Universidad del Aconcagua

Facultad de Ciencias Económicas y Jurídicas

Carrera de Administración

Blockchain, el internet del valor:

Beneficios y desafíos de su adopción.

Concurso Incentivo a la Investigación

Tutor: Marroquín, Eduardo

Alumno: Sánchez, Darío

2° año de Licenciatura en Administración

Septiembre de 2018

Índice:

Capítulo I: Introducción

"*Las especies que sobreviven no son las más fuertes, ni las más rápidas, sino aquellas que se adaptan mejor al cambio*". Charles Darwin.

Hace poco menos de 10 años, en enero de 2009, surgió una tecnología que muchos expertos llaman "la segunda generación de internet", la consideran la tecnología más relevante de "la cuarta revolución industrial" y creen que tendrá un impacto social tan grande como lo tuvo el internet, esta tecnología se llama blockchain, o cadena de bloques. Básicamente consiste en un software de código abierto[1] distribuido entre una red de ordenadores que permite compartir, de forma confiable e inmutable, información y valor, sin requerir ninguna autoridad central ni terceras partes que actúen como intermediarios.

Funcionando como un libro de contabilidad distribuido e inmutable, una red blockchain bien diseñada elimina la necesidad de intermediarios, reduciendo los costos y aumentando la velocidad y el alcance, al mismo tiempo que ofrece una mayor transparencia y rastreabilidad para muchos procesos comerciales. Esto hace de blockchain una tecnología disruptiva[2] con el potencial para cambiar radicalmente diversas industrias y paradigmas, además de que constantemente se descubren nuevas aplicaciones.

En la presente investigación se intentará explicar en qué consiste, cómo funciona y qué beneficios promete ésta tecnología, explicar algunas de sus aplicaciones más relevantes, esbozar su situación a nivel global y nacional, y plantear los desafíos que atraviesa para alcanzar una adopción masiva, exponiendo además qué se está haciendo para superaros.

[1] El software libre o de código abierto es el software que está licenciado de tal manera que los usuarios pueden estudiar, modificar y mejorar su diseño mediante la disponibilidad de su código fuente.
[2] Disruptiva: Que produce una interrupción súbita de algo.

Capítulo II: Marco teórico

"*La primera generación de la revolución digital nos ofreció el internet de la información. La segunda generación, impulsada por la tecnología blockchain, nos trae ahora el internet del valor: una nueva plataforma destinada a reconfigurar el mundo empresarial y a transformar, para mejor, el viejo orden de los negocios*". Don Tapscott, director ejecutivo del Tapscott Group.

1. Blockchain

Blockchain (cadena de bloques) es una tecnología informática que al estar distribuida entre múltiples nodos (computadoras) y utilizar algoritmos criptográficos[3], permite generar y conservar un registro certero y verificable de acontecimientos digitales en el que se incluyen todas las transacciones que se han realizado históricamente en la red sobre la que funciona. Siendo los nodos de la red quienes verifican y certifican la veracidad de los datos, por lo que esta tecnología no requiere de un ente central ni de terceras partes que brinden confianza a la red.

Primeramente fue planteado como una alternativa o solución a la dependencia de terceros que brinden confianza para poder intercambiar valor. Funciona como el libro de registros de contabilidad de una empresa en donde se registran todas las entradas y salidas de dinero, pero a diferencia de éste, detallando y registrando acontecimientos digitales, cuyas modificaciones no requieren de un intermediario centralizado que identifique y certifique la información, sino que está distribuida en los múltiples nodos, independientes entre sí que la registran y la validan sin necesidad de que se conozcan entre ellos. Cada uno de estos nodos tiene una copia completa de la información de la cadena de bloques y participa en la validación o rechazo de las transacciones realizadas, siendo necesaria la aprobación de más del 50% del total de nodos para que la transacción sea efectivamente validada.

Este beneficio, la eliminación de la figura del intermediario para validar las transacciones, va ligado a un cambio de paradigma con importantes consecuencias económicas. El hecho de hacer innecesario al tercero en un intercambio de valor supone un enorme ahorro de costes, de tiempo y da más seguridad, lo que ha hecho a esta tecnología muy atractiva para las empresas.

[3] Algoritmo criptográfico es un algoritmo que modifica los datos de un documento con el objetivo de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad.

Nadie es dueño de la propiedad intelectual, su creador, conocido solo por su seudónimo, Sathoshi Nakamoto, publicó un artículo sobre su invención (Anexo 1), codificó la primera implementación y luego desapareció, lo que significa que el núcleo de la tecnología es ahora de dominio público y solo variaciones y adiciones importantes podrían ser patentadas.

a. Características de blockchain

- **Distribuido**: La información es compartida, actualizada con cada transacción, y selectivamente replicada entre participantes casi en tiempo real. Como no es propiedad y no es controlado por ninguna organización individual, el sostenimiento de la plataforma no depende de ninguna entidad individual.
- **Seguro y privado**: Los permisos y la criptografía previenen el acceso no autorizado a la red y garantizan que los participantes son realmente quienes dicen ser. La privacidad se mantiene a través de técnicas criptográficas y técnicas de partición de datos para darles a los participantes una visibilidad selectiva en el "libro mayor". En todas las transacciones, la identidad de las partes puede ser protegida.
- **Inmutable**: Una vez que se acuerdan las condiciones, los participantes, ni nadie pueden manipular el registro de las transacciones. Los errores solo pueden revertirse con nuevas transacciones.
- **Transparente y auditable**: Porque todos los participantes en una transacción tienen acceso a los mismos registros, pueden validar transacciones y verificar las identidades o la propiedad sin la necesidad de intermediarios terceros. Las actas tienen un sello de tiempo[4] y se pueden verificar casi en tiempo real.
- **Transaccional y basado en el consenso**: Para que una transacción se apruebe más de la mitad de los participantes de la red deben aceptar que dicha transacción es válida. Lo cual se logra a través del uso de algoritmos de consenso. Pudiendo la red Blockchain establecer las condiciones bajo las cuales una transacción o intercambio de activos debe realizarse.
- **Instrumentado y flexible:** Porque se pueden establecer diferentes condiciones sobre la misma plataforma blockchain, mediante los "contratos inteligentes" (contratos que se auto ejecutan en base a una o más condiciones), brindando una enorme cantidad de posibilidades en cuanto a lo que puede ser establecido.

[4] Sellado de tiempo (timestamping) es un mecanismo en línea que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

b. Beneficios de blockchain

A continuación se detallarán los principales beneficios de blockchain frente a los sistemas tradicionales de transacciones:

- **Ahorro de tiempo**: Las transacciones son más rápidas ya que no requieren verificación de una autoridad central. En el caso de las remesas por ejemplo, el tiempo puede reducirse de días a minutos.
- **Ahorro de costes**: Debido a que no se necesita supervisión externa, ya que la red es auto controlada por los mismos participantes de la red; se eliminan los intermediarios, ya que los participantes pueden intercambiar objetos de valor directamente; y se disminuye la duplicación de esfuerzo porque todos los participantes tienen acceso a la información pública.
- **Seguridad más estricta**: Las características de seguridad de blockchain protegen contra la manipulación, el fraude y el cibercrimen. Para que una transacción sea aprobada debe ser previamente verificada por los demás miembros de la red, quienes controlarán que las partes que participan en la transacción sean realmente quienes dicen ser y que los bienes o activos negociados sean exactamente como los representados.
- **Privacidad mejorada**: A través del uso de identificaciones y permisos, los usuarios pueden especificar qué detalles de cada transacción puedan ver los demás participantes. Los permisos pueden ser ampliados para usuarios especiales, como auditores, que pueden necesitar acceso a más detalles de la transacción.
- **Auditabilidad mejorada**: Al tener todos los usuarios un mismo registro se mejora la capacidad de controlar y auditar las transacciones.
- **Mayor eficiencia operativa**: La digitalización de los activos agiliza la transferencia de propiedad, por lo que las transacciones puede llevarse a cabo en menor tiempo y con menor esfuerzo.

c. Tipos de blockchain

Existen 3 tipos de blockchain según su modalidad y son los siguientes:

• **Blockchain pública:** Esta fue la primera en surgir y consiste en una red distribuida con una gran cantidad de validadores en cualquier lugar del mundo, todos ellos anónimos, lo cual hace a esta red resistente a la censura y la manipulación. En los modelos públicos, el consenso está distribuido por defecto y no existe un único punto de fallo, ya que todo el proceso está distribuido en todos los niveles de la cadena.

La capacidad de almacenamiento que se requiere, por cada equipo, también es mínima al contar con muchos agentes que comparten la información. Por poner una analogía sencilla de comprender, sería un modelo parecido al de Internet, en el que un solo agente no tiene control sobre todo lo que se produce ya que cada una de las personas y empresas que participan de la red tienen poder sobre sí mismos y sus propias páginas web.

El único ejemplo de blockchain pública es la creada por Sathoshi Nakamoto, sobre la cual funciona Bitcoin, siendo a la vez la única completamente descentralizada al no tener supuestamente nadie que pueda influir directamente sobre ella, siendo mantenida exclusivamente por cada uno de los nodos o usuarios que conforman la red.

• **Blockchain privada o "de permiso":** Al ser el protocolo original de blockchain, libre y de código abierto, puede ser libremente descargado y modificado, por lo que muchas personas o empresas han hecho a partir del original, nuevos protocolos con características diferenciadoras que representen ventajas tales como mejorar la velocidad o la privacidad de las transacciones o añadir más opciones, como en el caso de los contratos inteligentes que se explicarán más adelante.

En este caso la cadena de bloques exige que los usuarios tengan ciertas credenciales y una licencia para operar en ellas; y tiene en principio un único validador, por lo que está sometida a la censura y la manipulación que éste quisiera ejercer. No existiendo, por lo tanto, consenso distribuido y sí la posibilidad de que un único punto de la cadena pudiera comprometer todo el sistema y la información que contiene, representando esto una clara desventaja para los usuarios.

Este modelo lo utilizan muchas organizaciones, desde empresas e instituciones, hasta gobiernos; quienes aprovechan las ventajas de la tecnología blockchain en sus procesos administrativos. Ejemplos prácticos pueden ser una universidad que quiere mejorar la seguridad de la información que maneja, una empresa productora que quiera tener un registro transparente de la procedencia de sus insumos para brindar seguridad a sus clientes o un

municipio que quiera llevar un registro inmutable de los ciudadanos, para posteriormente dar incentivos o castigos dependiendo del cumplimiento de las normas.

- **Blockchain híbrida o semiprivada:** Además de los dos modelos anteriores existe una propuesta híbrida, que busca combinar las ventajas del blockchain privado y del público. En este modelo sí hay varios validadores de la información, aunque, al menos hasta el momento, sin llegar a los números del modelo público y con la posibilidad de ser elegidos o restringidos por una única persona o grupo de personas. Por lo tanto, el consenso distribuido y la resistencia a la censura son relativos, dependiendo del grado de parecido que guarde el protocolo con el modelo privado o público.

La mayor parte de los proyectos actuales son híbridos, ya que evitan el riesgo de tener un único punto de error y se benefician de la participación de cada usuario, quienes contribuyen a la red en los procesos de validación de transacciones y a la seguridad de la misma.

2. Historia de blockchain

Las bases teóricas sobre las que se sustenta blockchain fueron publicadas en el documento "Bitcoin: A Peer-to-Peer Electronic Cash System", en octubre de 2008, por "Sathoshi Nakamoto", de quien actualmente se desconoce su verdadera identidad, incluso se piensa que podría tratarse de un grupo de personas o de alguna institución. Por esto se dice que blockchain y la criptomoneda bitcoin nacen al mismo tiempo, siendo blockchain la tecnología en que bitcoin funciona.

Nakamoto publicó un mensaje en la lista de criptografía general de metzdowd.com en el que anunciaba que ha estado trabajando en un sistema de dinero electrónico completamente "P2P"[5]. En el mismo mensaje publica el whitepaper[6] en el que define el funcionamiento y las características de la nueva tecnología blockchain. Esta idea fue materializada el 3 de enero de 2009 cuando entra en funcionamiento la red con el primer programa cliente[7] y la generación de

[5] Peer to peer: De par a par, es decir, de una persona a otra

[6] Whitepaper es un documento en forma de guía cuya función es tratar de explicar a los usuarios cómo resolver un problema o ayudarlos a entender un tema determinado.

[7] Programa cliente es un programa que requiere específicamente una conexión a otro programa, al que se denomina servidor y que suele estar en otra máquina

los primeros bitcoins. Al ser un software de código abierto, cualquiera puede contribuir y formar parte del sistema.

La primera innovación destacada de blockchain fue bitcoin, la primer criptomoneda. La capitalización de mercado de bitcoin, a fines de Junio de 2018, oscila los 116.500 millones de dólares y es utilizada por millones de personas para realizar pagos, incluido un gran y creciente mercado de remesas, sobre el cual se hará mención más adelante.

La segunda innovación se llamó "contrato inteligente", y se manifestó en un sistema de cadena de bloques llamado “Ethereum”, que incorpora pequeños programas informáticos sobre la cadena de bloques para representar instrumentos financieros, como préstamos o bonos, en lugar de sólo las fichas del estilo del efectivo de bitcoins. Ethereum tiene una capitalización de mercado, a fines de Junio de 2018, que oscila los 49.620 millones de dólares.

La tercera innovación importante, que actualmente es la última moda de la tecnología de la cadena de bloques, es la "prueba de participación". Las cadenas de bloque de la generación actual están aseguradas por "pruebas de trabajo" en las que el grupo con la mayor potencia computacional toma las decisiones. Estos grupos se llaman "mineros" y operan vastos centros de datos para proporcionar esta seguridad a cambio de pagos con criptomoneda. Los nuevos sistemas prescinden de estos centros de datos y los sustituyen con complejos instrumentos que ofrecen un grado similar de seguridad a un menor costo. Los sistemas de prueba de participación entraron en operación en 2017.

La cuarta innovación importante es la cadena de bloques escalada. Ahora mismo, en el mundo de las cadenas de bloques, cada ordenador de la red procesa cada transacción. Lo cual lo hace relativamente lento. Una cadena de bloques escalada acelera el proceso, sin sacrificar la seguridad, al averiguar cuántos ordenadores se requieren para validar cada transacción y dividir el trabajo de manera eficiente. Gestionar esto sin comprometer la gran seguridad y solidez de las cadenas de bloques es un problema difícil, pero no imposible. Se espera que una cadena de bloques escalada sea lo suficientemente rápida para alimentar al “internet de las cosas”[8] y enfrentarse a los importantes intermediarios de pagos (como VISA y SWIFT) del mundo de los bancos.

[8] Internet de las cosas es un concepto que se refiere a la interconexión digital de objetos cotidianos como por ejemplo una heladera, con Internet.

3. Cómo funciona blockchain

Funciona como un libro contable, común y público, que es distribuido en su totalidad a través de una red de nodos (usuarios), cada uno de los cuales tiene una copia completa de la información de la cadena de bloques. Todos los detalles de cada nueva transacción son registrados, marcados con la hora y verificados por agentes denominados mineros (entidades que ponen sus computadores al servicio de la red a cambio de criptomonedas), quienes compiten por ser los primeros en resolver problemas matemáticos complejos y poder publicar el siguiente bloque de transacciones en el libro contable (o la cadena del historial de transacciones). Cuando el bloque de transacciones es subido por el minero que fue el primero en resolver el cálculo, todos los nodos de la red validan automáticamente el libro contable y todas las transacciones que se encuentren en él. Siendo necesario que la mayoría de los nodos (50% más 1) acepten que el bloque es válido para que éste pase a formar parte de la cadena de bloques de transacciones. Estos bloques de transacciones son publicados en el libro contable compartido a intervalos de diez minutos.

Para facilitar la comprensión de dará un ejemplo de un caso de uso de la tecnología blockchain para transferir valor, supongamos que A quiere transferir a B una determinada cantidad de unidades de valor (bitcoins, pesos, dólares, etc.) y que ambos tienen acceso a una billetera o monedero digital en el celular, un computador o una web que les permite enviar y recibir la moneda. Cuando A decide gastar sus unidades de valor, lo que realmente está haciendo es enviar una instrucción de cambio a la base de datos informando que parte de sus unidades de valor ahora pertenecen a B. Esta instrucción es difundida en la red verificando que A tiene recursos para pagar y, si todo se encuentra correcto, se compila con otras transacciones en un bloque con información relativa a los últimos diez minutos.

Este bloque mezcla la información de las direcciones de las partes involucradas en cada transacción, la cantidad de unidades de valor en movimiento y una marca de tiempo, y luego las procesa a través de una función llamada “hash”[9]. Esta función es un algoritmo criptográfico, que se encarga de condensar, en un único código de 64 dígitos entre letras y números, información de cualquier extensión. Este hash se combina con la “solución-hash” del bloque anterior, y se convierte en el encabezado del bloque nuevo que se encuentra en validación. A su vez este es la base de un problema matemático que se resuelve usando de nuevo la función hash.

[9] Función hash: Sistema que mediante criptografía comprime determinada información generando un código de determinada longitud, en el caso del blockchain de bitcoin es de 30 dígitos.

Cuando finalmente algún nodo de la red encuentra la solución, ésta es compartida con el resto para su validación, en un proceso llamado “proof-of-work” (prueba de trabajo). Después que ha sido aprobada por la mayoría de nodos de la red, el bloque es añadido a la cadena y con ello todas las transacciones contenidas en él.

Ésta es el protocolo de funcionamiento de la primera red blockchain, la de bitcoin. En el caso de otras redes, al desarrollarse se pueden realizar modificaciones como por ejemplo disminuir la cantidad de nodos que deben validar las transacciones o disminuir el tiempo que tarda en comenzar a formarse un nuevo bloque para hacer más rápido el proceso.

A continuación se detallan a modo de resumen los principales pasos del funcionamiento:

1º Transacción: Dos partes, A y B, deciden intercambiar una unidad de valor (moneda digital o representación digital de cualquier elemento susceptible de registración) e inician la transacción.

2º Bloque: Las transacción es empaquetada con otras transacciones, creando así un “bloque de transacciones”. El bloque se envía a la red de nodos participantes del sistema.

3º Verificación: Los nodos evalúan las transacciones y, a través de cálculos matemáticos, determinan si son válidos, con base en reglas acordadas. Una vez que una cierta cantidad de nodos confirman la validez de la transacción, ésta se considera válida

4º Registro: Cada bloque verificado se estampa temporalmente con su código criptográfico (hash). Los mismos también contienen referencia a los códigos de bloques previos, creando así una “cadena” de registros inalterables.

5º Ejecución: La unidad de valor se mueve de la cuenta de la parte A a la de la parte B

a. ¿Es seguro blockchain?

Considerando el carácter público y compartido de blockchain, es natural que surjan preguntas respecto a la seguridad de las transacciones. Pero la realidad es que esta tecnología es más segura que cualquier otra red transaccional existente.

Uno de los motivos es que aunque la información registrada y todas las transacciones son públicas, las personas que participan en la cadena de bloques mantienen el anonimato, por

intermedio de claves cifradas públicas y privadas. Esto significa que incluso si todos conocen todas las transacciones y el saldo de todos los participantes en la cadena de bloques, no existe ninguna manera de relacionar las transacciones con las personas específicas.

En segundo lugar, debido a que cada nodo individual de la red posee un registro actualizado del libro contable, para modificar las transacciones en la cadena de bloques un hacker o pirata informático tendría que hackear[10] más del 50 por ciento de los nodos a nivel mundial, ya que sino no hay consenso y el bloque de transacciones no puede ser incluido en la cadena; y en un tiempo de diez minutos (que es la frecuencia con que un nuevo bloque de transacciones es validado y agregado a la cadena). Por ello, se estima el coste económico de hackear el sistema sería muchas veces superior al beneficio que se podría obtener, lo cual desincentiva cualquier intento.

En las noticias pueden verse varios artículos sobre criptomonedas o incluso redes blockchain que fueron hackeadas, pero hasta el momento los motivos siempre son los mismos 3. El más común es que hayan hackeado una exchange[11], robando criptomonedas de sus usuarios, lo cual no significa que la red sobre la que esas criptomonedas operan sean hackeadas. Otro caso es que haya un error en el desarrollo de la red, como el caso de la red de Ripple, donde alguien descubrió un error que le permitió desviar dinero a una cuenta propia, aunque fue descubierto y el problema solucionado; y el último caso es de veces en las que se logró manipular más de 50% de los nodos y con ello, manipular la red; pero solo ha sido posible hasta el momento en redes nuevas y por lo tanto muy pequeñas, el ejemplo más significativo es el de la red de Bitcoin Gold, de la cual robaron 18 millones de dólares y jamás se supo quienes lo hicieron, actualmente la red a seguido creciendo y con las cantidad de nodos que posee actualmente sus desarrolladores aseguran que es prácticamente imposible que esto vuelva a suceder.

[10] Hackear define la acción entrar y manipular de forma abrupta y sin permiso un sistema de cómputo o una red.
[11] Una cryptocurrency exchange o plataforma de intercambio de criptomonedas es un sitio web en el que se puede comprar, vender o cambiar criptomonedas por otra moneda digital o dinero fiduciario.

Capítulo III: Marco metodológico

1. Definición del problema

Blockchain fue materializado hace casi 10 años y a pesar que desde entonces ha demostrado cumplir con todo lo que promete, mayor seguridad, registros inmutables, reducción de costos y tiempo en transacciones, entre otros beneficios y que en el ámbito tecnológico es considerada una de las tecnologías más disruptivas de la actualidad y no hay discusión acerca de que su adopción está y seguirá estando en constante crecimiento; esta tecnología sigue distante de alcanzar un uso masivo o generalizado y su adopción tiene varios obstáculos que superar antes de esto, además más allá de estar teniendo un auge en 2018, poder verse como lenta y es muy variable entre países.

2. Hipótesis

Los potenciales beneficios de blockchain son suficientes para alcanzar una adopción generalizada en los próximos 5 a 10 años.

3. Objetivos de la investigación

a. Objetivo general

- Dar una perspectiva global de blockchain, sus aplicaciones en diferentes industrias y los retos para su adopción y escalabilidad, justificando los motivos o beneficios por los que entre acciones del sector gobierno, empresarial y emprendedor se podría alcanzar en los próximos años un uso masificado donde blockchain tenga una influencia directa o indirecta en la vida de casi todo ser humano.

b. Objetivos específicos

- Introducir al lector en la comprensión de la historia, el funcionamiento, casos de uso más relevantes y la filosofía que conlleva blockchain.
- Exponer el constante y prometedor crecimiento de la adopción de dicha tecnología.
- Justificar el potencial disruptivo de blockchain en los diversos sectores donde está siendo usado

4. Metodología

El diseño de la presente investigación es de tipo mixto, entre cualitativo y cuantitativo y es exploratorio.

5. Alcances y limitaciones

La mayor parte de la información contenida en el este documento deriva de fuentes públicas y privadas diversas, que además contienen diversas estimaciones, por lo que deben ser consideradas en todo momento como proyecciones.

Al ser blockchain una tecnología relativamente reciente es poco el material bibliográfico disponible, ya sea libros, investigaciones, informes o tesis, aunque si se cuenta con una gran cantidad de artículos en internet. Para la realización de la presente investigación se ha recurrido a cuatro libros, publicados entre 2016 y 2017, y se ha consultado a diversas personas con conocimiento del tema, en su mayoría gente con emprendimientos o proyectos sustentados en la tecnología, los cuales se incluyen más adelante.

