



FACULTAD DE CIENCIAS ECONÓMICAS
MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS
TRABAJO FINAL

¿Todas las empresas pueden usar Blockchain?

Eficientizando y acelerando PYMES argentinas

Autor: Adrián E. Piñeyro

Nº de Registro: 671830104

MBA 2020 1.ª Edición

Director de Trabajo Final: Adrián Herz

Agradecimientos

A mis padres y hermanos por apoyarme en cada paso de mi carrera profesional.

A Juan Cavallaro, Leandro Fournier, Mariano Valverde, Mariela Camerano y Martín Sani, quienes desinteresadamente han brindado su tiempo para participar de las entrevistas y pruebas realizadas para este trabajo.

A las autoridades, docentes y coordinadores de la Maestría en Administración de Empresas de la Universidad Católica Argentina por ser verdaderos facilitadores del aprendizaje.

A Adrián Herz, Ingrid Van Zele, Cecilia Stefanelli y Valeria Malach por su guía, consejo y motivación para realizar este trabajo.

A mis colegas de maestría por acompañarme en esta experiencia y brindarme el valor de su amistad.

A todas las personas que en forma directa o indirecta me han motivado y/o ayudado para realizar este trabajo.

Resumen

En los últimos años la tecnología *blockchain* ha atraído gran atención, tanto desde el sector privado y público, como desde el ámbito académico. La posibilidad de ejecutar sobre una *blockchain* acuerdos de forma automática y autónoma gracias a la incorporación de los denominados contratos inteligentes ha contribuido a ampliar el abanico de posibilidades. Sin embargo, la aplicabilidad de esta tecnología es aún cuestionable y no ha logrado una adopción masiva. *Blockchain* podría ayudar a las PYMES argentinas a gestionar subcontrataciones de forma más eficiente, acelerando así su desarrollo. Utilizando un proceso de diseño centrado en las personas, el presente trabajo realiza una investigación sobre la temática y desarrolla junto a los interesados una solución que resuelve el dilema entre el vendedor y comprador a la hora de realizar subcontrataciones: ¿Debe el vendedor confiar en el comprador y pagar antes de recibir el bien o servicio, o debe el vendedor confiar en el comprador y entregar o comenzar a trabajar en el bien o servicio antes de recibir el pago?

De esta forma, utilizando contratos inteligentes modelados en base a la teoría de juegos, este trabajo logra poner a prueba la solución alcanzada con PYMES, comprobando su limitada aplicabilidad y describiendo los obstáculos hallados que dificultan su adopción.

El material generado por y para estas experiencias se pone a disposición de todas las empresas para que pueda ser utilizado como una guía práctica de implementación y uso de la tecnología *blockchain*.

Palabras clave: *blockchain*, contratos inteligentes, teoría de juegos, diseño centrado en las personas, PYMES, subcontrataciones.

Abstract

In recent years blockchain technology has attracted great attention, both from the private and public sector, as well as from academic institutions. The possibility of executing agreements on a blockchain automatically and autonomously through the use of smart contracts has expanded the range of possibilities. However, the applicability of this technology is controversial and has not yet achieved mass adoption. Blockchain could help Argentine SMEs to manage outsourcing more efficiently, thus accelerating their development. Using a people-centered design process, this work conducts a research on the matter and collaborating with the stakeholders develops a solution that solves the dilemma between the seller and buyer during outsourcing: Should the seller trust the buyer and pay before receiving the good or service, or should the seller trust the buyer and deliver or start working on the good or service before receiving the payment?

Consequently, using smart contracts that behave based on a game theory analysis, it manages to conduct field tests on the solution reached with some SMEs, confirming its limited applicability and describing the difficulties encountered that hamper its adoption.

All the material created for and by these experiences is made available to all companies thereby it can be used as a practical guide for the implementation and use of blockchain technology.

Keywords: blockchain, smart contracts, game theory analysis, people-centered design, SME, outsourcing.

Índice de Contenido

1.	Capítulo I: Conocimiento.....	10
1.I.	Introducción.....	10
1.II.	Blockchain: ¿Qué es y cómo funciona?	12
1.II.i.	Ejemplo práctico	16
1.II.ii.	Usos posibles o conocidos de blockchain.....	18
1.II.ii.a.	Comercio Internacional.....	18
1.II.ii.b.	Cadena de suministros.....	18
1.II.ii.c.	Derechos digitales y Propiedad Intelectual.....	19
1.II.ii.d.	Prevención de falsificaciones y fraudes	19
1.II.ii.e.	Almacenamiento de datos descentralizado	20
1.II.ii.f.	Moneda Electrónica y medio de pago internacional	20
1.II.iii.	Operando con criptomonedas	21
1.II.iii.a.	Billeteras electrónicas.....	21
1.II.iii.b.	Venta y compra de criptomonedas.....	24
1.III.	Contratos inteligentes: ¿Qué son y cómo funcionan?.....	26
1.III.i.	Usos posibles o conocidos de Contratos Inteligentes.....	30
1.III.i.a.	Acuerdos entre empresas	30
1.III.i.b.	Sistema bancario	31
1.III.i.c.	Sistema de salud.....	31
1.III.i.d.	Seguros.....	32
1.III.ii.	Anatomía de un contrato inteligente.....	32
2.	Capítulo II: Investigación	35
2.I.	Beneficios teóricos de su aplicación.....	35
2.I.i.	Posibilidades y dificultades para utilizar blockchain	37
2.I.i.a.	Capacidad de crecimiento/Incremento en escala	37
2.I.i.b.	Migración	38
2.I.i.c.	Cambio cultural.....	38
2.I.i.d.	Regulaciones.....	38
2.II.	La tercerización en las PYMES y blockchain.....	39
2.II.i.	Problemática actual en las tercerizaciones de desarrollos tecnológicos	42
2.II.ii.	Alternativas existentes	44
2.III.	Aplicabilidad en PYMES argentinas	45
2.III.i.	El protocolo de depósito doble en un contrato inteligente	49
2.III.i.a.	Análisis teórico del Juego.....	52

3. Capítulo III: Desarrollo y Aplicación	56
3.1. Desarrollo de una solución	56
3.1.i. Etapa Empatizar	59
3.1.i.a. Problema y objetivo.....	59
3.1.i.b. Clichés	59
3.1.i.c. Hipótesis Disruptivas.....	60
3.1.i.d. Stakeholders.....	61
3.1.i.e. Competencia.....	62
3.1.i.f. Entrevistas.....	63
3.1.ii. Etapa Definir	67
3.1.ii.a. Mapa de trayectoria de subcontratación tradicional	67
3.1.ii.b. Insights	69
3.1.iii. Etapa Idear.....	70
3.1.iii.a. ¿Cómo podríamos?.....	70
3.1.iv. Etapa Prototipar.....	71
3.1.iv.a. Mapa de trayectoria del aprendizaje de la solución.....	71
3.1.v. Etapa Evaluar	74
3.1.v.a. Observaciones de las pruebas con prototipos	74
3.1.vi. Trabajo futuro	75
4. Conclusiones.....	76
5. Referencias bibliográficas.....	79
6. Bibliografía.....	84
Anexo I. Glosario de términos.....	91
Anexo II. Pasos para desplegar un contrato inteligente en una testnet privada.....	95
Anexo III. Desplegar un contrato inteligente doblemente fundado	109
Anexo IV. Transcripción de Entrevistas	118
Anexo V. Pruebas de campo	132

Índice de Figuras

Figura 1. Billeteras de criptomonedas según su facilidad de uso y seguridad	22
Figura 2. Navegador Firefox con complemento MetaMask, mostrado saldo en Ethereum ...	26
Figura 3. Contrato Inteligente simple	33
Figura 4. Interacción para la venta de un bien a través de un contrato inteligente.....	47
Figura 5. Interacciones entre el contrato, vendedor y comprador.....	51

Figura 6. Árbol de juegos de protocolo de depósito doble	54
Figura 7. Etapas del DCP.	58
Figura 8. Subcontratación tradicional entre empresa y profesional independiente con problemas en cumplimiento de los pagos.....	68
Figura 9. Plantilla para la generación de nuevos puntos de vista.....	69
Figura 10. Mapa de trayectoria de aprendizaje.....	73
Figura Anexo II-1. IDE Remix. Explorador de Archivos.	96
Figura Anexo II-2. IDE Remix. Plugin Manager.....	96
Figura Anexo II-3. IDE Remix. Solidity Compiler.....	97
Figura Anexo II-4. IDE Remix. Solidity Compiler. ByteCode.....	98
Figura Anexo II-5. Ganache. Lista de cuentas	98
Figura Anexo II-6. MyEthereumWallet. Lista de redes.....	99
Figura Anexo II-7. MyEthereumWallet. Agregar un nodo	100
Figura Anexo II-8. MyEthereumWallet. Despliegue de un contrato. Byte Code	101
Figura Anexo II-9. Ganache. Mostrar claves	101
Figura Anexo II-10. MyEthereumWallet. Despliegue de un contrato. Desbloquear billetera	102
Figura Anexo II-11. MyEthereumWallet. Despliegue de un contrato. Firmar transacción ...	103
Figura Anexo II-12. Ganache. Lista de bloques	103
Figura Anexo II-13. Ganache. Inspeccionar un bloque	104
Figura Anexo II-14. MyEthereumWallet. Interactuar con un contrato	105
Figura Anexo II-15. Remix IDE. Copiar la interfaz de un contrato.....	106
Figura Anexo II-16. MyEthereumWallet. Interacción con un contrato	107
Figura Anexo II-17. MyEthereumWallet. Elección de función de un contrato inteligente. ...	107
Figura Anexo II-18. MyEthereumWallet. Resultado de ejecución de una función sobre un contrato inteligente, valor cero	108
Figura Anexo II-19. MyEthereumWallet. Resultado de ejecución de una función sobre un contrato inteligente, valor uno.	108
Figura Anexo III-1. MetaMask. Selección de Red y cuenta.....	109
Figura Anexo III-2. Código de Contrato Inteligente.....	111
Figura Anexo III-3. Remix IDE. Compilar un contrato..	112

Figura Anexo III-4. Remix IDE y MetaMask. Autorizar conexión.....	113
Figura Anexo III-5. Remix IDE. Despliegue de un contrato.	113
Figura Anexo III-6. Remix IDE y MetaMask. Confirmar despliegue de un contrato.....	114
Figura Anexo III-7. Etherscan. Visualización de un contrato inteligente desplegado.	115
Figura Anexo III-8. Remix IDE y MetaMask. Ejecutar función sobre un contrato.....	116
Figura Anexo III-9. Etherscan. Visualización de un contrato inteligente con operaciones ...	116
Figura Anexo III-10. MetaMask. Visualización del saldo en cuenta comprador	117
Figura Anexo III-11. MetaMask. Visualización del saldo en cuenta vendedor	117

Índice de Tablas

Tabla 1. Lista de aplicaciones de blockchain.....	36
Tabla 2. Razones y beneficios de subcontratar.....	40
Tabla 3. Clichés categorizados según Interacción, producto y precio	60
Tabla 4. Negar/Oponer/Escalar Clichés	61
Tabla 5. Formulación de Hipótesis.	61
Tabla 6. Comparativa entre alternativas de gestión de tercerizaciones y contratos inteligentes.....	63

¿Todas las empresas pueden usar Blockchain?

Eficientizando y acelerando PYMES argentinas

1. Capítulo I: Conocimiento

1.1. Introducción

La tecnología *blockchain* se hizo conocida gracias a la criptomoneda Bitcoin, sin embargo, sus usos van más allá de las facilidades y oportunidades financieras que las criptomonedas puedan ofrecer. Marc Andreessen, el creador del primer navegador web más ampliamente usado, entiende a *blockchain* y a su modelo de consenso, como la invención más importante desde la creación de la internet (Fung, 2014).

Como toda nueva tecnología, comprenderla y comenzar a utilizarla puede ser dificultoso, sobre todo cuando sus aplicaciones son variadas. La web está plagada de artículos para introducirse en el mundo de las criptomonedas, aunque para las pequeñas y medianas empresas (PYMES) es difícil poder ver más allá de estas. Pensar en cómo adoptar la tecnología subyacente, *blockchain*, para mejorar procesos existentes o para innovar al incorporarla en un nuevo producto o servicio parece una tarea inabordable. Los grandes jugadores del sector tecnológico y de la consultoría han desarrollado soluciones a medida para grandes empresas usando *blockchain*, pero la información respecto de cómo aplicarla no está disponible y acceder a este conocimiento para las PYMES es muy costoso, no sólo desde el punto de vista económico. En Argentina, la adopción es aún más difícil, ya que el material disponible es genérico, sin una orientación práctica y sin contemplar el contexto y cultura local.

Las PYMES tienden a subcontratar desarrollos tecnológicos o servicios digitales. El sector tecnológico tiene muchos trabajadores independientes, que ofrecen servicios de desarrollo de software (en ocasiones con mejor calidad y a menor costo que las grandes empresas) aunque existe una problemática a la hora de asegurar que ambas partes cumplan con lo acordado. *blockchain* podría ayudar a acelerar y eficientizar estas contrataciones, asegurando que el comprador reciba el producto o servicio buscado y el vendedor reciba el pago acordado, ambas en tiempo y forma.

El presente trabajo pretende brindar más claridad sobre *blockchain*, describiendo sus posibles usos y experimentar con la misma como herramienta para resolver problemáticas existentes en las PYMES argentinas. Este primer capítulo se centra en el conocimiento: explicando la tecnología y todos sus componentes asociados en términos claros y simples, incluyendo ejemplos y describiendo posibles usos. El siguiente capítulo, el número dos, muestra una investigación sobre sus beneficios y limitaciones, describe las dificultades existentes en las PYMES para realizar subcontrataciones de forma efectiva y las alternativas existentes, y realiza un análisis sobre la aplicabilidad de una solución basada en *blockchain*. El último capítulo, el número tres, documenta el desarrollo de una solución, incluyendo las pruebas de campo con empresas y profesionales independientes de la industria de servicios de marketing digital, diseño y desarrollo de software, con el fin de comprobar su aplicabilidad. Finalmente, se brindan conclusiones respecto de la aplicabilidad, impacto y las limitaciones encontradas durante las experiencias realizadas.

El material generado por esta experiencia se pone a disposición de todas las empresas a los efectos de que pueda ser utilizado como una guía práctica de implementación y uso de la tecnología.

1.II. Blockchain: ¿Qué es y cómo funciona?

En un artículo publicado en 2008, Satoshi Nakamoto, describió un sistema “(...) punto a punto de dinero electrónico [que] permitiría que los pagos en línea se envíen directamente de una parte a otra sin pasar por una institución financiera (...)” (Nakamoto, 2008), y lo denominó *Bitcoin*. Fue así como nació la primera *blockchain*. Hoy todas las criptomonedas conocidas están basadas en *blockchain*, aunque *Bitcoin* domina el mercado de las criptomonedas con una capitalización de 161 mil millones de dólares (Blockchain Luxembourg S.A., s.f.).

Para entender el auge de las criptomonedas y *blockchain*, es importante entender cómo funcionan. Las operaciones que se realizan utilizando una moneda fiduciaria o dinero fiat dependen de un tercero que valida, verifica y salvaguarda la información, en un esfuerzo imperfecto por prevenir el fraude. Para operaciones o tenencias en efectivo, se puede imaginar a las notas de papel o billetes que los integrantes poseen simplemente como un sistema contable, regulado y garantizado por el emisor de la moneda. Para operaciones digitales, aun basadas en una moneda fiduciaria, también existe dependencia de un tercero, en este caso los bancos o entidades financieras que operan en línea validando, verificando y registrando los movimientos. La tecnología *blockchain* permite eliminar completamente la necesidad de un tercero, si se opera dentro del mismo sistema, utilizando el poder de cálculo de todos los integrantes del sistema para regularlo y garantizar su integridad, por medio de lo que se denominan pruebas criptográficas (Staples, y otros, 2017).

Al ingresar de forma segura a un sitio web con un navegador web (por ejemplo, al acceder a un servicio de correo electrónico), un certificado digital es ofrecido por el servidor

antes de comenzar a transmitir los datos, y este es validado por nuestro navegador web a través de una prueba criptográfica. El navegador contiene un almacén de confianza de certificados, contra los cuales puede validar criptográficamente al firmante de este certificado, permitiendo entonces establecer la comunicación con el sitio web, ya que ha verificado que el servidor es quien dice ser (en este caso el auténtico sitio web del servicio de correo electrónico).

Esto se logra gracias a la criptografía asimétrica o también llamada de dos claves. En el mundo digital, quien desee, por ejemplo, que sea posible que una contraparte verifique su identidad, puede crear un conjunto de claves: una privada y una pública. Mediante criptografía firma un mensaje con su clave privada, la que sólo es conocida por él y, quien recibe el mensaje sólo puede verificar su firma utilizando la clave pública. La operación de verificación sólo resulta exitosa si y sólo si, la contraparte posee y está segura de que utiliza la clave pública correcta para dicho destinatario y si quién firmó el mensaje está en poder de la clave privada, la que está matemáticamente vinculada a la pública. Las claves, en su forma más simple, no son más que una secuencia de unos y ceros resultado de una operación matemática compleja que, dependiendo del algoritmo utilizado, es casi imposible de reconstruir al no contar con ambas partes, garantizando así, en este caso, la identidad del autor del mensaje.

Del mismo modo, cada operador de un sistema de bloques tiene en su poder un conjunto de claves (es decir una clave pública y una privada), que le permite firmar cada transacción (con su clave privada) y a su contraparte verificarla utilizando su clave pública, realizando una operación criptográfica, asegurando así que quien envía la operación es el dueño y, por tanto, está autorizado a enviarla. Puesto en términos de Bitcoins (BTCs, en

adelante), quien posee BTCs, puede enviar a otro participante del sistema una determinada cantidad de BTCs, firmando estos bloques con su clave privada al transferirlos. De este modo, se logra asegurar la posesión y transferencia de activos digitales (que tendrán un determinado valor para sus integrantes), sin la necesidad de que estos deban confiar en un tercero que regule el sistema, logrando así un sistema de intercambio de valor que ya no se basa en la confianza, sino en un mecanismo de consenso basado en criptografía.

Es por este modelo de consenso que se la considera una de las mejores formas de lograr resguardar y obtener información en forma fehaciente, ya que cada registro es validado por el consenso de todos los participantes del sistema, lo que eventualmente convierte a todos ellos en registros irrefutables e inalterables.

Pero no todas las *blockchain* se utilizan para criptomonedas. Esta tecnología, entonces, se trata una base de datos distribuida para el registro de eventos de cualquier naturaleza, que han sido ejecutados por los participantes del sistema y cuya registración es compartida por todos los integrantes. Cada operación es verificada por el consenso de la mayoría, de modo que, una vez ingresada la información, esta no puede ser eliminada. El sistema almacena todos los registros de todas las transacciones que se hicieron, y estas pueden ser verificadas por cualquier participante (Crosby, Pattanayak, Verma, Kalyanaraman, & Nachiappan, 2016). Todas las transacciones se registran en lo que se denominan bloques y estos se encadenan entre sí. De existir una disputa, se resolverá teniendo en cuenta el consenso de la mayoría, al optar por la cadena de bloques validada más larga.

Entonces, una *blockchain* es una cadena de bloques. Pero, ¿qué es un bloque? Es posible decir que un bloque contiene tres partes distintivas: información, un digesto

matemático de la información que contiene (denominado *hash*) y el *hash* del bloque anterior. Es posible entender este *hash* como una huella digital sobre determinados datos. Estos son enviados a una función matemática que devuelve una cadena de caracteres que sólo es posible recrear si se conocen los mismos datos de entrada. Así, cualquier alteración en los datos de entrada, resulta en un *hash* totalmente diferente.

La información que contiene puede variar dependiendo del uso que se le dé a esa cadena de bloques. Podría ser desde transacciones financieras hasta la transferencia de propiedad de algún activo. El bloque contiene los detalles de las partes que interactuaron para conseguir guardar la información en él. Por ejemplo, en el caso de las criptomonedas como Bitcoin, el bloque contiene información encriptada que identifica a quien envía y a quien recibe la moneda (aunque de forma anónima). Una vez que el bloque tiene la información deseada y el *hash* del bloque anterior, calcula el nuevo *hash* para ese bloque. Así se logra que todos los bloques estén relacionados y que cualquier alteración en ellos sea fácilmente verificable.

Los participantes del sistema o nodos trabajan de forma independiente, aportando su capacidad de cálculo para registrar las operaciones en bloques que se vinculan matemáticamente con el último bloque aceptado. Esta operación que realizan los nodos se denomina *Proof of work* (prueba de trabajo) y conlleva una determinada dificultad que es administrada por la propia red, lo que implica mayor esfuerzo de cálculo. Una vez que un nodo logra resolver matemáticamente el bloque, lo ofrece al resto de los nodos para que estos lo validen (Nakamoto, 2008). Lo interesante de esto es que validar que el bloque es correcto lleva mucho menos trabajo que crear el *hash* que representa el bloque. Por este motivo, los nodos que resuelven un nuevo bloque reciben una retribución por ello. Este es el

concepto de minar bloques, es decir, crear nuevos bloques procesando operaciones de la *blockchain* y recibir una recompensa por ello: la primera operación del bloque, llamada *coinbase* constituye el pago correspondiente al nodo que realizó el trabajo (Nakamoto, 2008).

Si hay consenso, el bloque es aceptado como el último eslabón de la cadena, confirmando así las operaciones que este bloque posee y efectivizando entonces la transferencia de activos digitales. Ahora este bloque es el último validado de la cadena de bloques.

Simplificando, los pasos que ejecutan los nodos son los siguientes:

1. Las nuevas transacciones se transmiten a todos los nodos.
2. Cada nodo recoge nuevas transacciones en un bloque.
3. Cada nodo trabaja para encontrar una prueba de trabajo para su bloque.
4. Cuando un nodo encuentra una prueba de trabajo, difunde el bloque a todos los nodos.
5. Los nodos aceptan el bloque solo si todas las transacciones en él son válidas y no fueron previamente registradas.
6. Los nodos expresan su aceptación del bloque trabajando en la creación del siguiente bloque de la cadena (Nakamoto, 2008).

1.II.i. Ejemplo práctico

Habiendo realizado una descripción acerca de qué es y cómo funciona una *blockchain*, se desarrolla a continuación un ejemplo práctico. Roberto desea utilizar la *blockchain* de *Bitcoin* para transferirle *BTCs* a Arianna. Roberto tiene 1 *BTC*, lo que sería equivalente a U\$S

10.314,60, a valores de agosto de 2019 (CoinLore, s.f.), y quiere transferir 0,5 *BTCs*. ¿Pero qué es lo que realmente tiene Roberto? A diferencia del dinero tradicional que se mueve con un elemento físico (el papel o moneda), donde quien lo posee es a primera impresión su dueño, en una *blockchain*, el activo (*coin*) nunca sale del sistema. Siempre se encuentra en él y sólo sus dueños son capaces de transferirlos. ¿Cómo? Enviando una transacción a todos los nodos de la red, firmada con la clave privada que sólo Roberto posee. Cualquier nodo de la red puede verificar rápidamente si la operación está permitida, comprobando la firma con la clave pública. ¿Pero qué es lo que verifica exactamente? Para poder realizar la operación, Roberto envió también las claves públicas de las transacciones anteriores que lo hicieron el acreedor de 1 *BTC*. Esto quiere decir que, cada operación tiene al menos una entrada y una salida. Quien envía la operación debe enviar tres elementos: las claves públicas de las operaciones previamente existentes que le dan el balance necesario para realizar la operación, su firma (demostrando que tiene la clave privada en su poder) y la clave pública de quien ahora es el nuevo poseedor. Pero Roberto sólo quería enviar 0,5 *BTCs* a Arianna. ¿Cómo obtiene el cambio? Podría suponerse que Roberto tiene 3 claves privadas de operaciones anteriores, cuya suma es 1 *BTC*. Roberto crea una nueva transacción con sus 3 claves públicas, las firma con sus correspondientes claves privadas, (demostrando así que es poseedor legítimo de las mismas) e indica 2 claves públicas de destino: una de ellas es la clave pública de Arianna por 0,5 *BTC*, la otra vuelve a él, usando la misma u otra clave pública. Cuando la red genera un nuevo bloque con la esta operación, Arianna y Roberto, tienen disponibles entonces 2 claves públicas y su correspondiente clave privada para hacer uso de sus *BTCs* (0,5 cada uno) en una siguiente operación.

1.II.ii. Usos posibles o conocidos de blockchain

Blockchain tiene una variedad de aplicaciones, no sólo en el sector financiero, entre los cuales se encuentran los usos que se listan y describen brevemente a continuación:

- moneda electrónica;
- medio de pago internacional;
- comercio internacional;
- cadena de suministros;
- derechos digitales y propiedad intelectual;
- prevención de falsificaciones y fraudes;
- almacenamiento de datos descentralizado.

1.II.ii.a. Comercio Internacional

Recientemente la empresa R3 (una firma de desarrollo de software enfocada en el desarrollo de tecnologías *blockchain*, fundada con el apoyo de bancos como HSBC y Bank of America), anunció que fue capaz de generar maneras de facilitar procesos de financiamiento comerciales utilizando esta tecnología. Los Bancos han simulado una operación de emisión de una carta de crédito para una importación de bienes entre empresas de Singapur y Malasia. Las cartas de créditos son una de las formas más comunes de reducir riesgo en las operaciones de importación/exportación (Fintech News Malaysia, 2019).

1.II.ii.b. Cadena de suministros

Es posible realizar el registro y seguimiento de activos físicos a través de una cadena de suministros, registrando cada evento en una *blockchain*, tales como los cambios de la

custodia del activo y el medio en el que se encuentra siendo transportado. *Blockchain* puede dar visibilidad a todas las partes involucradas en el recorrido del activo, como productores, transportistas y consumidores, como única fuente de verdad, asegurando la integridad del mismo y su procedencia. Un ejemplo de esto es *BlockVerify*. Su solución permite a las empresas realizar un seguimiento y conocer en dónde se encuentran sus materias primas o productos en la cadena de suministro e, incluso, permite a los clientes finales verificar la autenticidad del bien que adquieren.

1.II.ii.c. Derechos digitales y Propiedad Intelectual

Blockchain también puede ser usado como fuente de verdad para el registro de activos digitales o cualquier tipo de propiedad intelectual, permitiendo administrar, delegar o transferir el derecho de acceso o utilización del mismo.

Bernstein es una aplicación web que permite registrar propiedad intelectual usando la *blockchain* de *Bitcoin*. Permite subir cualquier tipo de documento y luego crear un certificado a partir de él que será registrado en una *blockchain*.

1.II.ii.d. Prevención de falsificaciones y fraudes

Utilizando diversos métodos científicos de medición, es posible obtener las características únicas que diferencian a un determinado objeto (dimensiones, pesos, color, etc.). A partir de estos datos es factible crear un certificado digital que puede ser almacenado en una *blockchain*.

Everledger intenta combatir el fraude de seguros, la falsificación y el robo. Desde diamantes y piedras preciosas de colores, hasta bienes de lujo, pueden ser verificados

mediante *blockchain*. Su solución más conocida es *Everledger Diamond*, que puede emitir un certificado digital que contempla todas las características de un diamante, como tamaño, peso, color y medidas precisas de cada corte. Gracias a esto, las operaciones de compra y venta del mismo ahora pueden ser verificadas con este certificado, lo que es mucho más conveniente y seguro que utilizar certificados en papel.

1.II.ii.e. Almacenamiento de datos descentralizado

Hoy existen muchas soluciones en la nube para almacenar datos de forma centralizada. Es decir, un servicio que puede almacenar y administrar el acceso a diferentes tipos de documentos.

Utilizando tecnología *blockchain* es posible tener una base de datos descentralizada en la nube, en donde los datos encriptados son almacenados por todos los participantes de forma anónima. Un ejemplo de esto es *Storj*, donde los nodos se unen a su *blockchain* para ofrecer espacio de almacenamiento disponible y son recompensados por ello.

1.II.ii.f. Moneda Electrónica y medio de pago internacional

Blockchain permite transferir monedas digitales entre partes sin la necesidad de terceros intermedios. Hay más de 2.400 monedas que utiliza *blockchain*, con una capitalización bursátil total de u\$s 313.569.784.468 (CoinLore, s.f.).

Es posible utilizar *blockchain* como medio para transferir fondos internacionalmente con menores impuestos o comisiones, al convertir las criptomonedas operadas en la moneda fiduciaria local. *Litecoin* es una criptomoneda ideal para transferencias internacionales, rápida y con bajos costos de comisión.

1.II.III. Operando con criptomonedas

Para comenzar a utilizar esta tecnología, tanto un particular como una empresa, primero se deben realizar una serie de pasos y elecciones. El primer paso es elegir la forma en que se van a administrar los activos, es decir, dónde y cómo van operar con las criptomonedas. A estas herramientas se las denominan billeteras electrónicas (denominadas *wallets*), las que se encargan de administrar nuestras claves, públicas y privadas, es decir, aquello que nos permitirá disponer de nuestros *BTCs* o *ETCs*.

1.II.III.a. *Billeteras electrónicas*

Más específicamente las billeteras permiten disponer de los activos que se encuentran en una *blockchain*. Al firmar las operaciones usando la clave privada, se demuestra que quién realiza la operación es el verdadero dueño del activo. La *blockchain* sólo permitirá la operación si la firma es válida. Estos pares de claves son generados en milésimas de segundos por cualquier ordenador o teléfono celular y es un proceso que no necesita ninguna interacción con una red *blockchain*. Dado el largo de esta dirección, el número total de direcciones que se podrían generar es equivalente a 2^{160} , lo que resulta en un total de 1.461.501.637.330.902.918.203.684.832.716.283.019.655.932.542.976 claves o direcciones disponibles. Un número tan grande que es difícil ponerlo en perspectiva, aunque habla de la casi inexistente posibilidad de que alguien obtenga aleatoriamente el mismo par de claves. Mientras se conserve este par de claves, siempre se tendrá acceso a los activos. Si se pierde la clave privada, será prácticamente imposible recuperarlos, siendo optimistas. El fundador de *QuadrigaCX* (una empresa dedicada a realizar inversiones en Criptomonedas), el canadiense Gerald Cotten (1988-2018), se tomó muy en serio la seguridad. Las billeteras de

criptomonedas de los usuarios de *QuadrigaCX* se mantuvieron fuera de línea. Él era el único que poseía las claves privadas y tras su muerte, sus clientes, que tienen \$190 millones en criptomonedas con la compañía, aún se preguntan si alguna vez volverán a ver su inversión (Morris, 2019).

Una billetera digital permite crear nuevas claves o direcciones, enviar nuevas transacciones a una *blockchain* y, al registrar todas las direcciones utilizadas, puede calcular un balance, es decir, informar cuántos *BTCs* o *ETCs* el usuario tiene disponible. Actualmente existen varios tipos de billeteras de criptomonedas, que varían de acuerdo con la facilidad de uso y seguridad (ver *Figura 1*).

