los árbitros no van a cobrar recompensas directamente del proyecto donde están arbitrando. El objetivo de esta medida es evitar que tomen decisiones condicionadas al cobro de recompensas, asegurando así que sus decisiones sean lo más neutrales e imparciales posibles.

Evidentemente, los árbitros necesitan un incentivo y recibir recompensas por realizar su trabajo. Estas recompensas las cobrarán directamente de la pool del proyecto. La pool es el smart contract donde se van acumulando todas las comisiones que cobra la plataforma de cada proyecto. El 70% del dinero acumulado se reparte entre los árbitros. Es posible que en una semana un árbitro no tenga recompensa, pero en la siguiente sí será recompensado.

El objetivo de hacer que los árbitros cobren directamente de la pool y no del proyecto en el que están arbitrando es evitar que sus decisiones estén condicionadas por la recompensa que puedan cobrar de un proyecto. Además, esto les incita a tomar la decisión más justa en cada momento, ya que si toman malas decisiones, los usuarios no recomendarán la aplicación, habrá menos recompensas a repartir entre los árbitros, y podrían perder el aval depositado.

Si un árbitro no está arbitrando en ningún proyecto, no tiene recompensa. Si un árbitro está más de 4 días sin entrar en la aplicación, es eliminado de todos los proyectos donde está arbitrando y se asigna otro. Si un árbitro realiza alguna acción fraudulenta, este es eliminado y su aval se destina a la pool del proyecto.

Ahora que hemos visto detalladamente el rol de los árbitros, veamos en qué consiste nuestro protocolo de consenso.

Vamos a analizar el caso de transferencia de fondos; el caso de la retirada de fondos es muy parecido.

En cualquier momento de la vida del proyecto, el freelancer puede indicar que el proyecto ha finalizado y solicitar el pago por sus servicios. En ese momento, el freelancer emite un voto a favor de la transferencia de fondos, y se manda una notificación al manager del proyecto. Además, se bloquean las votaciones de retirada de dinero.

Si el manager vota a favor, entonces los fondos son mandados al freelancer y el proyecto se da por finalizado. Si el manager no vota a favor, entonces se registra una incidencia y se activa el protocolo. Los pasos que se siguen son:

- Se manda una notificación a todos los interesados del proyecto, notificando que una incidencia se ha abierto y describiendo el motivo.
- Se abren las vías de comunicación para que el manager y el freelancer puedan presentar las pruebas correspondientes a los árbitros, ya sea conversaciones con la otra parte, registro del trabajo completado, imágenes, documentación, enlaces a entregables, etc.
- Los árbitros también podrán ver las tareas que se habían registrado para ese proyecto, y los comentarios a las mismas, para así ver el estado real del mismo.
- Un dato fundamental será el último login que ha hecho cada usuario a la aplicación, ya que esto puede indicar que el usuario está inactivo y se ha desentendido del proyecto.

Con todos los datos, los árbitros deberán tomar una decisión. Es necesario que 3 de los 5 árbitros voten a favor. La incidencia puede ser desbloqueada siempre y cuando las dos partes estén a favor, excepto si solo falta un voto para llegar al consenso y quedan árbitros por votar; en tal caso, deberán esperar la resolución final. El objetivo de desbloquear incidencias es que si las partes ya han llegado a un acuerdo, puedan proceder lo más rápido posible.

Si los árbitros han llegado a un consenso, entonces se realizaría la transferencia. En caso negativo, los fondos permanecen en el contrato a la espera de la siguiente acción y se da por finalizada la transferencia. La acción natural si un freelancer ha indicado que el proyecto está finalizado cuando realmente no lo está, es que el manager inicie el protocolo para retirar fondos, el cual funciona de una manera muy similar al proceso que acabamos de describir.

Para iniciar una incidencia, no es necesario emitir ningún voto. Si no hay ninguna incidencia activa, el manager o el freelancer pueden activar una incidencia, y se inicia el protocolo descrito anteriormente. Puede ocurrir que cuando se inicie una incidencia, un voto para la acción contraria haya sido emitido, en ese caso los votos de la primera acción se perderán y se tendrá que votar esa incidencia.

III. Próximos pasos

Una vez definido el protocolo y los contratos que gobernarán el sistema, los próximos pasos se orientan hacia el diseño de la aplicación que permitirá la interacción entre los usuarios y el sistema. Esta aplicación, como hemos comentado, consistirá en una DApp, que tendrá una parte que residirá en la blockchain y

otra parte que estará en una base de datos tradicional. Los próximos pasos consisten en implementar el sistema de notificaciones que permita la comunicación de incidencias entre las partes interesadas, la implementación de la infraestructura necesaria para gestionar el avance de las tareas de los proyectos, y la búsqueda de financiación para respaldar la stablecoin del proyecto.

IV. Conclusiones

DIP representa una innovación significativa en la gestión de pagos entre compradores y vendedores, aprovechando las capacidades de la tecnología blockchain. Su enfoque descentralizado elimina la necesidad de confiar en una autoridad central o en cualquiera de las partes involucradas. Mediante el uso de contratos inteligentes como guardianes de fondos y un sólido protocolo de consenso, DIP garantiza la transparencia y la seguridad en las transacciones.

Al integrar contratos inteligentes guardianes de fondos y un protocolo de consenso robusto, DIP ofrece una solución confiable para ambas partes. Por un lado, los proveedores pueden cobrar una vez que el proyecto ha sido terminado, asegurando así su compensación. Por otro lado, los compradores tienen la certeza de que solo pagarán si el proveedor cumple con los criterios acordados. Esta confianza mutua se logra gracias a la automatización y transparencia que proporciona la tecnología blockchain.