Capítulo IV: Aplicaciones de blockchain

1. Criptomonedas

La primera innovación que permitió blockchain fue la de las criptomonedas o criptodivisas, las cuales son monedas virtuales que pueden ser intercambiadas y operadas como cualquier otra divisa tradicional, pero están fuera del control de los gobiernos e instituciones financieras. Existe un gran número de criptodivisas disponibles, todas con sus propias características y aplicaciones.

Pueden ser consideradas como una alternativa a las divisas tradicionales, pero en realidad fueron concebidas como una solución de pago completamente convencional. En estos momentos, bastantes tiendas aceptan criptomoneda como forma de pago, pero dependiendo del país en que se opere ya que en algunos, como por ejemplo China han sido prohibidas.

Aunque funcionan como método de pago habitualmente se parecen más a materias primas como el oro que al dinero fiduciario. Debido a que al igual que las materias primas el valor de una criptomoneda no está vinculado exclusivamente al comportamiento de una economía concreta, los cambios en los tipos de interés y el aumento en las reservas monetarias solo tienen un efecto indirecto en su valor y el valor de las criptomonedas depende del compromiso de los usuarios por mantener su precio al convertirlas a divisas tradicionales. Este valor es muy volátil, por ejemplo, cuando las prohibieron en China tuvieron una gran caída en su valor, pero en general ha ido en crecimiento y en algunos momentos de forma muy acelerada, la máxima capitalización de mercado, es decir, el máximo valor en el mercado que entre todas las criptomonedas han alcanzado, fue de U$D 572.968.153.356, en diciembre de 2017.

A continuación se detallan los principales beneficios y riesgos de las criptomonedas:

Beneficios:

• Visión global: Al ser divisas globales son mucho menos susceptibles a la economía o políticas de un país concreto. Todo el mundo puede acceder a ellas y pueden transferirse instantáneamente a cualquier persona en cualquier lugar del mundo.

• Descentralización: Están descentralizadas, por lo que no existe un mercado oficial y pueden ser operadas 24 horas al día durante los siete días de la semana.

• Volatilidad: Las criptomonedas suelen experimentar significativos movimientos de precio de manera repentina. Esto las hace problemáticas como divisa pero muy interesantes por las oportunidades de trading o inversión que ofrecen.

• Transparencia: Todas las transacciones se registran en un libro compartido y se operan sobre un mecanismo que asegura que al receptor solo le llegue la información que necesita del emisor (no todos sus datos).

Riesgos:

• Volatilidad: La volatilidad puede conllevar tanto riesgos como oportunidades, las grandes fluctuaciones de los precios pueden traer pérdidas enormes de un día al otro.

• Pérdidas: No hay una manera perfecta de protegerse frente al error humano, el fallo técnico o el fraude y no hay ningún sistema implantado para compensar las pérdidas.

• Amplia aceptación: Las criptomonedas tienen el valor que se les quiera dar, a pesar de su creciente popularidad, aún hay dudas sobre su futuro a largo plazo.

• Cambios regulatorios: Las criptomonedas están exentas de regulación por ahora, pero si se introducen nuevos mecanismos, muchas de sus ventajas sobre las divisas tradicionales pueden verse revertidas.

Existe duda y diferentes opiniones respecto a si las criptomonedas algún día sustituirán al dinero tradicional, esto es posible, pero no en el corto plazo. Hay varias razones por las que se necesita tiempo, entre ellas que aún no son aceptadas en todo el mundo, afectando tanto a individuos como a empresas; son demasiado volátiles, supondrían una completa revisión de la actual infraestructura económica y se tendría que planear una transición, para prevenir la redundancia de las divisas tradicionales y la pérdida de activos. No obstante si esto ocurriera tendría importantes beneficios, por ejemplo que no pueden ser manipuladas como las divisas tradicionales debido al registro de acceso público, al no requerir intermediarios los costes son menores y se reducen los obstáculos en transacciones internacionales y posibilitarían una renta básica universal.

Las criptodivisas pueden ser compradas o intercambiadas, pero tienen también una forma muy innovadora e interesante de conseguirlas y es el minado, lo cual consiste en formar parte del proceso a través del cual las transacciones de criptomoneda se verifican y registran. El objetivo de los mineros es recopilar las últimas transacciones del bloque actual y encontrar una solución a un complejo algoritmo. Haciendo esto se obtiene una recompensa: una cantidad fija de criptomoneda. Cantidad que varía según la criptomoneda en la que se trabaje.

La solución a este algoritmo supone un proceso continuo y depende de los resultados de algoritmos anteriores para poder realizar el siguiente cálculo. Del mismo modo, la dificultad del algoritmo puede ser ajustada frecuentemente, con el fin de hacer que el trabajo de los mineros sea constante aunque la capacidad de procesamiento vaya mejorando. Esto se asemeja al ritmo al que materias primas como el oro entran en el mercado (de ahí el término “minar”).

2. Smart contracts

Los “smart contracts” también conocidos como contratos digitales o contratos inteligentes, son programas informáticos, basados en criptografía, que facilitan, verifican y hacen cumplir de forma automática la negociación de un contrato sin necesidad de tener un documento contractual. Estos contratos inteligentes ejecutan automáticamente las cláusulas contractuales cuando se cumplen, o incumplen, las correspondientes condiciones pre-programadas, asociadas a activos reales. El programa puede definir reglas estrictas y sus consecuencias, de la misma manera que un documento legal tradicional. Pero a diferencia de este, puede hacer uso de la información del sistema y tomar las acciones necesarias en base a lo descrito en el contrato.

El término "smart contracts" fue acuñado por el informático Nick Szabo, en 1993, pero muchos defienden que no se puede atribuir a él la invención debido a que son el resultado de muchos esfuerzos independientes. A pesar de estar definido conceptualmente lo que es un contrato inteligente, no existía ninguna plataforma sobre la que pudieran implementarse, hasta el surgimiento de blockchain. Fue Vitalik Buterin, a sus 19 años de edad, quien en 2013, juntó ambas tecnologías y comenzó a desarrollar la Ethereum Virtual Machine (EVM), la primera plataforma en permitir ejecutar contratos inteligentes.

“Una vez publicados en el blockchain, los smart contracts no pueden ser modificados y su ejecución es autónoma. Por lo tanto, y a diferencia de los contratos tradicionales, con los smart contracts no hay posibilidad de incumplimiento, censura, fraude, o interferencia de terceras partes y al ser una aplicación de software, tampoco presentan ambigüedades o áreas grises sujetas a interpretación, y su estado de cumplimiento en cada momento puede ser fácilmente verificado. Todo ello agrega una capa de confianza adicional a las transacciones en un

blockchain". Detalla Juan Diego Bonelli, Responsable del laboratorio de innovación de Blockchain de Belatrix.

Esta innovación se puede extrapolar a cualquier transacción que requiera un acuerdo registrado entre partes, como, por ejemplo, la contratación de productos financieros o de seguros, los depósitos en garantía, las operaciones de trading, etc. Por lo que brindan grandes beneficios y sus aplicaciones son incalculables. Entre individuos permite realizar negociaciones sin riesgo de fraude y de forma muy sencilla, y a nivel empresarial brinda posibilidades como evitar el fraude fiscal o blanqueo de dinero y optimizar los flujos de cobros y pagos con el fin de maximizar los fondos líquidos de la empresa, entre muchas otras. (En el anexo 2 se ampliará acerca del funcionamiento).

3. Derechos de autor

Normalmente cuando el creador de una obra, como temas musicales, fotografías, artículos periodísticos, videos, entre muchas otras, quiere comerciarla, la registra o patenta y la deja en mano de intermediarios que la distribuyen, perdiendo control sobre ésta. Blockchain parece ser la respuesta a la gestión de los derechos de autor en internet ya que permite otorgar licencias de forma automática, garantizando el pago de los royalties[12] a las partes sin necesidad de intermediarios y hacer un seguimiento del uso que se le está dando a la obra. Este sistema puede además acabar con la piratería, que actualmente produce pérdidas multimillonarias, y con el proceso, muchas veces difícil, lento y costoso, de tener que localizar al autor y pedirle permiso para usar su imagen.

Actualmente existen muchos servicios que permiten registrar la autoría de creaciones propias en plataformas blockchain, como por ejemplo Mediachain, que permite registrar la propiedad intelectual sobre las creaciones y hacer un seguimiento de los contenidos a través de Internet para controlar los posibles casos de utilización de éstos sin previa autorización. Por ejemplo, un músico que quiera subir sus temas, deberá registrarlos, posteriormente se le otorgará un número registro y una identificación que establecen es el autor y, si es el caso, el titular de todos los derechos de explotación. Las personas que quieran hacer uso de él tendrán que

[12] Un royalty o regalía es el pago que se efectúa al titular de derechos de autor, patentes, marcas o know-how a cambio del derecho a usarlos o explotarlos.

aceptar los términos de un contrato inteligente y Mediachain pagará al autor cada vez que esto suceda. Además están trabajando en un sistema de micropagos para que sea el mismo usuario quien pague la cantidad correspondiente. Recientemente Mediachain fue comprada por Spotify lo que significa un enorme avance para este método de proteger los derechos de autor.

Otro ejemplo de empresas que están usando el sistema es Kodak, quien se asoció con Wenn Digital, para crear un libro de contabilidad digital codificado, utilizando la tecnología blockchain, con los derechos de autor de los fotógrafos, creando vínculos más sólidos entre las imágenes y sus creadores. También creó una criptomoneda, llamada KodakCoin, para pagar a los fotógrafos cuando se utilice una imagen tomada por ellos. Esta apuesta de Kodak por la tecnología fue con la principal intención de animar a los inversores y fue realmente un éxito, sus acciones subieron un 289% en pocos días. "Para muchos en la industria tecnológica, blockchain y criptomonedas son palabras de moda, pero para los fotógrafos que llevan tiempo luchando para ejercer el control sobre su trabajo y sobre el uso que se le da, estas palabras de moda tienen la llave para solucionar lo que parecía un problema irresoluble", declaró Jeff Clarke, consejero delegado de Kodak.

4. Remesas

El mayor flujo de dinero que llega a los países en vías de desarrollo no es de ayuda extranjera ni de inversiones directas de otros países, sino de dinero girado a los países en desarrollo por sus emigrantes. El proceso de poner un giro y el de posteriormente cobrarlo, puede considerarse dificultoso y hasta sacrificado, por el tiempo que demora y las altas comisiones que se cobran.

Pero actualmente hay compañías, como por ejemplo Abra, que están construyendo redes de pago con el sistema blockchain, el cual quita la necesidad de cajeros automáticos al permitir que el dinero sea transferido directamente de usuario a usuario. De esta forma el proceso, desde que sale el dinero de un país y llega a otro, tarda una hora, en lugar de aproximadamente una semana y la comisión es del 2% en lugar del 7% o más que cobran empresas que no han adoptado la tecnología como Western Union.

Abra permite operar con 50 diferentes monedas fiduciarias y más de 24 criptomonedas, y espera que en su primer año de funcionar a nivel global, los usuarios de su red superen en

número a todos los cajeros automáticos del mundo y superen a los aproximadamente 500.000 usuarios que Western Union tiene después de 150 años funcionando.

5. Initial coin offerings (ICO)

Una ICO es una nueva forma de financiamiento, posible gracias a blockchain, en la cual se emite un token, que es una unidad de valor emitida por una entidad privada, pudiendo representar partes del derecho de propiedad de la empresa (Security token), o “cupones digitales” para el servicio o producto que se está desarrollando (Utility token), o una criptomoneda (Cripto token). Dicho token es vendido, a cambio de dinero fiduciario o criptomonedas que posteriormente la empresa debería utilizar para su financiamiento.

El caso más relevante en una ICO en cuanto a la cantidad recaudada es el de EOS, un proyecto que permite a desarrolladores crear aplicaciones descentralizadas. La ICO fue lanzada en junio de 2017 y exactamente un año después ya había recaudado 4,234 millones de dólares. El segundo caso de éxito es Telegram, quien creó una plataforma basada en blockchain para ampliar sus servicios y recaudó a través de su ICO 1,700 millones de dólares.

Un informe de CB Insights muestra la creciente popularidad de esta forma de financiamiento: en 2017 se recaudaron entre todas las ICOs más de 5.000 millones de dólares provenientes de casi 800 startups, mientras que los fondos de venture capital invirtieron 1.000 millones en 215 negocios en el sector. Es decir que hubo cinco veces más capital moviéndose a través de las ICO que mediante el modelo de rondas de inversión más tradicional. También se muestra un incremento en la recaudación de las empresas que entre 2017 y 2018 ha incrementado en un 182%. Es importante aclarar que en el segundo semestre de 2017 el mercado de las criptomonedas tuvo un crecimiento muy acelerado pero en los últimos meses el mercado ha mantenido tendencias bajistas y esto sumado a la escasa regulación de las ICO (muy pocos países las están regulando), y la gran cantidad de ICOs que han resultado en estafas, han hecho que en los últimos meses esta forma de financiamiento esté sufriendo una caída enorme y su futuro sea incierto, al menos hasta que se logre una regulación efectiva a nivel global.

A continuación se hará mención de las ventajas y desventajas:

Ventajas:

- Rapidez y facilidad: Cualquier compañía puede iniciar una ICO a través de varias plataformas como Ethereum o NEM.
- Acceso online a un mercado internacional: El mercado potencial lo forman todos aquellos que tengan acceso a internet. La campaña se puede promocionar a través de redes sociales, webs especializadas y foros.
- Beneficios propios de blockchain: Se eliminan los intermediarios y los recursos necesarios para completar cada transacción son mucho menores a otras formas de financiamiento.
- Liquidez: Habitualmente, se pueden adquirir grandes sumas de capital en poco tiempo.
- Democratización de la inversión: El acceso a los tokens es público y se puede lograr desde cualquier punto del mundo.

Desventajas:

- Escasa seguridad para el inversor: Rara vez existen pruebas reales de la tecnología o el negocio que desarrolla la empresa. En muchos casos no es más que un proyecto que puede funcionar o no.
- Incertidumbre del valor de los tokens: Existe tanta expectación ante los posibles beneficios de una ICO que, en ocasiones, el valor de los tokens reside más en la demanda potencial que en el producto real. Si dicha demanda no se produce, el valor del token no crece.
- Volatilidad del mercado: Las inversiones en tokens y criptomonedas tienen una volatilidad superior a la de cualquier otro mercado.
- Desconocimiento de los inversores: Si no lo solicita expresamente, la empresa que lleva a cabo las ICOs nunca conoce la identidad real del inversor. Permitiendo que organizaciones ilegales lo usen para el lavado de dinero.
- Cambios inminentes en la regulación: Apenas existen precedentes regulatorios y se espera que en los próximos años la mayoría de países apueste por una legislación específica.

6. Logística

Muchas cadenas de suministro dependen de varias empresas diferentes, a veces incluso distribuidas en diferentes países y no hay una plena confianza entre ellas, por lo cual suele ser un verdadero desafío el supervisar cada empresa y el adquirir, rastrear, implementar y administrar bienes. Blockchain puede proporcionar a cada participante plena visibilidad en función de su nivel de permiso, permitiendo ver el estado de los documentos de aduana, los conocimientos de embarque, entre muchos otros datos y ver el progreso de los bienes a través de la cadena de suministro, incluyendo el origen, el tránsito y el destino, mostrando en tiempo real cada evento. Además ninguna de las partes puede modificar, eliminar ni anexar ningún registro sin el consenso de los demás.

Este nivel de transparencia ayuda a reducir los errores, imposibilitar el fraude, reducir el tiempo en que los productos pasan por el proceso de tránsito y mejorar la administración del inventario, lo cual reduce muchos costos y desperdicios. Por otro lado, en diversas industrias, permite brindar mayor confianza a los usuarios o consumidores al permitirles verificar el origen y tránsito, y por ende la originalidad de prácticamente cualquier producto, como pueden ser: diamantes, obras de arte, alimentos orgánicos, medicamentos, etc.

No obstante se debe ser precavido en cuanto a los obstáculos de usar blockchain en las cadenas de suministros ya que los datos, los cuales serán inmutables salvo consenso de los participantes para ser revocados, deben ingresarse de forma segura y precisa. Además de que es indispensable el uso de sensores inteligentes, etiquetas de identificación y otros elementos dependiendo que se transporte, los cuales se vuelven fundamentales para construir una cadena de suministro respaldada por blockchain.

7. Micropagos

Las infraestructuras de los sistemas bancarios actuales pierden mucha capacidad de interoperabilidad para poder garantizar adecuados niveles de seguridad, lo cual genera costos de transacciones que hacen inviables los pagos de sumas muy pequeñas. Pero esto es diferente si se realizan las transacciones a través de una red blockchain, los costos de

transacción pueden llegar a ser ínfimos, sin sacrificar la seguridad, y estos permite monetizar los contenidos digitales.

Por ejemplo un músico que toque sus temas en la calle y suba sus grabaciones a sitios web como YouTube, o un periodista que escriba artículos en un sitio web, podrían, en lugar de recibir “likes”, los cuales no tienen ningún valor económico, recibir el equivalente a centavos de dólar en una determinada criptomoneda, generándose a través de esto la posibilidad de que mucha gente consiga una forma de sustento económico que antes de blockchain no era factible, o al menos no en la misma medida ya que es muy difícil alcanzar ingresos significativos a través de generar contenido web.

Actualmente grandes compañías, como Telefónica, Caixabank, Santander, HSBC, entre otras, están invirtiendo para brindar esta posibilidad de permitir micropagos con ínfimos costes a sus usuarios. En el caso de banco Santander por ejemplo, tienen una aplicación para pagos internacionales construida sobre la red blockchain de Ripple y están experimentando para incluir micropagos para contenidos digitales. “Al hacer pagos se pueden crear pequeñas fracciones de dinero en blockchain y la transacción es tan barata que se puede conseguir que sea económica y eficiente”, explicó Julio Faura, responsable de investigación y desarrollo de blockchain en Santander.

Además se han desarrollado sitios web que usando éste sistema ofrecen a sus usuarios la posibilidad de recibir micropagos por sus contenidos, generando una clara ventaja competitiva y medida que esto crezca, es decir, más gente participe en estos sitios, los sitios web más relevantes de la actualidad, como Facebook o YouTube se podrían ver obligados a imitar esto para mantener su primacía.

Capítulo V: Blockchain en el mundo

1. Blockchain en Europa

“En el futuro, todos los servicios públicos utilizarán la tecnología blockchain. Blockchain es una gran oportunidad para Europa y los Estados miembros para repensar sus sistemas de información, promover la confianza del usuario y la protección de datos personales, ayudar a

crear nuevas oportunidades de negocio y establecer nuevas áreas de liderazgo, beneficiando a los ciudadanos, servicios públicos y empresas.” Mariya Gabriela, comisionada de economía y sociedad digital de la Comisión Europea

El 10 de abril de 2018 se publicó un comunicado oficial de la Comisión Europea, asegurando que un total de 22 países miembros firmaron la declaración de establecimiento de la Asociación Europea de Blockchain. Según este comunicado, la Asociación Europea de Blockchain servirá para impulsar la cooperación entre los países miembros, intercambiando conocimiento y experticia técnica sobre la tecnología blockchain y en materia regulatoria, así como para el desarrollo de aplicaciones digitales basadas en blockchain para el mercado europeo.

De esta forma Europa espera mantenerse a la vanguardia del desarrollo de la tecnología blockchain, de la cual creen que tiene el potencial de traer muchos beneficios tanto al sector público como al privado y posee un enorme potencial en una gran variedad de servicios.

Los países que han firmado esta declaración son Austria, Bélgica, Bulgaria, República Checa, Estonia, Finlandia, Francia, Alemania, Irlanda, Latvia, Lituania, Luxemburgo, Malta, Holanda, Noruega, Polonia, Portugal, Eslovaquia, Eslovenia, España, Suecia, Reino Unido y recientemente Italia. Siendo todos los demás países de la Unión Europea y del Espacio Económico Europeo, bienvenidos a unirse a esta asociación.

La Comisión Europea ya ha estado anteriormente involucrada en la creación de organizaciones encargadas de promover la tecnología blockchain en esta región. Por ejemplo el Observatorio y Foro Blockchain de la Unión Europea, cuya creación fue anunciada en febrero de 2018. Además, la Comisión Europea viene financiando proyectos relacionados con la cadena de bloques a través de los programas de investigación FP7 y Horizon2020. Comisión de la cual se calcula que para el año 2020 habrá realizado un financiamiento total en proyectos relacionados con la blockchain por más 340 millones de euros.

2. Blockchain en Estados Unidos

En los Estados Unidos además del uso para operar criptomonedas y administrar bases de datos, las autoridades locales reconocen el gran potencial de la blockchain en la prestación de servicios públicos y han puesto en marcha diversas series de proyectos, que actualmente se

encuentran en diferentes etapas de implementación además de uno de los pioneros en la regulación de esta tecnología.

El estado de Delaware fue el primero en anunciar la “Iniciativa Blockchain” en 2016. Este amplio programa lanzado por el entonces gobernador, Jack Markell, está diseñado para estimular el desarrollo y uso de tecnologías blockchain y contratos inteligentes tanto es los sectores públicos como privado. Las autoridades reconocieron oficialmente las transacciones electrónicas registradas en blockchain como datos verificables y el proyecto de ley fue firmado con el fin de legalizar transacciones blockchain para la contabilidad y registros de negocios para empresas locales. Se supone que la iniciativa debía llegar a ser un paso adelante en la prevención de futuros problemas relacionados con la tributación y manipulación de registros.

En 2017, el Estado de Illinois anunció otra iniciativa, en la que se pide al consorcio de organismos del Estado que coopere en la búsqueda de innovaciones presentadas en la tecnología de contabilidad distribuida. Las autoridades del Estado también tienen la intención de promover el uso de blockchain "para transformar la prestación de servicios públicos y privados, redefinir la relación entre el gobierno y el ciudadano en términos de intercambio de datos, la transparencia y la confianza, y hacer una contribución importante a la transformación digital del Estado."

Otros ejemplos de estados que están implementando la tecnología son Virginia Occidental, que lanzará una versión móvil piloto basada en blockchain para llevar a cabo la votación en las elecciones regionales de 2018, y Nueva York, con su proyecto “Microgrid”, basado en Ethereum, siendo desarrollado específicamente para las familias que quieren comprar y vender la electricidad generada por los paneles solares. Estos juntos con otros proyectos ponen a Estados Unidos en el número uno del ranking de países con mayor inversión en tecnología blockchain según un estudio realizado por la firma Deloitte a principios de 2018, donde también se declara que dicha inversión se ha triplicado en el último año, lo cual demuestra un crecimiento realmente prometedor.

3. Blockchain en Rusia

Rusia es un buen ejemplo de la seguridad y demás beneficios que ofrece blockchain, ya que hasta finales de 2015 el gobierno desconfiaba de dicha tecnología por el desconocimiento de su

origen y por ende de las intenciones con que fue creado, sin embargo actualmente es uno de los países que más la está estudiando e implementando. Incluso el Ministerio de Defensa ha creado un laboratorio de investigación, destinado al uso de la cadena de bloques para prevenir ataques de ciberseguridad a sus bases de datos. Especialmente por el hecho de que las plataformas basadas en blockchain hacen que sea difícil ocultar los rastros de los ciberataques. Según Alexei Malanov, experto en antivirus que trabaja para la compañía rusa de seguridad informática Kaspersky Lab, los atacantes suelen limpiar los registros de accesos no autorizados a los dispositivos, pero al ingresar en un ecosistema Blockchain las posibilidades de lograr esto disminuyen considerablemente.