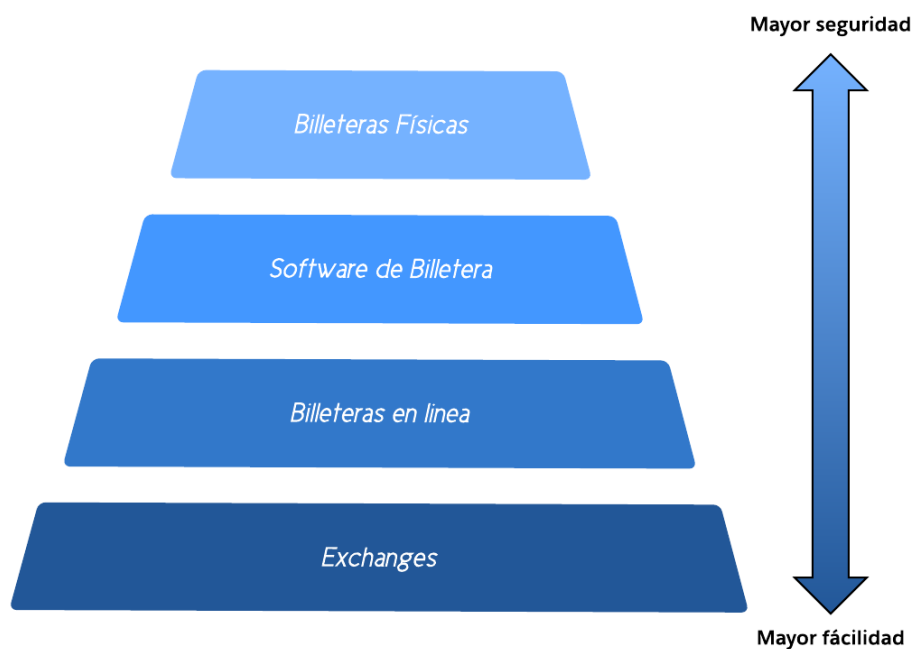


Figura 1. Billeteras de criptomonedas según su facilidad de uso y seguridad. Fuente: Elaboración propia en base a CriptoNoticias (2019).

Todas las billeteras permiten, con un simple clic, crear una nueva dirección donde puede recibir, por ejemplo, *BTCs*. Estas se conocen como direcciones Bitcoin (*Bitcoin*

addresses) y no son más que la clave pública de un nuevo par de claves que el usuario genera y, como se indicó anteriormente, son la piedra fundamental de un sistema de bloques.

Los *Exchanges* no sólo funcionan como una casa de cambio de criptomonedas sino también como bancos: los clientes pueden intercambiar moneda fiduciaria por criptomoneda, pero también dejarla en custodia del *Exchange*. Estos servicios son considerados más inseguros para almacenar criptomonedas, ya que la seguridad de los activos está al resguardo de un tercero al que se accede mediante un sitio web. Como todo sitio web, no están exceptos de ser vulnerables a ataques que podrían ocasionar la pérdida de los activos. Por lo general, los usuarios no acceden directamente a sus claves privadas y es el *Exchange* quien realiza todas las operaciones. Algunos servicios de Exchange son Coinbase, Xapo, Bitstamp entre muchos otros.

Las billeteras en línea como *Blockchain.info* y *MyEtherWallet* son dos de las más utilizadas. Estas no almacenan las claves privadas de los usuarios, sino que llevan registros de sus activos (es decir de sus direcciones públicas) al asociarlos a una cuenta de usuario. Para operar sobre las criptomonedas es necesario ingresar la correspondiente clave privada. Estas además permiten generar una abstracción de las claves en forma de doce o más palabras que debe ser resguardadas por el usuario en un lugar seguro, y preferentemente fuera de línea, para poder recuperar sus activos en caso de que pierda sus claves privadas.

Las billeteras basadas en software son similares a las billeteras en línea, la única diferencia será que el software se ejecutará localmente en el ordenador, permitiendo así mayor seguridad: las claves nunca son transmitidas a través de internet, sino solamente las operaciones firmadas con dicha clave.

También existen las billeteras físicas o *hardware wallets*, que son dispositivos físicos externos que son capaces de almacenar las claves en ellos y, junto con una billetera basada en software con soporte para *hardware wallets*, es posible disponer de las claves para poder operar con las criptomonedas siempre que se conecte el dispositivo. Incluso es posible conectarlo a equipos que se consideren inseguros, ya que las claves nunca abandonan el dispositivo, sino que el software le pide al dispositivo que use las claves para firmar la operación y la devuelva lista para ser transmitida, es decir firmada con una clave privada. Su aspecto, generalmente, se asemeja al de un dispositivo de almacenamiento externo (conocido popularmente como *pendrive*).

1.II.iii.b. *Venta y compra de criptomonedas*

Conocidas las diferentes alternativas de billeteras y habiendo seleccionado una, es posible con ellas comprar criptomonedas, por ejemplo, *ETCs*. Para esto es necesario generar un primer par de claves, cuya clave pública otorga una dirección donde un poseedor de *ETCs* pueda enviar los mismos. Aquí el concepto de “*enviar*” es un poco distinto al de una transferencia bancaria. Cabe destacar nuevamente que en realidad las criptomonedas nunca dejan el sistema, lo único que es transferido es su propiedad al cambiar su firma. Para lograrlo es necesario encontrar una forma de intercambiar un valor aceptado en el mercado de dinero por el valor de poseer este activo digital. Como se mencionó anteriormente, una forma de hacerlo es a través de un *Exchange*. Un *Exchange* permite usar moneda fiduciaria para comprar criptomonedas, ya sea mediante el uso de una tarjeta de crédito o mediante una transferencia bancaria.

Al tener las criptomonedas en su poder, o mejor dicho las claves que permiten disponer de ellas, los interesados estarán casi listos para fundar un contrato inteligente. Pero el contrato también necesita saber una dirección a donde enviar los fondos en caso de cumplirse el acuerdo. Para eso, es necesario saber la dirección de la contraparte. Esta también necesitará disponer de un par de claves, que puede generar con su propia billetera.

Una de las billeteras más populares para Ethereum es *MetaMask*. Se integra directamente al navegador web, como Chrome o Firefox, y permite enviar transacciones a una *blockchain*. Como también es responsable de generar pares de claves, es posible llevar registro de aquellas transacciones que fueron firmadas con la clave pública de poseedor y, por lo tanto, puede informar un determinado balance o saldo, que no es más que la suma de los montos de todas las transacciones que fueron firmadas previamente con aquellas claves que están en poder del usuario. En la *Figura 2* es posible ver una captura de pantalla de *MetaMask*, mostrando el saldo disponible.

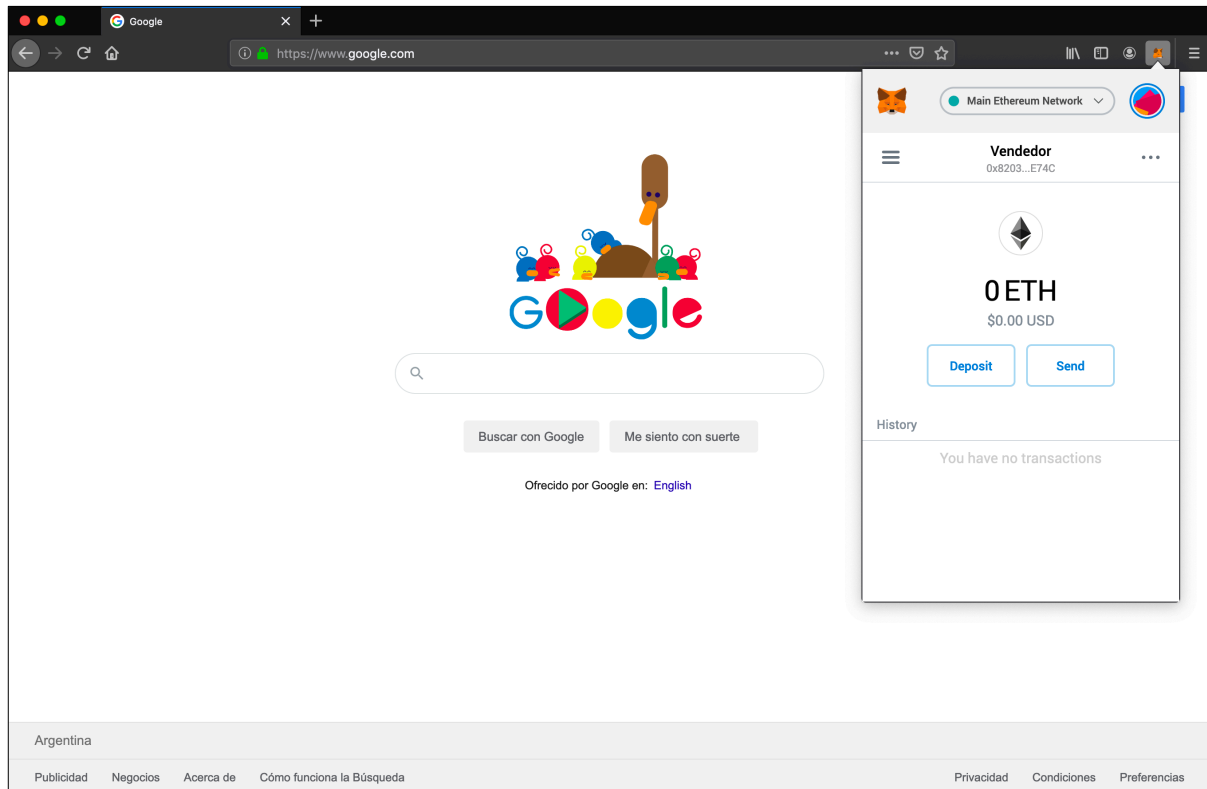


Figura 2. Navegador Firefox con complemento MetaMask, mostrado saldo en Ethereum. Fuente: Elaboración propia (2019).

1.III. Contratos inteligentes: ¿Qué son y cómo funcionan?

El término contratos inteligentes (traducido del término en inglés *smart contracts*) fue propuesto en el año 1996 por Nick Szabo, un desarrollador de software y abogado, más de 12 años antes que Satoshi Nakamoto diera a conocer su propuesta para crear *Bitcoin*. Curiosamente, en varias ocasiones se lo ha señalado a Nick Szabo como el hombre detrás del seudónimo de Satoshi Nakamoto, pero este lo ha negado. Para explicarlo en términos sencillos, Nick Szabo sostiene que es posible comparar a los contratos inteligentes con una máquina expendedora de gaseosas, ya que estas poseen las mismas propiedades (Sun & Xun, 2018), esto es, fueron construidas con un set de reglas específicas que definen qué acciones se deben tomar cuando ciertas condiciones se presentan, por ejemplo: si el cliente ingresa el

dinero en la máquina, recibe una gaseosa; si no lo hace, no recibe nada. El contrato ya está estipulado y es ejecutado por la lógica que la máquina posee. Así se logra celebrar un contrato sin la intervención de un tercero. De la misma forma, un contrato inteligente puede definirse como un set de reglas programadas que puede ser desplegado en una *blockchain*, a la espera de que ciertas condiciones se cumplan para ejecutar acciones previamente acordadas sobre determinados activos digitales, como puede ser la transferencia de criptomonedas de un usuario a otro.

Si bien la *blockchain Bitcoin* no posee capacidad nativa para ejecutar contratos inteligentes, existen otras blockchains que sí lo permiten. Ese es el caso de *Ethereum*, una *blockchain* con su propia criptomoneda (denominada *Ether* o *ETC*) que permite crear nuevas criptomonedas y usar las mismas para ejecutar y pagar contratos inteligentes. *Ethereum* ya está impulsando una amplia gama de aplicaciones en áreas como gobierno, banca, financiación colectiva, negociación y liquidación de derivados financieros, todo mediante el uso de contratos inteligentes (Crosby, Pattanayak, Verma, Kalyanaraman, & Nachiappan, 2016).

Estos contratos presentan varias ventajas con respecto a los contratos tradicionales:

- Pueden ser considerados como un **documento legal** y su registro es guardado por siempre en la *blockchain*, accediendo a todas las operaciones en orden cronológico.
- **El contrato se almacena en una *blockchain* y no puede ser alterado o removido**, lo que aumenta la credibilidad del mismo. Los acuerdos son inmutables e irrompibles y la posibilidad de fraude se reduce, ya que el resultado de su ejecución es validado por todos los integrantes del sistema.

- El contrato no puede ser detenido por ninguna de las partes, sin importar el poder que estas tengan.
- Permite una relación directa y transparente entre las partes al no existir intermediarios.
- Al eliminar la necesidad de intermediarios, el costo de crear y ejecutar un contrato se supone menor.

Entonces, ¿qué es un contrato inteligente? Tal como diría un desarrollador de software, no es ni más ni menos que código de programación, simplemente “código”. De la misma forma que los desarrolladores de software escriben código para generar una aplicación, se pueden escribir contratos inteligentes. ¿Pero qué es exactamente este código? El código son rutinas predefinidas de ejecución lógica en un lenguaje específico que los desarrolladores deben conocer para poder escribir. Son instrucciones escritas que son ejecutadas ante algún evento definido en el mismo y que tienen algún tipo de procesamiento lógico y un resultado. El código fuente de una aplicación entonces, generalmente, consiste en una serie de documentos de texto que contienen líneas de código que determinan la lógica de la aplicación más otros documentos de apoyo, como podrían ser imágenes, certificados digitales, archivos de definiciones (como un diccionario de datos), entre otros.

Hay cientos de lenguajes de programación y de diversos tipos, orientados a resolver diferentes tareas. Dependiendo de cuál se utilice, se encuentra mayor o menor facilidad para escribir una rutina o aplicación y su ejecución puede ser hecha de forma más o menos directa por el sistema operativo sobre el cual se ejecuta (que es quien administra los recursos físicos para realizar las operaciones, es decir, el hardware del que dispone). De la combinación de

todas estas particularidades depende la performance, es decir, la velocidad con la que se puede ejecutar la lógica escrita en un determinado lenguaje de programación.

GitHub.com es el repositorio de código más grande del mundo (CriptoNoticias) con más 100 millones de repositorios de código y más de 36 millones de desarrolladores usando sus servicios, según deja ver su página de inicio, en abril del 2019 (GitHub, Inc.). Para esa misma fecha, los lenguajes más populares entre los repositorios que contiene son JavaScript, Java y Python.

Simplificando, un contrato inteligente es una pieza de software capaz de monitorear, ejecutar y hacer respetar acuerdos. Formas complejas de contratos podrían ser desarrolladas en un contrato inteligente, incluyendo múltiples participantes con diferentes intereses y formas de ejecución más sofisticadas, dependiendo no sólo del comportamiento de las partes sino además de factores externos que podrían estar fuera del control de éstas. En comparación con los contratos tradicionales, estos pueden mejorar la eficiencia al remover a los intermediarios y no requieren de la existencia confianza entre las partes y el intermediario, ya que hay certeza sobre su ejecución. Desde un punto de vista social y técnico, el comportamiento de los participantes que operan con contrato inteligente podría ser modelado como un juego, conceptos que se exploran con mayor profundidad más adelante en este trabajo.

1.III.i. Usos posibles o conocidos de Contratos Inteligentes

1.III.i.a. *Acuerdos entre empresas*

En la teoría de juegos, dos o más tomadores de decisiones, llamados jugadores, compiten sin conocer de antemano la estrategia del otro jugador o jugadores. La combinación de estrategias de los competidores determina el valor del juego para los jugadores. La teoría de juegos se ha desarrollado para su aplicación en situaciones en que los jugadores que compiten son equipos, empresas, candidatos políticos, ejércitos y licitadores de contratos (Anderson, Sweeney, Williams, Camm, & Kipp, 2011; Asgaonkar & Krishnamachari, 2018).

Las empresas pueden competir, por ejemplo, por una determinada participación de mercado y pueden tener distintas estrategias para capturarlo. La eficiencia que estas estrategias tengan depende de las decisiones de las otras partes. La lógica de la teoría de juegos supone que cada empresa o jugador tiene la misma información y selecciona una estrategia que proporciona el mejor resultado posible desde su punto de vista. Pero esto podría no ser siempre así, ya que la información que ambos tienen podría ser diferente y, en consecuencia, las decisiones que un jugador supone el otro tomará podrían ser otras. Un contrato inteligente podría ser la forma de acercar a las partes para competir de forma más eficiente, sin conocer la información de las partes, en donde los participantes podrían fundar un contrato con un valor que podría ser usado como penalidad o premio para garantizar los beneficios que las partes pactaron. En situaciones en las que la competencia sin límites produce perjuicios para todas las partes, es preferible la cooperación y esta podría ser una alternativa para lograr acuerdos superadores.

1.III.i.b.Sistema bancario

El sistema bancario podría ser uno de los primeros en implementar de forma masiva los contratos inteligentes. Los préstamos personales, los créditos hipotecarios y cualquier otro tipo de contrato que los bancos hacen con sus clientes podrían ser modelados en un contrato inteligente y ejecutado sobre una *blockchain*. El beneficio más significativo sería la integridad y la transparencia del contrato, lo que incrementaría la confianza. Al igual que un buen abogado revisa un contrato para aconsejar y advertir a las partes de sus obligaciones o responsabilidades, derechos y riesgos, uno o varios desarrolladores especializados en *blockchain* podrían confirmar que el contrato hace lo que las partes esperan.

DREAM es una comunidad de desarrolladores *blockchain* independientes que ofrecen servicios de consultoría y desarrollo de software orientado a tecnología *blockchain*. Los precios oscilan entre 80 a 400 dólares estadounidenses la hora.

1.III.i.c. Sistema de salud

El sistema de salud también podría beneficiarse de estos contratos. Las diferentes instituciones que intervienen en el cuidado de la salud de un paciente, desde el centro médico hasta el seguro médico, podrían acordar las condiciones de cobertura juntas, brindando transparencia y tranquilidad a sus pacientes.

Dentacoin podría ser un ejemplo temprano de esto. Es la primera *blockchain* orientada al cuidado de la salud dental. Pacientes y dentistas usan un contrato inteligente en el cual los pacientes se comprometen a cuidar su salud dental diariamente (que son registrados con una aplicación en sus teléfonos) y reciben una pequeña retribución en *Dentacoins* por su

cumplimiento que son transferidos a los dentistas, mientras estos se comprometen a atenderlos.

1.III.i.d.Seguros

La empresa IBM, en asociación con la aseguradora multinacional American International Group (AIG) y el banco Standard Chartered, realizaron una prueba piloto del primer contrato inteligente para una póliza de seguros multinacional. La solución que fue construida por IBM se trata de una póliza maestra multinacional escrita en el Reino Unido, y tres pólizas locales en los Estados Unidos, Singapur y Kenia que proporciona una visión compartida de los datos, la documentación y los pagos en tiempo real. Las compañías involucradas decidieron probar y ejecutar este piloto para aplicar un seguro comercial con la finalidad de entender mejor su potencial, reducir la fricción entre las partes y aumentar la confianza (Valeska, 2017).

1.III.ii. Anatomía de un contrato inteligente

Los contratos, como se mencionó previamente, están escritos en un determinado lenguaje de programación. En el caso de la *blockchain* Ethereum el más popular es *Solidity*, un lenguaje muy similar a *JavaScript*. A continuación, se muestra un contrato simple a los fines de mostrar sus partes y explicar su funcionamiento (ver *Figura 3*).

```
pragma solidity >=0.4.22 <0.6.0;

contract Counter {

    int private count = 0;

    function incrementCounter() public {
```

```
    count += 1;
}

function decrementCounter() public {
    count -= 1;
}

function getCount() public view returns (int) {
    return count;
}
}
```

Figura 3. Contrato Inteligente simple. Fuente: Nash, 2017.

Como se observa en la *Figura 3* se trata de texto, en inglés, aunque con una notación especial. Es la forma en la que se escribe la lógica que ejecutan los contratos. Estos poseen un nombre (que no es más que una simple identificación), definiciones de variables (donde es posible conservar el estado de alguna de las características que el contrato posea), y funciones (que son las definiciones de cada acción que el contrato debe realizar al ser éstas invocadas).

Este contrato, llamado *Counter*, tiene tres funciones llamadas *incrementCounter*, *decrementCounter* y *getCount* y una variable, llamada *count*.

Este contrato sólo sirve al propósito de incrementar o decrementar un contador. Un ejemplo simple a los fines de comprender cómo funcionan los contratos: a llamar a las funciones *incrementCounter* y *decrementCounter*, este contrato actúa sobre este contador sumando o restando una unidad, según corresponda, y es posible ver el valor de ese contador

llamando a la función *getCount*. Como puede verse en la línea tres de código de este contrato, el valor inicial de este contador es cero (ver *Figura 3*).

Al desplegar este contrato en una *blockchain*, vivirá por siempre en él y se obtiene una dirección donde llamarlo, en la cual es posible solicitar ejecutar sus funciones. El código no podrá ser modificado, es decir, sus acciones quedarán por siempre congeladas o bien, dicho de otra forma, el contrato es inalterable y sólo pueden cambiar los estados que controla a través de sus propias funciones.

Para desplegar este contrato en una *blockchain* son necesarios algunos de los elementos descritos anteriormente, como un navegador web, una billetera y una *blockchain*. Dado que los desarrolladores necesitan probar sus contratos antes de ser utilizados, y que hacerlo sobre una *blockchain* pública tendría un costo, es preferible recurrir a otras alternativas. Una *blockchain* privada es aquella que por definición no está disponible para cualquier usuario a través de un medio público, como por ejemplo internet. A su vez los desarrolladores de *blockchain* y de contratos inteligentes necesitan poder probar sus contratos y cambios en el funcionamiento de la misma *blockchain* antes de ser desplegados en una *blockchain* pública. Por ese motivo, existen lo que se denominan las *testnet*, que son réplicas de una *blockchain* (en ocasiones más inestables y con software aun no probado) que sirven para este propósito. Los *tokens* o *coins* que poseen estas *blockchain* no tiene valor alguno y cualquier usuario con acceso a una *testnet* puede solicitar *tokens* o *coins* de la misma para realizar pruebas. En el anexo “Anexo II. Pasos para desplegar un contrato inteligente en una *testnet* privada” puede verse una descripción paso a paso para desplegar y utilizar este contrato.

2. Capítulo II: Investigación

2.1. Beneficios teóricos de su aplicación

Los beneficios de *blockchain* están dados por sus características técnicas fundacionales. Dichas características otorgan atributos tales como: Confianza, Apertura, Independencia, Velocidad, Robustez, Aplicabilidad Global y Efectividad (Morabito, 2017).

Los participantes hacen confiable al sistema ya que llegan a acuerdos y resuelven disputas rápidamente sobre lo ocurrido en base al consenso, basados en la capacidad computacional de la mayoría de los nodos, creando un sistema robusto y efectivo. Al no existir una autoridad central que lo regule, no existe arbitrariedad, ya que son los mismos participantes los que crean y alteran la información, lo que lo hace independiente de cualquier autoridad central.

El sistema está abierto ya que permite que nuevos nodos comiencen a operar en él y también que sea extensible para automatizar procesos, a través de contratos inteligentes, automatizando tareas. Por último, la tecnología es aplicable de forma local, por ejemplo, creando una *blockchain* privada de algunos nodos, o bien global, tan sólo permitiendo el acceso a internet.

Son varios los posibles usos de *blockchain* y es incierto aún cuáles serán las áreas en las que *blockchain* se adoptará como la solución de facto y tendrá un mayor impacto en nuestra sociedad. Un estudio conducido por la universidad de South Walesse (White, 2017) se dispuso a entender como espera que *blockchain* cambie el futuro de los negocios, por medio de la técnica *Delphi*. Entre ellas, se seleccionaron catorce posibles aplicaciones futuras de *blockchain* (ver *Tabla 1*).

Tabla 1

Lista de aplicaciones de blockchain

*Reemplazo de moneda física**Certificación Independiente de Calidad de Producto**Certificados digitales**Opiniones de consumidores verificadas**Servicio de depósito de garantía (para bienes)**Diligencia Debida Corporativa Verificada**Transferencia de bonos, escrituras o acciones**Registro de Contribución**Pago de facturas médicas**Sistemas de gestión del rendimiento**Registro de Votación Electrónica**Mecanismos de voz**Grabación de datos personales**Gestión global de la cadena de suministro*

Fuente: White, 2017.

El estudio reveló que los expertos consideran que la mayor probabilidad de implementación e impacto de *blockchain* será como reemplazo de la moneda física y para transferencia de bonos y acciones.

2.1.i. Posibilidades y dificultades para utilizar blockchain

La adopción de las tecnologías de *blockchain* está aún en su infancia. A nivel mundial, muchas empresas de servicios financieros, gobiernos y empresas están explorando la aplicabilidad de esta tecnología. Se espera que surjan nuevos negocios y modelos de negocios, pero hasta el momento hay muy pocos ejemplos de uso significativo de *blockchain* dentro de las industrias o el gobierno (Staples, y otros, 2017).

Compañías como HP, IBM, Samsung, Amazon y Microsoft, por nombrar algunas, han invertido dinero para investigar posibles usos alternativos para *blockchain*. Algunas hicieron alianzas con compañías de diversas industrias para su implementación (del Castillo, 2019).

Sin embargo, ninguna de estas tiene una clara oferta de soluciones basadas en *blockchain* aún, probablemente por la existencia de ciertos riesgos y dificultades para su adopción, a saber:

2.1.i.a. Capacidad de crecimiento/Incremento en escala

Los servicios basados en *blockchain* tienen dificultades para escalar. Agregar un nuevo nodo a una red existente puede tardar varias horas, ya que es necesario validar todas las cadenas de bloques existentes antes de comenzar a procesar un nuevo bloque (Crosby, Pattanayak, Verma, Kalyanaraman, & Nachiappan, 2016). Con un mayor número de operaciones, la red se vuelve “pesada” en términos de bytes. Actualmente, la *blockchain* de *Bitcoin* pesa más de 100GB, ya que todas las operaciones deben ser guardadas para validar las transacciones (Zheng, Xie, Dai, Chen, & Wang, 2018). Además, dado que los bloques tienen un tamaño determinado y un intervalo de tiempo usado para generar un nuevo bloque, se

pueden procesar alrededor de siete transacciones por segundo en una *blockchain* como *Bitcoin*.

2.1.i.b. Migración

Mover los activos digitales y físicos que las empresas ya tiene actualmente a registros en una *blockchain* es una tarea importante, que lleva tiempo y acarrea costos. Debe ser definida y planeada cuidadosamente, adaptando los procesos existentes y llevada a cabo con los nuevos recursos tecnológicos que las empresas quizás no posean. Tales recursos en muchas ocasiones ya se encuentran saturados por las crecientes demandas de digitalizar procesos y servicios en las compañías.

2.1.i.c. Cambio cultural

No todos los consumidores piensan que las operaciones electrónicas son seguras, y aquellos que así las consideran lo hacen tras haber depositado la confianza en terceros conocidos por su reputación. Un ejemplo de esto son las operaciones con tarjeta de crédito a través de internet: podría decirse que no todos los consumidores se sienten seguros de comprar en línea, pero aquellos que lo hacen posiblemente confían en que no habrá problemas y que, de haberlos, la empresa que emitió la tarjeta y/o su banco los respaldarán. En operaciones basadas en *BTC*, no existe una empresa o entidad que otorgue cierto grado de tranquilidad a los usuarios que no son afectos a la tecnología.

2.1.i.d. Regulaciones

En la medida que las aplicaciones de *blockchain* se expandan a nuevos horizontes, sin duda entrará en conflicto con los sistemas ya existentes, que ya están siendo regulados por

los gobiernos. Es esperable que éstos comiencen a crear nuevas regulaciones que podrían acelerar o detener la adopción de *blockchain*. En economías abiertas sería esperable que se acelere el crecimiento al crearse regulaciones que defiendan los derechos de los consumidores, mientras que, en aquellas más cerradas, probablemente los gobiernos generen regulaciones que protegen los sistemas ya existentes.

Para el Proyecto “*Belt and Road*”, el nuevo corredor ferroviario entre Hong-Kong y Rotterdam, el gobierno de Hong Kong desarrolló una prueba de concepto para utilizar una *blockchain* como plataforma de comercio internacional, buscando mejorar la transparencia. La autoridad monetaria de Hong Kong aún sigue intentando acordar las regulaciones necesarias para poder utilizar *blockchain* como mecanismo de reporte y control del intercambio comercial internacional (Tapscott & Tapscott, *Realizing the Potential of Blockchain*, 2017).

2.II. La tercerización en las PYMES y blockchain

La tercerización o subcontratación es el acto de trasladar parte de las actividades internas de una empresa y las responsabilidades sobre las decisiones a prestadores externos. Los términos del acuerdo se asientan en un contrato. La subcontratación es más que los contratos comunes de compraventa porque no sólo se transfieren las actividades, sino también los recursos con los que ocurren las actividades, incluyendo gente, instalaciones, equipo, tecnología y otros activos (Chase, Jacobs, & Aquilano, 2009).

Generalmente, dada su naturaleza, las PYMES necesitan mantener un estricto control de sus costos fijos y un aliado fundamental para lograr esto ha sido y será la tercerización. Mediante esta se logra adquirir servicios de forma temporal o permanente para atender una determinada responsabilidad, actividad, proceso, proyecto o parte del negocio a un costo

predecible. Además, y no menos importante, se evita así realizar inversiones de capital. Entendiendo que la mayoría de las empresas subcontratan tareas no críticas, es decir, aquellas que están alejadas de su negocio central y, por tanto, su resultado no está directamente relacionado al resultado general de la empresa, generalmente son a un bajo costo (comparado con el costo total). Estos son sólo algunos beneficios de la tercerización, aunque existen varios otros según la razón de la misma, tal como se sintetiza en la *Tabla 2* (ver a continuación).

Tabla 2

Razones y beneficios de subcontratar

Razones organizacionales

- Mejora la eficacia por enfocarse en lo que hace mejor.
- Aumenta la flexibilidad para adaptarse a los cambios de las condiciones del negocio, demanda de productos y servicios y tecnologías.
- Transforma a la organización.
- Aumenta el valor de productos y servicios, satisfacción de los clientes y valor para los accionistas.

Razones de mejoras

- Mejora el desempeño operativo (aumenta la calidad y la productividad, sea cortan los ciclos, etc.).
- Se gana experiencia, habilidades y tecnologías que de otro modo no se tendrían.
- Mejora la administración y el control.
- Mejora el manejo de riesgos.
- Adquiere ideas innovadoras.
- Refuerza la credibilidad y la imagen al asociarse con proveedores de renombre.

Razones financieras

- Reduce las inversiones en activos y libera estos recursos para otros fines.
- Genera efectivo al transferir los activos al proveedor.

Razones de utilidades

- Se gana acceso al mercado y oportunidades de negocios a través de la red del proveedor.

-
- Se acelera la expansión por que se aprovecha la capacidad, procesos y sistemas del proveedor.
 - Se expanden las ventas y la capacidad de producción en los periodos en que no puede financiarse la expansión.
 - Se explotan comercialmente las habilidades existentes.
-

Razones de costos

- Se reducen los costos por el mejor desempeño y menor estructura de costos del proveedor.
 - Los costos fijos se vuelven variables.
-

Razones de los empleados

- Da a los empleados plan de carrera más sólida.
 - Aumenta el compromiso y la energía en áreas secundarias.
-

Fuente: Chase, Jacobs, & Aquilano, 2009.

Hoy, por sí sola, la tecnología *blockchain* no permite la tercerización de ninguna de las actividades que las empresas generalmente subcontratan. En definitiva, se trata de una base de datos distribuida y sus funciones, aunque pueden ser muy complejas en su realización, permanecen básicas: creación de nuevos registros, movimientos de registros. Esto es lo que se puede considerar la primera evolución de *blockchain*: un registro público distribuido donde es posible ejecutar transacciones.

La siguiente evolución de *blockchain* viene de la mano de los contratos inteligentes. *Ethereum* es el más claro ejemplo de esto, ya que nos permite ejecutar estos contratos en una *blockchain*.

Hoy es posible ubicar la tecnología en la siguiente evolución, *blockchain 3.0*, en donde aplicaciones distribuidas usan *blockchain* y permiten que usuarios finales la utilicen para resolver determinadas problemáticas. Se las denomina *DApps* y viven dentro y fuera de una

blockchain. Mientras que en la *blockchain* se siguen ejecutando lo que hoy se conoce como contratos inteligentes, por fuera tienen servicios que extienden las capacidades actuales de *blockchain*, facilitando y masificando su uso. Un ejemplo de esto es *Chainlink*, una *DApp* que permite conectar contratos inteligentes, gracias a su implementación *on-chain*, con información, eventos y pagos en el mundo real, debido a su implementación *off-chain*.

De igual modo que hoy cualquier empresa puede contratar servicios en la nube, la siguiente evolución podría ser *blockchain 4.0*, en donde las *DApps* evolucionan para servir a la industria de forma directa, sin intermediarios.

2.II.i. Problemática actual en las tercerizaciones de desarrollos tecnológicos

Existe una problemática recurrente en algunas PYMES a la hora de realizar alguna tarea que requiera un cierto grado de habilidad o experiencia que no está disponible en ella y en consecuencia, es necesario buscar una empresa o un profesional independiente que pueda realizarla. Luego de analizar algunas opciones, deciden avanzar con una de ellas y pueden, por ejemplo, acordar pagar una parte por adelantado y así comienza el trabajo. Todo parece ir bien, hasta que aparecen los problemas: plazos que no se cumplen, malentendidos, problemas con los pagos, etc.

Por otro lado, en especial en el caso de los profesionales independientes, les es difícil asegurarse de que al finalizar el trabajo van a recibir la totalidad del pago. Muchos proyectos son entregados en tiempo y forma pero, a la hora de cobrarlos, las circunstancias, oportunidades o intereses de quien contrató el servicio pueden cambiar, generando atrasos o nuevos problemas.

Aquí surge el conflicto. “No hay hombre, grupo humano, raza, etnia, nación o civilización alguna que no haya tenido que soportarlo, con lo cual es dable afirmar que es parte de la naturaleza humana” (Murro, 2001). Este aparece fundamentalmente debido a las percepciones que tienen los involucrados sobre el hecho. El mismo posee una carga subjetiva, que pertenece a cada uno de los interesados. Lograr que las partes puedan separar esta carga para poder ver el hecho tal como es, alejado de las influencias de su entorno sociocultural, es una difícil tarea. Idealmente, terceros pueden mediar entre las partes para deconstruir la realidad percibida por los actores del conflicto. Crear una nueva realidad en donde estos puedan dejar de lado aquello que percibieron como amenaza y no como un hecho, en la que colaboran para buscar soluciones al conflicto, será la mejor manera de resolver el conflicto.

Lamentablemente, esta oportunidad de resolver los conflictos de forma profesional, no se presenta frecuentemente en las PYMES. Como menciona Murro, generalmente, es el mismo empresario quien intenta resolver los conflictos que los negocios generan, ya que existe una suerte de reticencia para delegar la administración de los conflictos, o “(...)en el mejor de los casos estos son administrados por aquellos profesionales que deberían ocuparse de tales conflictos en otra instancia: la confrontación judicial o extrajudicial(...)” (Murro, 2001). Esto disminuye la posibilidad de lograr acuerdos de calidad o, en ocasiones, pueden terminar en la justicia.

Afortunadamente, no todos los casos son así pero, sin duda, a las pequeñas y medianas empresas les lleva algo de tiempo poner en funcionamiento una forma efectiva de subcontratar estos trabajos.

2.II.ii. Alternativas existentes

Hoy existen varias alternativas para contratar y administrar tercerizaciones de tareas o proyectos relacionadas con el desarrollo de software.

UpWork es un servicio que permite conectar a clientes que están buscando desarrolladores, diseñadores, editores y otros tipos de profesionales independientes que trabajan por hora o por proyectos. Los trabajos requeridos por los clientes son publicados y, luego de un análisis inicial, *UpWork* ofrece una lista de posibles candidatos. Una vez que ambas partes llegan a un acuerdo, el cliente realiza el pago a *UpWork* utilizando una tarjeta de crédito y ésta les permite que colaboren juntos (por medio de mensajes, chat o video) para coordinar y concretar el trabajo. Si se paga por hora, el cliente puede acceder a capturas de pantalla para controlar que efectivamente el trabajo se esté realizando, o bien para verificar el cumplimiento de los objetivos intermedios que acordaron. Sólo cuando el cliente aprueba el trabajo, los fondos son liberados desde *Upwork* hacia quien realiza el trabajo.

Fiverr es otro servicio de similares características, aunque utiliza un abordaje diferente. Aquí los profesionales publican sus destrezas, experiencia e intereses y los clientes los buscan y los seleccionan por sí solos. Generalmente, se utiliza para trabajos pequeños y rápidos y los precios son más económicos. *Fiverr* no realiza una pre-selección sobre estos profesionales, aunque sí publica los comentarios y las calificaciones que los oferentes recibieron por sus trabajos anteriores. La forma de pago es similar, los fondos son liberados sólo cuando el cliente acepta el trabajo.

Otra alternativa es *Gigster*, una solución enfocada en desarrollo de software, totalmente gestionada. A diferencia de *UpWork* y *Fiverr*, aquí se ofrecen equipos completos

de profesionales, que incluyen un gerente de proyectos. Es indicada para proyectos más grandes y complejos. La experiencia parece similar a la de contratar una empresa de desarrollo de software, aunque la interacción será totalmente remota.

2.III. Aplicabilidad en PYMES argentinas

¿Es posible utilizar un contrato inteligente para lograr subcontrataciones más eficientes? Sabiendo qué es un contrato inteligente, es posible ver esto en un ejemplo para entender mejor su funcionamiento y aplicabilidad:

Analía quiere contratar un diseñador para diseñar el logo de su nuevo emprendimiento. Analía podría usar una plataforma como *UpWork* o *Fiverr* para buscar un diseñador y dicha plataforma regularía la contratación, lo que implicaría una comisión a pagar por una o ambas partes. Analía quiere contratar a Gustavo, un diseñador que parece talentoso y responsable. De existir algún inconveniente con respecto al cumplimiento del contrato, las partes deben resolverlo en primera instancia con este tercero (en este caso *Fiverr* o *UpWork*), lo que podría llevar tiempo, costos adicionales y podría resultar en una resolución que está lejana al contrato original que ambos celebraron según el entendimiento de las partes.

Una forma distinta de administrar esta contratación podría ser a través de un contrato inteligente basado en *blockchain*. El contrato se comportará de forma lógica e independiente, ejecutando las acciones que ambos acordaron, garantizando que se ejecute el contrato de la forma esperada y sin cambios arbitrarios, teniendo en cuenta el cumplimiento de cada parte.

De esta forma, tendrían lugar los siguientes pasos:

- Analía y Gustavo acuerdan que el contrato refleja correctamente los términos de su acuerdo.
- Lo envían a una *blockchain*.
- Analía funda el contrato, es decir, envía dinero a él.
- Gustavo puede empezar a trabajar sabiendo que Analía ya fundó el contrato.
- El contrato queda a la espera hasta que Gustavo finalice el trabajo y verifica que el trabajo entregado cumple con lo pactado en el mismo.
- De ser así, el contrato transfiere los fondos a Gustavo y la propiedad del trabajo a Analía.
- El contrato se considera realizado y permanece en la *blockchain* como registro de la operación.

En la *Figura 4* se puede observar esta interacción.

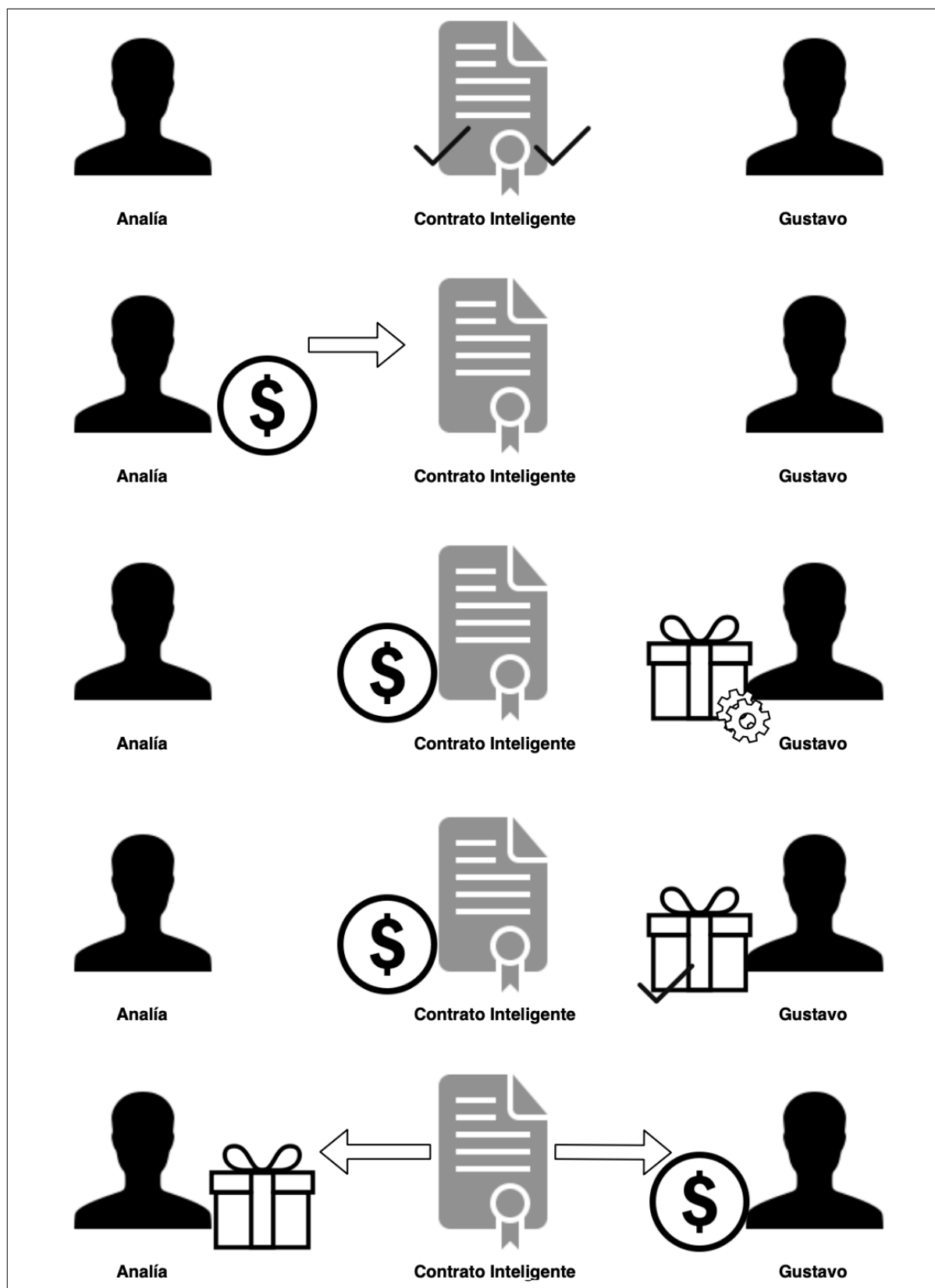


Figura 4. Interacción para la venta de un bien a través de un contrato inteligente. Fuente: Elaboración propia en base a Jackson Ng (2019).

Esto es, en esencia, la posibilidad de celebrar entre privados un contrato que, sin intermediarios, no sólo lo hace cumplir sin subjetividades (ni más ni menos lo que las partes acordaron), sino que además ejecuta las acciones en forma autónoma. Pero, aun utilizando este contrato, existe un riesgo latente o una iniquidad que este primer ejemplo de contrato no considera: ¿Qué pasaría si por cualquier motivo Gustavo no puede continuar con el trabajo? Analía ya no tiene control sobre los fondos depositados en el contrato, por lo tanto, el capital que fundó el contrato se perdería. Por otro lado, si no hubiese sido requerido que Analía funde el contrato, ¿cómo Gustavo podría haberse asegurado de que al finalizar su trabajo los fondos serían transferidos a él? Es claro que a este contrato le falta un incentivo para que ambas partes por igual tengan interés en que el acuerdo siempre se cumpla.

Esto es conocido como el problema del intercambio justo: cómo dos partes que desconfían mutuamente pueden intercambiar conjuntamente valores de manera que ambas partes reciban la contribución de la otra parte o ninguna de las dos lo haga (Goldfeder, 2017).

El estudio del intercambio justo conduce naturalmente al deseo de protocolos optimistas, en donde se considera que las partes tienen motivaciones para comportarse adecuadamente.

Un enfoque para construir estos protocolos es utilizar sanciones monetarias, donde se incentiva a las partes a completar el protocolo de manera justa y, si una de las partes recibe su resultado pero aborta antes que la otra parte, la parte que no cumple el acuerdo se ve obligada a pagar una multa. Una evolución de este enfoque, puede ser el protocolo de depósito doble (Asgaonkar & Krishnamachari, 2018), por el cual las partes adelantan un monto para cubrir una posible sanción ante incumplimientos. Esto se considera un depósito

que es reintegrado en caso de existir un buen comportamiento, generando así un incentivo para hacerlo. Modelar el protocolo de depósito doble en un contrato inteligente podría ser una alternativa viable.

2.III.i. El protocolo de depósito doble en un contrato inteligente

Para eliminar terceros confiables, debe haber restricciones que se impongan en el comportamiento de los dos actores participantes. Es importante tener en cuenta que al utilizar un contrato inteligente basado en *blockchain*, sólo aquellas interacciones que ocurren a través del contrato inteligente pueden ser verificadas, controladas o restringidas. Las interacciones que ocurren fuera del contrato inteligente (interacciones *off-chain* entre vendedores y compradores) no pueden serlo. Es decir que cuando comprador y vendedor realizan operaciones por fuera de esta (como, por ejemplo, la venta de un producto físico o que no es posible registrar digitalmente en una *blockchain*), las interacciones no pueden ser controladas por medio de un contrato inteligente.

Una alternativa de control podría ser restringir el acceso o permitir el uso de este bien por algún medio digital (por ejemplo, encriptándolo con una contraseña o solicitando una contraseña para su uso que podría ser obtenida del *on-chain*) o permitirle al contrato verificar si el bien o producto que fue intercambiado es o no el esperado. Como se mencionó anteriormente, el uso de un *hash* sobre un activo digital permite comprobar si el bien en cuestión ha sido intercambiado o alterado en alguna forma. Sin embargo, esto de por sí no influencia el comportamiento de las partes, sólo sirve como medio para vincular ambas vías de interacción.

Por lo tanto, la única forma de influir en el comportamiento *off-chain* de los participantes es proporcionar incentivos *on-chain* a las partes para que ambas se ajusten al buen comportamiento (Asgaonkar & Krishnamachari, 2018).

Es posible modelar un contrato que contemple esto y realizar un análisis teórico del juego de este esquema de incentivos, para generar un escenario en el que a ambas partes les conviene mostrar un comportamiento honesto y de ayuda mutua.

A diferencia del ejemplo anterior, se propone usar un contrato inteligente que funde por quién desea ser contratado (en adelante el vendedor, Gustavo siguiendo el ejemplo anterior). Este contrato inteligente requiere que, tanto el vendedor como el comprador (Analía), coloquen ambos un depósito suficientemente alto en el contrato inteligente que sirva de incentivo. En este caso, el vendedor primero envía un depósito, luego el comprador envía el pago y su propio depósito; el vendedor luego envía o entrega el bien. El comprador verifica el bien recibido y, si considera que lo recibido se ajusta a lo acordado, envía un mensaje de aprobación al contrato inteligente. Los depósitos realizados por ambas partes se devuelven sólo después de que se completa una operación exitosa (es decir, cuando el vendedor envía el bien de acuerdo a las especificaciones pactadas y el comprador lo verifica y acepta). En todos los demás casos, al menos una de las partes perdería su depósito, teniendo así ambas partes interés en que la operación sea completada. Para lograr que este incentivo sea suficiente y justo, es necesario que el valor del depósito sea igual para ambas partes y lo suficientemente alto para lograr el incentivo buscado. Una posibilidad podría ser que este depósito sea equivalente al precio del bien.

En la *Figura 5* puede ver esta interacción.

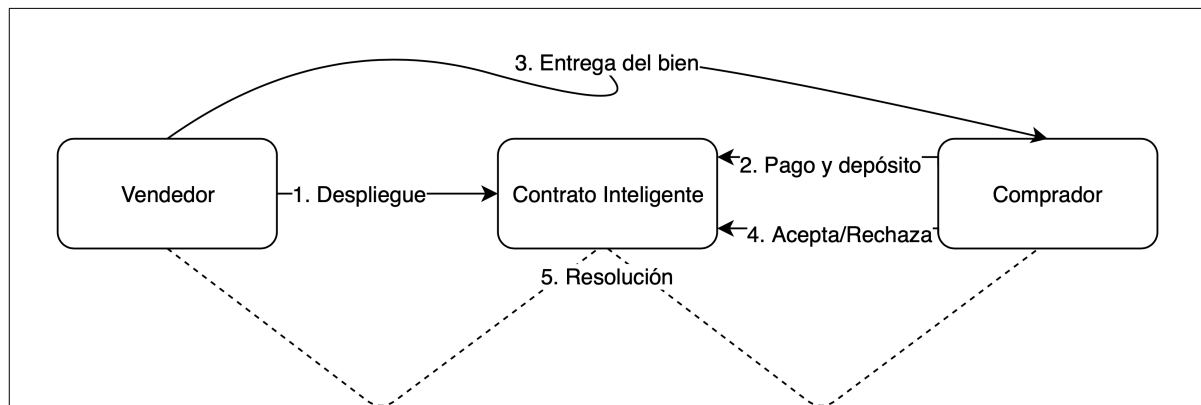


Figura 5. Interacciones entre el contrato, vendedor y comprador. Fuente: Elaboración propia (2019).

1. El vendedor despliega el contrato que contiene el precio del producto/bien (P_b : Precio del bien) y hace un depósito (D_v : Depósito vendedor) por el mismo valor que le será reintegrado luego. También da a conocer un *hash* del bien que va a entregar.
2. El comprador paga el precio del contrato (P_b) y realiza un depósito adicional (D_c : Depósito comprador) por el valor del bien que luego le será reintegrado. Se asume que el valor del bien (V_b), desde el punto de vista del comprador, es mayor al precio ($V_b > P_b$).
3. El vendedor hace la entrega del bien, en una operación *off-chain*.
4. El comprador acepta el bien comprobando que el *hash* coincide; caso contrario, lo rechaza diciendo que el bien recibido no se corresponde con lo pactado.
5. El contrato resuelve que:
 - Si el comprador recibió el bien y lo aceptó: Ambos depósitos son reintegrados (D_c , D_v), y el vendedor recibe P_b .
 - Si el comprador rechaza el bien:
 - En caso de que el *hash* del bien no coincida, se determina que el vendedor no ha actuado de forma honesta, por lo que el vendedor

pierde su depósito (Dv), y al comprador le son reintegrados el depósito (Dc) y el precio del bien (Pb).

- En caso de que el *hash* coincida, se considera que el comprador no está actuando de forma honesta, por lo que pierde su depósito (Dc) y el vendedor recibe Pb , pero pierde el depósito (Dv).

Es posible analizar este contrato de intercambio de depósito doble como un juego de forma extensiva y demostrar que el comportamiento honesto de ambas partes es el único equilibrio perfecto de Nash.

“El equilibrio de Nash es un concepto fundamental en la teoría de los juegos y el método más utilizado para predecir el resultado de una interacción estratégica en las ciencias sociales. Un juego (en forma estratégica o normal) consta de los siguientes tres elementos: un conjunto de jugadores, un conjunto de acciones (o estrategias puras) disponibles para cada jugador y una función de pago (o utilidad) para cada jugador. Las funciones de pago representan las preferencias de cada jugador sobre los perfiles de acción, donde un perfil de acción es simplemente una lista de acciones, una para cada jugador. Un equilibrio de Nash de estrategia pura es un perfil de acción con la propiedad de que ningún jugador puede obtener una recompensa mayor al desviarse unilateralmente de este perfil.” (Sethi, 2008, pág. 540).

2.III.i.a. Análisis teórico del Juego

La dinámica de esta interacción entre el vendedor y el comprador puede modelarse como un juego en forma extensiva, con el vendedor jugando el primer movimiento y el comprador jugando el segundo movimiento. Puede analizarse este juego para encontrar su

equilibrio de Nash perfecto en subjuegos, es decir, la estrategia para ambos jugadores que asegura que nadie tenga un incentivo para desviarse en ningún subjuego del juego original.

Se establecen las siguientes definiciones:

H, H' : comportamiento no fraudulento (honesto) por parte del vendedor y el comprador, respectivamente.

F, F' : corresponde al envío de un producto que no cumplen con las especificaciones acordadas en el contrato con el comprador por parte del vendedor (el *hash* no coincide). Esto correspondería a enviar un bien que no debería ser aceptado por el comprador. Para el comprador, correspondería rechazar la operación cuando el *hash* del bien coincide.

Q : queja del comprador. Esto corresponde a rechazar el bien por parte del comprador dado a su criterio que el producto no cumple con las especificaciones (el *hash* no coincide).

NR : No hay respuesta del comprador.

Primero se observa el análisis de los pagos de las diferentes interacciones entre el comprador y el vendedor:

- Si el comprador no cumple con (es decir, juega F'), independientemente de las acciones del vendedor, el contrato inteligente enviará el Pb de pago al vendedor y destruirá el EC del depósito del comprador. En el caso de que el vendedor fuera honesto (jugado H), entonces el comprador recibe el producto, y su recompensa solo aumenta en Vb (pierde Dc).
- En el caso de que el comprador no presente ninguna aceptación o queja (juega NR), los depósitos de ambas partes y el pago del comprador permanecen permanentemente

bloqueados. De ser el escenario final, pueden ser tratado como una pérdida en todos los pagos y depósitos. En el caso de que el vendedor fuera honesto (jugado H), entonces el comprador recibe el producto, y su recompensa solo aumenta dado Vb (pierde Dc).

- Si el comprador está siendo honesto (juega H'), entonces:

- Si el vendedor no envió el producto esperado (juega F), el depósito del vendedor se destruye y el comprador es compensado con depósito y pago. El vendedor pierde Dv .

- Si el vendedor envió los datos reales (juega H), entonces el comprador acepta la entrega. Esto da como resultado el pago al vendedor y el reembolso de los depósitos respectivos.

El juego resultante considerando las diferentes alternativas se muestra en la

Figura 6. A modo de ejemplo, para el juego representado en este árbol se asume: $Pb=1$, $Dv=Dc=1$, $Vd=1.1$. Se puede determinar, a partir del análisis de inducción hacia atrás sobre este árbol, que sólo hay un equilibrio de Nash perfecto en subjugos de $(Pb, Vb-Pb)$ que se logra mediante la estrategia perfil (H, H') , cuando ambas partes son no fraudulentas (es decir, honestas).

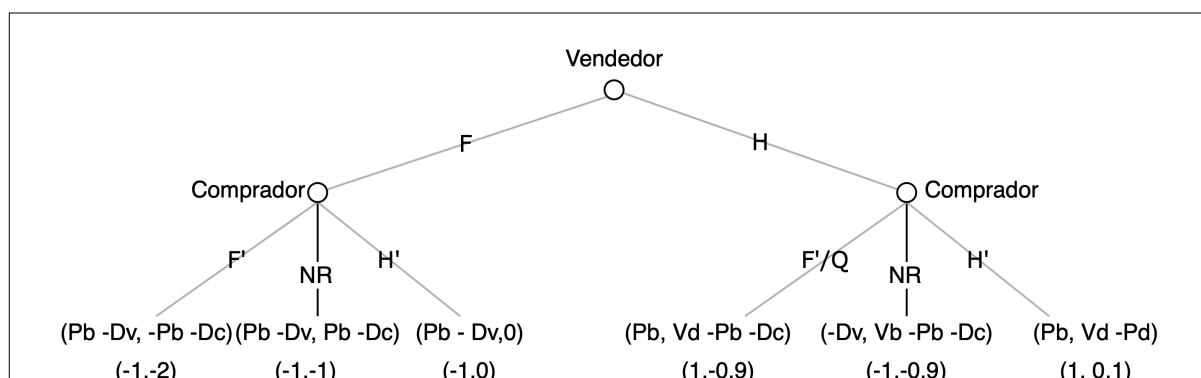


Figura 6. Árbol de juegos de protocolo de depósito doble. Fuente: Elaboración propia (2019).

Si bien este análisis es adecuado para participantes racionales pero egoístas, se debe tener en cuenta que no cubre explícitamente el caso en que las partes irracionalmente estén dispuestas a recibir un pago negativo para infligir daños a la otra parte (aunque el aumento en los depósitos puede proporcionar alguna mitigación contra tal comportamiento a costa de elevar la barrera de realizar la transacción utilizando este protocolo) (Asgaonkar & Krishnamachari, 2018). Aun así, existe una dificultad para aplicar este protocolo en la mayoría de los intercambios digitales, de bienes digitales no repetibles y cuyo acceso y uso no puede ser restringido o comprobado por un contrato inteligente.

“Una suposición central hecha en este trabajo es que el bien digital que se intercambia es verificable, en particular que el comprador (o el contrato inteligente en caso de disputa, cuando se presenta la evidencia relevante) tiene la capacidad de verificar que el bien correcto es recibido: para facilitar la exposición, suponemos que esto se logra mediante un hash del bien digital conocido por el comprador y un contrato inteligente antes de la transacción. El problema sería mucho más difícil (si no imposible) de lograr sin un tercero de confianza si el comprador no puede verificar la entrega de forma independiente.” (Asgaonkar & Krishnamachari, 2018, pág. 6).

3. Capítulo III: Desarrollo y Aplicación

En este capítulo se expone el trabajo realizado para lograr el desarrollo de una solución que permita determinar si es posible para las PYMES ejecutar subcontrataciones eficientes a través del uso de tecnología *blockchain* (más específicamente, por medio de contratos inteligentes). Utilizando una herramienta específica para el diseño de soluciones se realizó una investigación previa, llevando a cabo entrevistas a diferentes interesados y por medio del uso de las diferentes técnicas y metodologías se crearon diferentes prototipos que fueron evaluados con diferentes PYMES para determinar la viabilidad de la solución, sus limitaciones y sus posibles beneficios.

3.1. Desarrollo de una solución

A la hora de desarrollar una solución para cualquier tipo de problema o necesidad existen diversas formas de hacerlo. La gran mayoría de ellas tratan de atacar el problema o necesidad de forma directa, es decir: cómo lograr que el mismo ya no exista o que la necesidad se satisfaga. Estas formas de desarrollar soluciones suelen funcionar, sobre todo cuando el problema o necesidad es claro y está bien definido, ya que mediante la aplicación de la experiencia previa y/o conocimientos técnicos es posible arribar a una solución aceptable o funcional. Cuando se buscan soluciones a problemas complejos, que no es posible que sean definidos claramente, o simplemente existe la necesidad de innovar para lograr una mejora en la forma en la que se realiza habitualmente una determinada tarea (por ejemplo, por razones culturales o por la falta de cuestionamientos sobre ella), estas formas resultan poco efectivas. El pensamiento de diseño utiliza herramientas como la empatía y la experimentación para llegar a soluciones innovadoras. Al utilizar el pensamiento de diseño,

las decisiones se basan en lo que los usuarios realmente desean en lugar de depender exclusivamente de datos históricos o en el instinto, en lugar de la evidencia.

"El pensamiento de diseño es un enfoque de la innovación centrado en el ser humano que se basa en el conjunto de herramientas del diseñador para integrar las necesidades de las personas, las posibilidades de la tecnología y los requisitos para el éxito empresarial" (Brown, 2019).

Al emplear el pensamiento de diseño, es posible unir lo que es deseable desde un punto de vista humano con lo que es tecnológicamente factible y económicamente viable.

El Diseño Centrado en las Personas (DCP) es un proceso y un conjunto de técnicas que se usan para crear soluciones nuevas para el mundo. Estas soluciones incluyen productos, servicios, espacios, organizaciones y modos de interacción. La razón por la que este proceso se llama "centrado en las personas" es por el hecho de que, en todo momento, está centrado en las personas para quienes se quiere crear la nueva solución. El proceso DCP comienza examinando las necesidades, los sueños y los comportamientos de las personas que se verán beneficiadas por las soluciones resultantes. Se pretende escuchar y entender lo que estas personas desean, lo que necesitan. A eso se lo denomina la dimensión de lo que es deseable. A lo largo de todo el proceso de diseño se observa al mundo a través de esta perspectiva. Una vez identificado lo que es deseable, se puede comenzar a ver las soluciones a través de lo que es factible y lo que es viable (IDEO.org, 2019).

El Diseño Centrado en las Personas tiene cinco pasos elementales: **Empatizar, Definir, Idear, Prototipar y Evaluar** (ver *Figura 7. Etapas del DCP*).

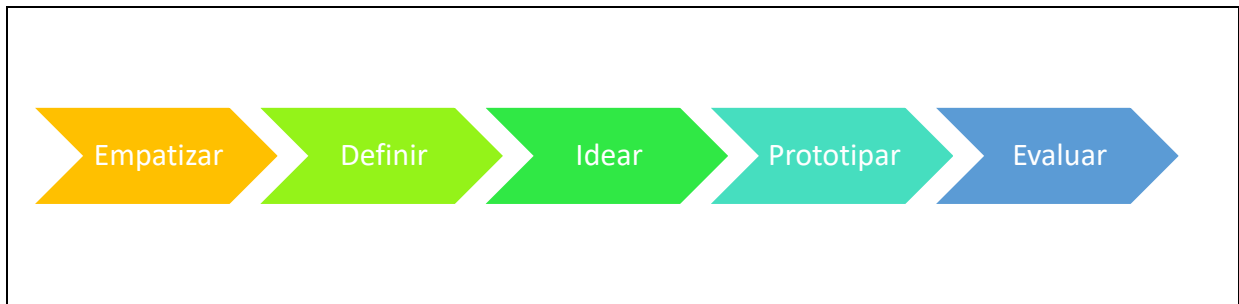


Figura 7. Etapas del DCP. Fuente: Elaboración propia (2019).