Por su parte, German Klimenko, un ex asesor tecnológico del presidente Vladimir Putin, afirmó que las investigaciones sobre la cadena de bloques han sido muy útiles para la industria rusa de ciberseguridad. El laboratorio en cuestión está siendo construido en la ciudad portuaria de Anapa, y una vez terminado responderá ante la Dirección de Operaciones del Estado Mayor General de las Fuerzas Armadas de Rusia.

Por otro lado, haciendo referencia al sector turismo, esperan que la tecnología blockchain transforme el mercado turístico del país. El director de la Agencia Federal de Turismo de Rusia, Oleg Safonov, aprovechó el más reciente Foro de Turismo celebrado en la ciudad de Kazan, para comentar: “Estamos convencidos de que Blockchain cambiará seriamente el mercado turístico, aunque creemos que no sucederá en dos años sino en un período de tiempo mayor: entre 5 y 10 años”. Al explicar la naturaleza de los cambios que la cadena de bloques podría traer, el funcionario añadió que las nuevas tecnologías permitirán a los turistas trabajar directamente con los proveedores de servicios, eliminando así la necesidad de intermediarios. Según Safonov: “Esto hace que los servicios sean de mejor calidad, menos costosos y que aumente la responsabilidad de los proveedores”.

Otros ejemplos relevantes de implementaciones de blockchain en Rusia son el sistema de registro de tierras basado en esta tecnología, el cual se puso en marcha a principios de 2018; o la intención de realizar las próximas elecciones usando la tecnología para controlar las votaciones, idea que surgió a partir de que en Marzo de 2018 debieron anular los votos de 26 colegios por supuestas manipulaciones.

Cabe destacar que, aunque Rusia mantiene una postura cautelosa en torno a las monedas digitales, la verdad es que siempre ha mostrado la disposición de explorar los usos generales de Blockchain. De hecho, el mes pasado el gobierno anunció planes para probar un. Por su

parte, el viceprimer ministro de Rusia ha comentado que la cadena de bloques podría contar con numerosos usos en la administración estatal.

4. Blockchain en China

A lo largo de 2018, el gobierno chino y las autoridades locales han demostrado una actitud muy a favor de blockchain. A pesar de la actitud negativa de las autoridades hacia las criptomonedas, las cuales fueron prohibidas en 2017, tienen mucha fe en la tecnología que las sustenta, financiando iniciativas multimillonarias para desarrollar redes basadas en esta tecnología. Por ejemplo, una inversión de U$D $ 1.600 millones, en abril de 2018, para financiar startups emergentes de blockchain y equipos de desarrollo.

. En el 13º Plan de Cinco Años para la Informatización Nacional de diciembre de 2016, haciendo referencia a la estrategia de digitalización del país, declararon: "Internet, la computación en la nube, big data[13], la inteligencia artificial y blockchain impulsarán la evolución de todo; los servicios digitales y de redes estarán en todas partes.

En abril de 2017, el Wuzhen Think Tank publicó un documento sobre el desarrollo de la industria blockchain de China. Éste introducía las tendencias mundial y nacional de la industria blockchain y proporcionó un valioso conocimiento de las entidades de investigación y empresas afines. Unos meses más tarde, el Comité Nacional de Expertos en Tecnología de Seguridad Financiera en Internet publicó su conformidad con las directrices blockchain.

Actualmente las autoridades chinas están estudiando activamente la blockchain, en términos de almacenamiento de datos más ordenado. El 24 de abril de 2018, la Oficina Nacional de Auditoría de China examinó el uso de la tecnología para resolver los problemas inherentes a la infraestructura de almacenamiento centralizado. Recientemente han anunciado públicamente el plan estándar nacional chino para blockchain, donde se incluyen las normas nacionales de la blockchain en la seguridad de la información y los estándares de las aplicaciones y negocios, y otros estándares de interoperabilidad y de credibilidad.

[13] Big data o macrodatos es un concepto que hace referencia a conjuntos de datos tan grandes que aplicaciones informáticas tradicionales de procesamiento de datos no son suficientes para tratar con ellos.

Está previsto que a cada oficina independiente y auditor acreditado le será asignado un nodo independiente, lo que ayudará a reducir la carga sobre el gobierno, además de proporcionar un libro de contabilidad con capacidad de ser rastreado, que registrará cada transacción.

Aunque este proyecto aún no pasa a la fase de ejecución, esto es un reconocimiento oficial del comienzo de una nueva era digital en China, que dio un gran impulso al desarrollo de tecnología blockchain, la cual es vista como una solución para el problema de la seguridad. Impulsada por la exitosa implementación de algunos de los mayores bancos, como el Standard Chartered, que después de tener pérdidas millonarias como resultado de fraudes con tarjetas de crédito, utilizaron la blockchain y desarrollaron un hash criptográfico único para cada factura, garantizando que no se lleven a cabo operaciones dobles y no se preste dinero por facturas falsas.

Según se declara en un estudio de la firma Deloitte, China será ampliamente el país con mayor inversión en blockchain a partir de 2023.

5. Blockchain en Emiratos Árabes Unidos

Dubái es considerada actualmente como una de las ciudades digitalmente más progresistas del mundo. Con tecnologías como trenes no tripulados, robots policías, taxis voladores, etc., puede ser considerada la ciudad más futurista en la actualidad. Pero las autoridades de los Emiratos no se detienen en lo que ya se ha alcanzado y están participando activamente en la ejecución de muchas ideas innovadoras. Según han anunciado las autoridades locales tienen el fin de convertir la ciudad en “la primera megalópolis inteligente basada en blockchain para 2020”.

En términos del número de proyectos ejecutados, basados en blockchain, Dubái ocupa el primer lugar en el mundo, gracias a que el gobierno apoya el Smart City Program. Programa lanzado en 2014, que consiste en la aplicación gradual de más de 545 proyectos que cambiarán la forma en que los residentes y visitantes de Dubái interactúan con la ciudad. Un ejemplo de estos proyectos es que planean crear un espacio digital sin papeles tanto en el sector público como privado, la circulación de documentos se realizará en forma completamente electrónica y todos los registros serán sustentados en la tecnología blockchain.

Otro ejemplo de programa piloto es el que está siendo desarrollado para rastrear, enviar y entregar las mercancías importadas y exportadas usando tecnología blockchain. La idea principal de su integración en el comercio exterior de la ciudad es crear una única plataforma segura y transparente. Se proyecta que la implementación de un sistema blockchain en la estructura urbana ahorre aproximadamente $1,5 mil millones y 25,1 millones de horas-hombre debido al aumento de la eficiencia en el procesamiento de los documentos, que, se supone, dejarán a las instituciones de gobierno libres de colas. Aplicándose también la tecnología en la logística y el almacenamiento, el cual ayudará a crear un sistema completo de camiones inteligentes no tripulados para el transporte de productos o materiales.

6. Blockchain en Latinoamérica

La implementación de esta tecnología también ha tenido un auge este año en diversos sectores, de los cuales, se hará referencia continuación de los más relevantes. En cuanto al sector financiero además de los beneficios en cuanto a ahorro de costos y tiempo, tiene un potencial de integración financiera nunca antes visto y esto en Latinoamérica puede tener un impacto muy significativo, según un informe de Endeavor el 60% de la población no tiene acceso a servicios financieros, lo que significa que más de 391 millones de personas adultas no tienen cuentas bancarias, ni créditos de ningún tipo; a la vez que el 67% de la población, más de 437 millones, se encuentra conectada a internet, por lo que bastaría la descarga de una aplicación móvil y la creación de un usuario para ser integrados al mundo financiero.

Otro sector donde blockchain promete un fuerte impacto es el empresarial. Un buen ejemplo de esto es que en Mayo de 2018, en la ciudad de Sao Paulo, comenzó a operar, a cargo de la compañía IBM, el primer “centro de soluciones dedicadas a blockchain” de América Latina, el “Blockchain Solutions Hub”, que además de Brasil, tiene o se están desarrollando sedes en todos los países del continente, y se ha anunciado que invertirá 5,5 millones de dólares hasta 2020. Según informaron, la tecnología que brindan, “garantiza la veracidad de las operaciones por internet y está diseñada para ayudar a los clientes de toda América Latina a construir una nueva generación de aplicaciones de blockchain con los niveles más altos de seguridad, abordando nuevas formas de transacciones empresariales”.

Endeavor, organización dedicada a la asesoría y aceleramiento de emprendimientos, hizo un estudio sobre el comportamiento y características de las compañías Blockchain en América Latina, titulado “Insight: Blockchain, ¿La promesa de una revolución?“. La cual en palabras del director Vicent Speranza, busca: “plasmar un panorama general de lo que es blockchain en sus diversas aplicaciones”. Para este estudio se entrevistó a CEOs de empresas que basan o desarrollan la tecnología blockchain como modelo de negocio: 26 de México, 13 de Argentina, 10 de Brasil, 8 de Chile, 3 de Colombia, 2 de Perú, 1 de Ecuador, 1 de Puerto Rico y 1 de Venezuela.

Uno de los resultados más relevantes es el crecimiento económico reportado. En 2017, la venta media de estas empresas fue de 212.000 dólares; en 2018 se espera que tengan un crecimiento promedio del 90% llegando a los 404.000 dólares, y para 2019 esta cifra aumentaría a 1.250.000 dólares, lo cual muestra un claro crecimiento en el sector.

Otro dato de gran relevancia es que en cuanto a los retos mencionados para la implementación de blockchain destacó la falta de disponibilidad de talento, la gran mayoría coincidió en que contar con personal calificado para el manejo y desarrollo de esta tecnología resulta más complicado incluso que acceder a financiamiento. Mientras tanto el segundo factor destacado fue la falta de regulación, por la incertidumbre que esto genera.

Finalmente, en cuanto al sector gobierno, blockchain representa grandes oportunidades, por ejemplo permitir una democracia más participativa y transparente. En 2017 se han dado los primeros anuncios de proyectos concretos, (muchos de los cuales impulsados por el Banco Interamericano de Desarrollo), más allá que aún existe gran incertidumbre del tema, la cual será superada según el éxito de los proyectos precursores.

Empezando por Chile, el gobierno la está probando para el manejo de las órdenes de compra dentro de Mercado Público, la plataforma de comercio electrónico más grande del país. En la cual más de 850 organismos del Estado realizan de manera autónoma sus compras, se contratan alrededor de 123.000 empresas que adquieren productos de todo tipo, desde materiales de oficina, medicamentos y alimentos, hasta servicios de transporte; y las transacciones alcanzan un valor de 10.200 millones de dólares anuales, según declaran en su sitio web. Según han expuesto encargados del proyecto, el objetivo es proporcionar un mayor nivel de transparencia en sus procesos, procurando que la nueva aplicación funcione como una especie de notario virtual que certifique la “no alteración” de los documentos. Formando parte de un plan de modernización digital, con el objetivo de potenciar la integridad del sistema. “Se

trata de una tecnología emergente que puede elevar la confianza entre la ciudadanía y el Estado. Quizás en un futuro no tan lejano, muchos elementos de identidad digital en las compras públicas puedan ser asegurados a través de blockchain". Trinidad Inostroza, directora de ChileCompra

También, en marzo de 2018, la Comisión Nacional de Energía de Chile (CNE), incorporó blockchain a sus servicios internos. Autenticando los precios del mercado, los costos marginales, los precios de la gasolina; y siendo un sustento para hacer cumplir ley ERNC (proyecto de ley que busca aumentar el porcentaje de las energía no convencionales), al utilizar la tecnología de contabilidad distribuida como un notario digital y mejorar el proceso de certificación de datos dentro el sector energético.

Por su parte Méjico además de ser país de Latinoamérica donde más usos están dando a la tecnología por parte del sector empresarial y emprendedor, está siendo pionero en el aspecto regulatorio. Aprobaron en diciembre de 2017 la Ley Fintech, la cual establece las normas para las instituciones que prestan servicios financieros a través de innovaciones tecnológicas, regulando también temas como las criptomonedas, mecanismos como el crowdfunding[14] y medios de pago electrónicos. A pesar de que no se incluye de forma directa a blockchain, establece pautas que brindan confianza a quien quiera trabajar con dicha tecnología y han declarado que será un tema a incluir para la próxima modificación que sería presentada en marzo de 2019.

El segundo país del continente con más casos de uso es Brasil, además de la decisión de IBM de instalar su centro de soluciones blockchain en Sao Paulo, lo cual significa un importante impulso para el ecosistema blockchain dentro del país, ya se venían desarrollando una variedad de proyectos sustentados en la tecnología, por ejemplo la empresa Odebrecht, tan reconocida por los casos de sobornos, está desarrollando junto con otras instituciones una plataforma digital apoyada en una red blockchain, para garantizar la transparencia en los procesos de adjudicación de obras públicas. Creando el "Instituto Observ", cuya misión será la vigilancia del proceso y rastreo de los documentos en cada licitación pública. Otro ejemplo interesante es el del candidato a presidente João Amoêdo, quien afirmó en Agosto de 2018 que planea constituir un "gobierno digital" basado en blockchain en caso de ser electo. Convertido así la digitalización de los datos gubernamentales en una de las caras de su campaña política.

[14] El crowdfunding o micromecenazgo consiste en la difusión pública de su negocio, por parte de la persona que busca financiación, y la financiación mancomunada por parte de prestamistas independientes, persiguen un crédito ofrecido por el prestatario o que simplemente simpatizan con la causa.

Como se puede ver, en América Latina, la tecnología blockchain ha comenzado a crecer de forma alentadora en los últimos años y es muy prometedora para diversos sectores, sin embargo se está lejos de alcanzar una adopción masiva. Más adelante se hará también mención de la situación en Argentina, donde el sector emprendedor es especialmente destacable, incluso a nivel mundial.

7. Proyectos internacionales

A continuación se ampliará sobre los 3 proyectos privados más significativos en cuanto a potenciar el ecosistema blockchain, favoreciendo y promoviendo su adopción masiva.

a. Ethereum

Es una plataforma de código abierto y descentralizada que fue desarrollada basada en el protocolo blockchain. Con grandes similitudes a la red blockchain de Bitcoin pero con dos diferencias a destacar, una es que busca servir como plataforma sobre la que se pueda construir otras aplicaciones descentralizadas, lo cual también es posible sobre la red Bitcoin pero Ethereum lo facilita considerablemente al estar desarrollada para dicho fin y la otra diferencia importante es que fue la primera en permitir la creación de “smart contracts” sustentados en la propia red. Dichos contratos consisten en un programa informático que ejecuta acuerdos establecidos entre dos o más partes, haciéndolos cumplir de forma automática y autónoma al cumplirse las condiciones previamente establecidas, sin posibilidad de tiempo de inactividad, censura, fraude o interferencia de terceros. (En el anexo 2 se ampliará acerca de los contratos inteligentes)

Ethereum fue comenzado a desarrollar por Vitalik Buterin, un joven ruso, quien en aquel momento tenía 19 años. Este desarrollo fue posible gracias a una plataforma de financiamiento colectiva, desde julio de 2014 hasta el 30 de julio 2015, cuando el sistema salió definitivamente, a través de Ethereum Foundation, una fundación sin fines de lucro que actualmente trabaja junto con empresas como IBM, Intel, Microsoft o JP Morgan Chase y junto con gobiernos, como el de Rusia o Estonia, en la creación de diversos proyectos sustentados en la tecnología.

De la misma forma en que en la primer blockchain se sustenta la criptomoneda bitcoin. En Ethereum se sustenta “ether”, su criptomoneda descentralizada subyacente, con la cual se ejecutan los contratos del mismo. Ether se puede intercambiar entre usuarios y también es utilizado para compensar a los nodos participantes por los cálculos realizados. A Julio de 2018 es la segunda criptomoneda con mayor capitalización de mercado, alcanzando los U$D 48.008 millones y aproximadamente 78% de los proyectos que utilizan el protocolo blockchain se han realizado sobre la plataforma Ethereum, lo que la convierte en la plataforma más popular para las ICO[15] y el desarrollo de aplicaciones descentralizadas.

b. Proyecto Hyperledger

Es un proyecto colaborativo de código abierto creado por Fundación Linux en diciembre de 2015 y que a principios de 2016 se fusionó con OpenBlockchain de IBM, con la finalidad de promover el avance de la tecnología blockchain en las diversas industrias. En esta colaboración mundial participan actualmente más de 220 compañías, muchas de ellas líderes de las finanzas, la banca, la manufactura, cadenas de suministro, el internet de las cosas[16] y de diversas tecnologías.

A grandes rasgos este proyecto consiste en unir una gran cantidad de iniciativas diferentes e independientes para lograr una infraestructura y el desarrollo de estándares que proporcionen un marco de trabajo que sustente y facilite la adopción de la tecnología blockchain por parte de cualquier empresa o institución, proporcionando una infraestructura neutral y abierta, dirigida por la comunidad, pero a la vez respaldada por un gobierno técnico y empresarial. Además de educar al público sobre la oportunidad de mercado que conlleva la tecnología blockchain y construir una comunidad de comunidades que genere herramientas y soluciones para la adopción de la tecnología.

Dentro de Hyperledger existen muchos proyectos, de los cuales se hará mención de tres de los más relevantes:

[15] Una ICO (initial coin offering) es una oferta inicial de criptomonedas, lo que consiste en una fuente de financiamiento donde se venden criptomonedas de nuevos proyectos blockchain de forma muy similar a las acciones de las empresas que cotizan en bolsa.

[16] Internet de las cosas (IoT): Es un concepto que se refiere a la interconexión digital de los objetos cotidianos con internet.

Interledger: que también es un proyecto colaborativo de código abierto, conducido por el Consorcio World Wide Web (W3C), la principal organización internacional de normalización para la red informática mundial. El objetivo que tiene Interledger es el de desarrollar un sistema universal de pagos que permita efectuar pagos entre los participantes de la red, independientemente del medio usado tanto por el receptor del pago como por el pagador.

Hyperledger Fabric: Es un framework[17] que facilita el construir redes blockchain empresariales para consorcios de organizaciones, brindando un ledger o libro mayor, contratos inteligentes y algoritmos de consenso estandarizados y una garantía de privacidad. Este proyecto está muy interrelacionado y potenciado por Hyperledger Composer, que es un software auxiliar específico para complementar y sobre todo facilitar el despliegue, mantenimiento, diseño y prototipado de las redes blockchain, es decir, es una herramienta que buscar permitir lo antes mencionado de la forma más fácil posible para que cualquier entidad pueda controlar, modificar e incluso crear redes blockchain.

c. Consorcio R3

Fundado en 2014 es un consorcio formado por más de 200 de los más grandes bancos, instituciones financieras y firmas de servicios profesionales, del mundo, entre ellos BBVA, Accenture, Bank of America, Intel, Microsoft, HSBC, Itaú, etc. (hasta hace unos meses formaban parte el J. P. Morgan Bank y Santander, pero salieron para iniciar otros proyectos similares), y cuya finalidad es aprovechar las posibilidades de una cooperación conjunta utilizando la tecnología Blockchain. Para esto han desarrollado una blockchain privada denominada “Corda”, que está diseñada para registrar y ejecutar acuerdos legales, entre las empresas, mediante el uso de smart contracts. El 30 de noviembre de 2016, R3 hizo público el código fuente que sustenta Corda, siguiendo la inercia existente en todas las iniciativas de redes blockchain privadas, que buscan seducir y atraer a desarrolladores a sus plataformas, como una forma de generar valor añadido. Y también buscando influir positivamente en el desarrollo de Hyperledger, al aportar parte de su investigación y desarrollo.

[17] Un framework es una estructura conceptual y tecnológica de soporte definido, normalmente con artefactos o módulos de software concretos, que sirve de base para la organización y desarrollo de software.

Corda, a diferencia de las redes blockchain públicas, ha sido diseñada siguiendo estrictamente las necesidades del sector financiero y bancario, es decir, por esto es considerada una blockchain privada y cerrada, confeccionada a medida para cumplir una función bien definida dentro de este sector, en la que sólo las partes participantes en los contratos tienen la capacidad de ver las anotaciones de transacciones. Por esto, Corda no está descentralizando realmente a los bancos, sino que está utilizando tecnologías inspiradas en blockchain para ayudar a los bancos a seguir operando de forma privada, pero de una manera más eficiente y autónoma.

Capítulo VI: Blockchain en Argentina

En cuanto al gobierno nacional no ha mostrado un interés como el de países del primer mundo, pero se está comenzando a hablar sobre la necesidad de regular la tecnología y ya se han hecho inversiones en su uso, por ejemplo están apoyando un proyecto para hacer una red blockchain a nivel federal y otro para mejorar la inclusión financiera, para lo cual el gobierno de la provincia de Buenos Aires está colaborando con el Banco Interamericano de Desarrollo. Además se ha adoptado esta tecnología para certificar las ediciones digitales del Boletín Oficial, mediante la plataforma OpenTimestamps, que funciona sobre la blockchain de Bitcoin. Las publicaciones pueden leerse en el sitio web otslist.boletinoficial.gob.ar.

Mientras tanto el Banco Central ha demostrado recientemente interés en la tecnología en distintas ocasiones, por ejemplo, un artículo que publicó en su sitio web en Abril de 2018, denominado “Blockchain: ¿Cómo puede contribuir esta tecnología al sistema financiero?”, o un llamado abierto, que hizo en Junio del mismo año, a proveedores de libros en Argentina, para fomentar la publicación de libros que permitan aprender acerca de criptomonedas y blockchain.

En cuanto al sector empresarial, blockchain está comenzando a tomar relevancia debido a los beneficios que ofrece en la trazabilidad de productos, la agilización y consecuente disminución de costos en registros y controles, y el potencial para favorecer la seguridad jurídica. En el pasado 22 de Agosto se juntaron especialistas y empresarios dedicados al comercio exterior, en el evento “Negocios con el mundo”, realizado en Buenos Aires, donde se estuvo de acuerdo de que blockchain llegó para “revolucionar el mercado”, hablándose muy entusiastamente de los beneficios que brindará a los exportadores.

El sector que más interés está demostrando en blockchain es el de las fintech, lo cual es de esperarse si se considera que es un sector que está en auge (según un estudio realizado por Finnovista, creció un 83% durante 20187) y esta tecnología le brinda grandes beneficios y oportunidades. Hay ya muchos casos de emprendimientos con gran potencial, incluso de renombre mundial, algunos de los cuales serán mencionados más adelante.

1. Blockchain Federal Argentina

A través de un acuerdo de articulación público-privado celebrado entre NIC Argentina, la Cámara Argentina de Internet (CABASE) y la Asociación de Redes de Interconexión Universitaria (ARIU) se está desarrollando una plataforma multiservicios de alcance federal y uso público basada en la tecnología blockchain.

A través de esta iniciativa conjunta, en el que las partes representan al sector público, la academia y el sector privado, se conformará la infraestructura sobre la que correrá la primera plataforma nacional de uso público basado en Blockchain, una innovadora tecnología de validación de transacciones que permite variados usos en el marco de la economía digital.

Por las características propias de la tecnología, más los atributos de interoperabilidad y uso público y colaborativo con los que se creará esta plataforma, se podrán correr sobre ella aplicaciones y sistemas que mejoren los procesos de organizaciones del sector público y privado de todo el país. Valiéndose de una bitácora de transacciones pública, segura e inmutable, la plataforma multiservicios que desarrollarán permitirá la utilización de aplicaciones verticales pensadas para hacer contratos, transacciones y un sinfín de otras operaciones en un entorno que busca asegurar eficiencia, transparencia y seguridad.