La empatía es la base del proceso de diseño que está centrado en las personas. En la etapa **Empatizar** se realiza un esfuerzo por comprender a los usuarios, las cosas que hacen y porqué, sus necesidades físicas y emocionales, como conciben el mundo y que es significativo para ellos.

La etapa de **Definir** es crítica para el proceso de diseño porque expresa explícitamente el problema que se está tratando de resolver. Se debe elaborar una declaración de problema específica y convincente para usar como un punto de partida para generación de soluciones.

La siguiente etapa, **Idear**, es donde empieza el proceso de diseño y la generación de múltiples ideas. Esta etapa se entrega los conceptos y los recursos para hacer prototipos y crear soluciones.

En la etapa de **Prototipar**, se crean prototipos para trasladar las ideas y exploraciones al mundo físico. Un prototipo puede ser cualquier cosa que tome una forma física. Se realizan prototipos para aprender, resolver desacuerdos, iniciar una conversación o para fallar rápida y económicamente.

En la última etapa, **Evaluar**, se obtienen opiniones sobre los prototipos que se han creado con el objetivo de refinar nuestras soluciones y mejorarlas (Plattner, 2018).

El DCP es muy flexible y se puede complementar o suplementar con varios otros enfoques o metodologías y lo utilizaremos como una de las estrategias para crear nuestra solución: una guía para utilizar contratos inteligentes entre PYMES.

3.1.i. Etapa Empatizar

3.1.i.a. Problema y objetivo

Las PYMES argentinas podrían usar tecnología *blockchain* para realizar subcontrataciones, acelerando y eficientizando las mismas, pero no saben cómo hacerlo. No hay una forma económica, fácil y práctica de enseñarles.

3.1.i.b. Clichés

Para cultivar el entendimiento y descubrir oportunidades es necesario observar los momentos claves que revelan lo que los usuarios sienten y hacen, en oposición a lo que dicen que sienten (Tomio, Geyer, & Cascio, 2019). En la etapa de empatizar, es posible pensar clichés del aprendizaje y/o uso de nuevas tecnologías como *blockchain* y los contratos inteligentes. La *Tabla 3* muestra los clichés encontrados agrupándolos en categorías de interacción, producto y precio.

Tabla 3

Clichés categorizados según Interacción, producto y precio

Interacción	Producto	Precio
<p><i>¿Cuáles son los pasos que atraviesa el cliente cuando compra o consume un producto/experiencia? ¿Hay interacción cara a cara? ¿Qué tan frecuentemente interacciona el cliente con el producto o servicio?</i></p>	<p><i>¿Cuáles son las características típicas y sus beneficios? ¿Qué atributos se publicitan comúnmente? ¿En qué áreas típicas compiten esos productos o experiencias?</i></p>	<p><i>¿De qué manera las compañías le adjudican precio a sus productos? ¿Cómo les cobran a los clientes? ¿Se ofrecen descuentos o incentivos?</i></p>
<ul style="list-style-type: none"> • Las nuevas tecnologías son difíciles de aprender. • Es necesario capacitarse formalmente. • No se puede aprender intuitivamente. • Un curso en donde te expliquen es la mejor alternativa. • Es necesario tomar las clases, repasar los conceptos y practicar luego. • Generalmente son varios encuentros, de varias horas. • En el curso hay que ir paso a paso, siguiendo un programa. 	<ul style="list-style-type: none"> • Los cursos son presenciales o remotos. • Hay un experto para evacuar dudas o preguntas. • Hay una evaluación para verificar que se haya aprendido. • Para usar <i>blockchain</i> hay que ser un experto en informática. • Para usar contratos inteligentes necesitas contratar a alguien para que lo desarrolle. 	<ul style="list-style-type: none"> • Es caro aprender nuevas tecnologías. • Cuanto más largo o prestigioso el curso más caro.

Fuente: Elaboración propia en base a Tomio, Geyer, & Cascio, (2019) que aportó esquema para análisis.

3.1.i.c. Hipótesis Disruptivas

Las hipótesis disruptivas sirven para mirar diferentes aspectos. Estas alimentan la observación y, su vez, la observación alimenta a las oportunidades. Estas hipótesis permiten realizar preguntas no convencionales, orientar la investigación a lugares inesperados y focalizar en lo que nadie pensó antes (Tomio, Geyer, & Cascio, 2019). La *Tabla 4* muestra el desarrollo de estas hipótesis utilizando las estrategias de negar, oponer y escalar los clichés.

La *Tabla 5* muestra las hipótesis formuladas a través de la utilización de un recurso interrogativo sobre la base de los clichés que resultaron más atractivos.

Tabla 4

Negar/Oponer/Escalar Clichés

Negar	Oponer	Escalar
<ul style="list-style-type: none"> • No es necesario tomar las clases, repasar los conceptos y practicar luego. • No es necesario capacitarse formalmente. • Un curso en donde te expliquen no es la mejor alternativa. • No hay que ser un experto en informática para usar <i>blockchain</i>. 	<ul style="list-style-type: none"> • Las nuevas tecnologías son fáciles de aprender. • Es posible aprender solo, donde quieras. • No hay que verificar que se haya aprendido, simplemente usas lo que aprendiste. • Aprenderlo es gratis. • No hace falta desarrollar un contrato inteligente, es posible usar uno ya existente. 	<ul style="list-style-type: none"> • Basta con un encuentro, de unos pocos minutos.

Fuente: Elaboración propia en base a Tomio, Geyer, & Cascio, (2019) que aportó esquema para análisis.

Tabla 5

Formulación de Hipótesis

¿Qué pasaría si...
...se pudiera aprender una nueva tecnología de forma fácil, informal, en unos pocos minutos y gratis?
...se pudiera usar <i>blockchain</i> en la empresa sin necesidad de ser un experto?
...se usara un contrato inteligente ya creado para realizar una subcontratación?
... al seguir una guía práctica se pudiera aprender a usar un contrato inteligente?

Fuente: Elaboración propia en base a Tomio, Geyer, & Cascio, (2019) que aportó esquema para análisis.

3.1.i.d. Stakeholders

Se identificaron a las personas claves para poder conocer mejor cómo influyen o se ven afectados por la solución/producto y cuáles son sus intereses.

- *Gerentes de compra/personal de administración encargados de administrar subcontrataciones y/o efectuar los pagos.* Estos son potenciales usuarios/clientes de la solución. Sus intereses podrían ser gestionar subcontrataciones de forma más eficiente, con mayor facilidad, menor fricción y/o conflictos entre las partes. Su deseo podría ser aprender a utilizar la tecnología de forma fácil y rápida.
- *Profesionales independientes que trabajan por encargo.* Estos son potenciales usuarios/clientes de la solución. Sus intereses podrían ser reducir el riesgo de no recibir el pago por el trabajo realizado. Su deseo podría ser aprender a utilizar la tecnología de forma fácil y rápida.
- *Gerentes/Dueños de PYMES.* Estos son los tomadores de decisión, es decir, son quienes deciden la forma en la que se realizan las contrataciones y se efectúan los pagos. Sus intereses podrían ser conseguir rápidamente profesionales independientes que puedan realizar el trabajo con menor riesgo, asegurando la entrega y reduciendo los costos adicionales que producen por subcontrataciones ineficientes. Podrían estar deseando que sus empleados pueden aprender a utilizar rápidamente nuevas tecnologías para gestionar las subcontrataciones con menor costo y riesgo.

3.1.i.e. Competencia

Se analizó la competencia, en primer lugar, desde el punto de vista de la solución técnica en sí. Las alternativas a la solución fueron revisadas en la sección *Alternativas existentes*. En la *Tabla 6* se muestra una comparación de las características de estas alternativas presentadas contra la tecnología de contratos inteligentes.

Tabla 6

Comparativa entre alternativas de gestión de tercerizaciones y contratos inteligentes

	Alternativas	Contratos inteligentes
Facilidad de uso	<i>Alta</i>	<i>Baja</i>
Accesibilidad	<i>Alta</i>	<i>Baja</i>
Conocimientos previos	<i>Bajo</i>	<i>Medio</i>
Garantías/Seguridad	<i>Medio</i>	<i>Alta</i>
Costo	<i>Medio</i>	<i>Bajo</i>
Contacto Inicial con el contratado	<i>No requerido</i>	<i>Requerido</i>
Resolución de disputas	<i>Mediante empresa</i>	<i>Inexistentes</i>

Fuente: Elaboración propia (2019).

En cuanto a la competencia desde el punto de vista del aprendizaje, es posible mencionar video tutoriales en YouTube, tales como los que tiene el canal *CuriousInventor* (CuriousInventor, 2016), cursos de *blockchain* en plataformas de educación online como *Coursera*, como por ejemplo el curso llamado “La disrupción *blockchain*” (Ast, 2019), y varias entradas en blogs de aficionados, como la publicada en el portal *Blockgeeks* que explica acerca de los contratos inteligentes (Mitra, 2019). La información se encuentra dispersa, apunta a diferentes audiencias y no tiene una mirada específica hacia una implementación real para la problemática abordada ni para el contexto en el cual este trabajo se desarrolla, sin olvidar mencionar que la mayoría se encuentra publicada en idioma inglés.

3.1.i.f. Entrevistas

Se realizaron entrevistas a personas que representan a expertos en la temática y a *stakeholders* con el objetivo de entender los pensamientos, emociones y motivaciones, a fin

de, a partir de esta base, poder para determinar cómo innovar para ellos. Entendiendo las decisiones que esa persona toma y su comportamiento, es posible identificar sus necesidades y diseñar para satisfacerlas (Plattner, 2018).

3.1.i.f.1. Experto en blockchain

Juan Cavallaro, Licenciado en Informática, trabaja hace más de cinco años con tecnologías *blockchain*, desempeñándose actualmente como Jefe de Seguridad y Riesgo en la empresa Xappo (fintech que ofrece servicios de *Exchange* y *wallet*). Cavallaro fue entrevistado con el objeto de conocer su opinión sobre la solución técnica bajo análisis y sobre cómo ayudar a otros a aprender y adoptar nuevas tecnologías.

A continuación, los puntos más relevantes de la entrevista:

- La dificultad que existe para entender las criptomonedas se da principalmente porque la relación de la gente con el dinero es natural. El concepto ha sido incorporado de forma intuitiva.
- La mejor manera de explicarlo en su experiencia es compartir algunos conceptos de economía básica y hacer analogías con lo que la gente ya conoce. Conceptos como la inflación y la forma en la que el mercado determina el precio de un bien ayudan a desarrollar algunos conocimientos claves.
- Un sistema autónomo (sin terceras partes) e independiente (objetivo) como los contratos inteligentes, capaz de incorporar la teoría de juegos, es interesante, ya que elimina una variable humana más, que introduce de otro modo cuestiones morales.
- Sin embargo, al usar un contrato inteligente, la confianza de las partes podría trasladarse al mismo contrato, ya que es probable que quien lo utilice no tenga los

conocimientos para confirmar objetivamente que el contrato siempre se ajustará a lo que las partes acordaron.

- Por otro lado, esto también sucede con la propia tecnología *blockchain*: muchos de los usuarios no podrían identificar problemas en su integridad y funcionamiento.
- Es el resultado de la experiencia lo que vuelve una tecnología confiable a través del tiempo.

Ver anexo “Anexo IV. Transcripción de Entrevistas” para acceder a la entrevista completa.

3.1.i.f.2. Profesionales independientes

Leandro Fournier es un desarrollador de aplicaciones *iOS* que trabaja de forma autónoma para PYMES desde hace más de 10 años. Mariela Camera, diseñador gráfica y audiovisual, con más de 5 años de experiencia trabajando de forma independiente. Ambos fueron entrevistados con el objeto de conocer su opinión sobre la solución técnica, así como también sobre cómo aprender y adoptar nuevas tecnologías.

A continuación, se destacan los puntos más relevantes de las entrevistas:

- Han tenido problemas con los pagos y han utilizado o utilizan plataformas online para ofrecer sus servicios y gestionar los pagos.
- Prefieren trabajar con personas con las que ya construyeron confianza y acordaron una forma de pago, para evitar inconvenientes.
- La tecnología les genera desconfianza (quizás por ignorancia) y se sienten más a gusto con un humano o entidad a la que puedan recurrir de existir un problema.

- Tienen preferencia para aprender nuevas tecnologías de forma independiente, idealmente con algún video explicativo y luego tener la posibilidad de experimentarla de forma directa. También les parece importante poder hablar con alguien que ya lo esté usando.

Ver anexo *“Anexo IV. Transcripción de Entrevistas”* para acceder a las entrevistas completas.

3.1.i.f.3. Dueño de PYME

Mariano Valverde es socio fundador de Cristalino, una empresa familiar dedicada a servicios de Marketing tales como desarrollos de marca, activaciones, gestión de comunicación y eventos. En el marco del presente trabajo, fue entrevistado a fin de conocer su experiencia en subcontrataciones, su opinión sobre la solución técnica y sobre cómo su empresa adopta nuevas tecnologías.

Los siguientes son los puntos más relevantes de la entrevista:

- Ha tenido problemas con las contrataciones y, si bien el contratista/proveedor se hizo cargo, el daño fue mayor que el económico ya que dañó la relación con el cliente. No volvieron a trabajar con ese contratista/proveedor. Esta solución sólo cubre el daño económico en cada oportunidad.
- No tiene problema en incorporar nueva tecnología para sus contrataciones. Es habitual que sus clientes le impongan el uso de nuevas tecnologías y considera que, a su vez, su empresa podría imponerlas a sus proveedores/contratistas.

- Considera que sería interesante que la solución permita modelar pagos intermedios de acuerdo al grado de avance y/o desempeño. También, involucrar al cliente final en el mismo contrato (Cliente, Empresa, Contratista).
- Es aplicable a baja escala, donde no existe ninguna confianza entre las partes, quizás para una primera interacción, por ejemplo, entre un emprendedor y un profesional independiente.
- La complejidad de su uso genera desconfianza.

Ver anexo *“Anexo IV. Transcripción de Entrevistas”* para acceder a la entrevista completa.

3.1.ii. Etapa Definir

3.1.ii.a. Mapa de trayectoria de subcontratación tradicional

Para ganar empatía con una persona o mejorar el entendimiento del proceso por medio de una experiencia, es preciso considerar los detalles de ese proceso para iluminar áreas de potenciales *insights*. Crear un mapa de trayectoria es una excelente forma para pensar sistemáticamente sobre los pasos e hitos del proceso (Plattner, 2018). En la *Figura 8* se puede ver el desarrollo del mapa de trayectoria de una subcontratación tradicional que presenta inconvenientes en los pagos.

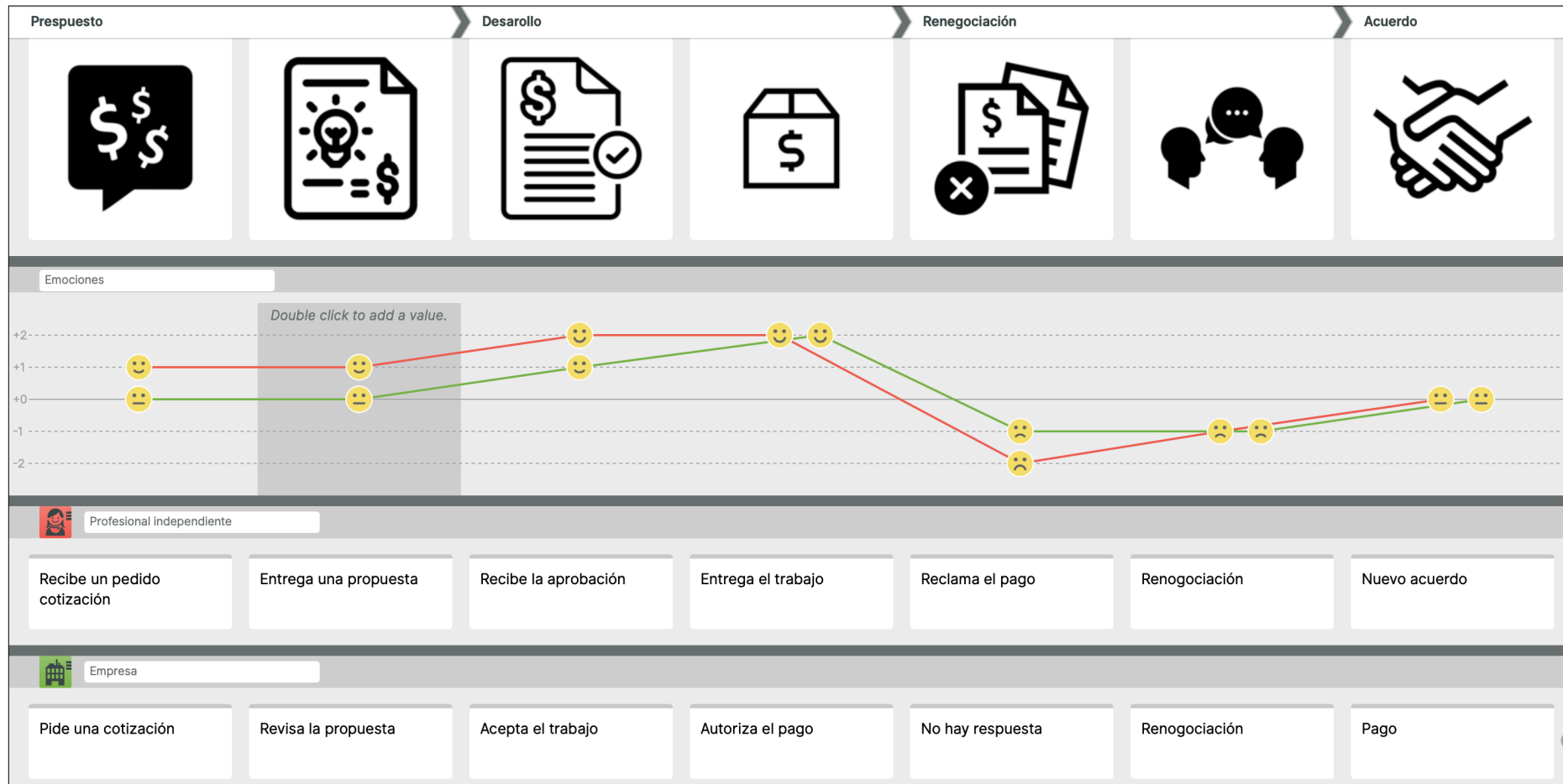


Figura 8. Subcontratación tradicional entre empresa y profesional independiente con problemas en cumplimiento de los pagos. Fuente: Elaboración propia (2019) utilizando herramienta Smaply.

3.1.ii.b. Insights

Es necesario sintetizar la información obtenida en las etapas anteriores para descubrir las verdaderas necesidades de los *stakeholders*. Para hallar nuevos *insights* es posible utilizar un método que permite descubrir nuevos puntos de vista. Este método es planteado como un juego ya se deben realizar diferentes combinaciones sobre una plantilla que contiene una frase que debe completarse (ver *Figura 9. Plantilla para la generación de nuevos puntos de vista. Fuente: Tomio, Geyer, & Cascio (2019).*).

Este juego actúa como catapulta para generar una declaración y definir el problema. Esto permite desarrollar ideas de una forma directa y lo más importante es que ayuda a capturar el concepto de diseño de manera significativa (Plattner, 2018).

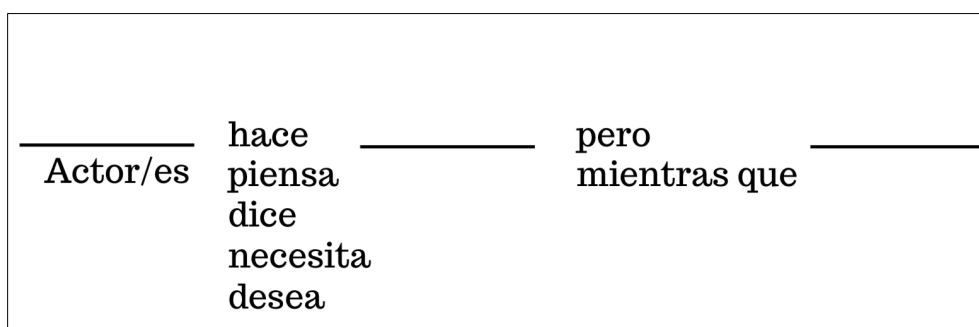


Figura 9. Plantilla para la generación de nuevos puntos de vista. Fuente: Tomio, Geyer, & Cascio (2019).

A continuación, se listan los puntos de vista, necesidades e *insights* más relevantes.

- Los profesionales independientes desean no tener una relación de dependencia, pero terminan trabajando con los mismos clientes para no tener problemas con los requerimientos o con los pagos.

- Los profesionales independientes dicen que, de tomar trabajos de un desconocido, prefieren tener una persona o entidad que intervenga en caso de que haya problemas con sus trabajos, pero no están seguros si ésta actuaría de forma objetiva.
- Los profesionales independientes dicen que prefieren aprender de forma autónoma nuevas formas de trabajar o cobrar, pero si conocieran a alguien que ya lo esté usando confiarían en su experiencia para que les explique su uso y aplicación.
- La empresa que realiza subcontrataciones dice que no tiene problemas con sus proveedores en general, mientras que la única forma que tiene de obtener un nuevo proveedor es ir probando con varios trabajos más pequeños y aumentar su complejidad hasta sentir que ha creado una relación de confianza.

3.1.iii. Etapa Idear

3.1.iii.a. ¿Cómo podríamos?

Las preguntas “¿Cómo podríamos?” son preguntas cortas que tienen la particularidad de disparar *brainstorms*. Estas preguntas se desprenden de la definición del problema o principios de diseño como semillas para la etapa de ideas. Genera una semilla lo suficientemente amplia para que haya una gran cantidad de soluciones y lo suficientemente acotada o limitada para determinar ciertos límites que sean de ayuda (Plattner, 2018).

A continuación, se destacan las preguntas más relevantes:

- ¿Cómo podríamos generar una solución que permita que ambas partes sientan la misma confianza que al trabajar con personas ya conocidas?

- ¿Cómo podríamos realizar contrataciones sin que la confianza sea un factor necesario?
- ¿Cómo podríamos enseñar a usar contratos inteligentes permitiendo a las partes que prueben sin incurrir en ningún costo?

3.1.iv. Etapa Prototipar

Gracias a las etapas previas, y para dar respuesta a las necesidades encontradas, se decidió utilizar un prototipo de contrato inteligente que implemente el protocolo de depósito doble para permitir que desconocidos puedan operar sin la necesidad de un tercero ni la existencia de confianza previa entre ellos (ya que el contrato establece incentivos para influir el buen comportamiento). Para esto se utilizó el contrato de ejemplo desarrollado por *Solidity* (Solidity, 2019), que permite que el vendedor cree un contrato con un valor igual al doble del bien a comerciar, para que luego el comprador pague el doble del bien para dar comienzo al trabajo a realizar. Al recibir el trabajo finalizado *off-chain*, si el comprador acepta el mismo, confirma la compra y el contrato devuelve el depósito a ambas partes y el precio del bien al vendedor.

Además, para facilitar el aprendizaje, se decidió utilizar la *testnet* de *Ethereum*, llamada *Ropsten*, permitiendo así que los interesados puedan experimentar en primera persona el uso de esta tecnología como alternativa para sus contrataciones.

3.1.iv.a. Mapa de trayectoria del aprendizaje de la solución

Se desarrolló el mapa de trayectoria de dos persona, Alice y Bob, comprador y vendedor respectivamente que desean aprender a utilizar un contrato inteligente. La

Figura 10. Mapa de trayectoria de aprendizaje. Fuente: Elaboración propia (2019) (Quadriga CCAA, s.f.) muestra las diferentes etapas, la acción que cada uno de ellos realiza, y sus estados de ánimo.

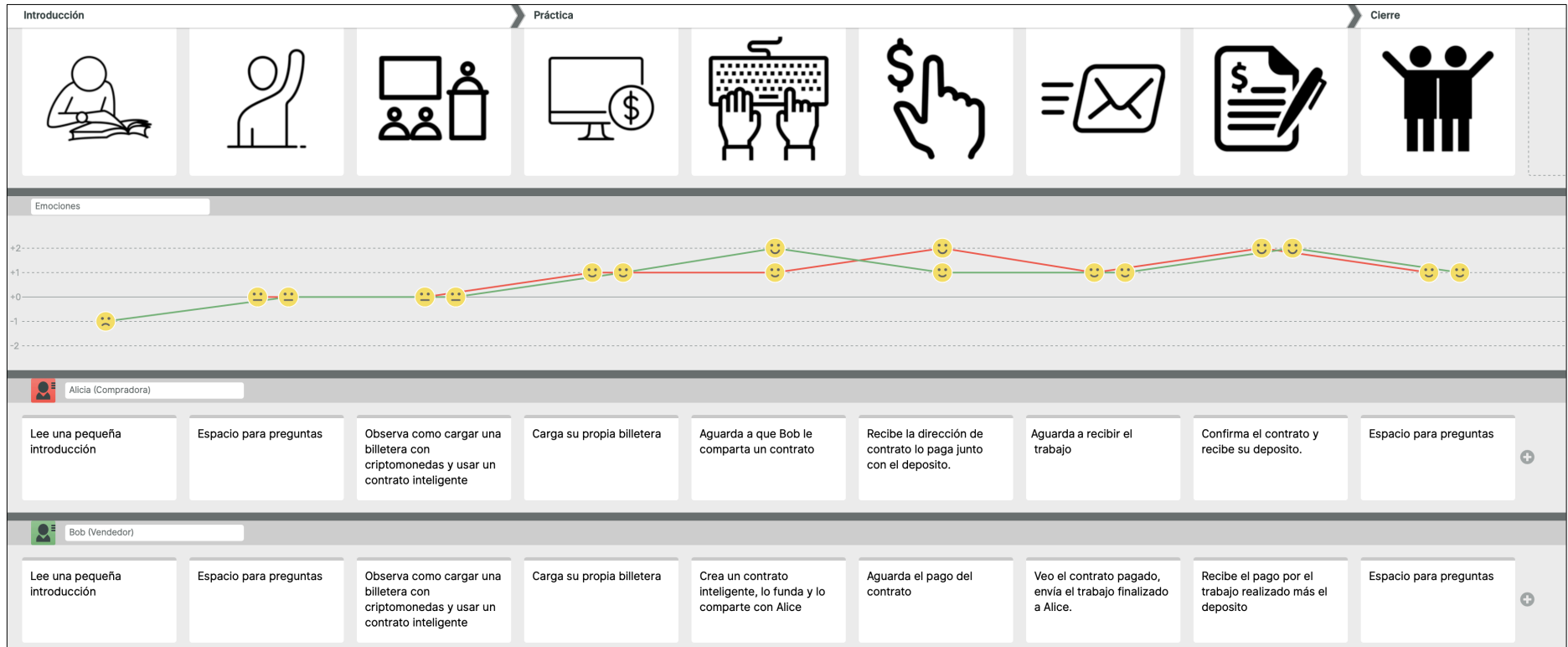


Figura 10. Mapa de trayectoria de aprendizaje. Fuente: Elaboración propia (2019) utilizando herramienta Smaply.

3.1.v. Etapa Evaluar

A fin de identificar la respuesta de los interesados al uso y la adopción de estas tecnologías, se ha llevado a cabo una prueba de campo. En el *“Anexo III. Desplegar un contrato inteligente doblemente fundado”* pueden verse la guía de los pasos. A continuación, se presentan las observaciones que surgen como resultado de las pruebas realizadas. En el *“Anexo V. Pruebas de campo”* puede verse los detalles de cada uno de estas pruebas.

3.1.v.a. Observaciones de las pruebas con prototipos

- La utilización de un recurso como un video para explicar qué es un contrato inteligente resulta efectiva.
- Ver saldo en una billetera electrónica ayuda a comprender rápidamente cómo funciona.
- Los profesionales independientes se encuentran más interesados en aprender a utilizar esta alternativa.
- Realizar un depósito en calidad de garantía es algo que incomoda a ambas partes, aunque quizás más al vendedor, dado que su capacidad financiera es generalmente menor.
- No tener una plataforma unificada para utilizar la tecnología genera desconfianza.
- No poder comprender qué es lo que hace exactamente un contrato inteligente es un factor crítico, que requeriría de terceros confiables que puedan confirmar que el comportamiento del mismo refleja fielmente lo que acordaron las partes, reintroduciendo el concepto de confianza.
- La explicación previa y prueba se realizan en 40 minutos aproximadamente.

- Desde el punto de vista del comprador, la experiencia es mucho más clara y práctica, al no tener la necesidad de utilizar herramientas para desplegar el contrato inteligente.

3.1.vi. Trabajo futuro

En base a la información obtenida durante la presente investigación, se considera que los siguientes aspectos deberían ser desarrollados para lograr mayor aceptación y una solución con un grado mayor de aplicabilidad de los contratos inteligentes en Argentina:

- Utilizar un contrato inteligente que esté respaldado por el mayor número posible de expertos y que permita pagos parciales y/o la inclusión de otros participantes que conforman la cadena de pago (de existir).
- Utilizar una interfaz gráfica que pueda explicar el comportamiento de contrato inteligente en lenguaje natural, similar a *Scratch*, para facilitar su comprensión y así aumentar la transparencia.
- Utilizar una interfaz gráfica o plataforma que unifique la experiencia del comprador y el vendedor para aumentar la confianza.
- La misma herramienta debería brindar más información acerca de cómo utilizar las criptomonedas y cómo convertirlas en moneda fiduciaria.
- Simplificar el número de pasos para su utilización con el fin de mejorar la experiencia de uso.

4. Conclusiones

Es evidente que la tecnología *blockchain* aún no ha alcanzado todo su potencial. Nuevas ideas deberán ser incorporadas en las plataformas que la utilizan a fin de poder ayudar a resolver problemas que aún no fueron resueltos o se encuentran resueltos de forma ineficiente. Quizás al continuar incorporando esta tecnología en el mundo empresarial, los avances necesarios para facilitar su uso y expansión de los niveles de adopción se aceleren cada vez más, no sólo debido a los avances técnicos, sino porque su creciente popularidad logre que se llegue a un entendimiento colectivo, de la misma forma que hoy las personas utilizan tecnología como internet sin cuestionarse sobre su funcionamiento. Tal como se ha descrito, *blockchain* presenta ventajas y desventajas sobre los sistemas o plataformas ya existentes, y quizás futuras investigaciones demuestren que esta podría ser la mejor alternativa en algún de los campos explorados a lo largo de este trabajo, aunque en muchos otros campos las tecnologías convencionales aún parecen seguir siendo más apropiadas. La investigación futura debería examinar el desarrollo y el impacto de *blockchain*. Los beneficios y las barreras para su adopción requerirán una mejor comprensión y se podrían obtener conocimientos útiles al explorar las características y la velocidad de su adopción. Algunas aplicaciones de *blockchain* tienen el potencial de alterar radicalmente aspectos de la sociedad y, por lo cual las ramificaciones legales y éticas de tales desarrollos necesitan la debida consideración antes y durante su implementación (White, 2017).

Los individuos que han participado de este caso de estudio pudieron comprender el funcionamiento de una *blockchain* y de un contrato inteligente e incluso tuvieron la oportunidad de experimentar su uso en un ambiente controlado. El uso de recursos tales como videos explicativos y la posibilidad de experimentar directamente con la tecnología

parecen ser un factor que acelera el aprendizaje. Sin embargo, aun siendo una temática difícil de comprender, dada la complejidad técnica y sus limitaciones, ésta no parece ser la principal barrera para su adopción.

Las PYMES y los profesionales independientes consultados demuestran ser coincidentes en su percepción y comportamiento: Aún ante la existencia de múltiples herramientas para conseguir nuevos clientes y asegurar el cumplimiento de sus acuerdos (incluyendo la alternativa desarrollada en este trabajo), prefieren trabajar con personas con las que ya han construido una relación de confianza. Esto conduce a concluir que la confianza y/o el temor al conflicto o al posible perjuicio económico constituyen una barrera de adopción que, al menos por el momento, esta nueva tecnología no ha podido derribar.

Si bien parece razonable pensar que muchas personas no comprenden exactamente cómo funciona la tecnología *blockchain*, no surge que esto haya sido un impedimento para que algunos de ellos decidan, por ejemplo, adquirir criptomonedas. En la actualidad, varias empresas han generado plataformas que facilitan el acceso a estas y pareciera que los usuarios acceden a comprar criptomoneda fácilmente, sin embargo, deciden hacerlo especialmente si conocen a alguien que ya lo haya hecho antes que ellos. Quizás el mismo destino le espera a la tecnología de los contratos inteligentes. Si se construyen herramientas para hacer el proceso de utilización de contratos inteligentes más fácil y claro, nuevos interesados pueden comenzar a utilizarla y, si la experiencia es satisfactoria atraerá a otros a comenzar su utilización.

Las PYMES y los profesionales independientes de la Argentina, aún en conocimiento de que no son eficientes en sus contrataciones y de que la construcción de confianza es un

proceso que demanda tiempo, no parecen estar listos para dar este paso, el de la adopción de una tecnología que, aunque se muestra superadora en relación a los instrumentos actuales de contratación, no ha alcanzado a probar aún que puede permitirles ampliar más rápidamente su red de proveedores de manera eficiente, alineando sus intereses a través de, por ejemplo, la aplicación de un protocolo de depósito doble en un contrato inteligente.

Quizás, tal cómo hemos visto en reiteradas ocasiones en la historia de la humanidad, la clave del éxito sea aguardar a que los hombres descubran una nueva necesidad que sólo esta tecnología puede resolver de forma eficiente, acelerando así su evolución y masificando, finalmente, su adopción.

5. Referencias bibliográficas

Anderson, D. R., Sweeney, D. J., Williams, A. T., Camm, J. D., & Kipp, M. (2011). *Métodos Cuantitativos Para Los Negocios 11A*. Ed. México: Cengage Learning.

Asgaonkar, A., & Krishnamachari, B. (06 de 2018). *Solving the Buyer and Seller's Dilemma: A Dual-Deposit Escrow Smart Contract for Provably Cheat-Proof Delivery and Payment for a Digital Good without a Trusted Mediator*. Obtenido de IEEE Xplore Digital Library: <https://ieeexplore.ieee.org/abstract/document/8751482/>

Ast, F. (2019). Los contratos inteligentes y el nacimiento de Ethereum [Archivo de video]. *La Disrupción del Blockchain*. Coursera. Obtenido de <https://www.coursera.org/learn/blockchain-espanol/lecture/ijKkW/los-contratos-inteligentes-y-el-nacimiento-de-ethereum>

Blockchain Luxembourg S.A. (s.f.). *Market Capitalization*. Recuperado el 06 de 2019, de [blockchain.com: https://www.blockchain.com/charts/market-cap](https://www.blockchain.com/charts/market-cap)

Brown, T. (Septiembre de 2019). *Design Thinking*. Obtenido de Ideou: <https://www.ideou.com/pages/design-thinking>

Chase, R. B., Jacobs, F. R., & Aquilano, N. J. (2009). *ADMINISTRACIÓN DE OPERACIONES. Producción y cadena de suministros. Duodécima edición*. México: Mc Graw Hill.

CoinLore. (s.f.). *All Cryptocurrencies*. Recuperado el 06 de 2019, de Coinlore: https://www.coinlore.com/all_coins

CriptoNoticias. (s.f.). *Cómo elegir una cartera de Bitcoin y otras criptomonedas*. Recuperado el 07 de 2019, de CriptoNoticias: <https://www.criptonoticias.com/criptopedia/como-elegir-monedero-cartera-bitcoin-criptomonedas-criptoactivos/#axzz4uARQiSeT>

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., & Nachiappan. (2016). *BlockChain Technology: Beyond Bitcoin*. *Applied Innovation Review*.

CuriousInventor. (2 de Julio de 2016). Demo: Create an Ethereum Smart Contract [Archivo de Video]. YouTube. Obtenido de <https://www.youtube.com/watch?v=IQ4USRtzWko>

del Castillo, M. (Abril de 2019). *Blockchain 50: Billion Dollar Babies*. Recuperado el 2019 de Septiembre, de Forbes.com: <https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/#7b4b120257cc>

Fintech News Malaysia. (14 de Octubre de 2019). *Fintech News Malaysia*. Recuperado el 10 de 2019, de HSBC Successfully Pilots Malaysia's First Letter of Credit Transaction on the Blockchain: <https://fintechnews.my/21774/blockchain/hsbc-pilots-blockchain-letter-of-credit-transaction-between-malaysia-and-singapore/>

Fung, B. (21 de Mayo de 2014). *Marc Andreessen: In 20 years, we'll talk about Bitcoin like we talk about the Internet today*. Obtenido de The Washington Post: <https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/>

GitHub, Inc. (s.f.). *GitHub*. Recuperado el 04 de 2019, de <https://github.com>

Goldfeder, S. B. (Diciembre de 2017). *Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin*. Obtenido de Princeton University Library: <http://arks.princeton.edu/ark:/88435/pr1c39c>

IDEO.org. (Septiembre de 2019). *Design Kit: The Human-Centered Design Toolkit, 2nd. Edition*. Obtenido de IDEO: <https://www.ideo.com/post/design-kit>

Mitra, R. (Febrero de 2019). *Contratos inteligentes: La tecnología de cadena de bloques que reemplazará a los abogados*. Recuperado el 11 de 2019, de blockgeeks.com: <https://blockgeeks.com/guides/es/contratos-inteligentes/>

Morabito, V. (2017). *Business Innovation Through Blockchain*.

Morris, C. (Abril de 2019). *Cryptocurrency Owners Can't Access Funds After Exchange CEO Dies—Because No One Knows the Password*. Recuperado el 09 de 2019, de Fortune.com: <https://fortune.com/2019/02/04/cryptocurrency-quadrigacx-gerald-cotten-frozen-funds/>

Murro, C. F. (2001). *Negociemos*. Buenos Aires: Del Nuevo Extremo.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Obtenido de Bitcoin.org: <https://bitcoin.org/bitcoin.pdf>

Nash, G. (07 de Diciembre de 2017). *Build Your First Smart Contract. A Tutorial for Beginners*. Recuperado el 10 de 2019, de medium.com: <https://medium.com/cryptocurrency/build-your-first-smart-contract-fc36a8ff50ca>

- Ng, J. (Mayo de 2019). *Escrow Service as a Smart Contract: The Business Logic*. Recuperado el 2019 de 09, de Medium, Coinmonks: <https://medium.com/coinmonks/escrow-service-as-a-smart-contract-the-business-logic-5b678ebe1955>
- Plattner, H. (2018). *GUÍA DEL PROCESO CREATIVO. Mini guía: una introducción al Design Thinking + Bootcamp bootleg*. Obtenido de Stanford.edu: <https://dschool-old.stanford.edu/sandbox/groups/designresources/wiki/31fbd/attachments/027aa/GUÍA%20DEL%20PROCESO%20CREATIVO.pdf>
- Sethi, R. (2008). Nash Equilibrium. En M. Guha, *International Encyclopedia of the Social Sciences (2nd edition)* (págs. 540-542). Macmillan Reference USA.
- Solidity. (Octubre de 2019). *Solidity by Example*. Obtenido de Safe Remote Purchase: <https://solidity.readthedocs.io/en/v0.4.24/solidity-by-example.html#safe-remote-purchase>
- Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Weber, I., . . . Zhu, J. (06 de Junio de 2017). *Research Publications Repository*. Recuperado el Abril de 2019, de Risks and opportunities for systems using blockchain and smart contracts: <https://publications.csiro.au/rpr/pub?pid=csiro:EP175103>
- Sun, W., & Xun, W. (2018). *Blockchain Quick Start Guide: A beginner's guide to developing enterprise-grade decentralized applications*. Birmingham: Packt Publishing.
- Tapscott, D., & Tapscott, A. (2017). *Realizing the Potential of Blockchain*. Switzerland: World Economic Forum.

Tomio, A., Geyer, S., & Cascio, G. (Junio de 2019). *Design Thinking Strategies*. Obtenido de Entornos Virtuales de Aprendizaje, Universidad Católica Argentina: https://eva.uca.edu.ar/pluginfile.php/632801/mod_resource/content/0/Clase%20-%20Design%20Thinking%20Strategies.pdf

Valeska, E. (17 de Junio de 2017). *Contratos inteligentes llegan a los seguros internacionales con IBM, AIG y Standard Chartered*. Recuperado el 09 de 2019, de CriptoNoticias: <https://www.criptonoticias.com/aplicaciones/contratos-inteligentes-llegan-seguros-internacionales-ibm-aig-standard-chartered/>

White, G. R. (Enero de 2017). *Future Applications of Blockchain in Business and Management: a Delphi study*. Recuperado el 07 de 2019, de ResearchGate: https://www.researchgate.net/publication/317564084_Future_Applications_of_Blockchain_in_Business_and_Management_a_Delphi_study

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 352. Obtenido de Blockchain Challenges and Opportunities: A Survey.

6. Bibliografía

Everledger Ltd. (s.f.). *Everledger*. Obtenido de www.everledger.io: <https://www.everledger.io>

Anderson, D. R., Sweeney, D. J., Williams, A. T., Camm, J. D., & Kipp, M. (2011). *Métodos Cuantitativos Para Los Negocios 11A*. Ed. México: Cengage Learning.

Asgaonkar, A., & Krishnamachari, B. (06 de 2018). *Solving the Buyer and Seller's Dilemma: A Dual-Deposit Escrow Smart Contract for Provably Cheat-Proof Delivery and Payment for a Digital Good without a Trusted Mediator*. Obtenido de IEEE Xplore Digital Library: <https://ieeexplore.ieee.org/abstract/document/8751482/>

Ast, F. (2019). Los contratos inteligentes y el nacimiento de Ethereum [Archivo de video]. *La Disrupción del Blockchain*. Coursera. Obtenido de <https://www.coursera.org/learn/blockchain-espanol/lecture/ijKkW/los-contratos-inteligentes-y-el-nacimiento-de-ethereum>

Blockchain Luxembourg S.A. (s.f.). *Market Capitalization*. Recuperado el 06 de 2019, de [blockchain.com: https://www.blockchain.com/charts/market-cap](https://www.blockchain.com/charts/market-cap)

Brown, T. (Septiembre de 2019). *Design Thinking*. Obtenido de Ideou: <https://www.ideo.com/pages/design-thinking>

Chase, R. B., Jacobs, F. R., & Aquilano, N. J. (2009). *ADMINISTRACIÓN DE OPERACIONES. Producción y cadena de suministros. Duodécima edición*. México: Mc Graw Hill.

Chohan, U. W. (4 de 8 de 2017). *Cryptocurrencies: A Brief Thematic Review*. Obtenido de SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330

- Clack, C. D., Bakshi, V. A., & Braine, L. (15 de Diciembre de 2016). *Smart Contract Templates: essential requirements and design options*. Recuperado el April de 2019, de ArXiv.org, Cornell University: <https://arxiv.org/abs/1612.04496>
- Clack, C. D., Bakshi, V. A., & Braine, L. (2017 de Marzo de 2017). *Smart Contract Templates: foundations, design landscape and research directions*. Recuperado el Abril de 2019, de arXiv.org, Cornell University: <https://arxiv.org/abs/1608.00771>
- CoinLore. (s.f.). *All Cryptocurrencies*. Recuperado el 06 de 2019, de Coinlore: https://www.coinlore.com/all_coins
- CriptoNoticias. (s.f.). *Cómo elegir una cartera de Bitcoin y otras criptomonedas*. Recuperado el 07 de 2019, de CriptoNoticias: <https://www.criptonoticias.com/criptopedia/como-elegir-monedero-cartera-bitcoin-criptomonedas-criptoactivos/#axzz4uARQiSeT>
- Cristalino SRL. (s.f.). *Cristalino*. Obtenido de <https://cristalino.com.ar>
- Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., & Nachiappan. (2016). *BlockChain Technology: Beyond Bitcoin*. *Applied Innovation Review*.
- CuriousInventor. (2 de Julio de 2016). *Demo: Create an Ethereum Smart Contract [Archivo de Video]*. YouTube. Obtenido de <https://www.youtube.com/watch?v=IQ4USRtzWko>
- del Castillo, M. (Abril de 2019). *Blockchain 50: Billion Dollar Babies*. Recuperado el 2019 de Septiembre, de Forbes.com: <https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/#7b4b120257cc>

Dentacoin Foundation. (s.f.). *Dentacoin: The Blockchain Solution for the Global Dental Industry*. Obtenido de <https://dentacoin.com>

DIXITPC. (s.f.). *DIXITPC.COM | INFORMÁTICA*. Obtenido de DIXITPC.COM: <http://dixitpc.com/>

Dream Management Limited. (s.f.). *Hire Blockchain Freelancers | DREAM*. Obtenido de DREAM: <https://dream.ac>

Fintech News Malaysia. (14 de Octubre de 2019). *Fintech News Malaysia*. Recuperado el 10 de 2019, de HSBC Successfully Pilots Malaysia's First Letter of Credit Transaction on the Blockchain: <https://fintechnews.my/21774/blockchain/hsbc-pilots-blockchain-letter-of-credit-transaction-between-malaysia-and-singapore/>

Fiverr International Ltd. (s.f.). *Fiverr*. Obtenido de www.fiverr.com: <https://www.fiverr.com>

Fung, B. (21 de Mayo de 2014). *Marc Andreessen: In 20 years, we'll talk about Bitcoin like we talk about the Internet today*. Obtenido de The Washington Post: <https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/>

Gigster. (s.f.). *Gigster*. Obtenido de gigster.com: <https://gigster.com>

GitHub, Inc. (s.f.). *GitHub*. Recuperado el 04 de 2019, de <https://github.com>

Goldfeder, S. B. (Diciembre de 2017). *Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin*. Obtenido de Princeton University Library: <http://arks.princeton.edu/ark:/88435/pr1c39c>

IDEO.org. (Septiembre de 2019). *Design Kit: The Human-Centered Design Toolkit, 2nd. Edition.*

Obtenido de IDEO: <https://www.ideo.com/post/design-kit>

Mitra, R. (Febrero de 2019). *Contratos inteligentes: La tecnología de cadena de bloques que*

reemplazará a los abogados. Recuperado el 11 de 2019, de blockgeeks.com:

<https://blockgeeks.com/guides/es/contratos-inteligentes/>

Morabito, V. (2017). *Business Innovation Through Blockchain.*

Morris, C. (Abril de 2019). *Cryptocurrency Owners Can't Access Funds After Exchange CEO*

Dies—Because No One Knows the Password. Recuperado el 09 de 2019, de

Fortune.com: <https://fortune.com/2019/02/04/cryptocurrency-quadrigacx-gerald-cotten-frozen-funds/>

Mougayar, W., & Buterin, V. (2016). *The Business Blockchain: Promise, Practice, and*

Application of the Next Internet Technology.

Murro, C. F. (2001). *Negociemos.* Buenos Aires: Del Nuevo Extremo.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtenido de Bitcoin.org:

<https://bitcoin.org/bitcoin.pdf>

Nash, G. (07 de Diciembre de 2017). *Build Your First Smart Contract. A Tutorial for Beginners.*

Recuperado el 10 de 2019, de [medium.com](https://medium.com/cryptocurrency/build-your-first-smart-contract-fc36a8ff50ca): <https://medium.com/cryptocurrency/build-your-first-smart-contract-fc36a8ff50ca>

Ng, J. (Mayo de 2019). *Escrow Service as a Smart Contract: The Business Logic*. Recuperado el 2019 de 09, de Medium, Coinmonks: <https://medium.com/coinmonks/escrow-service-as-a-smart-contract-the-business-logic-5b678ebe1955>

Plattner, H. (2018). *GUÍA DEL PROCESO CREATIVO. Mini guía: una introducción al Design Thinking + Bootcamp bootleg*. Obtenido de Stanford.edu: <https://dschool-old.stanford.edu/sandbox/groups/designresources/wiki/31fbf/attachments/027aa/GUÍA%20DEL%20PROCESO%20CREATIVO.pdf>

Quadriga CCAA. (s.f.). *QuadrigaCX*. Obtenido de www.quadrigacxtrustee.com: <https://www.quadrigacxtrustee.com>

Scratch Project. (s.f.). *Scratch*. Obtenido de [Scratch.com](https://scratch.mit.edu): <https://scratch.mit.edu>

Sethi, R. (2008). Nash Equilibrium. En M. Guha, *International Encyclopedia of the Social Sciences (2nd edition)* (págs. 540-542). Macmillan Reference USA.

Smaply. (s.f.). *Smaply*. Obtenido de [smaply.com](https://www.smaply.com/): <https://www.smaply.com/>

Solidity. (Octubre de 2019). *Solidity by Example*. Obtenido de Safe Remote Purchase: <https://solidity.readthedocs.io/en/v0.4.24/solidity-by-example.html#safe-remote-purchase>

Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Weber, I., . . . Zhu, J. (06 de Junio de 2017). *Research Publications Repository*. Recuperado el Abril de 2019, de Risks and opportunities for systems using blockchain and smart contracts: <https://publications.csiro.au/rpr/pub?pid=csiro:EP175103>

Sun, W., & Xun, W. (2018). *Blockchain Quick Start Guide: A beginner's guide to developing enterprise-grade decentralized applications*. Birmingham: Packt Publishing.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*.

Tapscott, D., & Tapscott, A. (2017). *Realizing the Potential of Blockchain*. Switzerland: World Economic Forum.

Tomio, A., Geyer, S., & Cascio, G. (Junio de 2019). *Design Thinking Strategies*. Obtenido de Entornos Virtuales de Aprendizaje, Universidad Católica Argentina: https://eva.uca.edu.ar/pluginfile.php/632801/mod_resource/content/0/Clase%20-%20Design%20Thinking%20Strategies.pdf

Truffle Blockchain Group 2019. (s.f.). *Ganache | Truffle Suite*. Obtenido de Ganache ONE CLICK BLOCKCHAIN: <https://www.trufflesuite.com/truffle>

Upwork® Global Inc. (s.f.). *Upwork*. Obtenido de www.upwork.com: <https://www.upwork.com>

Valeska, E. (17 de Junio de 2017). *Contratos inteligentes llegan a los seguros internacionales con IBM, AIG y Standard Chartered*. Recuperado el 09 de 2019, de CriptoNoticias: <https://www.criptonoticias.com/aplicaciones/contratos-inteligentes-llegan-seguros-internacionales-ibm-aig-standard-chartered/>

Venture Proxy Ltd. (s.f.). *Blockverify*. Obtenido de [blockverify.io](http://www.blockverify.io): <http://www.blockverify.io>

White, G. R. (Enero de 2017). *Future Applications of Blockchain in Business and Management: a Delphi study*. Recuperado el 07 de 2019, de ResearchGate: https://www.researchgate.net/publication/317564084_Future_Applications_of_Blockchain_in_Business_and_Management_a_Delphi_study

Xapo (Gibraltar) Limited. (s.f.). *Xapo*. Obtenido de Xappo.com: <https://xapo.com/>

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 352. Obtenido de Blockchain Challenges and Opportunities: A Survey.

Anexo I. Glosario de términos

Bloque: Paquete de datos que contiene transacciones que se registran en una *blockchain*.

Bitcoin: La primera criptomoneda basada tecnología *blockchain*. El documento fue publicado bajo el seudónimo de Satoshi Nakamoto el 31 de octubre de 2008. La red comenzó a operar el 3 de enero de 2009.

Blockchain: Una base de datos distribuida de registros de todas las transacciones o eventos digitales que se han ejecutado y compartido entre las partes participantes, almacenados en bloques que se encuentran vinculados por medio de una cadena criptográfica.

BTC: Unidad de Bitcoin, coin de la *blockchain* Bitcoin.

Coin: Una determinada cantidad de una criptomoneda. Sirven al propósito de ser utilizada como medio de resguardo, transferencia y unidad de valor. Ejemplos son ETH (de Ethereum) y BTC (de Bitcoin).

Comisión de Transacción: Comisión que se paga a los mineros para procesar una transacción con criptomoneda.

Confirmación: Acto realizado por los mineros que verifica una transacción y la agrega al *blockchain*.

Consenso: Ocurre cuando todos los participantes de la red se ponen de acuerdo en una cadena de transacciones, lo que asegura que todos los nodos tienen una copia exacta del mismo registro.

Contrato inteligente (Smart contract): Instrucciones escritas en forma de código en una red descentralizada, que se ejecutan tras la ocurrencia de cierto evento.

Criptomoneda: Representación de un activo digital construido sobre criptografía.

Dirección pública: Conjunto de caracteres alfanuméricos que se usa para enviar y recibir fondos en las transacciones de una red de criptomoneda.

DApp: Una aplicación descentralizada es una aplicación de código abierto (no propietario) que opera de manera autónoma y tiene sus datos almacenados en el *blockchain*. Son muy importantes dentro del *blockchain* de Ethereum.

ETH/Ether: Unidad de Ether, coin de la *blockchain* Ethereum.

Ethereum: *Blockchain* programable líder, creada en 2015. A diferencia de la *blockchain* Bitcoin fue concebida para facilitar la creación y ejecución de DApps y contratos inteligentes.

Firma Digital: Código digital generado por encriptación pública que se adhiere a un documento transmitido electrónicamente para verificar su contenido y la identidad del que lo envía.

Freelance: Se refiere al trabajador que desarrolla su actividad de manera autónoma: es decir, sin una relación fija y de dependencia con un empleador.

Ganache: Software que permite ejecutar rápidamente una *blockchain* personal/privada de Ethereum que puede ser usado para realizar pruebas e inspeccionar el estado de las operaciones mientras se controla cómo opera la cadena de bloques (Truffle Blockchain Group 2019, s.f.).

Hash o Función de hash criptográfica: Produce un valor de hash de tamaño fijo de un input de tamaño variable. El algoritmo SHA-256, utilizado por la red de *Bitcoin*, es un ejemplo de hash criptográfico.

Insight: La capacidad de obtener una comprensión precisa y profunda de alguien o algo, expresado en términos simples. Pueden expresar necesidades que no son visibles a simple vista.

MetaMask: Software de Billetera electrónica que se integra como un complemento a un navegador web.

MyEthereumWallet: Software de Billetera electrónica que se ejecuta de forma local y es accesible a través de un navegador web, dado que su interfaz gráfica fue construida en formato web.

Llave privada: Conjunto de datos que permite acceder a la criptomoneda en una *wallet*. Sirve como password que debe mantenerse oculto de otras personas.

Llave pública: Clave que se utiliza para cifrar una transacción en la red de *blockchain*.

Mineros: Nodos de la red de *blockchain* encargados de validar las transacciones, creando así bloques. Los mineros difunden estos bloques al resto de la red para que formen parte del registro distribuido. Por este trabajo, reciben comisiones de transacción.

Off-chain: Aquello que se realizan por fuera de un *blockchain*.

On-chain: Aquello que se realizan dentro de un *blockchain*.

Nodo: Copia del registro operado por una computadora de la red de *blockchain*.

Registro Distribuido: Registro donde los datos están almacenados en una red de nodos descentralizados.

Red Distribuida: Tipo de red donde el poder de cómputo y los datos están repartidos en nodos en lugar de en un agente centralizado.

Recompensa de Bloque: Pago en *bitcoin* que la red otorga a un minero que calculó exitosamente el hash de un bloque.

Ropsten: Es la red de pruebas de Ethereum, utilizada por desarrolladores para probar el funcionamiento de esta. No tiene cargo utilizarla y los *coins/tokens* que operan no tiene valor.

Scratch: Es un lenguaje de programación visual desarrollado por el MIT. Su sitio web permite crear aplicaciones de forma gráfica y leer el código en lenguaje natural para facilitar el entendimiento y aprendizaje.

Solidity: Un lenguaje de programación orientado a objetos para escribir contratos inteligentes. Se usa para implementar contratos inteligentes en varias plataformas *blockchain*, especialmente Ethereum.

Wallet: Software que permite realizar transacciones en el *blockchain*, como enviar/recibir pagos y consultar el saldo.

Anexo II. Pasos para desplegar un contrato inteligente en una testnet privada

Para este simple ejemplo, se utilizó una *blockchain* privada. El software *Ganache*, permite crear rápidamente una *blockchain* de Ethereum en un ordenador. Básicamente permite crear una nueva *blockchain*, de un sólo nodo, que no tiene ningún bloque inicialmente, pero tiene la capacidad de crear y verificar transacciones y de ejecutar contratos inteligentes. Del mismo modo que desde una página web es posible leer correos electrónicos, una vez instalado *Ganache*, se instalará un servidor web en el ordenador y es posible interactuar con él desde una interfaz web para enviar transacciones con un software de billetera (*wallet*).

La billetera utilizada es *MyEthereumWallet*, una billetera con similares características a las mencionadas anteriormente, pero que permite desplegar contratos y ejecutar sus funciones. A continuación, se muestran los pasos a realizar.

1. Ir a <https://remix.ethereum.org/>, crear un nuevo archivo y copiar en él el contenido del contrato. Desde el explorador de archivos ("*File Explorer*") presionar el símbolo más ("+") para crear un nuevo archivo. Nombrar el nuevo archivo "counter.sol" (ver a continuación la *Figura Anexo II-1* a modo de referencia).

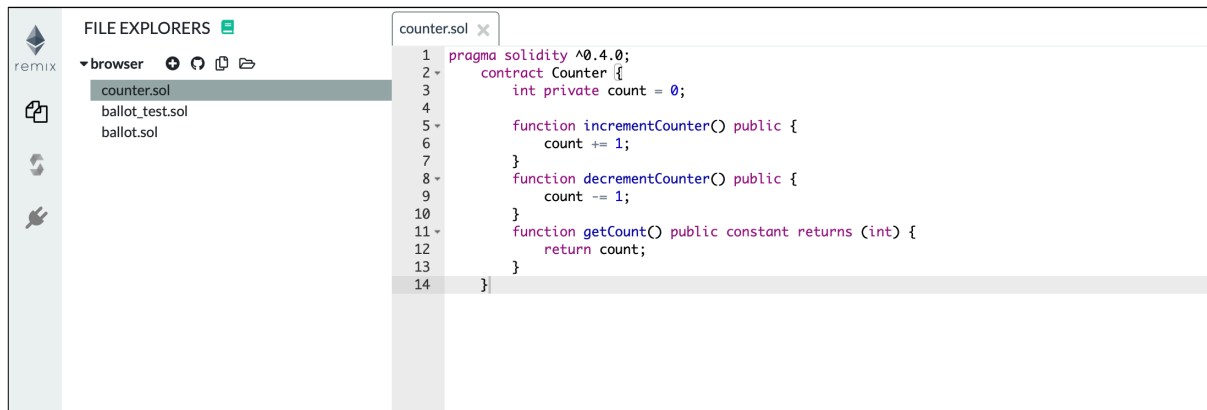


Figura Anexo II-1. IDE Remix. Explorador de Archivos. Fuente: Elaboración propia (2019).

2. Activar el compilador de Solidity (“Solidity Compiler”) desde el “Plugin Manager”, al cual es posible acceder al presionar el icono de enchufe en la barra lateral izquierda (ver a continuación la *Figura Anexo II-2* a modo de referencia).

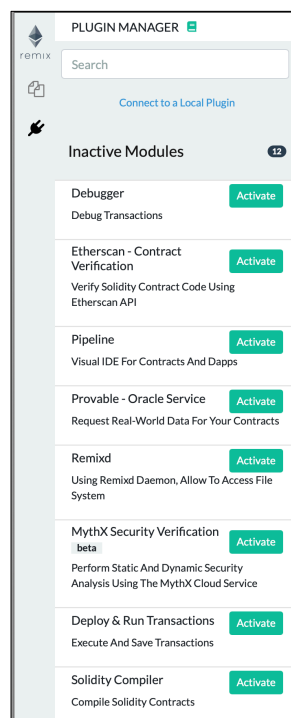


Figura Anexo II-2. IDE Remix. Plugin Manager. Fuente: Elaboración propia (2019).

3. Ir a la pestaña del compilador, y compilar el contrato presionando “*Compile counter.sol*” (ver a continuación la *Figura Anexo II-3* a modo de referencia).