Blockchain Federal Argentina, contempla una primera etapa, que ya se ha puesto en marcha, en la que se montará la infraestructura de base compuesta por una "granja" de 15 servidores distribuidos y el framework[18] de desarrollo sobre el que correrán las aplicaciones de los usuarios. La plataforma, pensada para funcionar estrictamente sin criptomoneda asociada, se espera que esté operativa a fines del 2018.

[18] Framework es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.

"La idea de tener una red federal de blockchain es seguir construyendo y desarrollando la infraestructura para mejorar internet en la Argentina. Lo que estamos haciendo las entidades que hoy forman parte de lo que se llama la comunidad técnica de argentina es seguir agregando valor y desarrollando servicios básicos para los usuarios, empresas y que cualquier ente pueda desarrollar nuevas aplicaciones y nuevos servicios sobre la infraestructura montada sobre la red de internet que estamos desarrollando. Esta iniciativa permitirá nuevos negocios, aplicaciones, servicios y empleos. Estamos seguros que mejoraremos y desarrollaremos más la internet en Argentina ", explicó Ariel Graizer, presidente de CABASE.

Según Rodolfo Andragnes, director ejecutivo de Fundación Bitcoin Argentina, este proyecto está en desarrollo y con la intención de concretarse, pero con dificultades en cuanto a asegurar la seguridad de la red, lo cual está frenando el desarrollo y podría modificar las fechas de implementación estimadas.

2. Proyecto de inclusión financiera

El proyecto originalmente nació en 2015 con el programa SystemaD, impulsado por la ONG Bitcoin Argentina, para desarrollar una identidad digital, facilitar el acceso a servicios públicos básicos y promover la inclusión financiera. Actualmente también participan en el proyecto el Banco Interamericano de Desarrollo (BID), el Fondo Multilateral de Inversiones (FOMIN), el gobierno de la provincia de Buenos Aires y RSK Labs.

El principal objetivo es dar solución a algunos de los principales problema de quienes viven en la marginalidad, que es la falta de documentos confiables para poder encontrar un trabajo formal, acceder a un crédito o abrir una cuenta bancaria. Para revertir esta situación, los actores detrás del proyecto están desarrollando una aplicación móvil para resguardar y gestionar datos personales que permitirán a los usuarios construir una reputación en base a su comportamiento y voluntad de crecimiento.

A través de la creación de una base de datos descentralizada, transparente e inalterable que proporciona la tecnología blockchain, la app servirá para registrar tanto datos básicos del ciudadano (nombre, fecha de nacimiento, estado civil, domicilio, etc.) como también información extrajudicial que pueda ser parte de una identidad digital; historiales de trabajo (formales e informales) y certificados académicos.

Además, tendrá integrada una billetera digital para facilitar la trazabilidad de pagos y el acceso a mejores créditos. La misma permitirá al usuario guardar pesos digitales y servirá como herramienta para el atesoramiento, la transferencia de dinero persona-a-persona (P2P) y las transacciones con comercios.

"Los altos niveles de vulnerabilidad de los habitantes de villas de emergencia se asocian, entre otros, al concepto de penalización de la pobreza, que se refiere al mayor costo relativo que enfrentan estas personas para acceder a determinados bienes y servicios; y es que el mercado no cuenta con información sobre la identidad y el comportamiento de las personas más vulnerables. No puede incluirlas, o lo hace a un costo mucho más alto que para el promedio de la población", publicó el Grupo BID en un informe.

Si bien los datos que registra la blockchain son permanentes e inalterables, cada usuario tendrá la potestad de elegir qué datos revelar a sus pares. Lejos de ser una invasión a la privacidad, se busca que la identidad digital construida sobre blockchain permita que las personas sean dueñas de sus propios datos. Por ejemplo, la identidad que un usuario permita que sea visible a un doctor no necesariamente será la misma que muestre a un banco. Este proyecto actualmente es un piloto que se implementará en tres barrios vulnerables de Buenos Aires, entre ellos Villa 31, donde más de 43.000 personas y estiman que requerirá una inversión de USD 2.575.000 en 42 meses.

3. Proyecto Rootstock, de RSK Labs

Hay una empresa argentina que dentro del mundo blockchain se ha ganado un fuerte renombre a nivel mundial, siendo considerada como la gran competencia de Ethereum. Esta empresa es RSK Labs, con su proyecto Rootstock, que nació en 2016 con la idea de implementar contratos inteligentes sostenidos en blockchain, tal como lo hace Ethereum pero con la principal diferencia de que en lugar de utilizar una alt-coin[19], como lo es Ether, los contratos pueden llevarse a cabo utilizando bitcoins, suponiendo esto una clara ventaja ya que esta es la criptomoneda más importante del mercado.

El proyecto surgió como la unión de dos equipos de trabajo, uno técnico y otro social. En 2015, Rubén Altman, licenciado en Computación; el ingeniero en Informática y especialista en

[19] Alt-coin es un término usado para hacer referencia a cualquier criptomoneda diferente a bitcoin.

Marketing Adrián Eidelman y Sergio Lerner, magíster en Ciencias de la Computación y ex auditor de seguridad de la Fundación Bitcoin, se juntaron con el economista Gabriel Kurman y Diego Gutiérrez Zaldívar, quien venía desarrollando comunidades sobre Bitcoin en Latinoamérica.

A principios de 2018 lanzaron una red blockchain paralela a la de Bitcoin, lo que se conoce como sidechain, o cadena paralela. Ellos crean la infraestructura para que otros desarrollen sus aplicaciones y los mineros puedan colaborar con la seguridad de la red. "Nuestro modelo de negocios se basa en la adopción de la plataforma. Si esta crece, una parte de las comisiones que cobran los mineros es nuestra y otra la usamos para incentivar nuevos proyectos", explica Zaldívar. Actualmente, entre las organizaciones que trabajan con la plataforma están Tarjeta Naranja, el Banco del Pacífico de Ecuador y el Banco Davivienda de Colombia y tienen un proyecto de inclusión financiera que integra al Banco Interamericano de Desarrollo y al Gobierno de la Ciudad de Buenos Aires. Para 2018 esperan facturar unos U$D 10 millones.

Han recibido la aprobación de importantes figuras de la criptoindustria. El criptógrafo e ideador de los contratos inteligentes, Nick Szabo dijo que combinaban lo mejor de Bitcoin y lo mejor de Ethereum, siendo la primera red completamente descentralizada en incluir contratos inteligentes. Y Marek Palatinus, fundador del primer pool de mineros[20] y creador de la billetera Trezor, comentó: "Estoy impresionado por el desarrollo de RSK. Especialmente me gusta que no tengan una alt-coin, sino que construyeron su plataforma sobre Bitcoin. Esto puede ser la próxima gran cosa". Gracias a tal aprobación de parte del sector han recibido inversiones por más de US$ 4,5 millones. En la primera ronda recibieron US$ 1 millón de grandes empresas como Digital Currency Group, Coinsilium y Bitmain, la principal empresa de minería de bitcoins. Luego, en una segunda ronda, recibieron otros US$ 3,5 millones para implementar su plataforma de contratos inteligentes, la cual permite crear aplicaciones totalmente descentralizadas, conocidas como "D-Apps[21]".

Parte del objetivo de RSK es también la inclusión financiera. "Ahora es posible crear un sistema inclusivo gracias a que con blockchain no hay costo de mantenimiento de las cuentas y el costo de las transacciones es cada vez menor", detalló Diego Zaldívar. Y dado que, según el

[20] Los pool de mineros son las agrupaciones de equipos mineros que se unen en una red determinada para compartir y ampliar su capacidad o poder de procesamiento, agilizando así su capacidad para resolver una cadena de bloques criptográficos.

[21] D-Apps: Aplicación que no depende de un sistema central, sino que depende de la comunidad de usuarios que la utilizan.

Banco Mundial, casi 50 por ciento de los argentinos no está bancarizado, la región aparece como una gran oportunidad.

Actualmente la empresa se enfoca en balancear sus gastos en desarrollo y en difundir el proyecto para aumentar su adopción. Tiene aún mucho camino que recorrer para estar al nivel de Ethereum, la plataforma más utilizada, pero Rootstock, a pesar de haber salido tan recientemente al mercado, ya es visto como una de las principales alternativas. En 2017, el 0,32% de los nuevos proyectos fueron realizados sobre su plataforma, ubicándose como la sexta plataforma de protocolo blockchain más utilizada, y para 2018, según declaran un su sitio web tienen previstos ingresos por arriba de los U$D 10 millones.

4. Kleros

Kleros es un proyecto iniciado por Federico Ast, Clément Lesaege y Nicolás Wagner; su principal centro de desarrollo está ubicado en la provincia de Tucumán y consiste en un protocolo de justicia que funciona en internet, basado en el sistema judicial que usaban en la Antigua Atenas. Busca ofrecer un arbitraje rápido, seguro y accesible para prácticamente cualquier situación; conectando a los usuarios que necesiten resolver sus disputas y los jurados con las habilidades necesarias para solucionarlas de forma justa.

Según Federico Ast: “El mundo atraviesa un acelerado proceso de globalización y digitalización. Un número creciente de transacciones se realiza en línea entre personas de todo el mundo y entre el 3 y el 5% termina en disputas, más de 700 millones sólo en 2015. Por ejemplo compradores en eBay que afirman que el vendedor no envió el producto como se especificaba en el acuerdo, o usuarios de Airbnb que protestan porque la casa no era como la de las imágenes. Los métodos existentes de arbitraje son excesivamente lentos, costosos y poco confiables para un mundo en línea y en tiempo real”.

Cuando los usuarios crean un contrato inteligente pueden elegir a Kleros como protocolo de resolución de conflictos. Toda la información relevante es enviada de forma segura a Kleros. Se forma un tribunal a partir de jurados dispuestos a colaborar quienes evalúan la evidencia y emiten su voto. La decisión tomada por el tribunal es ejecutada automáticamente por el contrato inteligente. Posteriormente, los miembros del jurado que hayan votado por la alternativa

ganadora reciben una recompensa en la criptomoneda Kleros, la cual puede ser intercambiada por otras criptomonedas.

Actualmente el proyecto está recibiendo muy buena aceptación por parte de personas de renombre en la industria tecnológica y según sus desarrolladores en los próximos años será utilizado en más de 130 países. (En el anexo 3 se ampliará sobre el funcionamiento).

5. Proyecto Cóndor

Este proyecto lo empezó Santiago Selva, un mendocino, estudiante de abogacía, con financiamiento de la municipalidad de Capital y de Godoy Cruz. El modelo de negocio no está terminado pero por ahora consiste en la creación de una criptomoneda que se llamará Cóndor, que básicamente se consigue al andar en bicicleta. Está siendo desarrollado sobre una plataforma Ethereum, ya que ésta permite crear otras criptomonedas sobre su sistema, ahorrando años de trabajo en desarrollo.

Habrán tres formas de conseguir las criptomonedas: La primera será invertir en ellas, es decir comprarlas en casas de cambio, ya sea con dólares o con otras criptomonedas; segundo, funcionar como un nodo de la red, para lo cual es necesario simplemente crear un usuario y tener criptomonedas cóndor guardadas, mientras más se tengan será proporcionalmente mayor la probabilidad de ganar la próxima que se libere al mercado, y la tercera será “minarlas”, lo cual se hará andando en bicicleta, el sistema dará el equivalente a 3 dólares en cóndor, cada 10 km recorridos, para lo cual compraron un software a Amazon que permite comprobar que realmente fueron recorridos los 10 km en bicicleta. Con este último método de obtención se busca fomentar el uso de las bicicletas y con ello la actividad física, la vida sana y que además sirva para fomentar el turismo.

Antes de lanzarla al mercado quieren firmar con al menos 50 empresas en las que la gente pueda gastan las cóndor y luego ir entrando en más comercios, por lo que aún no se sabe la fecha de lanzamiento. La gente podrá gastarlas en esos comercios o tenerlas como inversión. Las empresas que los acepten tendrán convenio con las casas de cambio que entren en el sistema, pudiendo cambiar sus cóndor a efectivo y tener de esa manera “cash flow” (fluidez), y luego la casa de cambio puede venderla a inversionistas que quieran invertir en la

criptomoneda, a gente que quiera ser nodo, o a empresas que quieran comprar crédito de carbono[22], terminando de esta forma el ciclo de la criptomoneda.

6. Nydro

Nydro es una plataforma colaborativa que busca solucionar la escasez energética que ocurre tanto por la sobrecarga de la red que afecta a la mayoría de los barrios de las ciudades durante el verano; así como por la falta de infraestructura que hay en diferentes zonas, principalmente, en zonas de bajos recursos y villas de emergencia. El objetivo es que los usuarios puedan generar, almacenar y distribuir energía entre ellos a través de una aplicación móvil.

Los creadores de la plataforma son David Trejo, ingeniero en electrónica y especialista en redes e inteligencia artificial, Lutmila García Blanksman, ingeniera industrial y encargada de diseño de producto; Nicolás Ambroso, ingeniero en química especializado en energías renovables y Maartje Geerlings, que es responsable del uso de datos y análisis de impacto social del sitio.

"Nydro busca ser un lugar donde puedas vender tu electricidad, es decir la que generas, así como comprar electricidad de tus vecinos. También podes ofrecer tu propia casa o lugar como un sitio de almacenamiento. Busca ser el mercado donde puedas acceder a electricidad en Argentina", explica Trejo.

Según explican los creadores de Nydro, la idea es que quienes se asocien a la plataforma instalen, junto a su medidor inteligente, un dispositivo que les permite conectarse a la web. Este gadget[23] conectado a internet les permitirá controlar cuándo se compra y vende electricidad. Actualmente el sistema no está operativo. Desde abril hay una demo de la plataforma online y el sistema ya está siendo probado.

"Por un lado buscamos generar una alternativa que permita un nuevo negocio: poner un panel solar o baterías para almacenar energía; y el otro caso donde queremos enfocarnos es en barrios, asentamientos precarios o lugares que están fuera de la red eléctrica y que hoy no

[22] Un crédito de carbono es una licencia que representa una tonelada de dióxido de carbono que se ha eliminado de la atmósfera o bien que se ha evitado emitir.
[23] Un gadget es un dispositivo que tiene un propósito y una función específica, generalmente de pequeñas proporciones, práctico y a la vez novedoso.

tienen acceso a la electricidad, además usamos blockchain para identificar cada persona, cada nodo en la red y también registramos a los usuarios por su DNI", detalla Trejo.

No hay que pagar ningún costo para adherirse a la red. Y todo lo que se comercializada allí se paga con criptomonedas como bitcoin y con los tokens de la misma plataforma (Nib). Luego se pueden convertir esas criptomoneda en dinero fiat[24] dentro del mismo sitio y recibir el monto en la cuenta bancaria del usuario. La plataforma cobra una comisión del 1,5% por esa transacción.

En 2017 surgieron regulaciones que permiten que los usuarios puedan comprar o vender electricidad desde su medidor. Eso quiere decir que, si un usuario conecta un panel solar y genera más energía de la que utiliza, puede comercializar el excedente. A su vez, puede almacenar energía de la red (como Edenor o Edesur) en baterías y luego vender en la web lo que no necesite.

Los medidores eléctricos todavía no llegaron a todos los hogares del país. Recientemente se comenzó una prueba piloto de Edesur con 5.000 medidores en Buenos Aires, que se suma a la prueba que ya está realizando Edenor. Para 2019 se estima que entre 10 y 15% de los usuarios en todo el país tendrán estos medidores, por lo que podrán beneficiarse del uso de Nydro.

7. Decentraland

Decentraland es el primer mundo virtual descentralizado, lo que significa que desde su lanzamiento, en junio del 2015, nadie controla la plataforma, no se pueden alterar las reglas del software y cada usuario tiene absoluta libertad. Está sustentado sobre la red blockchain de Ethereum, por lo que se hace un registro inalterable de todo el contenido, teniendo los usuarios plena propiedad sobre lo que han desarrollado o adquirido, por ejemplo, de las parcelas de tierra virtual, que son limitadas y de 10 metros cuadrados. En el lanzamiento fueron vendidas por hasta 120.000 dólares, recaudándose 26 millones de dólares en los primeros 30 segundos.

En este mundo se puede crear, experimentar e incluso monetizar contenidos y aplicaciones. Las posibilidades son casi ilimitadas, desde recorrer las diferentes ciudades e interactuar con otros usuarios, hasta hacer negocios, por ejemplo, un distribuidor de Adidas puede ofrecer la indumentaria en una tienda digital y los demás usuarios comprarlas para que posteriormente les

[24] El dinero fiat es el dinero establecido como moneda por regulación gubernamental o por ley.

sean enviadas en el mundo físico, o una institución educativa puede ofrecer cursos online en sus oficinas digitales con certificados reales.

Sus fundadores son 3 argentinos: Esteban Ordano, Ari Meilich y Manuel Araoz, quien ya no forma parte del proyecto. Las parcelas de tierra suelen ser adquiridas simplemente como una inversión ya que su precio ha mantenido un constante y acelerado aumento, al igual que Mana, la criptomoneda con que este mundo virtual se maneja, la cual, durante el tercer trimestre de 2018 ha sido una de las 5 criptomonedas con mayor crecimiento en valor de mercado, del mundo.

Capítulo VII: La adopción de blockchain

1. Desafíos intrínsecos

A pesar de ser una de las tecnologías más prometedoras y ser de código abierto su implementación conlleva ciertos desafíos que la retrasan. A continuación se hará mención de ellos, empezando por aquellos que para ser superados sólo requieren de casos de éxito y de tiempo:

- La curva de aprendizaje: Obligación de pensar distinto tanto para técnicos, entidades reguladoras y las áreas de negocios.
- Falta de madurez: Al ser una tecnología relativamente nueva falta mucha gente con suficiente conocimiento técnico y esto la hace muy susceptible a problemas de capacidad, fallas en el sistema, errores imprevistos y una probable decepción de los usuarios técnicamente poco sofisticados.
- Falta de confianza: Como todo lo nuevo, conlleva una incertidumbre que la gente sólo supera a través de experiencias exitosas.
- Costos: Al ser una innovación relativamente nueva, puede ser difícil integrarla con los sistemas tradicionales. A pesar de que blockchain es una herramienta efectiva para reducir costos asociados a la transferencia de valor y por la agilización de los procesos operativos, muchas entidades no estarán dispuestos a emprender hasta tener la suficiente seguridad de los beneficios.

Ahora se hará mención de los desafíos que necesitan de otros factores para superarse, intentando además justificar el por qué deberían ser superados en los próximos años:

- Escalabilidad de las redes públicas: Algunas personas afirman que la forma correcta de mitigar esto es mediante mejores algoritmos de consenso. Sin embrago actualmente ya se está dando una solución creando cadenas laterales a la cadena de bloques originas, las cuales se apoyan en su estructura.
- Falta de seguridad: A pesar de la relativa seguridad que ofrecen los actuales sistemas criptográficos, las redes blockchain no son totalmente seguras y esto podría acrecentarse con el surgimiento de los computadores cuánticos. No obstante en cuanto a esto último ya existen y se seguirán desarrollando algoritmos subcuánticos con el potencial de hacer demasiado difícil el hackeo aun con estos computadores y el mayor motivo de seguridad no es la criptografía sino el conceso distribuido, redes como la de Bitcoin, que tiene decenas de miles de nodos, no pueden ser hackeadas salvo que se controle más de la mitad del poder de cómputo de la red. Por esto, este problema se sigue dando en la mayoría de redes privadas y en las redes públicas que no tienen el tamaño suficiente, pero blockchain sigue siendo el sistema de registro de datos más seguro en la actualidad. "Si bien la tecnología blockchain en sí misma es intrínsecamente segura, hemos visto numerosas aplicaciones de comercio de criptomonedas, proveedores de procesamiento, wallets[25] e intercambios violados con éxito, ya que los hackers logran violar implementaciones con medidas de seguridad insuficientes buscando vulnerabilidades en la forma en que las empresas implementan blockchain y esto podría tener un serio impacto". Azeem Aleem, director global de RSA security.
- Falta de regulación: Actualmente es escasa la regulación de esta tecnología a nivel mundial y esto genera mucha incertidumbre a la hora de su adopción, como se mostrará más adelante en encuestas. Sin embargo algunos países como Suiza, Estonia, México o Estados Unidos ya están avanzando en esto y a medida que el uso de blockchain aumento los gobiernas se verán cada vez más forzados a llevar esto a cabo, Lo que no asegura que se acabe con la incertidumbre ya que las regulaciones de cada país podrían ser muy diferentes, si algunos países se manifestaran en contra de la tecnología, esto afectaría al ecosistema blockchain en su conjunto. Además de que la sobre regulación puede dificultar la innovación.

[25] Un wallet es un software o hardware que hace de billetera o cartera virtual encriptada otorgando seguridad para guardar, enviar y recibir criptomonedas o cualquier dato. Existen wallets físicos, similares a un pen drive y wallets no físicos, que funcionan dentro de un sitio web.

- Conexión con la ilegalidad: Las criptomonedas han sido asociadas desde hace tiempo con el mercado negro y el lavado de dinero, y como ésta ha sido la primera interacción de mucha gente con la tecnología blockchain, muchas de ellas podrían mantener una opinión negativa acerca de la tecnología. La realidad es que estas actividades ilegales también pueden llevarse a cabo con moneda fiduciaria e incluso blockchain puede ser la solución o al menos un obstáculo para algunas de estas actividades. Sin embargo toda tecnología puede ser usada para fines maléficos y para que blockchain sea realmente aceptada por el público debe primero diluir esta asociación.

2. Reinvención de los servicios financieros

El sistema financiero global mueve billones de dólares al día, sirve a miles de millones de personas y sostiene una economía global de más de 100 billones de dólares, siendo la industria más poderosa del mundo. Sin embargo este sistema lleva mucho sin modernizarse al nivel de otras industrias. Constantemente se acoplan nuevas tecnologías, pero sobre las mismas infraestructuras obsoletas, que desentonan del mundo digital que avanza a pasos agigantados, he incluso muchas veces lo frena. Además tiene inconvenientes como no lograr incluir a miles de millones de personas, las cuales por ende no acceden a mecanismos de financiación básicos; está centralizado y expuesto a robos de datos y otros ataques, y es monopolista lo cual desincentiva la innovación.

Ejemplos de ineficacia pueden ser los bancos que permiten operar por internet pero siguen emitiendo cheques de papel, o cuando un cliente paga una compra con tarjeta de crédito, su dinero pasa por no menos de 5 intermediarios hasta llegar a la cuenta bancaria del vendedor, es decir que la transacción se hace en el momento pero el pago tarda días; o que empresas multinacionales tienen que mantener decenas o incluso centenas de cuentas bancarias en moneda local para facilitar la operaciones en los diferentes países en que operan, por lo que para transferir dinero entre sucursales de distintos países tienen que esperar días o incluso semanas, tiempo en el cual ninguna de las sucursales puede usar el dinero, y deben pagar un interés a los intermediarios.

“Lo que la tecnología blockchain fundamentalmente hizo fue convertir un proceso basado en el papel a un proceso semiautomático y semielectrónico, pero la lógica seguía dependiendo del papel” declaró Vikram Pandit, exconsejero de Citigroup

Además existe un gran problema en cuanto a la inclusión financiera, según informe del Banco Mundial, a fines de 2017, 31% de la población adulta a nivel mundial, es decir 1.700 millones de adultos, no tienen cuenta bancaria en ninguna institución financiera ni proveedor de dinero móvil (49% en 2011). 2.000 millones de personas viven con menos de 2 dólares al día. Los pagos que hacen son demasiado pequeños como para que puedan hacerse por redes de pago tradicionales debido a las comisiones. Para los bancos servir a esta gente no es rentable, por lo que el servicio financiero que ofrecen no es realmente global, ni por su escala ni por su alcance.