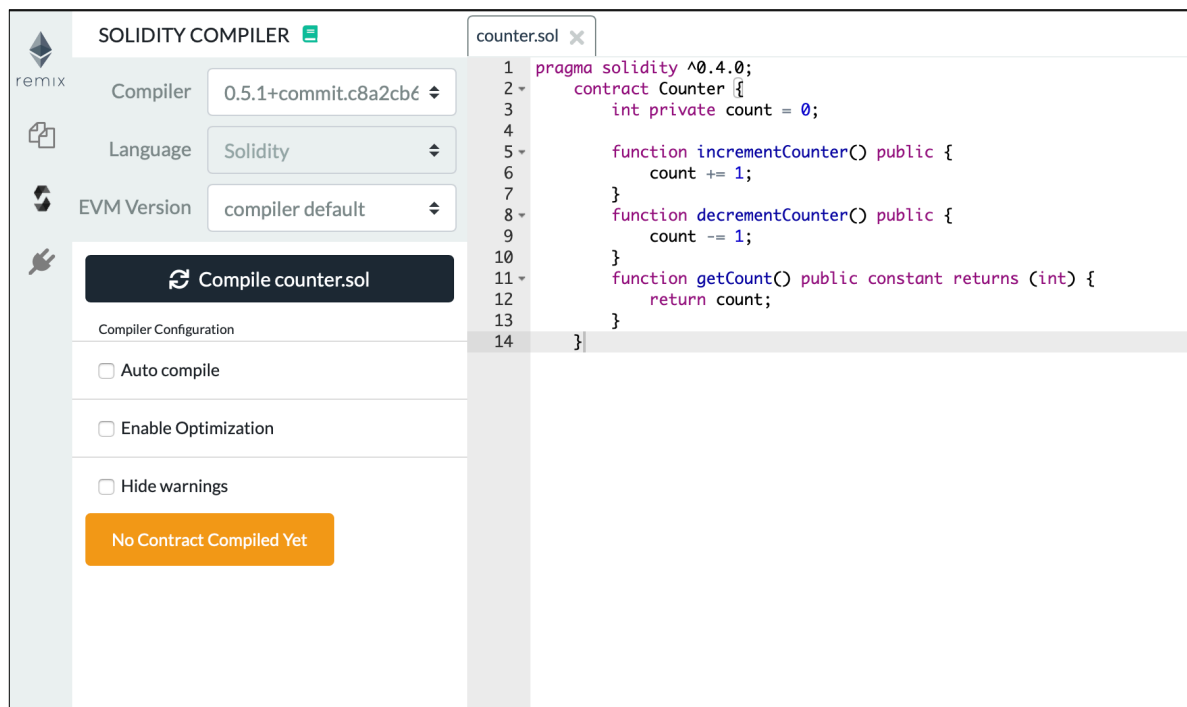


Figura Anexo II-3. IDE Remix. Solidity Compiler. Fuente: Elaboración propia (2019).

4. Clickear en “*Compilation Details*” y copiar el contenido del campo “*ByteCode*” (ver a continuación la *Figura Anexo II-4* a modo de referencia).

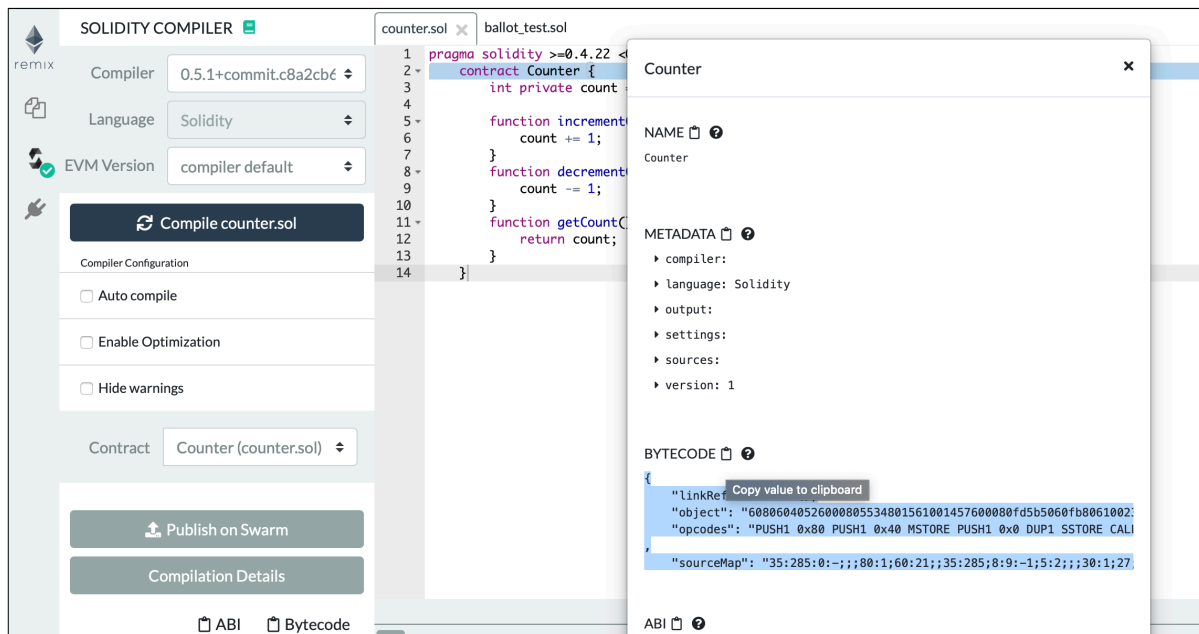


Figura Anexo II-4. IDE Remix. Solidity Compiler. ByteCode. Fuente: Elaboración propia (2019).

5. Descargar, instalar y abrir la aplicación *Ganache*. Una vez instalado, puede verse la lista de cuentas de prueba (ver a continuación la *Figura Anexo II-5* a modo de referencia).

ACCOUNTS		BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS	SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 0	GAS PRICE 2000000000	GAS LIMIT 6721975	HARDFORK PETERSBURG	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING	WORKSPACE QUICKSTART
MNEMONIC pair culture wool high legal switch clip equip marine bar toe patch							HD PATH m/44'/60'/0'/0'/account_index
ADDRESS 0xb30b76D3364E3e6FDD5Bff5D4221D56C28Fb3BdF	BALANCE 100.00 ETH	TX COUNT 0	INDEX 0				
ADDRESS 0xb4c9661324e3f376e69A1A5aE9F57cd1e48BDE16	BALANCE 100.00 ETH	TX COUNT 0	INDEX 1				
ADDRESS 0xb5a6929E4CF30618Be1ad3b55D6b32AB4089ea2D	BALANCE 100.00 ETH	TX COUNT 0	INDEX 2				
ADDRESS 0x527a14E7c2e640Ae4cff96b0877A5D1609D7a59B	BALANCE 100.00 ETH	TX COUNT 0	INDEX 3				
ADDRESS 0xda1d395D5f51d0a148C30b1F088c8aF1692EA8E6	BALANCE 100.00 ETH	TX COUNT 0	INDEX 4				

Figura Anexo II-5. Ganache. Lista de cuentas. Fuente: Elaboración propia (2019).

6. Descargar *MyEthereumWallet*, descomprimir y abrir *index.html*. Ir al menú desplegable del margen superior derecho y elegir la última opción: “*Add custom Network*” / “*Node*” (ver a continuación la *Figura Anexo II-6* a modo de referencia).

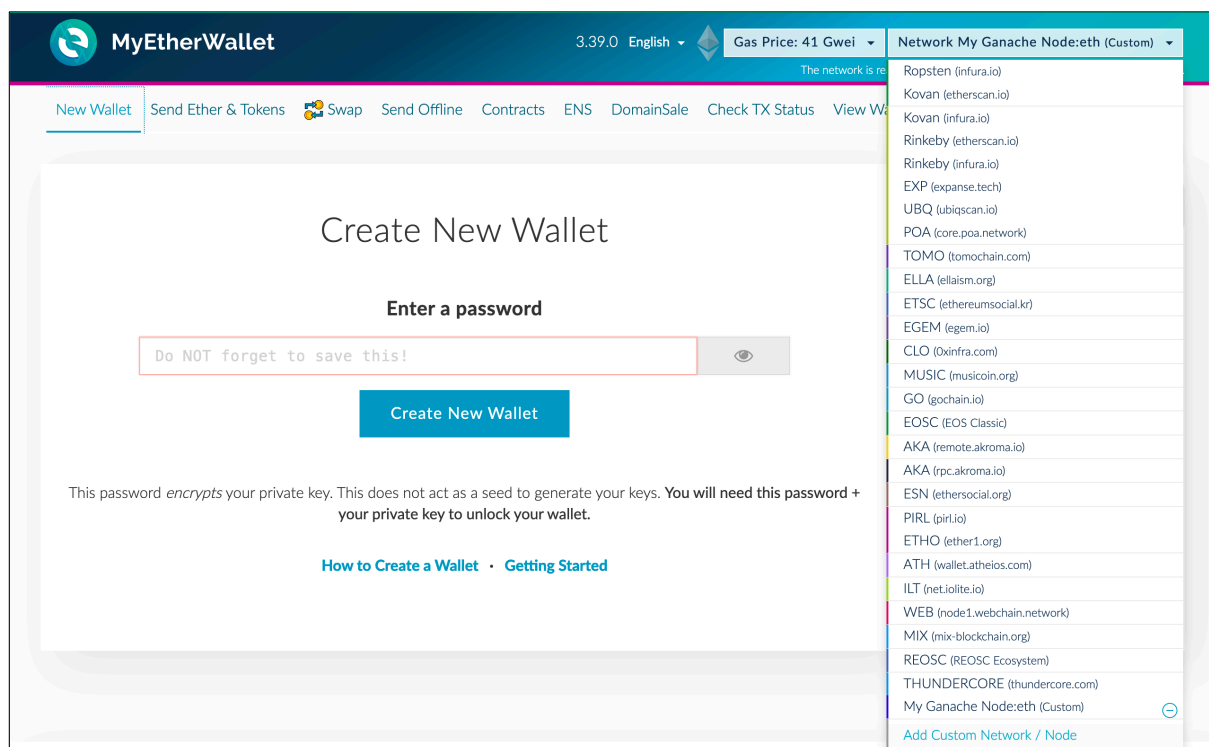


Figura Anexo II-6. MyEthereumWallet. Lista de redes. Fuente: Elaboración propia (2019).

7. Insertar “Ganache node” en el campo “*Node Name*”, “*http://localhost*” en el campo “*URL*” y “*7545*” en el campo “*Port*”, tal como se muestra en la *Figura Anexo II-7*.

Set Up Your Custom Node ✕

[Instructions can be found here](#)

Your node must be HTTPS in order to connect to it via MyEtherWallet.com. You can [download the MyEtherWallet repo & run it locally](#) to connect to any node. Or, get free SSL certificate via [LetsEncrypt](#)

Node Name

URL **Port**

HTTP Basic access authentication

ETH **ETC** **Ropsten** **Kovan** **Rinkeby** **Custom**

Cancel
Save & Use Custom Node

Figura Anexo II-7. MyEthereumWallet. Agregar un nodo. Fuente: Elaboración propia (2019).

8. Ir a la solapa “Contracts” y clicar “Deploy Contract”. En el campo “Byte Code” pegar el contenido copiado en el paso 4 (ver a continuación la *Figura Anexo II-8* a modo de referencia).

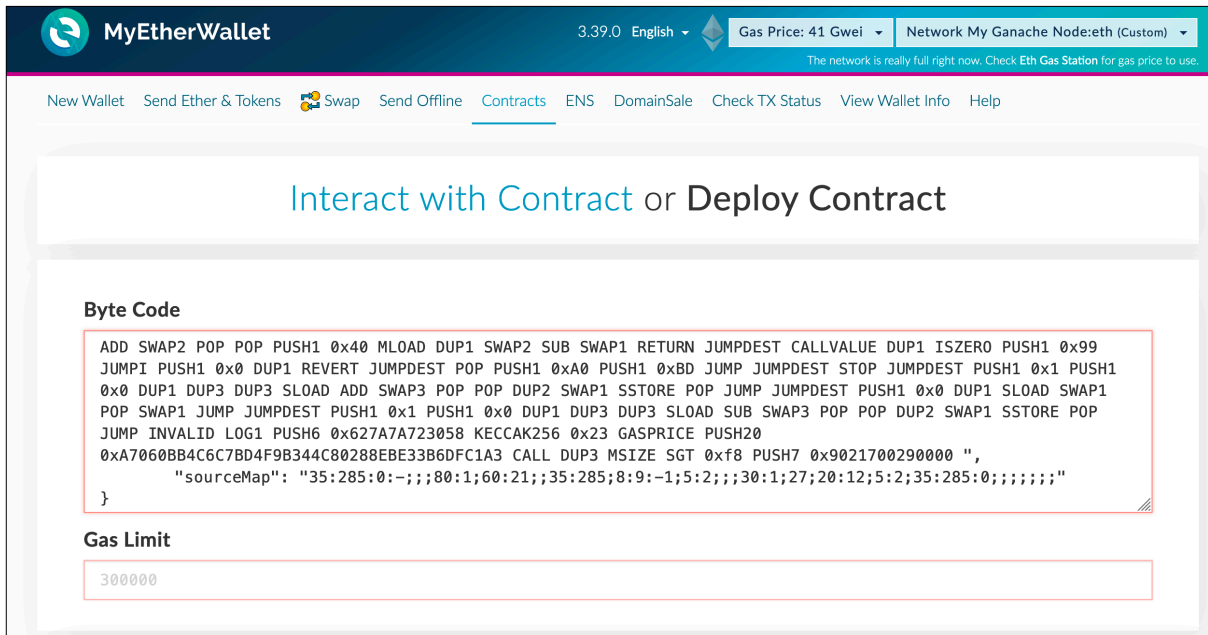


Figura Anexo II-8. MyEthereumWallet. Despliegue de un contrato. Byte Code. Fuente: Elaboración propia (2019).

9. Volver a *Ganache* y clicar en el icono de llave (“*Show Keys*”) de cualquiera de las cuentas listadas. Se muestra una clave privada. Copiar dicha clave (ver a continuación la *Figura Anexo II-9* a modo de referencia).

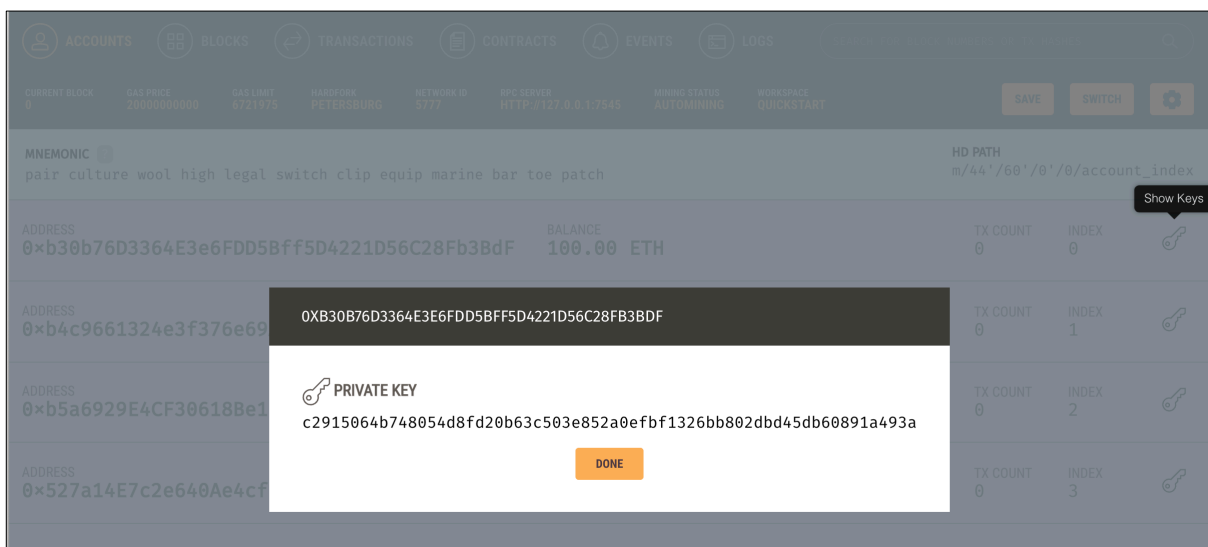


Figura Anexo II-9. Ganache. Mostrar claves. Fuente: Elaboración propia (2019).

10. Regresar a *MyEthereumWallet*, y seleccionar la opción *“Private Key”*. En el campo *“Private Key”* pegar la clave privada copiada en el paso anterior. Luego presionar el botón *“Unlock”* (ver a continuación la *Figura Anexo II- 10* a modo de referencia).

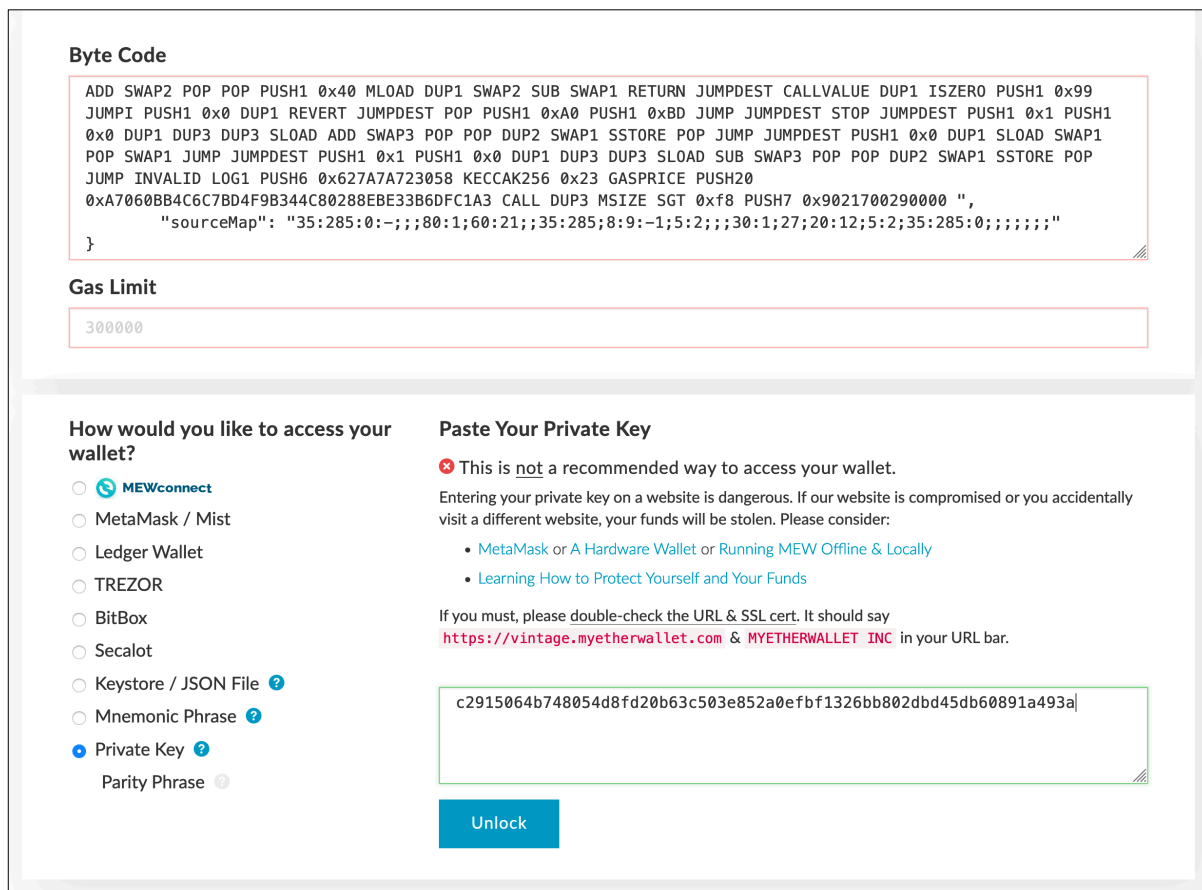


Figura Anexo II- 10. MyEthereumWallet. Despliegue de un contrato. Desbloquear billetera. Fuente: Elaboración propia (2019).

11. Presionar *“Sign Trasaction”*, luego *“Deploy contract”* (ver a continuación la *Figura Anexo II-11* a modo de referencia).

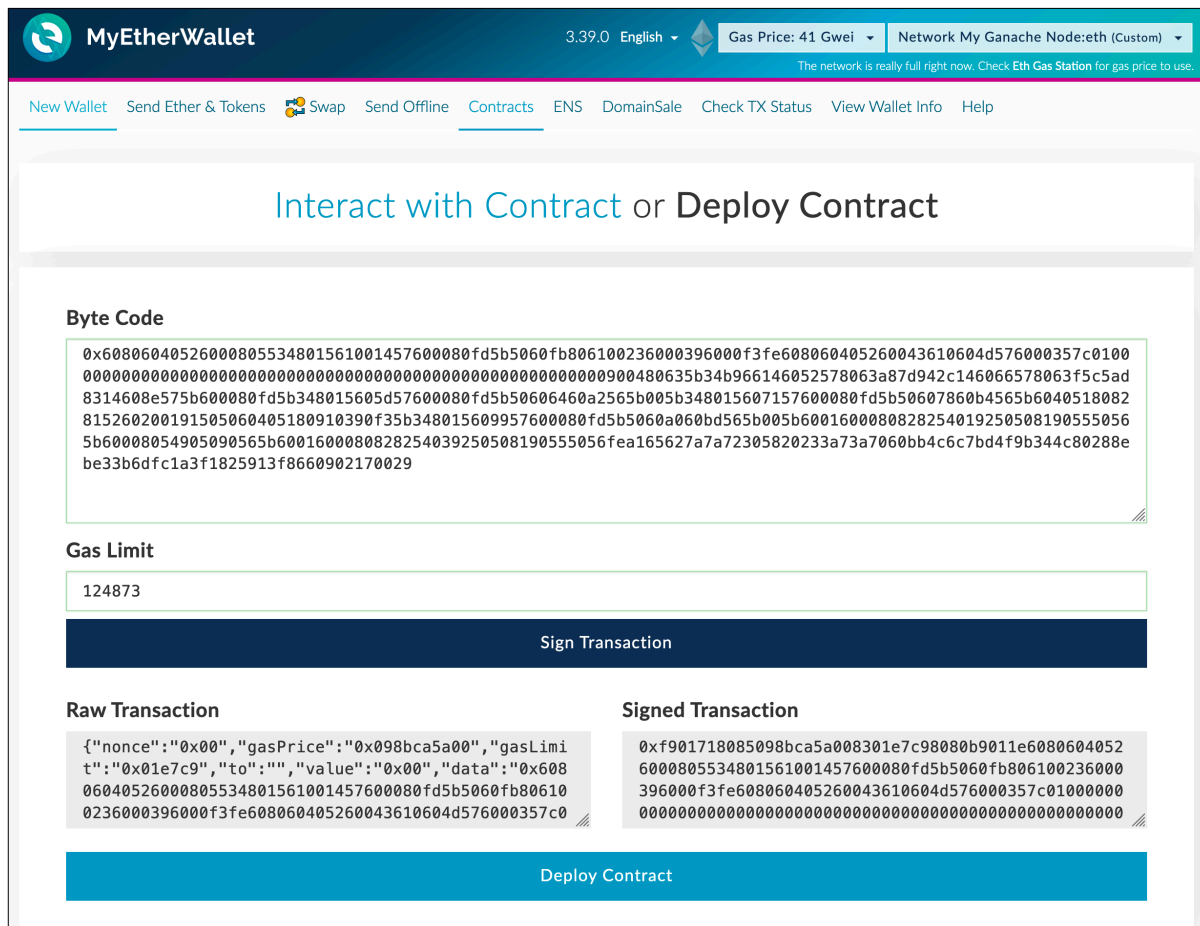


Figura Anexo II-11. MyEthereumWallet. Despliegue de un contrato. Firmar transacción. Fuente: Elaboración propia (2019).

12. Volver a Ganache para verificar si se ha creado un nuevo bloque con el contrato (ver a continuación la Figura Anexo II-12 a modo de referencia).

ACCOUNTS		BLOCKS		TRANSACTIONS		CONTRACTS		EVENTS		LOGS	
CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE	SEARCH FOR BLOCK NUMBERS OR TX HASHES			
1	2000000000	6721975	PETERSBURG	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART	SAVE	SWITCH	⚙️	
BLOCK 1	MINED ON 2019-08-19 12:49:19		GAS USED 124873		1 TRANSACTION						
BLOCK 0	MINED ON 2019-08-19 11:26:51		GAS USED 0		NO TRANSACTIONS						

Figura Anexo II-12. Ganache. Lista de bloques. Fuente: Elaboración propia (2019).

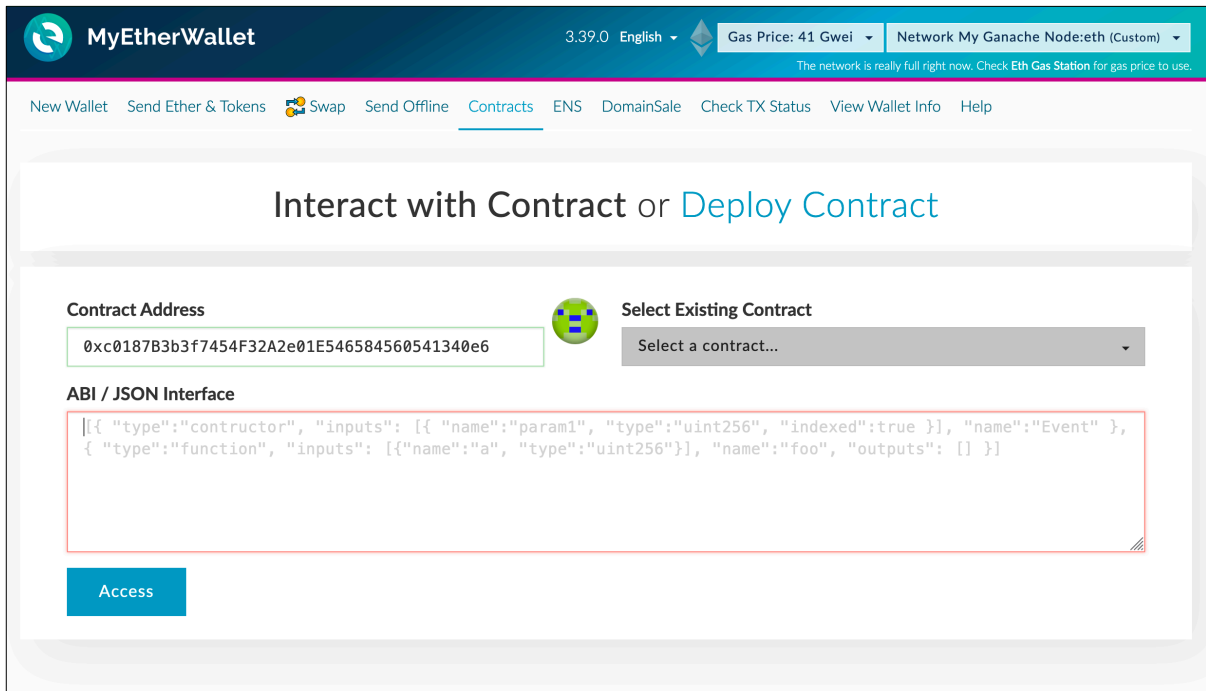


Figura Anexo II-14. MyEthereumWallet. Interactuar con un contrato. Fuente: Elaboración propia (2019).

15. Volver al *IDE Remix* para copiar la interfaz de contrato, haciendo en el campo "ABI", tal como se muestra a continuación en la *Figura Anexo II- 15*.

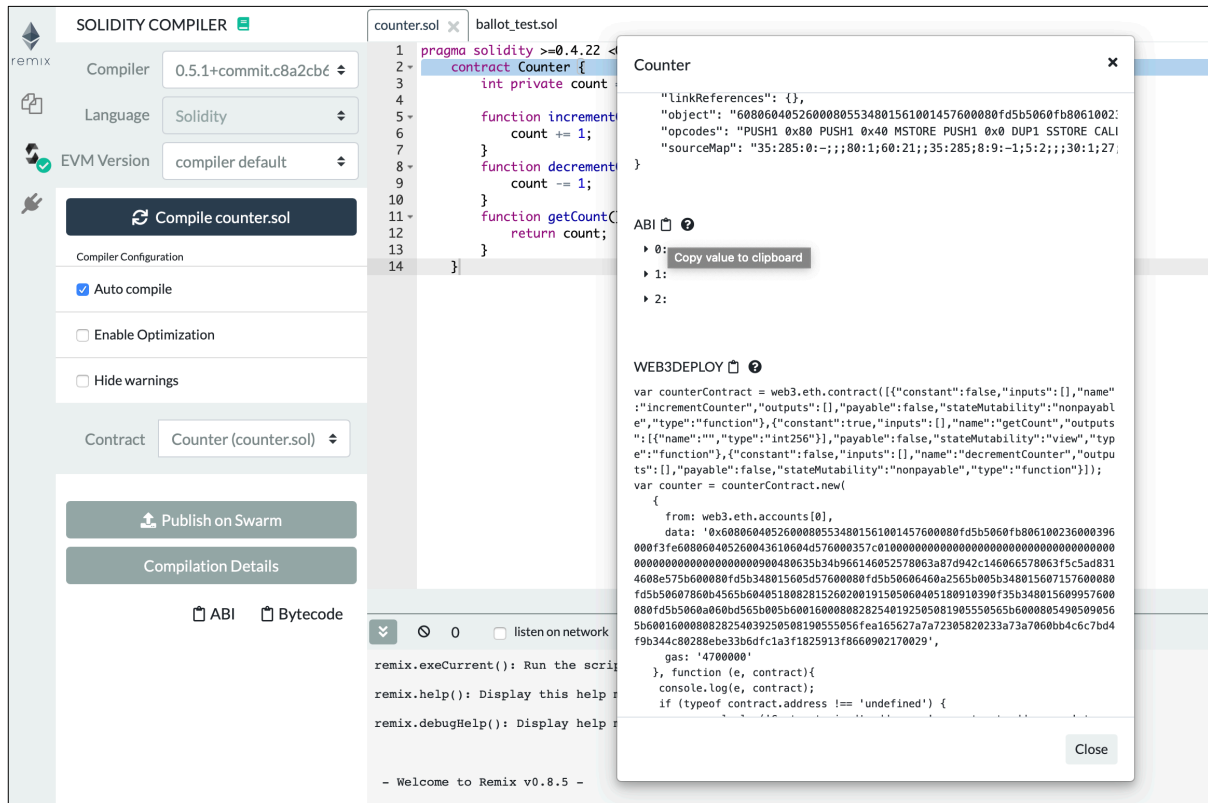


Figura Anexo II- 15. Remix IDE. Copiar la interfaz de un contrato. Fuente: Elaboración propia (2019).

16. Regresar a *MyEthereumWallet*, y pegar en el campo “ABI / JSON Interface” y valor copiado en el paso anterior. Luego cliquer en “Access” (ver a continuación la *Figura Anexo II-16* a modo de referencia).

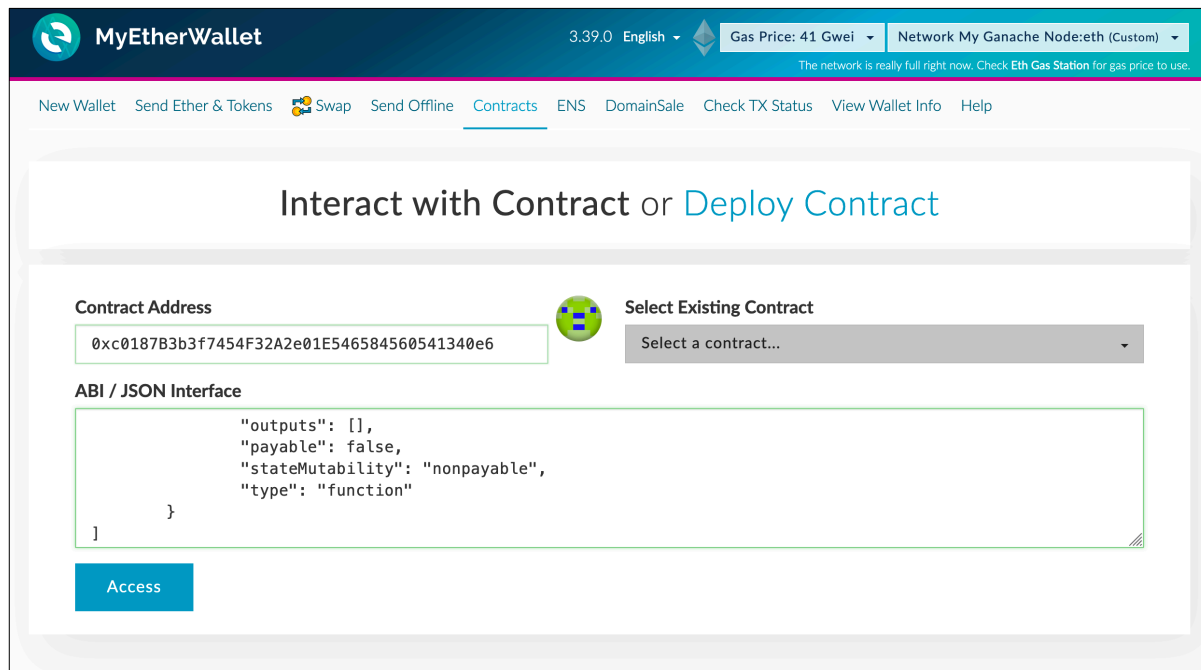


Figura Anexo II-16. MyEthereumWallet. Interacción con un contrato. Fuente: Elaboración propia (2019).

17. Elegir la opción, “*getCount*” del menú desplegable (ver a continuación la *Figura Anexo II-17* a modo de referencia).

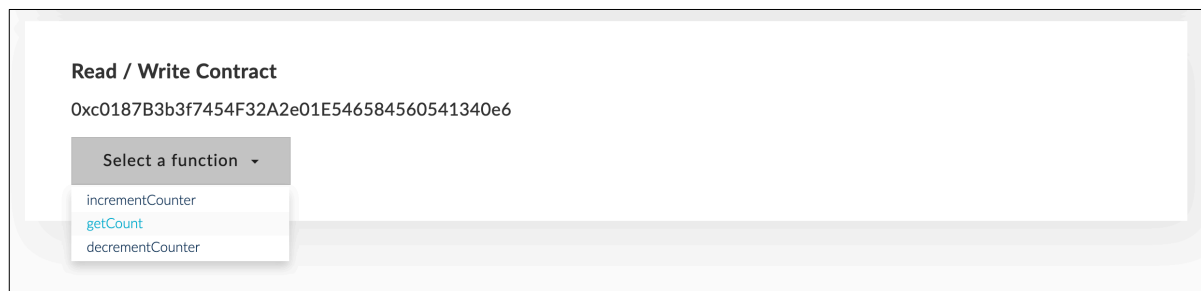


Figura Anexo II-17. MyEthereumWallet. Elección de función de un contrato inteligente. Fuente: Elaboración propia (2019).

18. El resultado será 0 (ver a continuación la *Figura Anexo II-18* a modo de referencia).



Figura Anexo II-18. MyEthereumWallet. Resultado de ejecución de una función sobre un contrato inteligente, valor cero. Fuente: Elaboración propia (2019).

19. Ahora es posible incrementar el valor de contrato, eligiendo la opción “IncrementCounter”. Se pedirá la clave privada y es posible usar la misma que se obtuvo en el paso 9 y luego presionar “Write”. Tras confirmar la operación es posible volver a ejecutar la función “getCount”. El resultado ahora será “1” (ver a continuación la Figura Anexo II-19 a modo de referencia).

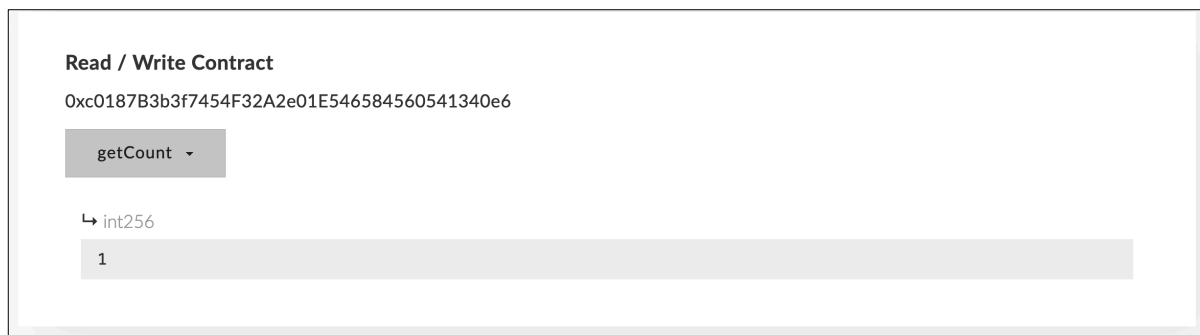


Figura Anexo II-19. MyEthereumWallet. Resultado de ejecución de una función sobre un contrato inteligente, valor uno. Fuente: Elaboración propia (2019).

Con estos pasos fue posible desplegar un contrato inteligente en una *blockchain* privada y ejecutar el mismo, tanto para ver el valor que posee (*getCount*) como para incrementar su valor (*IncrementCounter*).

Anexo III. Desplegar un contrato inteligente doblemente fundado

Requisitos:

- Browser compatible: *Chrome, Firefox* (última versión).
- *MetaMask* configurado en Ropsten Network.
- Dos cuentas en *MetaMask* (Comprador y Vendedor) con 3 ETHs cada una como mínimo (visitar <https://faucet.metamask.io/> para obtenerlos).
- *Remix IDE* (<https://remix.ethereum.org/>) con *plugins "Solidity Compiler" y "Deploy & run transactions"* activados.

1. Verificar usando *MetaMask* que se está utilizando la testnet de pruebas de Ethereum ("Ropsten Test Network") y que ambas cuentas tienen el saldo requerido (ver a continuación la *Figura Anexo III-1* a modo de referencia).

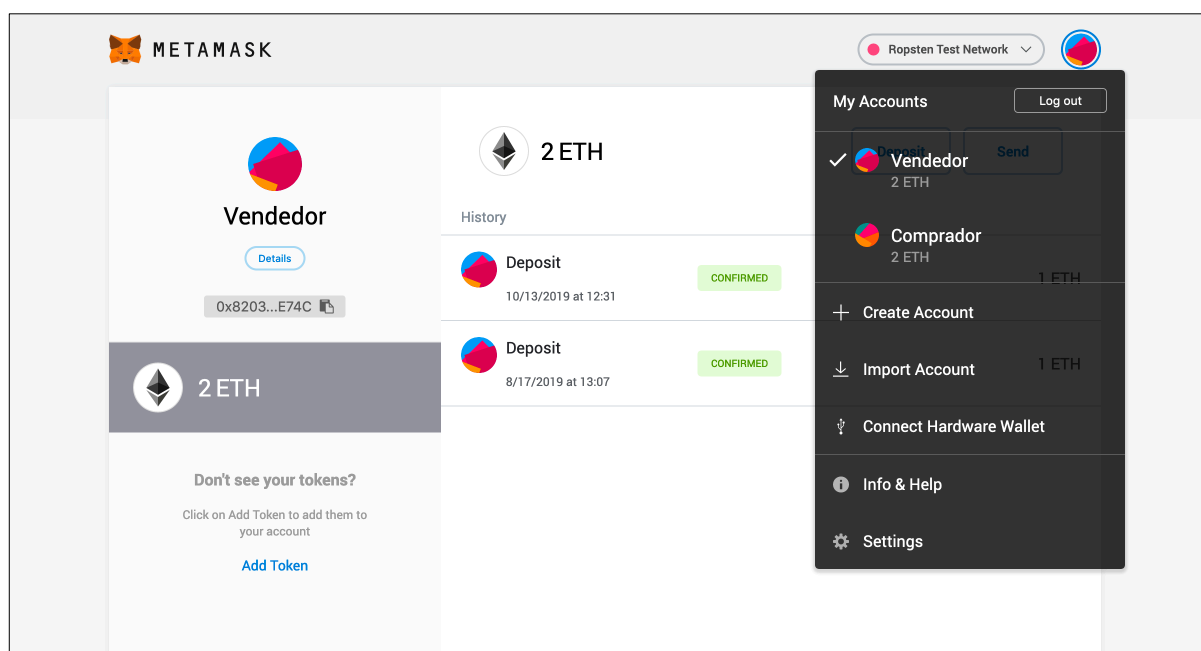


Figura Anexo III-1. MetaMask. Selección de Red y cuenta. Fuente: Elaboración propia (2019).

2. Dirigirse al *Remix IDE*, crear un nuevo archivo (llamado *subcontrataciones.sol*) y utilizar el código del contrato que se muestra a continuación en la *Figura Anexo III-2*.

```

1.  pragma solidity >=0.4.22 <0.7.0;
2.
3.  contract Purchase {
4.      uint public value;
5.      address payable public seller;
6.      address payable public buyer;
7.      enum State { Created, Locked, Inactive }
8.      // The state variable has a default value of the first member,
      `State.created`
9.      State public state;
10.
11.     // Ensure that `msg.value` is an even number.
12.     // Division will truncate if it is an odd number.
13.     // Check via multiplication that it wasn't an odd number.
14.     constructor() public payable {
15.         seller = msg.sender;
16.         value = msg.value / 2;
17.         require((2 * value) == msg.value, "Value has to be even.");
18.     }
19.
20.     modifier condition(bool _condition) {
21.         require(_condition);
22.         _;
23.     }
24.
25.     modifier onlyBuyer() {
26.         require(
27.             msg.sender == buyer,
28.             "Only buyer can call this."
29.         );
30.         _;
31.     }
32.
33.     modifier onlySeller() {
34.         require(
35.             msg.sender == seller,
36.             "Only seller can call this."
37.         );
38.         _;
39.     }
40.
41.     modifier inState(State _state) {
42.         require(
43.             state == _state,
44.             "Invalid state."
45.         );
46.         _;
47.     }
48.
49.     event Aborted();
50.     event PurchaseConfirmed();
51.     event ItemReceived();
52.
53.     /// Abort the purchase and reclaim the ether.
54.     /// Can only be called by the seller before

```

```

55.     /// the contract is locked.
56.     function abort()
57.         public
58.         onlySeller
59.         inState(State.Created)
60.     {
61.         emit Aborted();
62.         state = State.Inactive;
63.         seller.transfer(address(this).balance);
64.     }
65.
66.     /// Confirm the purchase as buyer.
67.     /// Transaction has to include `2 * value` ether.
68.     /// The ether will be locked until confirmReceived
69.     /// is called.
70.     function confirmPurchase()
71.         public
72.         inState(State.Created)
73.         condition(msg.value == (2 * value))
74.         payable
75.     {
76.         emit PurchaseConfirmed();
77.         buyer = msg.sender;
78.         state = State.Locked;
79.     }
80.
81.     /// Confirm that you (the buyer) received the item.
82.     /// This will release the locked ether.
83.     function confirmReceived()
84.         public
85.         onlyBuyer
86.         inState(State.Locked)
87.     {
88.         emit ItemReceived();
89.         // It is important to change the state first because
90.         // otherwise, the contracts called using `send` below
91.         // can call in again here.
92.         state = State.Inactive;
93.
94.         // NOTE: This actually allows both the buyer and the seller to
95.         // block the refund - the withdraw pattern should be used.
96.
97.         buyer.transfer(value);
98.         seller.transfer(address(this).balance);
99.     }
100. }

```

Figura Anexo III-2. Código de Contrato Inteligente. Fuente: Solidity (2019).

3. Compilar el contrato desde la pestaña del compilador, y presionar “Compile subcontrataciones.sol” (ver a continuación la *Figura Anexo III-3* a modo de referencia).

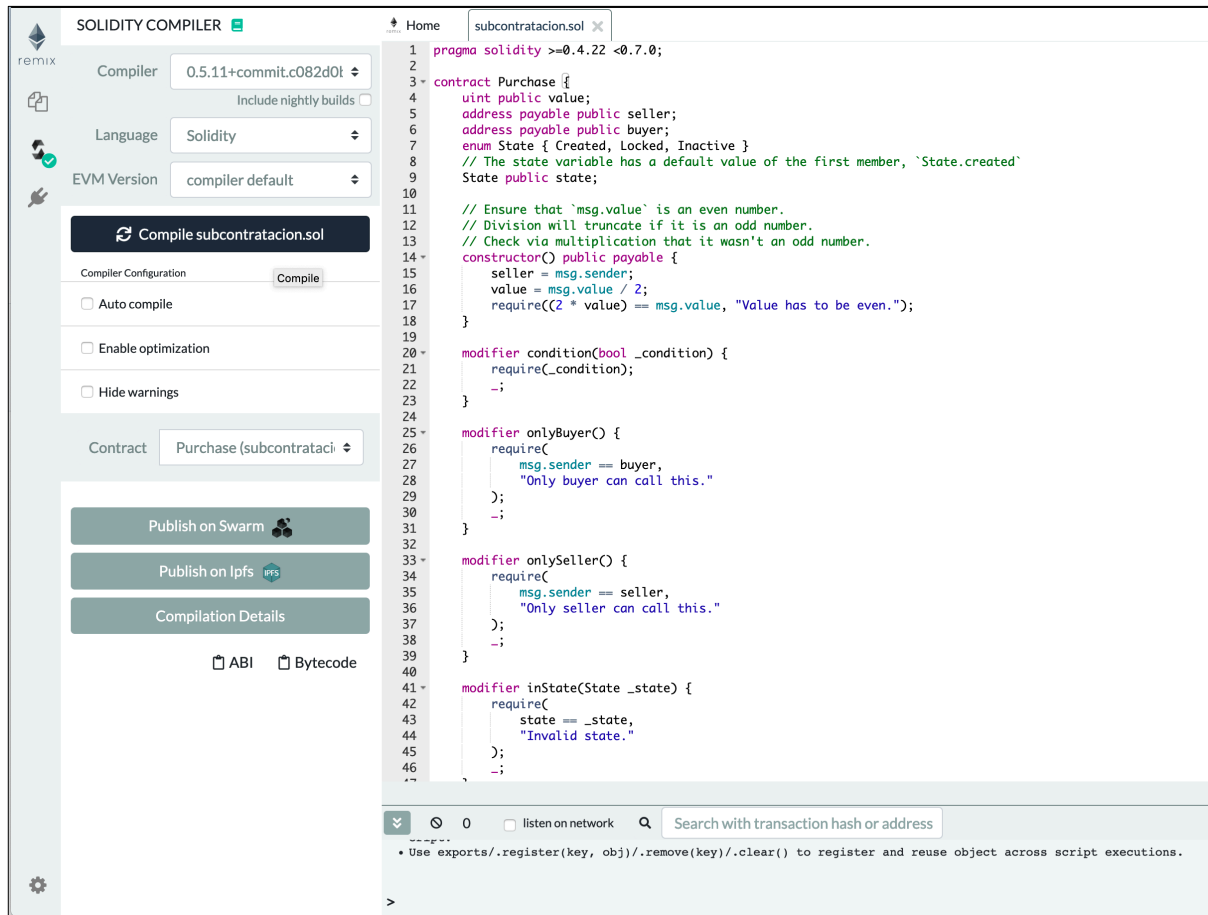


Figura Anexo III-3. Remix IDE. Compilar un contrato. Fuente: Elaboración propia (2019).

4. Ir a la solapa “Deploy & Run Transactions” y elegir el “Environment” llamado “Injected Web3” para poder conectarse Remix con MetaMask. Conceder permiso aceptado el cuadro de dialogo al elegir “Connect” (ver a continuación la *Figura Anexo III-4* a modo de referencia).

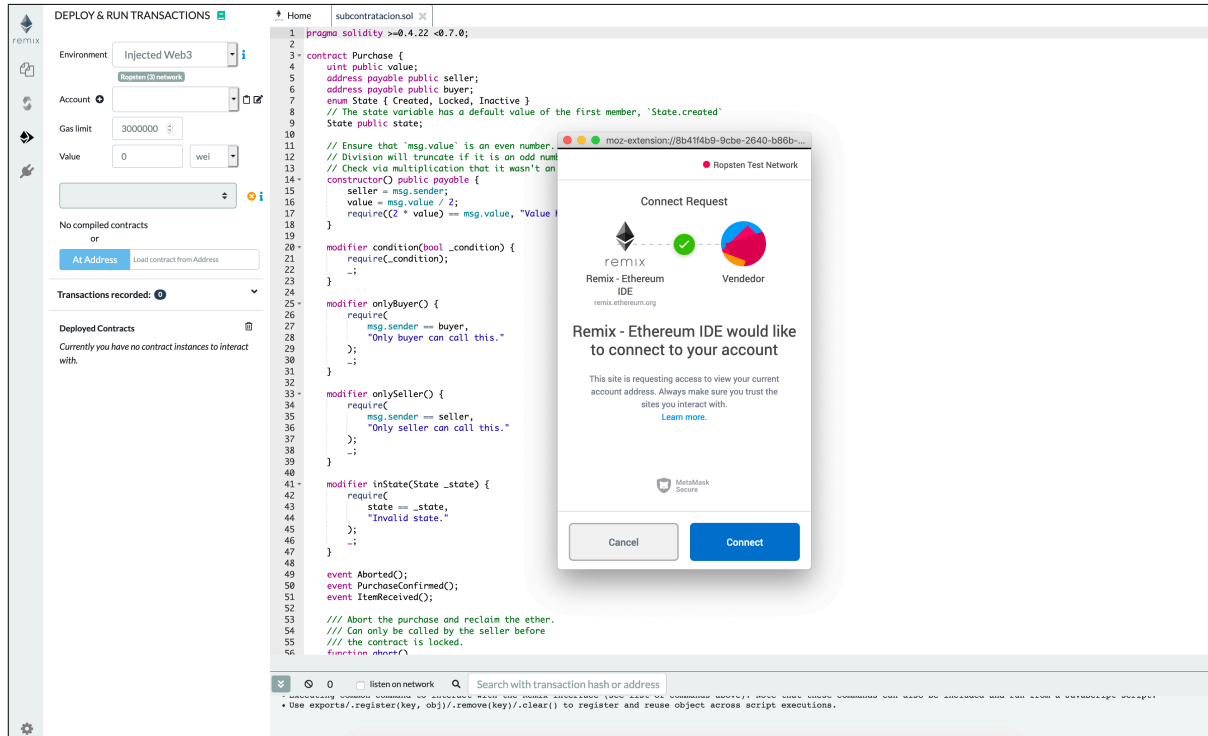


Figura Anexo III-4. Remix IDE y MetaMask. Autorizar conexión. Fuente: Elaboración propia (2019).

5. Desplegar el contrato, enviando 2 ETH y presionando "Deploy" (ver a continuación la Figura Anexo III-5 a modo de referencia).

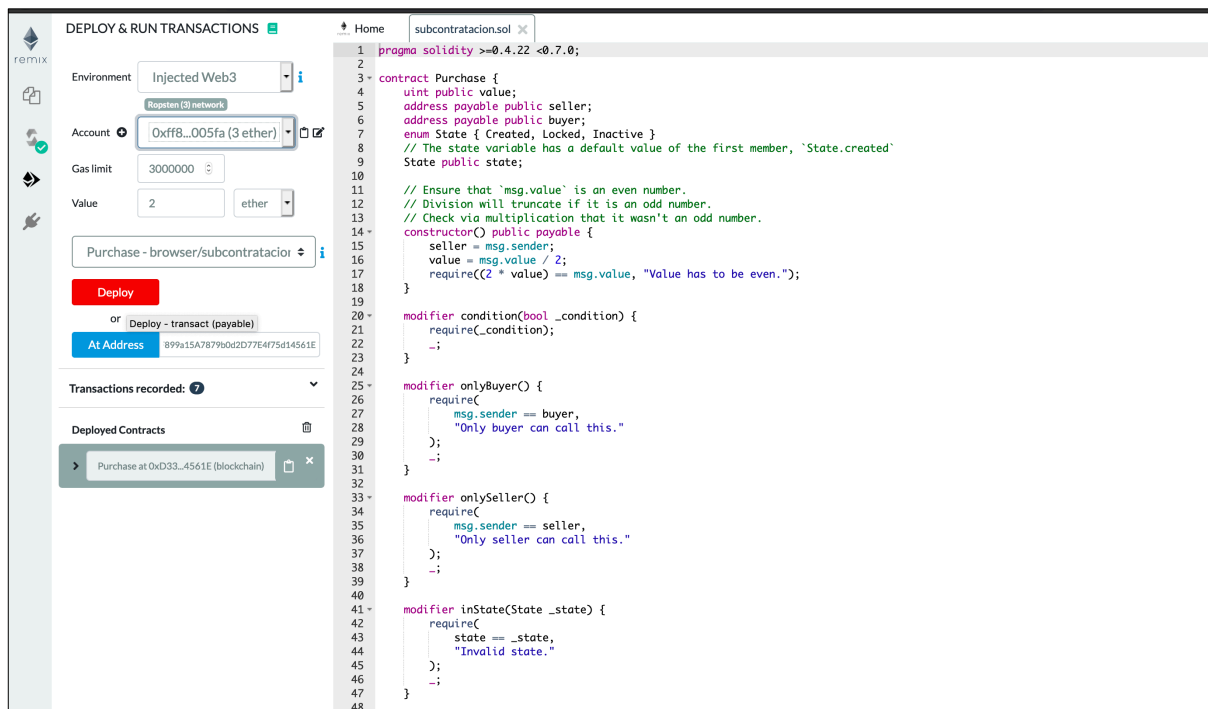


Figura Anexo III-5. Remix IDE. Despliegue de un contrato. Fuente: Elaboración propia (2019).

6. Cambiar a la cuenta del comprador en *MetaMask*, copiar y pegar la dirección del contrato inteligente desde el campo “*Deployed Contract*” al campo “*At Address*”, ingresando “2” en el campo “*Value*” y luego ejecutar la operación de compra seleccionando “*ConfirmPurchase*”. Luego confirmar la operación desde *MetaMask* presionando “*Confirm*” (ver a continuación la *Figura Anexo III-6* a modo de referencia).

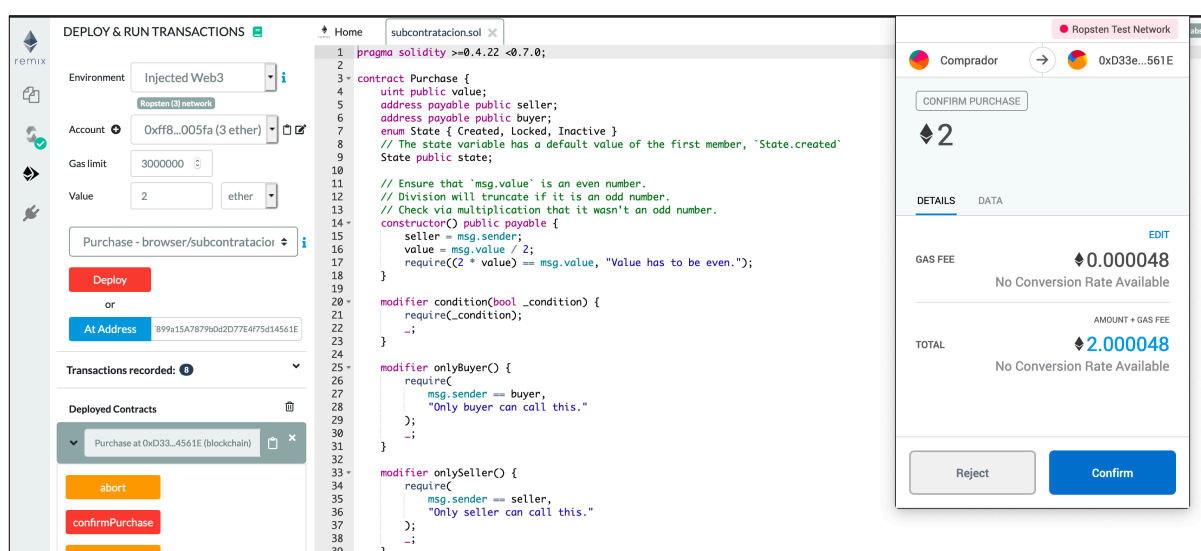


Figura Anexo III-6. Remix IDE y MetaMask. Confirmar despliegue de un contrato. Fuente: Elaboración propia (2019).

7. Es posible verificar ahora que el contrato ya contiene el pago del comprador y el depósito de ambas partes (4 ETHs) con la dirección del contrato copiada en el paso anterior visitando <https://ropsten.etherscan.io/> (ver a continuación la *Figura Anexo III-7* a modo de referencia).

Etherscan
Ropsten Testnet Network

Contract: 0xD33e539EaF899a15A7879b0d2D77E4f75d14561E

Sponsored by MythX: Smart contract security analysis, Pro options for mission-critical dapps. [Start analyzing now](#)

Contract Overview

Balance: 4 Ether

More Info

My Name Tag: Not Available

Contract Creator: 0x82031a9f0c9dc0... at txn 0x660e817a351fa93...

Transactions

Txn Hash	Block	Age	From	To	Value	[Txn Fee]
0x659d7499293246...	6565259	1 min ago	0xff8b526ba0eec8f...	0xd33e539eaf899a1...	2 Ether	0.000046431
0x660e817a351fa93...	6565138	28 mins ago	0x82031a9f0c9dc0...	Contract Creation	2 Ether	0.000559978

[Download CSV Export]

Figura Anexo III-7. Etherscan. Visualización de un contrato inteligente desplegado. Fuente: Elaboración propia (2019).

8. Desde *Remix*, el comprador puede confirmar ahora la compra si está de acuerdo con el bien recibido *off-chain*, presionando “ConfirmReceived” y luego “Confirm” desde *MetaMask* (ver a continuación la *Figura Anexo III-8* a modo de referencia).

DEPLOY & RUN TRANSACTIONS

Environment: Injected Web3

Account: 0xff8...005fa (0.99995)

Gas limit: 3000000

Value: 0 ether

Purchase - browser/subcontratacion

Deploy

At Address: 899a15A7879b0d2D77E4f75d14561E

Transactions recorded: 0

Deployed Contracts: Purchase at 0xD33...4561E (blockchain)

abort

confirmPurchase

confirmReceived

buyer

seller

state

value

```

1 pragma solidity >=0.4.22 <0.7.0;
2
3 contract Purchase {
4     uint public value;
5     address payable public seller;
6     address payable public buyer;
7     enum State { Created, Locked, Inactive }
8     // The state variable has a default value of the first member, 'State.created'
9     State public state;
10
11     // Ensure that 'msg.value' is an even number.
12     // Division will truncate if it is an odd number.
13     // Check via multiplication that it wasn't an odd number.
14     constructor() public payable {
15         seller = msg.sender;
16         value = msg.value / 2;
17         require(2 * value == msg.value, "Value has to be even.");
18     }
19
20     modifier condition(bool _condition) {
21         require(_condition);
22         _;
23     }
24
25     modifier onlyBuyer() {
26         require(
27             msg.sender == buyer,
28             "Only buyer can call this."
29         );
30         _;
31     }
32
33     modifier onlySeller() {
34         require(
35             msg.sender == seller,
36             "Only seller can call this."
37         );
38         _;
39     }
40
41     modifier inState(State _state) {
42         require(
43             state == _state,
44             "Invalid state."
45         );
46         _;
47     }
48
49     event Aborted();
50     event PurchaseConfirmed();
51     event ItemReceived();
52
53     /// Abort the purchase and reclaim the ether.
54     /// Can only be called by the seller before
55     /// the contract is locked.
56     function abort()
57     public

```

Comrador → 0xD33e...561E

CONFIRM RECEIVED

0

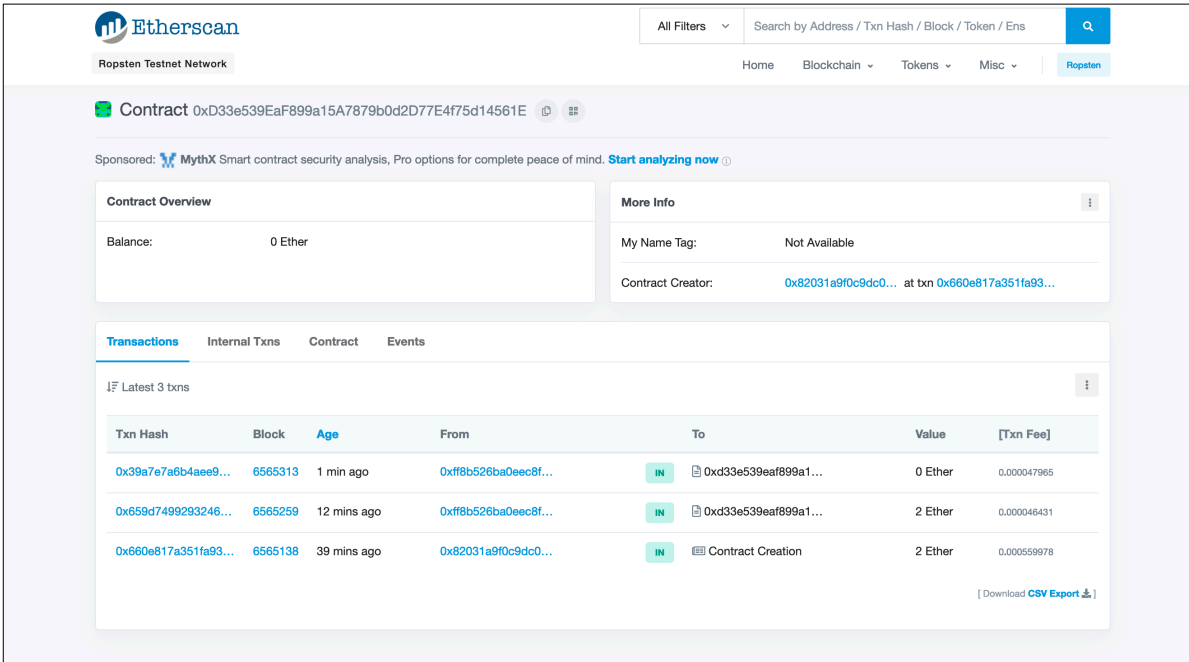
GAS FEE: 0.00005

TOTAL: 0.00005

Reject Confirm

Figura Anexo III-8. Remix IDE y MetaMask. Ejecutar función sobre un contrato. Fuente: Elaboración propia (2019).

9. Todos los pasos han sido completados. El contrato ha quedado con 0 ETH. El vendedor recibió 1 ETH por la venta más el reintegro de su depósito de 2 ETH (Total 3 ETH). El comprador recibió el producto *off-chain* y el reintegro por su depósito (1 ETH) (ver a continuación la Figura Anexo III-9, Figura Anexo III-10 y Figura Anexo III-11 a modo de referencia).