El motivo de esta ineficiencia, proveniente de la falta de modernización, es que las finanzas son un monopolio y por esto muchas empresas no encuentran incentivos para perfeccionar sus productos, incrementar la eficiencia o mejorar la experiencia de los usuarios.

El sistema blockchain promete resolver dichos problemas y muchos más, traer profundos cambios a la industria, acabar con el monopolio y ofrecer a individuos e instituciones la posibilidad de crear y administrar valor como ellos quieran, ya que permite desarrollar nuevas formas de generar valor.

A continuación se mencionan 5 motivos por los que blockchain tiene el potencial de hacer todo lo antes mencionado:

Autenticación: Por primera vez en la historia dos partes, sin siquiera conocerse, pueden hacer negocios entre sí, con confianza y necesidad de intermediarios.

Menores costos: Con el sistema blockchain la red realiza y liquida transferencias de valor entre iguales de forma casi instantánea, estando el registro siempre actualizado. Según afirma el banco Santander, si los bancos aprovechan este recurso ahorrarán más de 20.000 millones de dólares solo en gastos de oficina y sin cambiar su modelo de negocio básico

Velocidad: Actualmente los giros de dinero tardan entre 3 a 7 días en liquidarse y las transacciones de préstamos bancarios tardan una media de 23 días. Mientras que la red blockchain de bitcoin tarda 10 minutos en realizar y liquidar todas las transacciones hechas en ese espacio de tiempo y otras redes de blockchain son aún mucho más rápidas, como la de Ripple Labs que es prácticamente instantánea.

Gestión de riesgos: El sistema blockchain, con sus pagos instantáneos, verificación instantánea del historial financiero y la irreversibilidad de las transacciones, permite eliminar varias formas de riesgo, por ejemplo el riesgo a que una transacción sea devuelta por fallas en el sistema, que la parte a quien se le ha hecho una transacción quiebre antes de liquidar el pago, o intente incumplir con dicho pago; o que administradores aprovechen la dilación y el papeleo para ocultar malas prácticas.

Innovación del valor: La forma de representar y transmitir el valor cambian radicalmente, ya que dejan de ser necesarios los intermediarios. En un principio muchos defendían la teoría de que el uso de blockchain significaría el fin de las instituciones financieras, o al menos enormes pérdidas para la industria. Pero esta amenaza ha hecho que sean estas instituciones las primeras las que más han invertido en aplicar la tecnología. Un buen ejemplo es el consorcio R3 antes mencionado, con su sistema Corda y su criptomoneda Ripple. Actualmente muchas entidades financieras, incluidas las 70 más grandes a nivel mundial, usan blockchain para registrar, intercambiar y negociar activos y pasivos y se espera que suplente a toda forma de intercambio tradicional y a los mercados centralizados, siendo la forma estándar de almacenar, asegurar y transferir todo tipo de valor.

Todas las ventajas mencionadas pueden transformar no sólo las formas de pago, sino también el mercado de valores, la banca de inversión, la forma de llevar la contabilidad y auditorías, el capital de riesgo, los seguros, la banca comercial y muchos otros pilares de la industria. Pero es sistema financiero está prácticamente monopolizado y en algunos aspectos cerrado a la innovación. Sin embargo según el Foro Económico Mundial, se prevé que el 80 por ciento de los bancos del mundo tendrán iniciados proyectos de blockchain para fines de 2018 y afirman que en los últimos tres años ya se han invertido 1.400 millones de dólares en la tecnología, inversión que crecerá cerca del 100%, es decir, casi se duplicará, durante los próximos 3 años.

3. Publicaciones de importantes empresas sobre el uso y la adopción

Deloitte:

En Abril de 2018 la firma Deloitte realizó una encuesta a 1.053 ejecutivos de Alemania, Canadá, China, Estados Unidos, Francia, Méjico y Reino Unido, preguntando cuales son las

principales barreras de sus compañías a la hora de apostar por el blockchain y los resultados fueron los siguientes:

- Asuntos reglamentarios 39%
- Reemplazando o adaptándose al sistema heredado 37%
- Posibles amenazas de seguridad 35%
- Retorno de inversión incierto 33%
- Falta de habilidad / comprensión interna 28%
- No es una prioridad comercial actual 22%
- La falta de una aplicación convincente de la tecnología 22%
- La tecnología no está probada 20%
- Preocupaciones sobre la información competitiva de sensibilidad 20%
- Ninguna 6%

En los resultados esta encuesta de Deloitte también destaca que el 53% afirma que sus compañías están trabajando para utilizar el blockchain en su cadena de suministro, que para el 43% de los ejecutivos esta tecnología se sitúa entre las 5 principales prioridades de su compañía y que el 45% señala que participarían en un consorcio de blockchain.

El interés creciente que genera esta tecnología se hace patente al comparar los resultados de estos estudios realizados ambos en 2018, con los de 2017 cuando en una encuesta de Gartner a 3.160 CIOs de empresas globales, la adopción del blockchain se situaba en el 1% y solo el 8% planeaba su implementación.

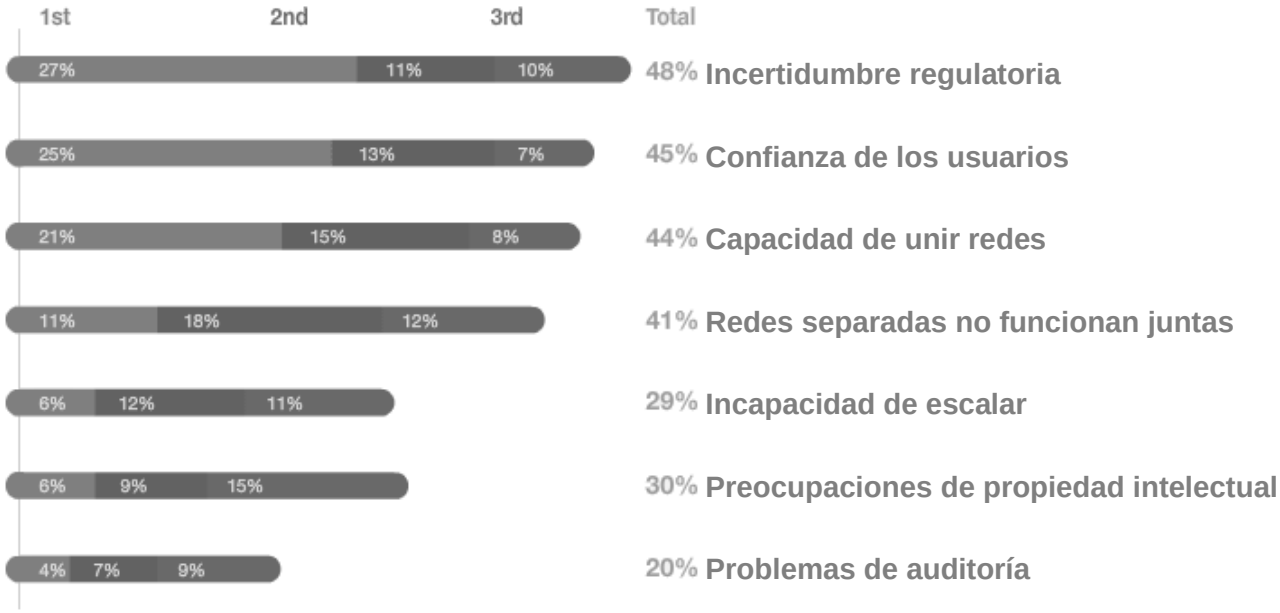
PwC:

Por otro lado la firma PwC publicó en agosto de 2018 un artículo sobre la adopción de blockchain donde encuestaron a 600 ejecutivos de 15 países del primer mundo, declarando que casi el 86 por ciento de los encuestados dijo que sus empresas están activamente involucradas con la tecnología. De los cuales estaban: 20% en investigación, 32% en desarrollo, 10% en pruebas piloto, 15% con aplicaciones en pleno uso y 7% con proyectos en desarrollo pero pausados.

Además, en esta encuesta se preguntó cuáles consideraban como los principales obstáculos en la adopción generalizada de blockchain y los principales resultaron ser la incertidumbre y

falto de confianza, lo cual según afirma PwC es alentador ya que son los obstáculos principales para toda tecnología emergente y superarlos es sólo cuestión de tiempo.

A continuación se muestra una gráfica con dichos resultados:

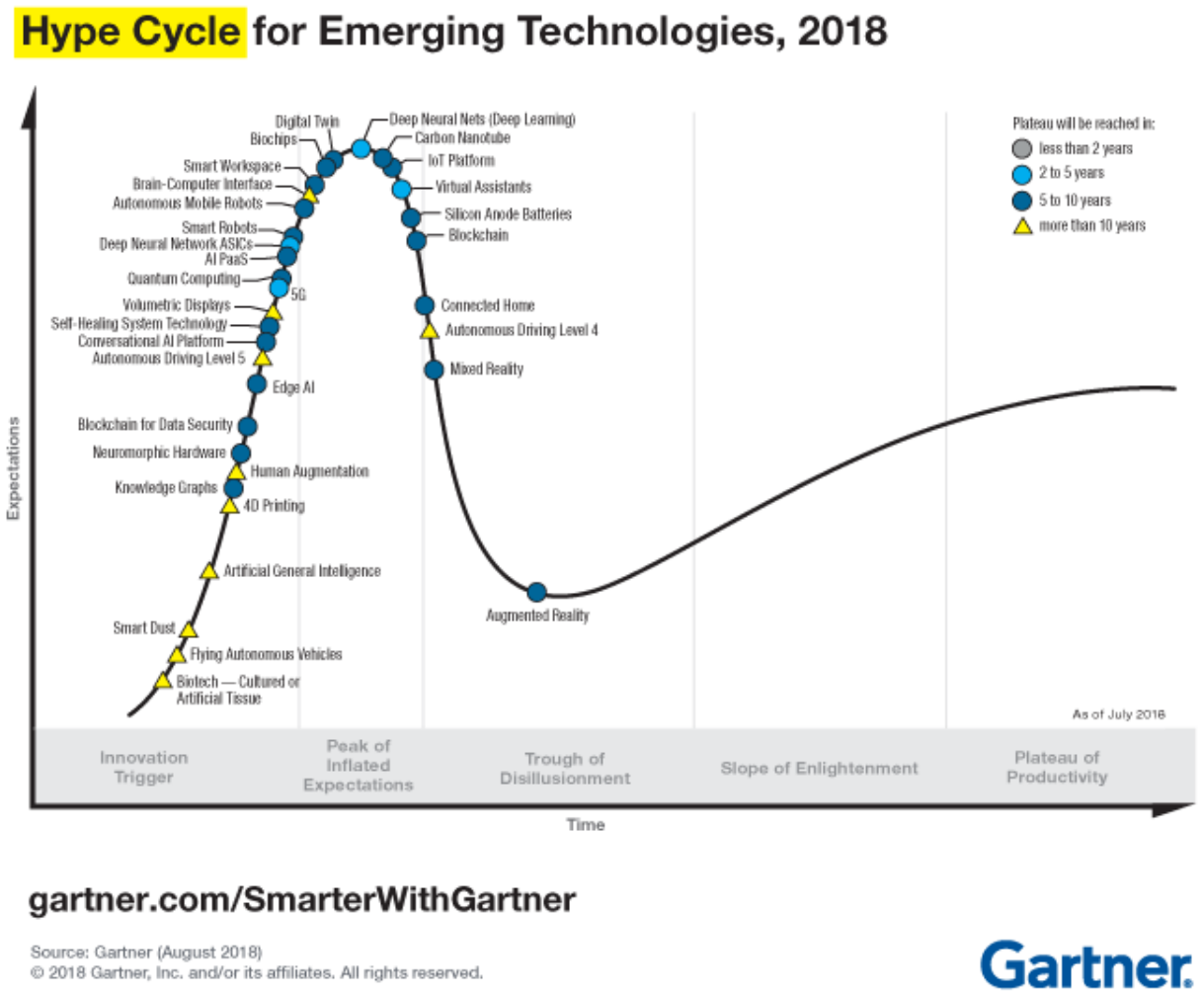


Finalmente en este artículo hacen referencia a una investigación de Cowen Outperform en la que estiman que para 2014 blockchain obtendrá una adopción generalizada.

Gartner:

Gartner publicó un artículo en su sitio web donde pronostica que blockchain generará un valor comercial anual de más de USD $ 3 billones para el año 2030 y que entre el 10% y el 20% de la infraestructura económica mundial se ejecutará en sistemas basados en blockchain para ese mismo año.

Además presenta anualmente un informe en que muestra la etapa de adopción por la que diferentes y relativamente nuevas tecnologías están pasando y a continuación se muestra el gráfico correspondiente a la publicación de 2018:



En esta gráfica se muestra que blockchain está saliendo de la etapa donde las expectativas son infladas (las implementaciones han tenido un crecimiento exponencial en 2018 a pesar de no darse el marco regulatorio e institucional idóneo) y entrando en la etapa donde se da cierta desilusión para posteriormente, en caso de superarse ésta última masificarse la implementación.

Capítulo VIII: Conclusión

El interés por la tecnología blockchain está en un constante e importante crecimiento por parte de muchas industrias ya que posibilita grandes ahorros, de tiempo y de costos de infraestructura y de procesos como los administrativos, contables, de seguimiento de clientes, de logística, entre otros. Además posibilita y facilita el desarrollo de nuevos negocios digitales con novedosos modelos de negocio y nuevos productos y servicios. Pudiendo ser además una herramienta para fortalecer los derechos de todos los seres humanos y empoderar a la sociedad, al ser un medio de comunicar la verdad, repartir prosperidad, acabar con las transacciones fraudulentas y reemplazar a los intermediarios.

A pesar de esto, aún no se alcanza una adopción masiva de esta tecnología, debido a desafíos y dificultades que aún no han sido totalmente superadas. Desde el punto de vista tecnológico se debe tener en cuenta que la sustitución de los actuales sistemas de información por la tecnología blockchain requiere de la suficiente disposición organizacional, de un análisis del consumo energético adicional requerido y planes concretos de transformación tecnológica en la infraestructura de las entidades. Siendo esto variable según el sector, por ejemplo, en el caso de los bancos, la interoperabilidad entre los diversos sistemas de información que usan es una gran barrera a superar.

También en lo que respecta al entorno regulatorio la situación es compleja. Ya que, dependiendo del tipo de servicios o de procesos que sean ofrecidos usando la tecnología blockchain, se debe aplicar una regulación específica, ya sea por ejemplo referido al conocimiento de cliente, a la prevención de lavado de activos, al financiación del terrorismo, a los mercados de capitales, etc. Además, el hecho de no existir un marco regulatorio similar entre países alimenta la incertidumbre sobre la jurisdicción aplicable según la ubicación específica.

Es necesario dar una solución a estos desafíos para que blockchain tenga una aceptación generalizada en todas las industrias. Siendo además importante que bancos, empresas, emprendedores y entes reguladores trabajen de manera conjunta, lo que puede significar complejas discusiones y por ende demoras en la implementación. Lo alentador es que este esfuerzo se está dando, entidades como las incluidas en el desarrollo de la presente investigación, están trabajando e invirtiendo de forma prometedora en la adopción masiva de esta tecnología y los beneficios prometen ser lo suficientemente superiores a las dificultades.

Esto último brinda relativa seguridad para asegurar que la inevitable arremetida de la adopción de blockchain hará que numerosas prácticas se vuelvan obsoletas. Servicios como los de la banca se volverán redundantes a medida que el mundo aprenda a operar y financiarse a sí mismo mediante redes blockchain. Sin querer decir que estos sectores desaparecerán, sino que deberían cambiar radicalmente sus modelos de negocio, al punto de tener un importante impacto en la sociedad en su conjunto.

Anexos

1. Anexo 1

En este anexo se muestra una traducción al español del protocolo original publicado por “Sathoshi Nakamoto”, en 2009, en el sitio web bitcoin.org acerca del funcionamiento de la criptomoneda bitcoin y el sistema blockchain. Dicho protocolo puede verse actualmente en el mismo sitio web, con algunas ampliaciones de la información y en el idioma inglés.

“Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario”

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Resumen: Una versión puramente electrónica de efectivo permitiría que los pagos en línea fuesen enviados directamente, de un ente a otro, sin tener que pasar por medio de una institución financiera. Las firmas digitales proporcionan parte de la solución al problema, pero los beneficios principales se pierden si tiene que existir un tercero de confianza para prevenir el doble gasto. Proponemos una solución al problema del doble gasto utilizando una red usuario a usuario. La cual coloca marcas de tiempo a las transacciones que introduce en una cadena continua de pruebas de trabajo basadas en el cálculo de hashes, formando un registro que no puede ser cambiado sin volver a recrear la prueba de trabajo completa. La cadena más larga no solo sirve como testigo y prueba de la secuencia de eventos, sino que asegura que está vino desde la agrupación con procesamiento de CPU más grande. Siempre que la mayoría del poder de procesamiento de CPU esté bajo el control de nodos que no cooperan para atacar la red, estos generarán la cadena más larga y llevarán ventaja a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes son enviados bajo la premisa del menor esfuerzo, y los nodos pueden irse y volver a unirse a la red cuando les parezca, aceptando la cadena más larga de prueba de trabajo, como prueba de lo que sucedió durante su ausencia.

1. Introducción:

El comercio en Internet ha llegado exclusivamente a depender de las instituciones financieras, las cuales sirven como terceros de confianza, para el procesamiento de los pagos electrónicos. Mientras que el sistema funciona suficientemente bien para la mayoría de las transacciones,

aún sufre de las debilidades inherentes del modelo basado en confianza. Las transacciones completamente no reversibles no son realmente posibles, debido a que las instituciones financieras no pueden evitar la mediación en disputas. El costo de la mediación incrementa los costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de realizar pequeñas transacciones casuales, existiendo un costo mayor por esta pérdida y la imposibilidad de hacer pagos no reversibles por servicios no reversibles. Con la posibilidad de revertir, la necesidad de confianza se expande. Los comerciantes deben tener cuidado de sus clientes, molestándoles pidiendo más información de la que se necesitaría de otro modo. Un cierto porcentaje de fraude se acepta como inevitable. Estos costos e incertidumbres en los pagos pueden ser evitados si la persona utiliza dinero físico, pero no existe un mecanismo para hacer pagos por un canal de comunicación sin un tercero confiable. Lo que se necesita es un sistema de pagos electrónicos que esté basado en pruebas criptográficas en vez de en confianza, permitiendo a las dos partes interesadas realizar transacciones directamente sin la necesidad de un tercero confiable. Las transacciones que son computacionalmente poco factibles de revertir protegerían a los vendedores de fraude, del mismo modo que mecanismos rutinarios de depósito de garantía podrían ser fácilmente implementados para proteger a los compradores. En este trabajo, proponemos una solución al problema del doble gasto utilizando un servidor de marcas de tiempo usuario a usuario distribuido para generar una prueba computacional del orden cronológico de las transacciones. El sistema es seguro mientras que los nodos honestos controlen colectivamente más poder de procesamiento (CPU) que cualquier grupo de nodos atacantes.

2. Transacciones:

Definimos una moneda electrónica como una cadena de firmas digitales. Cada dueño transfiere la moneda al próximo al firmar digitalmente un hash de la transacción previa y la clave pública del próximo dueño y agregando ambos al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad.

El problema está en que el beneficiario no puede verificar si alguno de los dueños previos no hizo un doble gasto de la moneda. La solución común es introducir una autoridad central confiable, una especie de casa de la moneda, que revisaría si cada transacción tiene doble gasto o no. Después de cada transacción, la moneda debe ser devuelta a la casa de la moneda para generar una nueva moneda, de modo que solo las monedas generadas directamente por esta casa de la moneda, son en las que se confían de no tener doble-gasto. El problema con esta solución es que, el destino del sistema monetario entero, depende de la compañía que

gestiona la casa de la moneda, con todas las transacciones teniendo que pasar por ellos, tal y como actuaría un banco. Por tanto, necesitamos encontrar una forma para que el beneficiario pueda saber que los dueños previos no firmaron ninguna transacción anterior. Para nuestros propósitos, la transacción última o más temprana es la que cuenta, así que no nos importarán otros intentos de doble gasto posteriores. La única forma de confirmar la ausencia de una transacción es estando al tanto de todas las transacciones existentes. En el modelo de la casa de la moneda, era ésta casa la que estaba al tanto de todas las transacciones y decidiría cuales llegaban primero. Para lograr esto sin un tercero confiable, las transacciones deben ser anunciadas públicamente, y necesitaremos de un sistema de participantes que estén de acuerdo en una historia única, del orden en que éstas transacciones fueron recibidas. El beneficiario necesita saber que en el momento de cada transacción, la mayoría de los nodos estuvieron de acuerdo en cuál fue la primera que se recibió.

3. Servidor de marcas de tiempo:

La solución que proponemos comienza con un servidor de marcas de tiempo. Un servidor de marcas de tiempo funciona al realizar el hash de un bloque de datos a ser fechados y publicándolo ampliamente, tal y como se haría en un periódico o en una publicación de Usenet. La marca de tiempo prueba que el dato, obviamente, debió de haber existido en ese momento para poder incluirse dentro del hash. Cada marca de tiempo incluye en su hash la marca de tiempo previa, formando una cadena, de modo que cada marca de tiempo adicional refuerza las anteriores a una dada.

4. Prueba de trabajo:

Para implementar un servidor de marcas de tiempo siguiendo un esquema usuario-a-usuario, necesitaremos utilizar un sistema de prueba de trabajo similar al Hashcash de Adam Back [6], en vez de usar una publicación en un periódico o en Usenet. La prueba de trabajo implica la exploración de un valor, tal que, al calcular un hash, como SHA-256, éste empiece con un número determinado de bits con valor cero. El trabajo promedio requerido será exponencial al número de bits requeridos con valor cero pero que puede ser verificado ejecutando un solo hash.

Para nuestra red de marcas de tiempo implementamos la prueba de trabajo incrementando el valor de un campo nonce, perteneciente al bloque, hasta que se encuentre un valor que dé el número requerido de bits con valor cero para el hash del mismo. Una vez que el esfuerzo de

CPU se ha gastado para satisfacer la prueba de trabajo, el bloque no puede ser cambiado sin rehacer todo el trabajo. A medida que más bloques son encadenados después de uno dado, el trabajo para cambiar un bloque incluiría rehacer todos los bloques después de éste.

La prueba de trabajo también resuelve el problema de determinar cómo representar la decisión por mayoría. Si ésta mayoría se basara en un voto por dirección IP, podría ser alterada por alguien capaz de asignar muchas IPs. La prueba de trabajo equivale esencialmente a “una CPU igual a un voto”. La decisión de la mayoría es representada por la cadena más larga, la cual posee la prueba de trabajo con mayor esfuerzo invertido. Si la mayoría del poder de CPU está controlada por nodos honestos, la cadena honesta crecerá más rápido y dejará atrás cualquier otra cadena que esté compitiendo. Para modificar un bloque en el pasado, un atacante tendría que rehacer la prueba de trabajo del bloque y de todos los bloques posteriores, y luego alcanzar y superar el trabajo de los nodos honestos. Luego demostraremos que la probabilidad de que un atacante más lento pueda alcanzar a la cadena más larga, disminuye exponencialmente a medida que más bloques subsecuentes son incorporados.