The screenshot displays the Etherscan interface for a smart contract on the Ropsten Testnet. The contract address is 0xD33e539EaF899a15A7879b0d2D77E4f75d14561E. The contract overview shows a balance of 0 Ether. The transactions table lists three recent transactions:

Txn Hash	Block	Age	From	To	Value	[Txn Fee]
0x39a7e7a6b4aee9...	6565313	1 min ago	0xf8b526ba0eec8f...	IN 0xd33e539eaf899a1...	0 Ether	0.000047965
0x659d7499293246...	6565259	12 mins ago	0xf8b526ba0eec8f...	IN 0xd33e539eaf899a1...	2 Ether	0.000046431
0x660e817a351fa93...	6565138	39 mins ago	0x82031a9f0c9dc0...	IN Contract Creation	2 Ether	0.000559978

Figura Anexo III-9. Etherscan. Visualización de un contrato inteligente con operaciones. Fuente: Elaboración propia (2019).

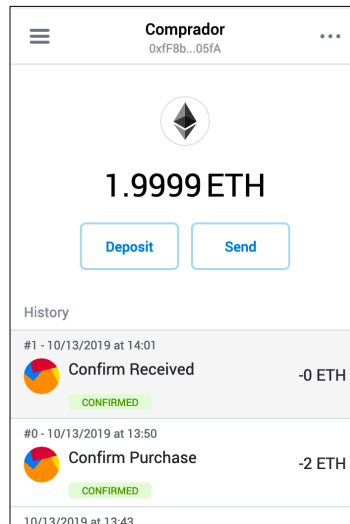


Figura Anexo III-10. MetaMask. Visualización del saldo en cuenta comprador. Fuente: Elaboración propia (2019).

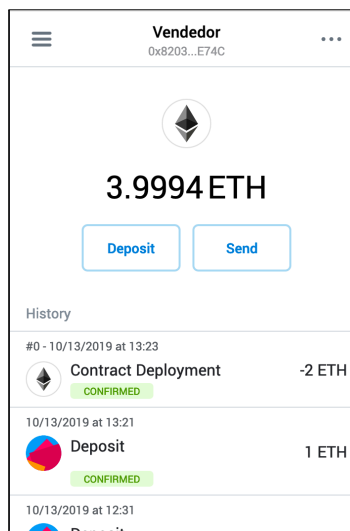


Figura Anexo III-11. MetaMask. Visualización del saldo en cuenta vendedor. Fuente: Elaboración propia (2019).

Anexo IV. Transcripción de Entrevistas

1. Profesional Independiente I

Entrevistado: Mariela Camerano

Entrevistador: Adrián E. Piñeyro

Duración: 30 Minutos.

Fecha: 19/10/2019

La entrevista completa puede ser vista en <https://youtu.be/wZ8s66PSDj4>

- **Entrevistador:** Hola Mariela, ¿A qué te dedicás? ¿y desde hace cuánto?
- **Entrevistado:** Soy diseñadora de imagen y sonido desde hace más de 6 años y desarrolladora web desde hace 10 años.
- **Entrevistador:** ¿Cómo te llegan los trabajos? ¿Fue cambiando?
- **Entrevistado:** Arranqué con una pasantía y quedé en relación de dependencia por cinco años. Luego estuve dos años de *freelancer*, por gente que me recomendaba, boca a boca. Ahora trabajo con tres empresas. Con la primera tengo un set de horas mensuales fijo. Con la segunda le cobro por hora. Una tercera que le cotización antes.
- **Entrevistador:** ¿De qué forma cobrás por los trabajos que realizas? ¿Tenés alguna preferencia?
- **Entrevistado:** Depende con quién trabaje. Cuando trabajo por proyecto, me piden una cotización por pieza. Paso primero un presupuesto. Los primeros que hice cobré la mitad por adelanto, para asegurarme el pago y luego el resto. Ahora me manejo pasándole el total a fin de mes. Cobro por transferencia electrónica siempre.

- **Entrevistador:** ¿En qué porcentaje de los trabajos que realizaste tuviste problemas con el cumplimiento de los pagos y/o sus plazos?
- **Entrevistado:** Siempre hay demoras con los pagos, y tengo que reclamarlo, ahora me puse como condición siempre pedir un adelanto. Sé que es normal pedirlo, pero me cuesta mucho. Solo una vez pasó que no me pagaron y encima tuve que pagar honorarios a un tercero. No cobré nada; asumí el riesgo porque no hice un contrato ni pedí un depósito. Prefiero evitar el trabajo *freelance* por esta experiencia. Muchos me escriben y les digo que no por el tiempo, pero también porque me da seguridad seguir trabajando con esta empresa porque ya sé cómo va hacer el pago y tengo una relación. Sí hubiese una forma de asegurar el pago quizás tomaría más trabajo *freelance* pero ahora no tengo tiempo; con las plataformas online, como UpWork, pude hacer eso. Me daba seguridad que lo iba a cobrar. Así arranqué en realidad, me lo recomendaron mis compañeros de la facultad.
- **Entrevistador:** ¿Y por qué preferís trabajar con estas empresas?
- **Entrevistado:** Para el cobro me quedo con UpWork, es lo mejor, porque tiene plazos/fechas y sabés que te van a pagar. Pero en cuanto al trabajo prefiero trabajar con gente que ya conozco porque mi trabajo es muy subjetivo.
- **Entrevistador:** ¿Cómo aprendés o incorporas una nueva forma de trabajar o cobrar?
- **Entrevistado:** Busco en internet, y soy más auto-didacta, pero si conozco alguien que ya lo usa prefiero preguntarle. Las primeras veces que tenía que cobrar con Payoneer (*una empresa dedicada a cobranzas, estilo PayPal*), consulté a colegas, pero también busqué como era. Pero después en la experiencia me di cuenta de cosas, como las comisiones, y le propuse a mi entonces cliente no usar más UpWork, y usar directamente Payoneer. Es prueba y error a veces.

Luego de haber explicado la solución que se desarrolló en este trabajo, se realizaron las siguientes preguntas.

- **Entrevistador:** ¿Qué ventajas percibís en esta solución? ¿Qué atributos valoras más?
- **Entrevistado:** Está bueno porque hay garantía de que lo voy a cobrar, no está la posibilidad de no cobrar. Yo nunca voy a entregar un trabajo. Puede gustarle o no, estar bien o mal. Pero entiendo que es una garantía para los dos lados, ya que la otra persona también podría decir que siempre me va pagar, así que es una forma de tener confianza de los dos lados. Me sonó raro poner una garantía de mi parte, pero bueno, está bien, nunca lo había pensado así.
- **Entrevistador:** ¿Qué elementos te podrían dificultar la tarea?
- **Entrevistado:** Me parece raro de mi bolsillo, porque siempre lo voy a entregar. Aunque lo entiendo.
- **Entrevistador:** ¿Qué elementos te generan desconfianza o confianza?
- **Entrevistado:** Me pregunto qué pasa si sale mal, no hay una persona que saque una conclusión, después de haber analizado. En este caso hay una computadora, no sé si puede llegar a equivocarse: ¡mirá si pierdo el dinero! Me da tranquilidad que haya una garantía, pero bueno. A no tener nada, prefiero tenerlo.
- Me parece que hay menos posibilidad que se equivoque una máquina, quizás es que no estamos acostumbrados; y cuando tenemos un problema creemos que necesitamos que lo resuelva una persona. Quizás en un futuro puede ser diferente.
- **Entrevistador:** ¿Qué problemas enfrentas o crees que puede haber al usar o querer aprender una tecnología como esta? ¿Cómo se podrían administrar o evitar?

- **Entrevistado:** Me gusta más mirar un video que te lo explique para una noción general. No haría un curso, me aburre. Prefiero experimentarlo de primera mano y probar.
- **Entrevistador:** ¿Cuál crees que sería la mejor forma de enseñar a utilizarlo
- **Entrevistado:** Le contaría mi experiencia, y las cosas positivas de la solución. Le contaría como se usa y de mi experiencia.
- **Entrevistador:** ¿Algo más que quieras contarme de la solución?
- **Entrevistado:** Está buenísimo. Es una herramienta que no existe, si bien ahora está creciendo más, hay pocas cosas desarrolladas.

2. Profesional Independiente II

Entrevistado: Leandro Fournier

Entrevistador: Adrián E. Piñeyro

Duración: 35 Minutos.

Fecha: 21/10/2019

La entrevista completa puede ser vista en <https://youtu.be/vX2ucSKtwck>

- **Entrevistador:** Hola Leandro, ¿Me contás un poco de tu experiencia y como arrancaste?
- **Entrevistado:** Soy autónomo y surgen otras cosas free lance, aunque trabajo más que nada para una empresa más que nada. En el 2015 me cansé de la relación laboral, y quise arrancar solo. Apareció un cliente y arranqué. Fueron surgiendo clientes por LinkedIn y con mi página web. Me mandé bastante solo, me acuerdo que fui una MeetUp de Workana. Ahí me di cuenta de las primeras dos cosas importantes: Tener una tarjeta de

presentación y tener una página web. Así que hice eso, y consigué clientes. Las tarjetas no me sirvieron. Después mucha boca en boca, y a través de amigos y también por plataformas como Workana y Nubelo.

- **Entrevistador:** ¿En qué porcentaje de los trabajos que realizaste tuviste problemas con el cumplimiento de los pagos y/o sus plazos?
- **Entrevistado:** En bastantes, tal vez en un 30% o 40% de los trabajos tuve problemas: incumplimientos de pagos (perdí pagos) y retrasos. Corte de proyecto y no hubo pagos. Te bicicletean mucho, tipo te pago dentro de un mes. También me paso uno que dijo no te pago: Tomé un laburo que estaba mal, me demoré dos semanas. Solo me quedé con el adelanto.
- **Entrevistador:** ¿De qué forma cobrás por los trabajos que realizas? ¿Tenés alguna preferencia?
- **Entrevistado:** Aprendí por las malas que hay que ser desconfiado, era inocente en ese aspecto. Las plataformas tienen algo positivo, es que actúan dado que hay un contrato y la empresa actúa, pero la elección de la forma de pago es limitada y trae problemas. Hay bastantes complicaciones con los bancos, la AFIP y demás
- **Entrevistador:** ¿Qué cambios realizaste en la forma de trabajar para evitar problemas con los pagos?
- **Entrevistado:** Fueron apareciendo clientes mejores y tomé trabajos por fuera de la plataforma. Pero volví a caer en el mismo error; es difícil porque a veces son conocidos/amigos y es una cadena, y después si el cliente no pagó estás en un problema. En algún momento se torna más difícil ya que te asocias con colegas y es aún más complejo. Lo ideal es trabajar con gente que conocés, yo me quedé con esos clientes. Sino tenés que caer en elaborar un contrato, pero igual si no te quieren pagar no te pagas,

la verdad es que la relación laboral es muy compleja. Hay que tener una actitud muy osca.

El cliente quiere que seas copado, que le des flexibilidad, pagarte cuando quiere, que este mejor que lo que él quiere, y que este para ayer.

- **Entrevistador:** ¿Cómo aprendes o incorporas una nueva forma de trabajar o cobrar?
- **Entrevistado:** Fue todo probando, no me fije mucho el tema de comisiones, y tampoco me importaba mucho como cobrar por la situación económica, era muy flexible en ese momento. Encima si en las plataformas optás por las cuentas que son free, cobrás con retraso y todo el proceso lleva demasiado tiempo. Necesitas un colchón importante para poder sostener eso. Son errores que cometí por no investigar o informarme, aunque tampoco creo que hay mucha información; no sé si hay curso de free lance. Lo que hay es para llevarte a usar una determinada plataforma, no es muy objetivo. Toda la parte de cobranzas y demás no se informa bien.

Luego de haber explicado la solución que se desarrolló en este trabajo, se realizaron las siguientes preguntas.

- **Entrevistador:** ¿Qué ventajas percibís en esta solución? ¿Qué atributos valoras más?
- **Entrevistado:** Salteas las altas comisiones. No se usa el sistema bancario que tiene sus comisiones. Por eso me parece que favorece a ambas partes, pero sobre todo al freelancer.
- **Entrevistador:** ¿Qué elementos te podrían dificultar la tarea?
- **Entrevistado:** Hay proyectos que son muy caros, por ejemplo, dos mil, cuatro mil dólares, poner la garantía puede ser un problema, y quizás no pueda tomar el trabajo así.
- **Entrevistador:** ¿Qué elementos te generan desconfianza o confianza?

- Son relaciones laborales/humanas, creo que debería haber un humano en el medio. Es un tema complejo. No estoy seguro de la seguridad del script [*código fuente del contrato inteligente*]. Quizás sería mejor usar micro-pagos: 10% cuando se inició, 20%, 20% y después el resto cuando se entrega. No estoy muy informado de las criptomonedas, pero me genera mucha desconfianza, quizás por ignorancia. No sé cuánto valen, me genera mucha inestabilidad. Para una solución así, entre las Plataformas y una solución *blockchain*, creo que no la usaría o me animaría solo con un proyecto muy chico, sobre todo por el tema de que usa criptomonedas.
- **Entrevistador:** ¿Qué problemas enfrentas o crees que puede haber al usar o querer aprender una tecnología como esta? ¿Cómo se podrían administrar o evitar?
- **Entrevistado:** El conocimiento está disperso sobre criptomonedas. Luego está el tema de usarlo en nuestro país y hacerme del dinero físico, que hace todo más complicado. Estaría bueno que la herramienta misma te de esa respuesta. Creo que preguntaría a un amigo, que me lo explique y luego Investigaría por mi cuenta.
- **Entrevistador:** ¿Cuál crees que sería la mejor forma de enseñar a utilizarlo?
- **Entrevistado:** Es una muy buena pregunta. Por lo general, como free lance sos un “che pibe”, como antes era el “programador de la página web”. Que este te lo proponga, lo veo medio utópico; menos que el cliente acepte usar otra forma, en general ya están muy encasillados con sus formas. La forma o actitud generalmente que tiene es inflexible, y hay que aceptar las condiciones. De todos modos, si yo estuviera convencido, podría mostrarle las ventajas. La documentación ni la leen. Tendría que ser algo visual; tipo un video de YouTube explicativo, con los beneficios de uno y lo de otro; algo entretenido que de confianza. Luego, lo aplicaría con alguna etapa mínima, para ver si tiene beneficios e ir paulatinamente aplicándolo al resto del proyecto. Es una buena idea probar.

3. Experto en *blockchain*

Entrevistado: Juan Cavallaro

Entrevistador: Adrián E. Piñeyro

Duración: 20 Minutos.

Fecha: 21/10/2019

La entrevista completa puede ser vista en <https://youtu.be/sIQID81fn8g>

- **Entrevistador:** Hola Juan, ¿A qué te dedicás? ¿y desde hace cuánto?
- **Entrevistado:** Trabajo hace 5 años en Xappo, fue mi primera experiencia con *blockchain*. Arranqué haciendo módulos que se integraba con *blockchain*. Xappo es una un fintech. Desde hace 4 años estoy en el Departamento de riesgo: Estoy a cargo de la seguridad, encargado de identificar y mitigar fraudes. Utilizamos heurística, Machine learning y analistas (expertos). De un primer análisis automático pasa a un análisis manual.
- **Entrevistador:** ¿A cuánta gente le has explicado a usar alguna tecnología relacionada con *blockchain*?
- **Entrevistado:** No menos de 50 personas.
- **Entrevistador:** ¿Qué creés que es los más difícil de explicar o entender? ¿Qué genera mayor resistencia?
- **Entrevistado:** El primer punto de resistencia es que la gente no entiende la naturaleza del dinero, del mercado y un sistema de dinero. La gente lo entiende de forma intuitiva. Preguntan quién emite el dinero y quién es responsable. Lo mejor es comenzar por los

conceptos básicos de economía. Así que trato de transmitir lo necesario para que lo comprendan.

- **Entrevistador:** ¿Cuál consideras que es la mejor forma de explicar o enseñar a utilizar estas tecnologías?
- **Entrevistado:** En la informalidad, lo mejor que me resultó es usar ejemplos que se asocian a las cuestiones comunes de la vida cotidianas. Como, por ejemplo, la inflación y como se establece el precio de las cosas. Lo más difícil a es transmitir la noción de descentralizado.

Luego de haber explicado la solución que se desarrolló en este trabajo, se realizaron las siguientes preguntas.

- **Entrevistador:** ¿Qué ventajas percibís en esta solución? ¿Qué atributos valoras más?
- **Entrevistado:** La teoría del juego genera incentivos para ambas partes es uno de los puntos más interesantes. Lo mejor es que no involucra una tercera parte, que es una variable más, en donde esta tercera parte pueda tener problemas para mantener la moralidad.
- **Entrevistador:** ¿Qué elementos te generan desconfianza o confianza?
- **Entrevistado:** El nivel de experiencia requerido para escribir un smart contract es alto. Que este sea fiel a la intención original puede ser un problema. Estás confiando en un elemento tecnológico que no sabés como funciona. Una alternativa es hacerlo revisar por un experto, de la misma forma que lo haces con un contrato tradicional al consultar con un abogado. El *blockchain* en sí, que no haya terceros es realidad un tema polémico, ya esta está hecha por personas, y estamos confiando en ellas. Confiamos en la *blockchain*, porque la gente que participa es muy meticulosa y el código es abierto. Existe

la posibilidad de que pasé algo, pero cuantos más ojos hay, la probabilidad se reduce. En 10 años no ha pasado nada, con lo cual eso da cierta tranquilidad. Con los smart contracts quizás podría pasar lo mismo.

- **Entrevistador:** ¿Qué problemas enfrentas o crees que puede haber al usar o querer aprender una tecnología? ¿Cómo se podrían administrar o evitar?
- **Entrevistado:** Mientras se popularice, la gente naturalmente lo va ir incorporando. Va a ver más información disponible y eso va a hacer las cosas más fáciles. Generalmente lo mejor es una conversación haciendo analogías con el mundo conocido.

4. Dueño de PYME

Entrevistador: Adrián E. Piñeyro

Entrevistado: Mariano Valverde

Duración: 35 Minutos.

Fecha: 21/10/2019

La entrevista completa puede ser vista en <https://youtu.be/NWG7KwyjVvU>

Ha continuación se encuentran las anotaciones más relevantes:

- **Entrevistador:** Hola Mariano, ¿A qué se dedica Cristalino?
- **Entrevistado:** Es una startup familiar que brinda solución de marketing medianas y grandes empresas. Hacemos eventos, activaciones y promociones. Tenemos una estructura por proyectos, y subcontratamos, aunque recurrentemente son las mismas personas (Tenemos 2 o 3 personas).

- **Entrevistador:** ¿Cómo buscan nuevos contratistas?
- **Entrevistado:** Boca a boca. Ya tenemos una base de datos propia después de 4 años, y cotizó con ellos (son dos o tres proveedores generalmente).
- **Entrevistador:** Los contratistas, o proveedores como lo llaman ustedes, ¿son empresas o profesionales independientes?
- **Entrevistado:** Tengo un mix, tengo gente con la que trabajo que son independientes, a veces con una empresa.
- **Entrevistador:** ¿Qué pasa cuando hay más trabajo del que pueden manejar con los contratistas actuales?
- **Entrevistado:** Tenemos dos o tres niveles para poder cubrir diferentes niveles de demanda, pero sino salimos a reclutar por LinkedIn. Es una labor activa desarrollar proveedores.
- **Entrevistador:** ¿Cómo realizan los pagos? ¿Tienen alguna preferencia?
- **Entrevistado:** Varía por proyecto, depende de mi cliente. Generalmente a los treinta días de la facturar, aunque podría ser sesenta días. A veces piden anticipación algunos proveedores, generalmente cuando alquilamos alguna locación piden un depósito; ahí vemos si lo podemos adelantar nosotros, si es que el cliente tiene una postura inmóvil. Ante igual calificación del proveedor, el que me evita el costo financiero, está mejor posicionado.
- **Entrevistador:** ¿Qué medio utilizan para efectivamente transferir el dinero? ¿Hay problemas con los tiempos?
- **Entrevistado:** Transferencia y ocasionalmente cheques. Con los profesionales independientes depende de la experiencia. Si tiene buen seniority, generalmente no tiene problema con los pagos. El junior no conoce la dinámica de los pagos/mercado.

- **Entrevistador:** ¿En qué porcentaje de los trabajos que subcontrataron tuvieron problemas con el cumplimiento de los pagos y/o sus plazos?
- **Entrevistado:** En general con el ciclo de pago y cobro no tenemos problemas: estamos bien posicionados. Algunas veces se demoró un pago de un cliente y ahí lo asumimos nosotros y lo cubrimos. Así que diría que bajo, porque contratamos profesionales. Tuvimos errores al principio, por no ser claros, de no prever retrasos del cliente o al definir los requerimientos.
- **Entrevistador:** ¿Pasó alguna vez que el trabajo entregado no cumpla con las expectativas? ¿Cómo lo resolvieron? ¿Cómo hicieron para evitar que vuelva a suceder?
- **Entrevistado:** De cara al cliente, no, no se tiene que escapar al cliente los problemas. Si algo importante nunca contratamos a un junior o alguien no que no hemos probado previamente. Si hay problemas salgo a buscar otro proveedor y no se lo vuelve a contratar. Si es una empresa la que contratamos, hay un espacio de negociación para cambiar la persona con la que trabajamos. Una vez pasó que nos falló un proveedor clave, y nos dañó la relación con el cliente. El proveedor no cobró, pero aun así nos perjudicó.

Luego de haber explicado la solución que se desarrolló en este trabajo, se realizaron las siguientes preguntas.

- **Entrevistador:** ¿Qué ventajas percibís en esta solución? ¿Qué atributos valoras más?
- **Entrevistado:** Percibo valor por el resguardo económico. Aunque el daño del que me cubre es solo económico, no veo un retorno en eso. Lo veo aplicable para un algo de primera instancia, donde no existe confianza. Es decir, cuando la desconfianza puede sumar bastante, o quizás con algún proveedor de otro país, que existe una barrera cultural. Quizás a muy a baja escala funciona: Emprendedor y profesional independiente.

Estaría bueno incorporar desempeños intermedios, quizás debería tener diferentes objetivos y pagos asociados; que podría ser parcial: ¡Qué sea posible modelar el desempeño en un contrato sería genial! Que pague de acuerdo a eso.

- **Entrevistador:** ¿Qué elementos te podrían dificultar la tarea?
- **Entrevistado:** A veces al tecnificar demasiado trae cierta desconfianza. Traer algo nuevo, a veces, podría herir la relación comercial. Debería ser paulatina la implementación. Otro punto es que a veces el proveedor no tiene dinero para poner la garantía. Quizás hacerlo para toda la cadena funcionaría mejor.
- **Entrevistador:** ¿Qué elementos te generan desconfianza o confianza?
- **Entrevistado:** Del mismo modo que confié en un banco, confiaría en esto. Tengo Bitcoins, y no tengo desconfianza. Solo cuando falle, me daría desconfianza.
- **Entrevistador:** ¿Qué problemas enfrentas o crees que puede haber al usar o querer aprender una tecnología como esta? ¿Cómo se podrían administrar o evitar?
- **Entrevistado:** Con Bitcoins fue muy simple, lo hice con una plataforma online, sin problemas. Parece que tiene bastante seguridad la plataforma. Mientras que sea simple no debería haber problemas. A veces una transferencia bancaria puede ser bastante complicado; el foco debería estar en la experiencia, eso daría más confianza. Una barrera podría ser el uso que tiene aceptado. La barrera es el desconocimiento, entonces hay desconfianza.
- **Entrevistador:** ¿Cuál crees que sería la mejor forma de enseñar a utilizarlo a tu personal?
- **Entrevistado:** Cuando es una condición en un contrato, se incorpora rápidamente: se puede imponer. Si es fácil, y es condición, como la persona está interesado en tomar el trabajo no tenés problemas. A mayor complejidad mayor necesidad de explicar más, comunicar más. Si la empresa tiene que asumir el costo de explicar es complicado.

Idealmente la plataforma debería formar a los proveedores. A veces, te tiene que llamar para explicar. Videos explicativos ayudarían. La aceptación cultural es la mayor barrera.

- **Entrevistador:** ¿Te pasó de tener que aprender a operar de una nueva forma? ¿Cómo fue la experiencia?

Entrevistado: Sí, con un cliente. Me mandaron la documentación por mail y tuve que salir a aprender. Tardamos dos meses para incorporarnos en el sistema.

Anexo V. Pruebas de campo

1. Prueba I

Coordinador: Adrián E. Piñeyro

Participante: Martín Sani

Duración: 18 minutos

Fecha: 21/10/2019

La prueba completa puede ser vista en <https://youtu.be/emFObRlzwWA>

Martín Sani es uno de los dueños de una PYME ubicada en la zona sur de la provincia de Buenos Aires. La empresa, DIXITPC, se dedica a la venta de productos informáticos y ofrece servicios de mantenimiento y desarrollo de sitios web. Realizan subcontrataciones de manera tradicional para estos servicios. Se pactó un encuentro virtual para explicar la tecnología y luego realizar una prueba.

Se configuró remotamente el IDE *Remix* y la billetera *MetaMask* en el ordenador de Sani antes de comenzar con la prueba. El primer paso fue explicar verbalmente la tecnología *blockchain* y de los contratos inteligentes sin ningún soporte. Luego se procedió a explicar el protocolo de depósito doble, para finalmente desplegar el contrato inteligente actuando como vendedor (Proveedor/Contratista), y se le envió a Sani un link en donde pudiera depositar dinero en el contrato.

La prueba fue exitosa y aportó nuevas ideas sobre cómo mejorar el prototipo:

- Es necesario explicar la tecnología de contratos inteligentes con un soporte distinto que centre la atención. Por ejemplo, se puede utilizar un video.
- Es mejor mostrar primero el funcionamiento completo del contrato antes de permitir que el participante realice la prueba.

2. Prueba II

Coordinador: Adrián E. Piñeyro

Participante: Mariela Camerano

Duración: 41 minutos

Fecha: 31/10/2019

La prueba completa puede ser vista en <https://youtu.be/UKWKOIfDSY>

Se configuró remotamente el IDE *Remix* y la billetera *MetaMask* en el ordenador de Camerano antes de comenzar con la prueba. El primer paso fue mostrar un video que explique los contratos inteligentes. Para esto se seleccionó un video de un curso online de la plataforma Coursera (Ast, 2019). Luego de un espacio para preguntas, se procedió a explicar el protocolo de depósito doble, y se mostró cómo desplegar el contrato inteligente, pagarlo y confirma la compra. A continuación, el coordinador asumió el rol de comprador, y Camerano el rol de vendedor y se le solicitó al participante fundar el contrato desde su ordenador y compartirlo con el coordinador para que este pueda pagarlo y luego confirmar la compra.

La prueba resultó exitosa y arrojó las siguientes conclusiones sobre el prototipo:

- El video aporta claridad sobre el concepto de confianza, e incluso ayuda a dar otro punto de vista respecto de la parcialidad de un intermediario.
- Mostrar primero el funcionamiento completo del contrato ayuda a reducir el nivel de incertidumbre al que se expone el participante.
- Surge la idea de incluir a toda la cadena de pago en el contrato: cliente final, el intermediario, y el contratista/proveedor.
- Surge la idea de poner una fecha límite para confirmar la compra.
- El participante considera que si todos aceptarían esta solución, sería ideal.
- Hay preocupación con respecto al valor de la criptomoneda y respecto de cómo presupuestar los trabajos.

3. Prueba III

Coordinador: Adrián E. Piñeyro

Participante: Leandro Fournier

Duración: 44 minutos

Fecha: 05/11/2019

La prueba completa puede ser vista en <https://youtu.be/94v88jHPJFY>

Se configuró remotamente el IDE *Remix* y la billetera *MetaMask* en el ordenador de Fournier antes de comenzar con la prueba. Se realizaron los mismos pasos que en la prueba anterior. A continuación, el coordinador asumió el rol de comprador, y Fournier el rol de

vendedor y se le solicitó al participante fundar el contrato desde su ordenador y compartirlo con el coordinador para que este pueda pagarlo y luego confirmar la compra.

La prueba resultó exitosa y arrojó las siguientes conclusiones sobre el prototipo:

- Según el participante son demasiados pasos los que debe realizar el vendedor.
- El participante considera que, aunque los pasos son claros y sencillos y la mecánica se entiende, las herramientas utilizadas tienen demasiados distractores que dificultan el aprendizaje y la menoscaban la experiencia.
- Surge la idea de que se pueda modelar en el mismo contrato diferentes etapas y liberar pagos parciales de cumplirse determinados hitos.
- Para comprender mejor el contrato el participante sugirió utilizar un abordaje similar al de la herramienta *Scratch*.
- Existe gran resistencia por parte del participante a realizar un pago previo en calidad de garantía.
- Se discutieron otras alternativas a la de realizar un depósito en garantía, como la de establecer penalidades que no permitan el uso de la solución a quienes no cumplen con él por un determinado tiempo, pero no se pudo llegar a una solución superadora.
- El participante expresa que de existir una plataforma que integre esta tecnología bajo el concepto de gamificación, calificando los usuarios según su reputación, se podría lograr participación sin necesidad de utilizar un incentivo económico.

4. Prueba IV

Coordinador: Adrián E. Piñeyro

Participante: Mariano Valverde

Duración: 38 minutos.

Fecha: 08/11/2019

La prueba completa puede ser vista en <https://youtu.be/OSobRTHbRTE>

Se configuró remotamente la billetera *MetaMask* en el ordenador de Valverde antes de comenzar con la prueba. Al comenzar la prueba se mostró un video que explica que son los contratos inteligentes y luego se dio un espacio para preguntas. Luego de las preguntas se mostró como interactuar con un contrato inteligente que modela el protocolo de depósito doble utilizando un sitio generado con *One Click DApp*. A continuación, el coordinador asumió el rol de vendedor, y Valverde el rol de comprador y se le solicitó al participante pagar el contrato y luego confirmar la compra utilizando la *DApp*.

La prueba resultó exitosa y arrojó las siguientes conclusiones sobre el prototipo:

- Es mucho más sencillo para el comprador utilizar un contrato inteligente que para el vendedor.
- Los pasos se pueden realizar en cuestión de minutos y son simples y claros.
- En la medida que el contrato tenga algún tipo de aval demostrable, pareciera no haber necesidad de compartir el código del contrato inteligente con el comprador.
- El participante sostiene que luego de usar un contrato inteligente considera que es una mejor solución para resolver la problemática de las contrataciones y no es tan compleja utilizarla.

- Sin embargo, considera que la complejidad está en la adopción, dado que hay una resistencia a aquello que es nuevo o diferente, sobre todo cuando hay dinero real involucrado.
- El participante considera que dispositivos o formas de pago que hoy están totalmente incorporadas en nuestra sociedad (como los teléfonos inteligentes y el pago con tarjeta de crédito a través de internet o por medio de un código QR), sufrieron el mismo rechazo inicial, por lo que la tecnología de contratos inteligentes podría tener el mismo destino en un futuro.