Para compensar el incremento de la velocidad del hardware y el interés variable de ejecutar nodos en el tiempo, la dificultad de la prueba de trabajo es determinada por una media móvil dirigida por un número promedio de bloques a la hora. Si estos se generan muy rápido, la dificultad se incrementa.

5. La Red:

Los pasos que ejecuta la red son los siguientes:

Las transacciones nuevas son emitidas a todos los nodos.

Cada nodo recolecta nuevas transacciones en un bloque.

Cada nodo trabaja en encontrar una prueba de trabajo difícil para su bloque.

Cuando un nodo encuentra una prueba de trabajo, emite el bloque a todos los nodos.

Los nodos aceptan el bloque si todas las transacciones en el bloque son válidas y no se han gastado ya.

Los nodos expresan su aceptación del bloque al trabajar en crear el próximo bloque en la cadena, utilizando el hash del bloque aceptado como hash previo.

Los nodos siempre consideran la cadena más larga como la correcta y empiezan a trabajar en extenderla. Si dos nodos emiten versiones diferentes del próximo bloque simultáneamente, algunos nodos puede que reciban uno o el otro primero. En ese caso, trabajan en el primero que reciban pero guardan la otra rama en caso de que esta se vuelva más larga. El empate se

rompe cuando se encuentra la próxima prueba de trabajo y una rama se vuelve más larga; los nodos que estaban trabajando en la otra rama posteriormente se cambian a la que ahora es más larga.

Las emisiones de nuevas transacciones no necesariamente necesitan llegar a todos los nodos. En el momento que éstas llegan a muchos nodos, acabaran entrando en un bloque antes de que pase mucho tiempo. La emisión de los bloques también es tolerante a la pérdida de mensajes. Si un nodo no recibe un bloque, lo pedirá cuando reciba el próximo bloque y se dé cuenta que perdió uno.

6. Incentivo:

Por convención, la primera transacción en el bloque es una transacción especial que genera una nueva moneda cuyo dueño es el creador del bloque. Esto agrega un incentivo para que los nodos apoyen a la red, y provee una forma inicial de distribuir y poner en circulación las monedas, dado que no hay una autoridad para crearlas. Esta adición estable de una cantidad constante de monedas nuevas, es análoga a los mineros de oro que gastan recursos para ponerlo en circulación. En nuestro caso, los recursos son el tiempo de CPU y la electricidad que se gastan.

El incentivo también puede establecerse con los costes de transacción. Si el valor de salida de una transacción es menor que la entrada, la diferencia será una tarifa de transacción que se añadirá al valor del incentivo del bloque que la contiene. Una vez que un número predeterminado de monedas han entrado en circulación, el incentivo puede evolucionar enteramente a tarifas de transacción y estar completamente libres de inflación.

El incentivo también puede ayudar a animar a los nodos a mantenerse honestos. Si un atacante egoísta es capaz de reunir más potencia de CPU que todos los nodos honestos, éste tendría que elegir entre utilizarlo para defraudar a la gente robando sus pagos, o usarlo para generar monedas nuevas. Debería encontrar más rentable jugar siguiendo las reglas, ya que éstas lo favorecerán con más monedas que combinando a todos los demás nodos, que socavar el sistema y la validez de su propia riqueza.

7. Reclamando espacio en disco:

Una vez que la última transacción está enterrada bajo suficientes bloques, las transacciones gastadas anteriores a esta pueden ser descartadas para ahorrar espacio en disco. Para facilitar

esto sin romper el hash del bloque, las transacciones se comprueban en un árbol de Merkle[26], con solo la raíz incluida en el hash del bloque. Los bloques viejos pueden compactarse al sacar ramas del árbol. Los hashes interiores no necesitan ser guardados.

La cabecera de un bloque sin transacciones será de unos 80 bytes. Si suponemos que cada bloque se genera cada 10 minutos, 80 bytes * 6 * 24 * 365 = 4.2MB por año. Con ordenadores vendiéndose generalmente con 2GB de RAM en 2008, y la ley de Moore prediciendo un crecimiento actual de 1.2GB por año, el almacenamiento no debe ser un problema aun si las cabeceras de los bloques deben permanecer en memoria.

8. Verificación de Pagos Simplificada:

Es posible verificar pagos sin ejecutar un nodo de red completo. Un usuario solo necesita mantener una copia de las cabeceras de los bloques de la cadena más larga de la prueba de trabajo, la cual puede obtenerse haciendo una búsqueda en los nodos de la red hasta que esté convencido de tener la cadena más larga, y obtener la rama del árbol de Merkle, que enlaza la transacción con el bloque en que ha sido fechado. Aunque no puede verificar la transacción por sí mismo, al enlazarla a algún lugar de la cadena, puede ver que algún nodo de la red la ha aceptado, de modo que los bloques añadidos después confirmarían aún más esta aceptación por parte de la red.

Como tal, la verificación es confiable a medida que los nodos honestos controlen la red, pero se vuelve más vulnerable si la red es dominada por un atacante. Mientras que los nodos de la red puedan verificar las transacciones por sí mismos, el método simplificado puede ser engañado por transacciones fabricadas por un atacante mientras éste pueda dominar la red. Una estrategia para protegerse es aceptar alertas de los nodos de la red cuando detecten un bloque inválido, pidiéndole al usuario que se baje el bloque completo y las transacciones alertadas para confirmar la inconsistencia. Los negocios que frecuentemente reciban pagos, querrán ejecutar sus propios nodos para tener una seguridad más independiente y una verificación más rápida.

9. Combinando y dividiendo valor:

Aunque sería posible manipular monedas individualmente, sería difícil de manejar el hacer transacciones separadas por cada céntimo de una transferencia. Para permitir que el valor se

[26] Un árbol hash de Merkle es una estructura de datos en forma árbol, binario o no, en el que cada nodo está etiquetado con el hash de la concatenación de las etiquetas o valores de sus nodos hijo.

divida y se combine, las transacciones contienen múltiples entradas y salidas. Normalmente habrá o una sola entrada, de una transacción previa más grande, o múltiples entradas combinando cantidades más pequeñas, y al menos dos salidas: una para el pago, y una para devolver el cambio, si es que hay alguno, de vuelta al emisor.

Hay que tener en cuenta que este sistema se abre el abanico, de modo que una transacción puede depender de varias transacciones, y esas a su vez depender de muchas más, lo que no es ningún problema. Nunca existe la necesidad de extraer una copia completa única de la historia de las transacciones.

10. Privacidad:

El modelo bancario tradicional, logra su nivel de privacidad, al limitar el acceso a la información a las partes involucradas y al tercero de confianza. La necesidad de anunciar todas las transacciones públicamente se opone a este método, pero la privacidad aún puede mantenerse rompiendo el flujo de información en otro lugar: manteniendo las claves públicas anónimas. Públicamente puede verse que alguien está enviando una cierta cantidad a otra persona, pero sin información que relacione la transacción con nadie en particular. Esto es similar al nivel de información que se muestra en las bolsas de valores, donde el tiempo y el tamaño de las transacciones individuales, la “cinta”, son públicos, pero sin decir quiénes son las partes.

Como un cortafuego adicional, un nuevo par de claves debe utilizarse para cada transacción de modo que puedan asociarse a un dueño en común. Son inevitables algunos tipos de asociación con transacciones de múltiples entradas, las cuales pueden revelar que sus entradas pertenecen al mismo dueño. El riesgo estaría en que si el dueño de una clave se revela, entonces el enlazado podría revelar otras transacciones que pertenecieron al mismo dueño.

11. Cálculos:

Consideramos el escenario en el que un atacante intenta generar una cadena alterna más rápido que la cadena honesta. Aún si esto se lograse, no abriría el sistema a cambios arbitrarios, tales como crear valor del aire o tomar dinero que nunca perteneció al atacante. Los nodos no aceptarían una transacción inválida como pago, y los nodos honestos nunca aceptaran un bloque que las contenga. Un atacante puede únicamente intentar cambiar solo sus propias transacciones para retomar dinero que ha gastado recientemente.

La carrera entre una cadena honesta y la cadena de un atacante puede ser caracterizada como un Camino Binomial Aleatorio. El evento de éxito es la cadena honesta siendo extendida en un bloque adicional e incrementado su ventaja en +1, y siendo el evento de fracaso que la cadena del atacante sea extendida en un bloque reduciendo la distancia en -1.

La probabilidad de que un atacante pueda alcanzarnos, desde un déficit dado, es análogo al problema de la Ruina del Jugador. Supóngase que un jugador con crédito ilimitado empieza en déficit y juega potencialmente un número infinito de intentos para intentar llegar a un punto de equilibrio. Podemos calcular la probabilidad de que llegase al punto de equilibrio, o que llegue a alcanzar a la cadena honesta, como sigue:

p = probabilidad de que un nodo honesto encuentre el próximo bloque

q = probabilidad de que el atacante encuentre el próximo bloque q

Qz = probabilidad de que el atacante llegue a alcanzar desde z bloques atrás.

Dada nuestra hipótesis de que p > q, la probabilidad cae exponencialmente mientras que el número de bloques que el atacante debe alcanzar incrementa. Con las probabilidades en contra, si no hace una jugada afortunada desde el principio, sus oportunidades se vuelven extremadamente pequeñas a medida que se queda más atrás.

Ahora consideremos cuánto necesita esperar el beneficiario de una nueva transacción antes de tener la certeza suficiente de que el emisor no puede cambiarla. Asumimos que el emisor es un atacante el cual quiere hacer creer al beneficiario que se le pagó durante un rato, luego cambiar la transacción para pagarse a sí mismo de vuelta una vez que ha pasado un tiempo. El beneficiario será alertado cuando esto suceda, pero el emisor espera que sea demasiado tarde.

El beneficiario genera un nuevo par de claves y entrega la clave pública al emisor poco después de hacer la firma. Esto previene que el emisor prepare una cadena de bloques antes de tiempo, y pueda estar trabajando en ella continuamente hasta que tenga la suerte de adelantarse lo suficiente, y luego ejecutar la transacción en ese momento. Una vez que la transacción es enviada, el emisor deshonesto empieza a trabajar en secreto en una cadena paralela que contiene una versión alterna de su transacción.

El beneficiario espera a que la transacción sea añadida a un bloque y que z bloques hayan sido enlazados después de la transacción. No necesitará saber la cantidad exacta de progreso que ha logrado el atacante, pero asumiendo que los bloques honestos tardaron el promedio

esperado por bloque, el progreso potencial del atacante será una distribución de Poisson con un valor esperado.

Para obtener la probabilidad de que el atacante aún pueda alcanzarnos ahora, multiplicamos la densidad de Poisson por la cantidad de progreso que pudo haber hecho por la probabilidad de que pudiera alcanzar ese punto:

Re-organizamos para evitar la suma de la cola infinita de la distribución…

Convertimos a código en C…

Ejecutamos algunos resultados, podemos ver que la probabilidad cae exponencialmente con z.

q=0.1 - z=0 P=1.0000000 hasta z=50 P=0.0000006

Resolvemos para P menor que 0.1%…

P > 0.001 q=0.45 z=340

12. Conclusiones:

Hemos propuesto un sistema de transacciones electrónicas que no dependen de la confianza. Comenzamos con el marco habitual de monedas hechas en base al uso de firmas digitales, el cual provee un fuerte control de la propiedad, pero que está incompleto sino existe una forma de prevenir el doble gasto. Para solucionarlo, proponemos una red usuario a usuario que utiliza la prueba de trabajo para registrar una historia pública de transacciones y que rápidamente se convierte en computacionalmente irresoluble para un atacante que quiera cambiarla, si los nodos honestos controlan la mayoría del poder de CPU. La red es robusta por su simplicidad no estructurada. Los nodos pueden trabajar todos al mismo tiempo con poca coordinación. No necesitan ser identificados, dado que los mensajes no son enrutados a ningún lugar en particular y solo necesitan ser entregados bajo la base del mejor esfuerzo. Los nodos pueden ir y volver de la red a voluntad, aceptando la cadena de prueba de trabajo como prueba de lo que sucedió mientras estuvieron ausentes. Votan con su poder de CPU, expresando su aceptación de los bloques válidos al trabajar extendiendo y rechazando bloques inválidos al reusar trabajar en ellos. Cualquier regla necesaria o incentivos pueden hacerse cumplir con este mecanismo de consenso.

2. Anexo 2

Contratos inteligentes:

Es un programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas. Es decir, cuando se da una condición programada con anterioridad, el contrato inteligente ejecuta automáticamente la cláusula correspondiente.

Los contratos inteligentes llevan desarrollándose desde 1993, cuando el famoso criptógrafo Nick Szabo acuñó el término por primera vez. Nick propuso este sistema de contratos por aquel entonces, sin embargo la infraestructura tecnológica del momento lo hacía inviable. Era necesario un sistema de pagos que los pudiese llevar a la práctica y esa situación no apareció en escena hasta la creación del Bitcoin en el año 2009.

No obstante, Bitcoin no estaba pensado para nada más que ser una herramienta financiera: una criptomoneda. Pero la tecnología con la que funcionaba, el blockchain, sí que hacía posible estos contratos inteligentes y fue a principios de 2014, con la creación de Ethereum, cuando pasaron a ser una realidad.

Estos contratos inteligentes “viven” en una atmósfera no controlada por ninguna de las partes implicadas en el contrato, en un sistema descentralizado. Esto significa que se programan las condiciones, se firman por ambas partes implicadas y se “coloca” en una blockchain para que no pueda modificarse. Teniendo como objetivos principales: Implementar un estado de seguridad mayor al del contrato tradicional, reducir costes y reducir el tiempo asociado a este tipo de interacciones. En otras palabras, buscan mejorar los contratos actuales siendo más seguros, más baratos, ahorrando tiempo y evitando fraudes.

A diferencia de los contratos tradicionales el lenguaje no es natural, sino que es un lenguaje virtual, un lenguaje de programación informática. Esto hace que en el modo de cumplimiento no haya diferentes puntos de vista, sino una única lectura: Si se da la condición establecida, el contrato ejecuta automáticamente la consecuencia a dicha acción. Ósea que no requiere de un intermediario, como por ejemplo un notario, ya que el contrato en sí mismo es el intermediario de confianza, reduciendo así los costes y el tiempo de las interacciones.

¿Cómo funcionan los contratos inteligentes?

Tomando como ejemplo una máquina expendedora de comida, esta está programada para que cuando alguien introduzca cierta cantidad de dinero y pulse una combinación de números, automáticamente el producto seleccionado salga de la máquina para ser de la persona. Otra orden que podría tener programada es la de que, en caso de haber introducido más dinero del que costaba el producto, la máquina devuelva el cambio, o de que en caso de no haber un producto seleccionado marque en la pantalla “producto agotado”.

Ésta programación de la máquina es lo que sería el contrato inteligente, y las partes implicadas serían la máquina y la persona. Las reglas del contrato inteligente son las mismas reglas mencionadas anteriormente y que son ejecutadas por sí solas si se cumplen las acciones correspondientes y el lenguaje informático funciona con una sentencia llamada “if-then”, que significa “si… entonces…”, la cual simboliza que: “si se cumple el acuerdo… entonces se da la condición determinada”.

Volviendo al ejemplo anterior, el acuerdo sería algo así: Si se cumple que el usuario introduce dinero suficiente y pulsa la combinación ‘032’, entonces saldrá la botella de agua. Si se cumple que el usuario ha introducido más dinero que el necesario, entonces se le devuelve la diferencia. Si el usuario introduce el dinero y pulsa ‘032’ pero no hay artículo, entonces poner mensaje de “producto agotado”.

De esta forma funciona un contrato inteligente, pero añadiendo muchas posibilidades, por ejemplo añadir que “si se acaba el producto ‘032’… entonces” -de forma autónoma y automática- la máquina mandará una señal al proveedor de botellas de agua para que vaya a reponerlas. Eliminando a un intermediario que tiene que estar vigilando la máquina y así disminuyendo los costes de tiempo y dinero en dicho proceso y simplificando la tarea.

Otro ejemplo podría ser en el caso de un hotel, el contrato inteligente podría establecer que si se ha pagado hasta el día 30 del mes en curso y las normas del hotel son que se tiene que salir antes de las 11:00 am, la tarjeta funcionará hasta el día 30 a las 11:00. Esto mismo haría posible sistemas similares a los de empresas como por ejemplo Airbnb o Uber, pero sin su mediación ni sus comisiones. Produciéndose toda la interacción entre la gente interesada, la cual ahorraría las comisiones de dichas plataformas y el tiempo de gestión.

A través del siguiente gráfico se puede entrever la lógica empresarial de los contratos inteligentes:

Fuente: BBVA Research

Función de "oráculo":

Este término hace referencia a un tercero, es decir una persona de confianza que puede ser establecida como quien determinará como se resolverá el contrato. Por ejemplo en el caso de que dos personas apuesten entre sí, en un partido de futbol, podrían determinar en el contrato que una vez terminado el partido sea otra persona, alguien de confianza para ambos, quien determine quién ganó la apuesta. Como aclaración, al utilizarse el sistema Ethereum la apuesta solo puede realizarse en ether, no pudiéndose usar ningún otro medio de pago.

Continuando con el caso del ejemplo anterior, también podría establecerse que el contrato se resuelva automáticamente buscando el mismo sistema el resultado del partido en la web, una vez cumplido el horario establecido.

Como alternativa al tercero que hace de intermediario en la cadena, hay proyectos que actúan como portadores de información, como por ejemplo Oraclize, un programa que combina todos los portales de información que sean indicados en el contrato y en función de los resultados que obtenga, tomará su decisión final.

Función multifirma:

Es una función a través de la cual dos o más partes se deben de poner de acuerdo para hacer cumplir las condiciones del contrato. Por ejemplo un curso de un secundario en el que quieren juntar dinero para irse de viaje a fin de año, el contrato inteligente bloqueará los fondos hasta que se cumplan las condiciones del contrato, en las cuales se podría establecer que todos o determinada cantidad de personas deban aprobar la extracción, haciendo así que ninguno se pueda apoderar de la totalidad del dinero.

Depósitos dobles:

Esta es una característica de los contratos inteligentes que hace que funcionen correctamente, eliminando al intermediario del proceso, aun en casos de las partes no se conozcan entre sí y carezcan de confianza.

Este contrato les obliga a depositar en una dirección de la cadena de bloques unos fondos para el cumplimiento del contrato y que tiene una duración determinada, y si no llegan a un acuerdo, el contrato inteligente mandará directamente los fondos que ambas partes tuvieron que abonar a otra dirección de la cadena de bloques de la que nadie podrá sacarlos nunca. Lo que hace esta condición es forzar a cumplir a cada uno con su parte del contrato. De lo contrario, los fondos desaparecerían.

Usos de los contratos inteligentes de Ethereum:

A continuación se mencionarán algunos de los posibles usos que se le podrían dar:

En servicios financieros:

• Préstamos: si la persona que contrata el préstamo no realiza el pago en el tiempo estipulado, se ejecutaría el contrato para retirarle las garantías.

• Liquidación de operaciones: los contratos calculan importes de liquidación y transfiere fondos automáticamente.

• Pagos de cupones y bonos: los contratos calculan y pagan automáticamente de forma periódica los cupones y devuelve el capital al vencimiento de los bonos.

• Microseguros: Calculan y transfieren micropagos basados en datos de uso de un dispositivo conectado a Internet (por ejemplo, un seguro automotriz de pago por uso)

• Depósito en garantía en el registro de la propiedad: el contrato supervisa la información externa a la cadena de bloques y una vez transferida la propiedad de un vendedor a un comprador, el contrato ingresa automáticamente los fondos al vendedor.

• Herencias: una vez que el contrato puede verificar el fallecimiento de la persona, automáticamente las propiedades quedan repartidas y asignadas entre los herederos.

• Automatización de pagos y donaciones: se pueden acordar pagos o donaciones periódicas o puntuales a personas o entidades. El contrato inteligente lo que haría es verificar que se cumplen las reglas para realizar automáticamente la donación.

En servicios de la salud:

• Expedientes médicos electrónicos: los contratos proporcionan transferencias y accesos a los historiales médicos tras la aprobación de múltiples firmas entre pacientes y proveedores.

• Acceso a los datos sanitarios de la población: se conceden a las organizaciones de investigaciones sanitarias el acceso a determinada información sanitaria personal. A cambio, a través de los contratos, se realizan micropagos automáticamente al paciente para su participación.

• Seguimiento de la salud personal: se realiza un seguimiento de las acciones relacionadas con la salud de los pacientes a través de dispositivos “IoT” (conectados a Internet). Los contratos generan automáticamente recompensas basadas en hechos específicos.

En servicios de propiedad intelectual:

• Distribución de royalties: el contrato inteligente calcula y distribuye los pagos de royalties a artistas y otras partes asociadas según los términos acordados.

En servicios energéticos:

• Estaciones autónomas de recarga para vehículos eléctricos: el contrato procesa un depósito, habilita la estación de recarga y devuelve los fondos restantes una vez completados.

En servicios del sector público:

• Votación: valida los criterios del votante, registra el voto en la cadena de bloques e inicia acciones específicas como resultado del voto mayoritario. Esto es posible en una votación tanto a nivel de encuesta como a nivel estatal.

• Apuestas: dos o más partes pueden apostar sin que se resienta su seguridad y sin necesidad de un tercero a través de un contrato inteligente que asegure unas condiciones concretas.

• Propiedades inteligentes: una casa, un coche, una nevera, una lavadora…todos los objetos que se puedan conectar a Internet se consideran propiedades inteligentes (del inglés, smart property). Y todos pueden ser gestionados con contratos inteligentes para poder venderlos o alquilarlos de forma automatizada.

Beneficios de los contratos inteligentes de Ethereum:

Autonomía: Estos contratos se dan siempre entre una o varias personas o entes legales, pero sin ningún intermediario. No es necesario alguien que valide el contrato, como podría ser un abogado. Por ello reducen, e incluso pueden llegar a eliminar cualquier persona extra que no esté implicada en el contrato.

Costes: Al ser contratos en los que no se depende de un tercero, se reducen los costes. Menos intervención humana resulta en costes reducidos.

Confianza: Todos los contratos inteligentes van directos a la cadena de bloques. Esto hace que estén encriptados, por lo que solo las personas implicadas pueden leerlo, y permite la interacción entre personas que no se conocen entre sí sin que haya riesgo de estafa.

Velocidad: Los contratos inteligentes utilizan código de software para automatizar las tareas que de otro modo se realizarían por medios manuales. Por lo tanto, aumentan la velocidad de los procesos de negocio y son menos propensos a errores manuales.

Seguridad: Al basarse estos contratos inteligentes en la cadena de bloques pública de Ethereum no se pueden perder. Todo queda registrado de forma inmutable. Nada ni nadie lo pueden hacer desaparecer y siempre se tiene acceso a ellos. El proceso de ejecución descentralizado elimina el riesgo de manipulación, ya que la ejecución es gestionada automáticamente por toda la red, en lugar de por una parte individual.

Nuevos modelos de negocio: Los contratos inteligentes, a través de sus bajos costos para asegurar transacciones confiables, permiten nuevos tipos de negocios como el acceso automatizado a vehículos y unidades de almacenamiento.

¿Cómo crear un contrato inteligente?

Similar a los contratos en papel, que son creados por gente que conoce todo el ámbito legal alrededor de ellos, en los contratos inteligentes sería necesario conocer el código informático, llamado Solidity, o tener a alguien que sepa de ello. Como esto puede generar complicaciones se han desarrollado plataformas que gestionan la creación de los contratos inteligentes. Una de ellas es SmartContract, donde se puede crear contratos inteligentes a través de Chainlink, su propia blockchain, que hace de nexo entre Ethereum y fuentes de datos externas a éste.

Conclusión:

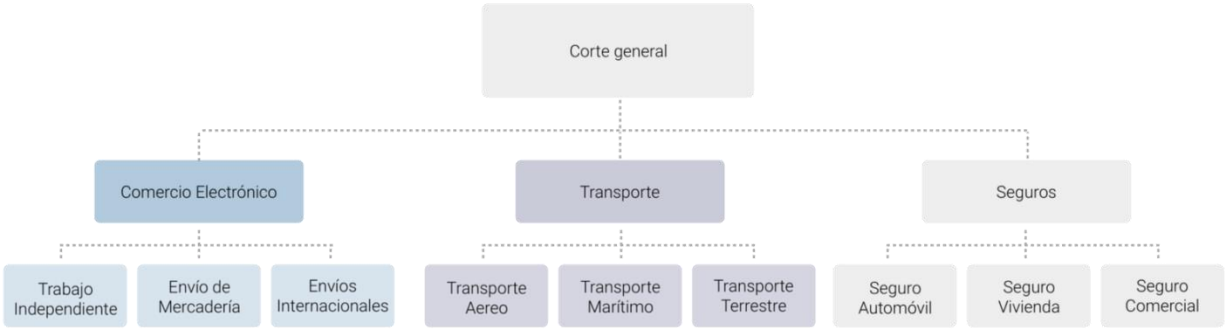
Muchos expertos sugieren que los contratos inteligentes entrarán en nuestra vida cotidiana en multitud de maneras distintas. La primera es la sustitución de los contratos tradicionales, transformándolos en plantillas estandarizadas de contratos inteligentes o fusionándose en un híbrido de papel y contenido digital donde los contratos se verifican a través de blockchain y se corroboran mediante copia física.

Sin embargo como hemos visto anteriormente a lo largo del artículo, sus usos se van a expandir a prácticamente todos los ámbitos de la vida diaria. En todas las áreas donde sea necesaria una comunicación entre dos o más partes (ya sean éstas entes vivos o máquinas) este tipo de contratos permiten que esa comunicación sea cien por cien veraz, segura, rápida y de bajo coste.

3. Anexo 3

1) El Contrato

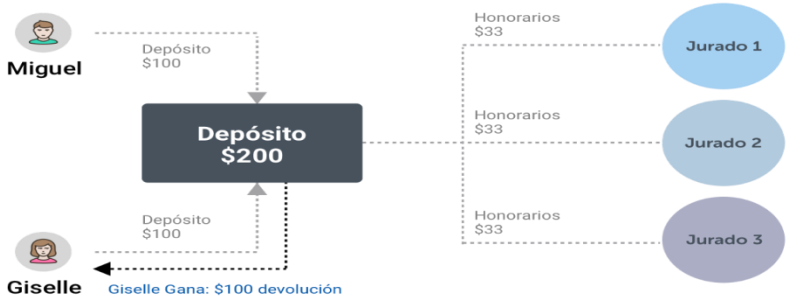
Kleros es un sistema voluntario. Para utilizarlo, el contrato entre las partes debe tener una cláusula que indique que, en caso de disputa, ésta será adjudicada en Kleros. El contrato establece en qué subcorte ocurrirá el arbitraje. Algunas se especializan en comercio electrónico. Otras en finanzas. Otras en contratos de seguros.



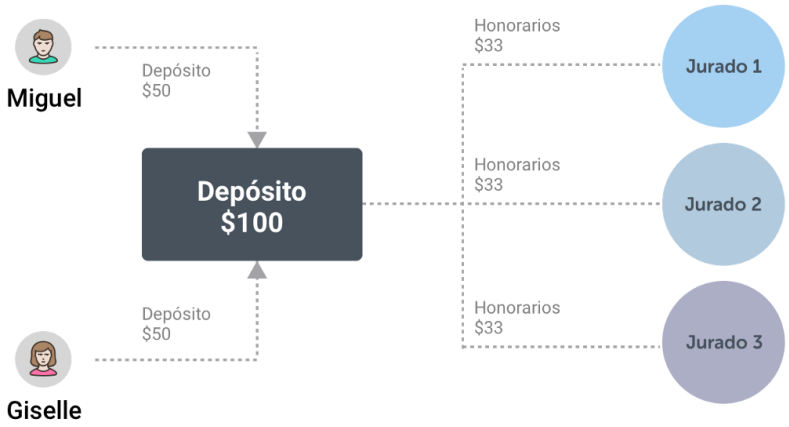
El sistema de subcortes de Kleros se compone de una raíz y diferentes ramas. La raíz es una Corte General, de donde surge una serie de ramas (subcortes). Cada subcorte se dedica a un tipo específico de disputa.

Cada subcorte tiene un valor honorario, dependiendo de la complejidad de las disputas y de la escasez de jurados con las habilidades adecuadas para resolverlas.

Desde el punto de vista de Kleros, es irrelevante quién pague los honorarios. Éstos podrían repartirse por igual entre las partes, ser pagados en su totalidad por una de ellas o por un mecanismo de seguro. Lo importante es que haya suficiente dinero para compensar al jurado por analizar las pruebas y votar un veredicto.



Modelo 1: Depósito y reintegro. El costo total de la disputa es de 100$. El contrato estipula que ambas partes realizarán un depósito cuando el caso vaya a arbitraje y que el ganador recibirá un reembolso. El jurado vota a Giselle como ganadora. El dinero depositado por el perdedor es usado para pagar los honorarios. Giselle recibe un reembolso.



Modelo 2. Ambas Partes Pagan. El contrato estipula que ambas partes compartirán el costo del arbitraje y que ninguna parte obtendrá un reembolso, sin importar quien gane.

2) Asegurando la Evidencia

El proceso comienza cuando al menos una de las partes cree que hubo un incumplimiento de contrato. Cuando esto ocurre, el contrato en formato digital y las pruebas pertinentes son enviados a Kleros con seguridad criptográfica.

El tipo de pruebas dependerá de la disputa en cuestión. En el caso Giselle vs. Miguel, puede tratarse del texto del acuerdo y los archivos digitales entregados como producto. En una disputa en unos juegos en línea donde una parte acusa a la otra de hacer trampa, la evidencia podría ser una grabación de la partida. En un conflicto por un seguro de accidente de automóvil, las pruebas podrían ser el contrato de seguro y las fotos del vehículo estrellado.

3) Selección del Jurado

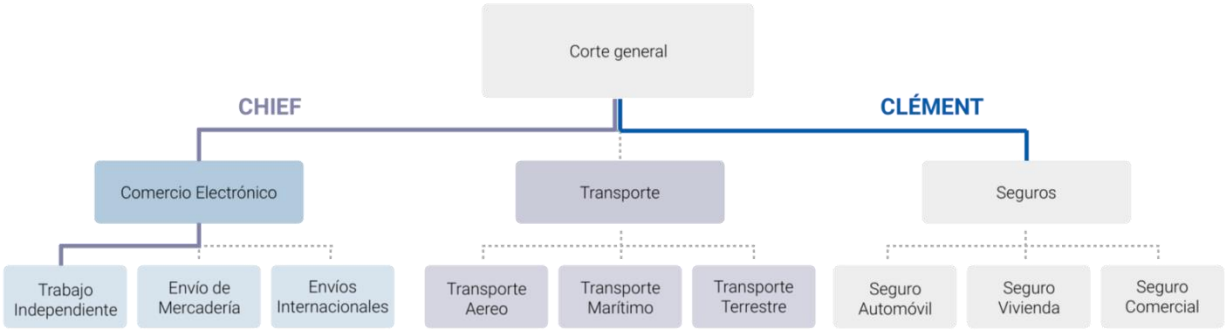
La selección del jurado se basa en dos elementos: auto postulación de candidatos y sorteo. Para evitar represalias e intimidación, los jurados no están obligados a proporcionar una prueba de identidad. (3)

El desafío clave es: ¿cómo crear los incentivos adecuados para que jurados anónimos juzguen las disputas de manera honesta?

Hace 25 siglos, los griegos entendieron que el problema puede resolverse a través de una combinación entre un token y un mecanismo de selección aleatoria. Cualquiera puede postularse como candidato a jurado en una subcorte depositando un token llamado pinakion (PNK). Éste representa la posibilidad de ser elegido como jurado en una disputa. Cuanto mayor sea la cantidad de tokens activados por un usuario, mayor será la probabilidad de que sea elegido como jurado. La selección se realiza de manera aleatoria entre todos los usuarios que activaron su token en una subcorte específica.

El mecanismo es extremadamente resistente a ataques e intentos de manipulación. Los candidatos se postulan en una subcorte, no en casos individuales. Cada subcorte tiene múltiples casos simultáneos. Un mecanismo de sorteo asigna al candidato a un caso específico. Esta forma de selección actúa como protección contra sobornos. Desde el punto de vista del atacante, una parte muy importante del dinero tendría que ser utilizada para sobornar jurados que ni siquiera acabarían formando parte del tribunal.

Una vez que los jurados han sido elegidos, los pinakion quedan congelados. Sólo serán liberados una vez que el tribunal haya emitido su veredicto.



Clément, un experto en seguros, puede ser seleccionado como jurado en la Corte General y en la Subcorte de Seguros. Chief puede ser elegido como jurado en la Corte General, en la Subcorte de Comercio Electrónico y en la Subcorte de Trabajo Independiente.

4) Análisis

Los usuarios sorteados como jurados reciben acceso a la evidencia. Ahora, cada uno tiene que analizarla y dar su veredicto. Diferentes subcortes tienen distintos parámetros respecto del procedimiento y el tiempo que los jurados tendrán para tomar una decisión, la complejidad de las opciones de votación y la posibilidad de comunicarse con las partes.

Las disputas más sencillas involucrarán sólo dos partes y dos opciones. Por ejemplo, en la disputa entre Giselle y Miguel, la decisión podría ser: “¿Quién tiene razón en la disputa? ¿Giselle o Miguel?”. Una opción algo más compleja podría ser: “De 0 a 100, ¿cuán culpable es Miguel?”.

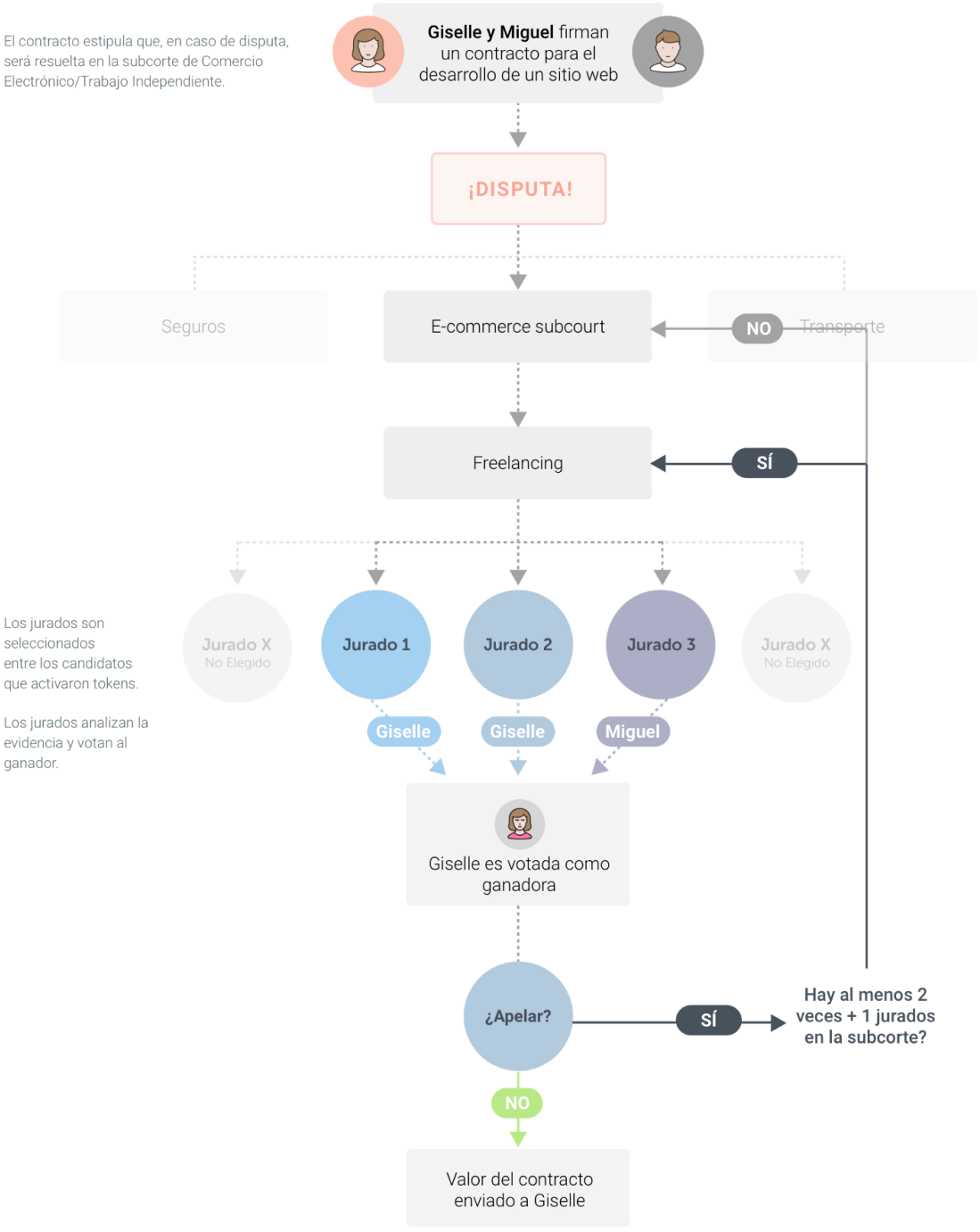
En la etapa inicial, Kleros se concentrará en disputas simples, entre dos partes y con dos opciones. A medida que la tecnología se vaya perfeccionando, el sistema será capaz de adjudicar disputas cada vez más complejas.

5) Votación

Una vez procesadas las pruebas, los jurados votan una de las opciones. Están obligados a proporcionar una justificación para su decisión. La opción ganadora es la mediana del voto de los jurados. Esta opción da un resultado consensuado y es robusta al voto estratégico.

6) Apelación

En caso de que una parte no esté conforme con la decisión, siempre tiene la posibilidad de apelar. Las sentencias pueden ser apeladas múltiples veces. En cada ronda, se forma un nuevo tribunal con el doble de jurados que en la ronda anterior más uno. La parte que apela tendrá que pagar la tasa de justicia. En caso de volver a perder, puede apelar nuevamente, siempre haciéndose cargo de los costos del proceso.



7) Redistribución de Tokens

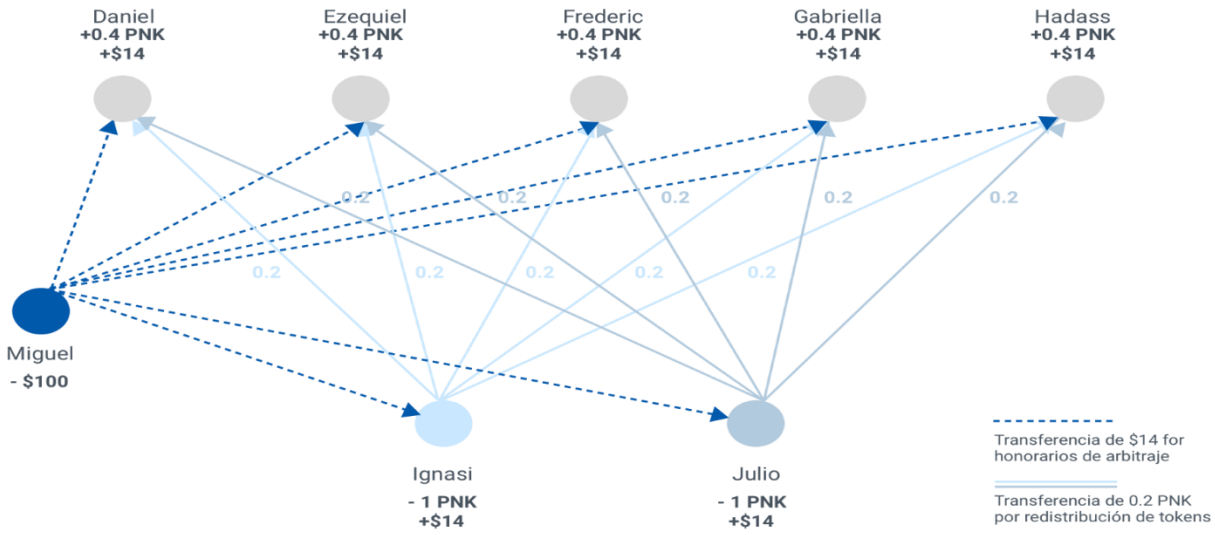
Una vez que el jurado llega a una decisión definitiva, los pinakion son descongelados y redistribuidos entre los jurados. Cada jurado ganará o perderá tokens en función de la coherencia de su voto con el de la mayoría.

La redistribución se basa en la lógica del punto focal o Schelling Point, concepto desarrollado por Thomas Schelling, experto en teoría de los juegos y Premio Nobel de Economía 2005. Schelling llamó punto focal a una solución que los agentes tienden a utilizar para coordinar su comportamiento en ausencia de comunicación o cuando las partes no confían en la otra.

Si los jurados fueron seleccionados correctamente, si tenían acceso a la misma evidencia y si tenían los incentivos correctos, el concepto de punto focal sostiene que deberían llegar a un veredicto similar sobre el mismo caso. Según este concepto, los jurados que votaron de manera incoherente con el resto no estaban debidamente calificados (se postularon en una subcorte para la que no tenían suficiente conocimiento) o no realizaron un análisis apropiado (tal vez, votaron demasiado rápido, sólo para cobrar sus honorarios).

Los incentivos de los jurados vienen de dos fuentes: 1) Los honorarios de arbitraje, que todos los jurados reciben por igual, como compensación por el tiempo invertido en analizar evidencia y votar; 2) La redistribución de pinakion desde los jurados que votaron de manera incoherente hacia los que votaron de manera coherente.

Imaginemos que la disputa entre Giselle y Miguel fue resuelta con 7 jurados. Ignasi y Julio, que votaron de manera diferente a la mayoría, pierden sus tokens. Estos son redistribuidos entre los jurados que votaron de manera coherente. El efecto neto sobre cada jurado dependerá de la diferencia entre el valor de los honorarios ganados y el valor de los tokens perdidos.



Miguel, declarado perdedor en la disputa contra Giselle, pierde su depósito de $100, que se utiliza para pagar honorarios a todos los miembros del jurado. Ignasi y Julio, los dos jurados que votaron incoherentemente con los demás, pierden su pinakion, que son transferidos a los jurados que votaron de manera coherente. Daniel, Ezequiel, Frédéric, Gabriela y Hadass, los jurados que votaron coherentemente, ganan honorarios y tokens. Ignasi y Julio, los jurados que votaron incoherentemente, ganan honorarios pero pierden tokens.

Como de costumbre, algunos usuarios intentarán abusar del sistema. Pero Kleros es robusto contra ataques. Manny lo aprendió de la peor manera. Él siempre se había considerado el más listo del barrio. Cuando descubrió Kleros, vio una oportunidad de ganar algo de dinero fácil. Compró unos pinakion y comenzó a activarlos en subcortes que pagaban altos honorarios de arbitraje. Por supuesto que, cuando era elegido como jurado, ni siquiera se molestaba en leer la evidencia. Sólo votaba al azar, recaudaba los honorarios y pasaba a otra disputa.

Algunas semanas después de empezar con su “brillante plan”, Manny descubrió que estaba perdiendo dinero. Aunque ganaba en honorarios de arbitraje, como su voto era a menudo incoherente, sistemáticamente perdía pinakion. A cabo de unas semanas, se dio cuenta de que el efecto neto era negativo y abandonó el plan.

El pinakion es un elemento crítico del sistema porque proporciona los incentivos para que Kleros produzca decisiones verdaderas. La expectativa de ganar o perder tokens brinda a los usuarios un incentivo a postularse en las subcortes donde realmente tienen experiencia, a analizar las pruebas cuidadosamente y a votar honestamente. Un jurado que escoge los casos

equivocados, que no analiza cuidadosamente la evidencia o que no vota honestamente sufrirá una pérdida económica.

Kleros: un Protocolo de Justicia Multipropósito

Aunque en este artículo se utiliza el ejemplo de una disputa de desarrollo de software, Kleros es capaz de adjudicar una amplia gama de casos. Algunos comenzarán a funcionar en un futuro inmediato. Otros sólo serán viables en un plazo mayor.

Arbitraje de Pequeñas Disputas

A comienzos de los años '60, el 11,5% de los casos presentados en tribunales estadounidenses llegaba a juicio. En 2002, era sólo el 1,8%. El declive no se debe a que haya menos disputas, sino a la creciente utilización de procesos alternativos de resolución.

En las últimas décadas, con el fin de recortar el presupuesto de administración de justicia, distintos gobiernos promovieron el uso de la resolución alternativa de conflictos (ADR) en áreas tales como disputas comerciales, protección al consumidor y empleo. Algunas aplicaciones de Kleros incluirán arbitrajes de pequeñas demandas como fraudes de tarjeta de crédito, reclamos de consumo y en alquileres de vivienda. Los casos se decidirían en línea y la ejecución estará a cargo del gobierno, al igual que los arbitrajes voluntarios tradicionales.

Trabajo Independiente

El mercado de trabajo está mutando desde las relaciones tradicionales empleador-empleado a contratos a distancia y flexibles con proveedores independientes (Friedman 2005). El caso de Giselle vs. Miguel explicado más arriba es una típica disputa con un freelancer.

La tecnología de Kleros podría contribuir de manera notable a ampliar las oportunidades de trabajadores de todo el mundo, especialmente los de países con marcos jurídicos débiles. Un cliente de Alemania o Estados Unidos podría contratar servicios de programación o diseño a trabajadores independientes de Vietnam, Zimbabwe o Bolivia. En caso de disputa, Kleros podrá brindar un servicio de arbitraje que actualmente no existe. Esto aumentará significativamente las oportunidades de ser contratados para trabajadores de países con marcos jurídicos débiles.

Financiamiento Colectivo

El crowdfunding (financiamiento colectivo) es una creciente fuente de recursos para equipos emprendedores. Esto plantea una serie de preocupaciones sobre la capacidad del equipo de cumplir con los resultados prometidos a los patrocinadores.

Un equipo emprendedor realiza una ronda de crowdfunding para financiar el desarrollo de un software. El acuerdo indica que los fondos serán transferidos una vez que se alcancen ciertos hitos de desarrollo. El próximo pago se realizará después del lanzamiento de la versión 2 del producto. Sin embargo, una vez que el equipo presenta el software, algunos patrocinadores reclaman: “Esto es realmente la versión 1 con algunas modificaciones menores”.

Kleros podría constituir un jurado para analizar la evidencia y tomar una decisión. Para esto, los contratos de crowdfunding del futuro podrían tener a Kleros como mecanismo de decisión sobre el cumplimiento de hitos de un proyecto.

Social Media

A medida que las interacciones sociales empiezan a ocurrir online, problemas de acoso, invasión de privacidad e información falsa se vuelven cada vez más importantes. Pueden causar graves pérdidas reputacionales y monetarias, así como daños psicológicos.

Soushiant y Uri están teniendo una discusión en una plataforma de social media. Uri denuncia a Soushiant por un comentario que viola los términos y condiciones de la plataforma. Soushiant responde: “Mi comentario no violó los términos y condiciones. No es mi culpa si Uri es demasiado sensible”. La evidencia es analizada por un jurado en Kleros. El jurado decide que el comentario de Soushiant violó los términos y condiciones. La plataforma quita a Soushiant 20 puntos de reputación.

Propiedad Intelectual

En un futuro no muy lejano, plataformas descentralizadas de música como Ujo Music permitirán a los artistas subir música a la nube y recibir pagos a través de contratos inteligentes. Esto generará reclamos vinculados con infracciones a derechos de autor.

Imaginemos que la banda de rock The Misfits carga su nueva canción en Ujo Music. Otra banda, The Holograms, afirma que ésta viola sus derechos de autor. En plataformas centralizadas como YouTube, el reclamo se resuelve a través de un algoritmo propietario como Content ID, que bloquea los contenidos identificados como una violación a derechos de autor.

Una solución más transparente sería tomar la decisión a través de un jurado de Kleros: “The Holograms son los propietarios de los derechos de la canción. Todos los ingresos que ésta genere serán redirigidos a su cuenta”.

Juegos en Línea

League of Legends es un videojuego en línea con más de 100 millones de jugadores mensuales. El Campeonato del Mundo de 2016 repartió más de 6 millones de dólares en premios. Con tanto dinero en juego, es necesario asegurarse de que la competencia se desarrolle de manera limpia.

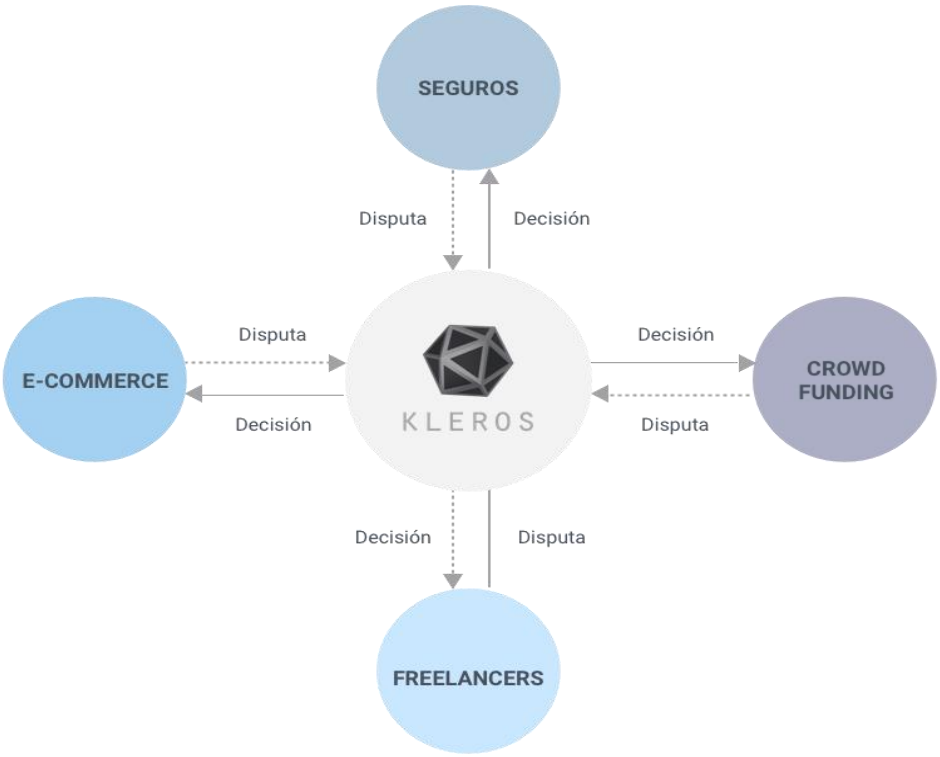
Los creadores desarrollaron un sistema que usa a miembros voluntarios de la comunidad para detectar y castigar a jugadores tramposos. Las sanciones van desde una advertencia hasta la expulsión. Valve, otra empresa de videojuegos, implementó Overwatch, un sistema similar. El desarrollo de un sistema de detección y castigo de jugadores tramposos en línea es otra aplicación clave de Kleros.

Un Sistema de Justicia para la Internet Descentralizada

Una parte cada vez mayor de nuestras vidas ocurre en línea. Nuestras interacciones sociales y económicas están mediadas por plataformas globales que conectan a productores de contenido, consumidores y anunciantes (Facebook y YouTube), compradores y vendedores (Amazon y eBay), conductores y pasajeros (Uber), y viajeros y anfitriones (Airbnb).

Algunos creen que, en los próximos años, la tecnología de blockchain permitirá el surgimiento de modelos distribuidos y propiedad de los usuarios de estas mismas plataformas. Realizaremos transacciones en versiones descentralizadas de eBay (Open Bazaar), contrataremos viajes en un Uber descentralizado (Arcade City), escucharemos música en un Spotify descentralizado (Ujo Music), contrataremos trabajadores en un Upwork descentralizado (Ethlance) y nos conectaremos en redes sociales descentralizadas (Steemit).

La visión de Kleros es construir una red descentralizada de jurados para adjudicar disputas en diferentes industrias. De esta forma, se convertirá en una parte fundamental de la infraestructura de la próxima generación de Internet.



La visión de Kleros es convertirse en una red de adjudicación descentralizada para un amplio número de disputas.

Los contratos inteligentes son acuerdos escritos en código que se ejecutan automáticamente cuando se cumplen las condiciones predefinidas. Sin embargo, la ejecución automática contradice un principio básico de la filosofía del derecho: todos los contratos son incompletos. En el momento en que se firma, ningún contrato puede prever todas las posibles situaciones que pudieran ocurrir hasta el momento de la ejecución. A veces, la aplicación estricta podría derivar en una situación injusta.

Los griegos llamaron epikeia a un principio moral que eximía a un ciudadano del cumplimiento de una ley o contrato para ser fiel a su espíritu. Los sistemas jurídicos modernos reconocen que una parte puede ser relevada de la obligación de cumplimiento si tal obligación se ha vuelto irrazonable después de un cambio de circunstancias.

La adopción masiva de contratos inteligentes requiere de la implementación de un mecanismo de “escotilla de escape”. Pero, ¿cómo crear una escotilla de escape sin introducir un tomar de decisiones centralizado que represente un nuevo punto único de falla en el sistema?

Kleros puede ofrecer esta solución: una escotilla de escape descentralizada, un método de corrección de errores para revocar contratos inteligentes cuando el cumplimiento se ha vuelto irrazonable. Una escotilla de escape que funciona sin reintroducir arbitrariedad y corrupción en el sistema. Esto permitirá extender el uso de contratos inteligentes a un número creciente de industrias.

Conclusión

El comercio electrónico crece a un ritmo de dos dígitos. Se espera que alcance un mercado de 2 billones de dólares en 2020. Se estima que la economía colaborativa alcanzará un valor de 335 mil millones de dólares en 2025. El Banco Mundial prevé que el uso del crowdfunding para la compra de acciones alcanzará un mercado de 96 mil millones de dólares anuales sólo en los países en desarrollo hacia 2025.

Los sistemas jurídicos de la era de los estados nacionales fueron exitosos en la creación de un marco institucional para el crecimiento económico y la prosperidad social. Frente a la revolución digital, sin embargo, están alcanzando sus límites de complejidad. En el contexto de la nueva economía, los sistemas legales requieren un profundo replanteo. Pero son pocos los que investigan la infraestructura legal desde una perspectiva sistémica.

Los abogados investigan lo que es la ley. Los economistas estudian lo que la ley debería ser para cumplir con objetivos como la promoción del comercio. Pero casi nadie estudia lo que determina la eficacia del derecho como un sistema (Hadfield 2015: 215).

La incapacidad de los sistemas legales para resolver las disputas de la era de la Internet llevó a plataformas como eBay o Alibaba a desarrollar sus propios mecanismos de arbitraje. Sin embargo, más allá de estas iniciativas aisladas para resolver problemas específicos, no ha surgido ningún sistema horizontal que pueda aplicarse en todos los ámbitos y que pueda beneficiarse de una mayor especialización a lo largo del tiempo. Kleros busca convertirse en este sistema.

Aunque se basa en tecnologías de punta como el blockchain, la criptografía, la teoría de los juegos y la inteligencia colectiva, su lógica ya era conocida por los griegos hace 25 siglos: la justicia puede ser hecha entre pares.

Las criptomonedas están contribuyendo a la causa de la inclusión financiera. La inclusión de justicia es un objetivo igualmente importante. Así como el bitcoin democratiza el acceso a servicios financieros. La promesa de Kleros es la democratización de la justicia para todos.

Glosario

Altcoin: Toda criptomoneda que no sea el bitcoin.

Ataque del 51%: Cuando más de la mitad del poder de cómputo de un blockchain es controlado por un único agente, éste puede realizar transacciones maliciosas contra la red.

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

Bitcoin: La primera criptomoneda basada en tecnología de blockchain. Fue creada por una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto en 2009.

Blockchain: Registro compartido entre múltiples computadoras donde las transacciones se registran en bloques unidos con una cadena criptográfica.

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: Instrucciones escritas en forma de código en una red descentralizada, que se ejecutan tras la ocurrencia de cierto evento.

Criptografía: Del griego kryptós (secreto) y graphein (escritura), es una disciplina que se ocupa de la construcción de protocolos para garantizar la confidencialidad, la integridad y la autenticidad de los datos.

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 open source que opera de manera autónoma y tiene sus datos almacenados en el blockchain. Son muy importantes dentro del blockchain de Ethereum.

DAO: Una organización autónoma descentralizada es como una corporación que corre sin intervención humana y que opera a través de una serie de reglas de negocio imposibles de modificar por una sola persona.

Desintermediación: Proceso de reducción del uso o necesidad de intermediarios. En el contexto del blockchain, se refiere a la reducción de la necesidad de terceras partes intermediarias para la validación y facilitación de transacciones.

Doble gasto: Ocurre cuando un activo digital es gastado más de una vez.

Explorador de Bloques: Herramienta online que sirve para visualizar transacciones en el blockchain.

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.

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.

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: Computadoras de la red de blockchain encargadas de validar las transacciones. Los mineros agrupan transacciones individuales en bloques y los difunden al resto de la red para que formen parte del registro compartido. Por su contribución, reciben comisiones de transacción y pagos en criptomoneda.

Multisig: Dirección de bitcoin que provee una capa extra de seguridad al requerir que más de una llave firme una transacción para que ésta sea realidad.

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

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.

Registro centralizado: Registro mantenido por un agente central.

SHA-256: Algoritmo criptográfico utilizado por criptomonedas como el bitcoin.

Wallet: Archivo que almacena llaves privadas. Contiene un cliente de software que permite un acceso para ver y crear transacciones en un blockchain.

Bibliografía

Ashford, W. (19 de Julio de 2018). *searchdatacenter.techtarget.com*. Recuperado el 18 de Septiembre de 2018, de https://searchdatacenter.techtarget.com/es/noticias/252444452/Cuidado-con-los-puntos-ciegos-de-seguridad-en-blockchain-advierte-RSA

Ast, F. (20 de Septiembre de 2017). *medium.com*. Recuperado el 15 de Julio de 2018, de https://medium.com/kleros/kleros-un-protocolo-de-justicia-para-internet-920c28a588f1

Atmira. (s.f.). *atmira.com.* Recuperado el 21 de Julio de 2018, de http://www.atmira.com/documents/10180/43613278/BLOCKCHAINBROCHURE.pdf/10a9bdde-e9c6-4461-bdeb-ee523c7edce8

Banco Mundial. (19 de Noviembre de 2016). *bancomundial.org*. Recuperado el 19 de Julio de 2018, de http://www.bancomundial.org/es/topic/financialinclusion/overview

BBVA. (5 de Diciembre de 2017). Recuperado el 28 de Junio de 2018, de https://www.bbva.com/es/historia-origen-blockchain-bitcoin/

Carballo, I. (23 de Abril de 2018). *eleconomista.com.ar*. Recuperado el 18 de Julio de 2018, de https://www.eleconomista.com.ar/2018-04-nuevo-mapa-la-inclusion-financiera/

ComunicaRSE. (28 de Marzo de 2018). *comunicarseweb.com.ar*. Recuperado el 14 de Julio de 2018, de http://www.comunicarseweb.com.ar/noticia/tecnologia-blockchain-para-la-inclusion-financiera-de-zonas-vulnerables

Decentraland. (s.f.). Recuperado el 22 de Julio de 2018, de https://decentraland.org/

Diariobitcoin. (27 de Mayo de 2018). *diariobitcoin.com*. Recuperado el 15 de Julio de 2018, de https://www.diariobitcoin.com/index.php/2018/05/27/el-gobierno-chino-ordena-un-desarrollo-mas-rapido-de-blockchain/

Endeavor. (2018). *Insight blockchain ¿La promesa de una revolución?* México D. F.

Estrada, J. (6 de Junio de 2018). *infobae.com*. Recuperado el 14 de Julio de 2018, de https://www.infobae.com/cripto247/bitcoin/2018/06/06/el-bid-invirtio-118-millones-en-una-app-para-combatir-la-pobreza-en-la-villa-31/

Ethereum. (s.f.). *ethereum.org*. Recuperado el 8 de Julio de 2018, de https://www.ethereum.org/

Ethereum. (s.f.). *ethereumdapps.net*. Recuperado el 8 de Julio de 2018, de http://ethereumdapps.net/2018/07/07/lider-de-blockchain-de-ibm-latinoamerica-la-tecnologia-tendra-una-de-las-tasas-de-crecimiento-mas-rapidas-hasta-el-ano-2021/

Eude Business School. (19 de Enero de 2018). *eude.es*. Recuperado el 25 de Junio de 2018, de http://blog.eude.es/la-tecnologia-blockchain-aplicaciones-en-finanzas

Fernandez, J. (18 de Agosto de 2018). *hablemosdeempresas.com*. Recuperado el 23 de Septiembre de 2018, de https://hablemosdeempresas.com/empresa/que-es-una-ico/

Ferraris, J. C. (3 de Julio de 2018). *canal-ar.com.ar*. Recuperado el 22 de Julio de 2018, de http://www.canal-ar.com.ar/26095-Argentina-tendra-una-Plataforma-Federal-de-Blockchain-De-que-se-trata.html

Fraga, A. (9 de Junio de 2018). *ticbeat.com*. Recuperado el 14 de Julio de 2018, de http://www.ticbeat.com/tecnologias/estos-son-los-tipos-de-blockchain-que-existen-y-asi-puedes-usar-cada-uno-de-ellos/

Fred. (19 de Agosto de 2016). *infocoin.net*. Recuperado el 9 de Julio de 2018, de http://infocoin.net/2016/08/29/proyecto-r3-de-blockchain-es-patentado-en-nueva-york/

Garcia, C. (19 de Julio de 2018). *criptonoticias.com*. Recuperado el 20 de Julio de 2018, de https://www.criptonoticias.com/banca-seguros/banco-central-argentina-busca-aprender-blockchain-criptomonedas/

Georges, J. (2017). *La cadena de bloques: Una tecnología disruptiva con el poder de revolucionar el sector financiero.* Informe técnico, EquiSoft.

Gómez, R. (12 de Julio de 2018). *criptonoticias.com*. Recuperado el 17 de Julio de 2018, de https://www.criptonoticias.com/mercado-cambiario/abra-habilita-compra-bitcoins-visa-mastercard-cualquier-parte-mundo/

González, G. (18 de Julio de 2018). *criptonoticias.com*. Recuperado el 19 de Julio de 2018, de https://www.criptonoticias.com/adopcion/gobierno-chile-lanza-piloto-uso-blockchain-proceso-compras-publicas/

Gupta, M. (2017). *Blockchain for dummies.* John Wiles and Sons Inc.

Harvard Business Reviev. (9 de Marzo de 2017). *hbr.es*. Recuperado el 28 de Junio de 2018, de https://hbr.es/tecnolog/497/breve-historia-de-blockchain-y-del-largo-futuro-que-nos-espera-juntos

Hyperledger. (s.f.). *hyperledger.org/abou*t. Recuperado el 01 de Septiembre de 2018, de https://www.hyperledger.org/about

IBM. (12 de Marzo de 2018). *ibm.com*. Recuperado el 25 de Junio de 2018, de https://www.ibm.com/developerworks/ssa/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

IG. (s.f.). *ig.com*. Recuperado el 20 de Julio de 2018, de https://www.ig.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas

Infocoin. (12 de Abril de 2018). *infocoin.net*. Recuperado el 4 de Julio de 2018, de http://infocoin.net/2018/04/12/europa-aspira-a-ser-lider-en-tecnologia-blockchain/

Infotechnology. (5 de Octubre de 2017). *infotechnology.com*. Recuperado el 15 de Julio de 2018, de https://www.infotechnology.com/online/Que-son-las-ICO-las-ofertas-iniciales-de-criptomonedas-20171005-0005.html

Jaimovich, D. (26 de Marzo de 2018). *infobae.com*. Recuperado el 15 de Julio de 2018, de https://www.infobae.com/tecno/2018/03/26/nydro-el-airbnb-energetico-con-acento-argentino/

Labarta, P. (24 de Mayo de 2018). *infotechnology.com*. Recuperado el 12 de Julio de 2018, de https://www.infotechnology.com/online/La-millonaria-empresa-argentina-que-esta-trabajando-para-hacer-un-Bitcoin-inteligente-20180524-0002.html

Leal, A. (30 de Junio de 2018). *criptonoticias.com*. Recuperado el 3 de Julio de 2018, de https://www.criptonoticias.com/registros-notarias/corte-china-acepta-registros-blockchain-evidencia-caso-demanda/

Lopardo, L. (2 de Septiembre de 2018). *lanacion.com.ar*. Recuperado el 27 de Septiembre de 2018, de https://www.lanacion.com.ar/2167831-negocios-mundo-desafio-exportar-contexto-volatil

Lopez, G. (8 de Noviembre de 2017). *diariobitcoin.com*. Recuperado el 2 de Julio de 2018, de https://www.diariobitcoin.com/index.php/2017/11/08/funcionario-ruso-blockchain-cambiara-la-industria-del-turismo-en-el-pais/

Magas, J. (18 de Junio de 2018). *cointelegraph.com*. Recuperado el 2 de Julio de 2018, de https://es.cointelegraph.com/news/smart-cities-and-blockchain-four-countries-where-ai-and-dlt-exist-hand-in-hand

Martínez, J. (6 de Junio de 2016). *elespanol.com*. Recuperado el 30 de Septiembre de 2018, de https://www.elespanol.com/economia/empresas/20160606/130487135_0.html

Matus, D. (2 de Enero de 2018). *digitaltrends.com*. Recuperado el 8 de Julio de 2018, de https://es.digitaltrends.com/negocios/que-es-ethereum-criptomoneda/

Mendez, I. (22 de Noviembre de 2017). *firmadopor.wordpress.com*. Recuperado el 21 de Julio de 2018, de https://firmadopor.wordpress.com/2017/11/22/la-tecnologia-blockchain-y-los-derechos-de-autor/

Montoya, G. (2017). *Blockchain: mirando más allá del Bitcoin.* técnico, Asobancaria.

Murua, H. (7 de Marzo de 2018). *clarin.com*. Recuperado el 22 de Julio de 2018, de https://www.clarin.com/economia/argentinos-blockchain_0_rJhSUST_f.html

Oliveros, J. (7 de Julio de 2018). *criptotendencia.com*. Recuperado el 21 de Julio de 2018, de https://criptotendencia.com/2018/07/09/blockchain-y-los-derechos-de-autor/

OpenExpo Europe. (12 de Diciembre de 2017). *openexpoeurope.com*. Recuperado el 27 de Junio de 2018, de https://openexpoeurope.com/es/caracteristicas-de-blockchain/

Perez, I. (24 de Octubre de 2017). *criptonoticias.com*. Recuperado el 22 de Julio de 2018, de https://www.criptonoticias.com/adopcion/boletin-oficial-argentina-certifica-ediciones-digitales-blockchain/

Preukschat, A. (2017). *Blockchain: La revolución industrial de internet.* España: Gestión 2000.

PwC. (2017). *Blockchain, a catalyst for new appraches in insurance.*

PwC. (2018). *The Developing Role of Blockchain.*

PWC Global. (s.f.). *pwc.com*. Recuperado el 22 de Septiembre de 2018, de https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html

Revoredo, A. (5 de Noviembre de 2017). *gestion.pe*. Recuperado el 21 de Julio de 2018, de https://gestion.pe/blog/cyberlaw/2017/11/derechos-de-autor-y-blockchain.html?ref=gesr

Rooney, K. (28 de Agosto de 2018). *cnbc.com*. Recuperado el 22 de Septiembre de 2018, de https://www.cnbc.com/2018/08/27/84percent-of-companies-are-dabbling--in-blockchain-new-survey-says-.html

Rosa, F. d. (11 de Abril de 2018). *criptonoticias.com*. Recuperado el 4 de Julio de 2018, de https://www.criptonoticias.com/adopcion/paises-asociacion-europea-blockchain/

RSK. (s.f.). *rsk.co*. Recuperado el 13 de Julio de 2018, de https://www.rsk.co/

Russ, G. (12 de Mayo de 2018). *tecnologia.press*. Recuperado el 2 de Julio de 2018, de https://www.tecnologia.press/2018/05/02/el-gobierno-de-dubai-revela-el-registro-comercial-de-blockchain/id=rusbell/

sandoval, J. (19 de Agosto de 2016). *criptonoticias.com*. Recuperado el 21 de Julio de 2018, de https://www.criptonoticias.com/colecciones/herramientas-registro-derechos-de-autor-blockchain/

Sandoval, J. (17 de Mayo de 2017). *criptonoticias.com*. Recuperado el 14 de Julio de 2018, de https://www.criptonoticias.com/aplicaciones/aragon-network-impulso-organizaciones-autonomas-descentralizadas/

Santander Río. (s.f.). *santanderrio.com.ar.* Recuperado el 30 de Septiembre de 2018, de https://www.santanderrio.com.ar/banco/wcm/connect/2ea2c3d0-6310-4dcd-91eb-6c85fffd8a89/TyC-MonederoTag.pdf?MOD=AJPERES&ContentCache=NONE

Shen, M. (2 de Junio de 2018). *coindesk.com*. Recuperado el 3 de Julio de 2018, de https://www.coindesk.com/the-russian-military-is-building-a-blockchain-research-lab/

Soto, J. (21 de Marzo de 2018). *eleconomista.com.mx*. Recuperado el 19 de Julio de 2018, de https://www.eleconomista.com.mx/tecnologia/IBM-ofrecera-servicios-de-blockchain-en-America-Latina-desde-Sao-Paulo-20180321-0029.html

Sputnik. (28 de Marzo de 2018). *sputniknews.com*. Recuperado el 3 de Julio de 2018, de https://mundo.sputniknews.com/russia-elections-2018-news/201803271077374872-rusia-tecnologia-elecciones/

Tapscott, D. (2017). *La revolución blockchain.* (J. M. Salmerón, Trad.) Buenos Aires: Valletta.

Velázquez, K. (18 de Septiembre de 2018). *marketing4ecommerce.mx*. Recuperado el 23 de Septiembre de 2018, de https://marketing4ecommerce.mx/banco-de-mexico-regulara-las-criptomonedas-y-el-blockchain/

Wikipedia. (s.f.). *wikipedia.org*. Recuperado el 8 de Julio de 2018, de https://es.wikipedia.org/wiki/Ethereum