Universidad de San Andrés

Escuela de Administración y Negocios

Magister en Gestión de Servicios Tecnológicos y de Telecomunicaciones

Smart Contracts descentralizados como facilitadores de gestión

Autor: Tarek Fuad O'Neill Said

DNI: 94.921.109

Director del Trabajo de Graduación: Alejandro Prince

Buenos Aires, de Febrero de 2019

ÍNDICE

1 INTRODUCCIÓN

Internet permitió que la interacción corporativa se realice dentro de un entorno digital, las empresas intercambian información o realizan transacciones de manera electrónica en mayor medida. Pero si bien hay circunstancias en las que estas interacciones funcionan de manera fluida y directa, como cuando se envía un correo electrónico, tenemos videoconferencias o realizamos trabajos de manera colectiva, por otro lado existen procesos que marchan de forma lenta, es decir, no al paso acelerado que necesitamos.

La integración de los procesos de negocio a través de las organizaciones se convierte en un proceso crítico en el momento que depende de alguien más que cumpla su parte o cada que necesitamos poner en otra persona nuestra confianza. La manera tradicional en la que se refuerzan las reglas de los acuerdos, se articulan las tareas y cómo se controla la transferencia de valor o los activos, requiere de un mínimo de confianza para que la transacción sea comercialmente viable y en la mayoría de los casos necesitamos poner esta confianza en una o varias entidades basados sólo en su reputación reputación; sea en un banco, corporación auditora, entidad reguladora u otro humano. Existen muchos casos en los que estas entidades comparten datos sensibles o cometen fraudes para beneficiar a una u otra organización o no brindan la privacidad necesaria.

La falta de confianza entre las compañías es en la mayoría de los casos un impedimento o un problema que puede frenar las negociaciones y ejecución fluida de las tareas. Esta fricción asociada con la administración normal de los acuerdos en papel en un ecosistema As-A-Service donde existen múltiples proveedores puede llegar a ser agobiante y consecuentemente los acuerdos funcionan en teoría pero no siempre en la práctica ya que no permiten por ejemplo realizar ajustes automáticos cuando cambia una tarifa de un bien o servicio. Muchas veces estos costos se estiman a futuro como cuando una aerolínea compra el combustible a una tarifa durante todo el año de acuerdo a las estimaciones de cómo prevé que será el

precio promedio del mercado durante el año. En este sentido, sería mucho más sensato pensar que los precios se ajustan automáticamente de acuerdo al precio de mercado, pero estas condiciones son muy difíciles de modificar en el ecosistema tradicional.

El poder disruptivo de la tecnología del Bitcoin que nace con el protocolo y la tecnología Blockchain, representa una oportunidad para modificar los procesos actuales en la medida que permite a los ecosistemas interactuar directamente a través una red peer-to-peer excluyendo los intermediarios y formar una comunidad sin control de un organismo central.

La tecnología Blockchain permite desintermediar, compartir y realizar transacciones de información de forma descentralizada a través de una red de participantes en los cuales prescinde de confiar pues la confianza está dada por el sistema mismo. La red Blockchain puede ser usada para encontrar un acuerdo compartido acerca del estado de las partes colaboradoras sin necesidad de confiar en una sola autoridad central de manera que podría eliminar procedimientos burocráticos que ralentizan las operaciones.

Uno de los aspectos más prometedores dentro de esta tecnología son los contratos inteligentes (en inglés *smart contracts*). Estos son un código de computadora escrito dentro de una Blockchain o libro contable distribuido que especifica las acciones del acuerdo. Por ejemplo, estos contratos pueden incluir los términos y condiciones, tareas a realizar y penalidades con el objetivo de verificar y reforzar esas condiciones y de ser necesario aplicar de forma automática penalidades u otros términos específicos del acuerdo cuando hay un cambio en el servicio, como así también, pueden automatizar los pagos entre las partes.

2 PROBLEMÁTICA

Indiscutiblemente la mayoría las empresas realizan los pagos a través de un intermediario, más de 10.000 instituciones financieras de 212 países del mundo utilizan la red SWIFT para el envío de mensajes o la red FEDWIRE para realizar transacciones entre entidades bancarias y que estas posteriormente realicen el "settlement" lo cual concluye con el traslado del dinero, es tanto ya una costumbre como un absurdo el tener que esperar desde un viernes en la tarde hasta el próximo día laboral para que todo este proceso se realice y en ocasiones puede que suceda algún error y el pago no llegue porque las empresas se encuentran en lugares geográficos diferentes y utilizan diferentes monedas locales.

Si dos o más empresas intercambian información que requiere cierto nivel de confianza entre ellas para la ejecución de transacciones o acuerdos legales, la integración de los procesos de negocio a través de estas organizaciones se convierte en un proceso crítico pues depende de alguien más que cumpla su parte.

La falta de confianza entre éstas, es en en la mayoría de los casos un impedimento o un problema que puede frenar las negociaciones y ejecución fluida de las tareas.

Muchas de las empresas que por ejemplo se basan en una arquitectura orientada al servicio aún no aprecian el potencial que las redes de blockchain tienen para mejorar sus procesos, todavía es poco evidente que ya está disponible una infraestructura computacional para correr programas autónomos descentralizados llamados smart contracts o incluso correr aplicaciones descentralizadas (DAPPS) que pueden ser utilizadas en conjunto para hacer más eficiente la gestión empresarial. Creemos que parte del problema radica en que es poco claro el surgimiento y potencial de las diferentes plataformas existentes como son Ethereum, Rootstock de Argentina, Eris Industries, Codius, Symbiont, Bitt, Bitshares, y soluciones sobre la red de bitcoin como el Lightning Network, entre otras, pueden tener casos de uso disponibles aplicables que harían funcionar a las

empresas de una manera más "neuronal", eliminando no sólo fricción en los procesos sino también en los de auditoría, financieros o de almacenamiento y distribución de la información y permisos.

Siendo esta una maestría en administración de servicios tecnológicos y de telecomunicaciones, es de nuestro interés saber el rol que esta nueva tecnología va a tener en la gestión empresarial del futuro. Por ejemplo, un caso de uso que nació junto con el concepto de los smart contracts en una blockchain es el de las organizaciones autónomas descentralizadas, (DAO por sus siglas en inglés) con un fundamento interesante que pretende eliminar la mayoría de los procedimientos burocráticos, empoderar a la gente en la toma de decisiones y darles mayor participación financiera en ocasiones por medio de fichas o tokens que se comportan de la misma manera que una acción de una empresa. Este tipo de organizaciones prometen ser más flexibles en cuanto a su arquitectura, se podría decir que proponen un nuevo paradigma en la estructura organizacional en la medida que el nivel jerárquico y de autoridad se encuentra descentralizado entre los nodos que tienen participación una determinada participación en el sistema, se convierte en un experimento no sólo económico sino también social pues empodera al individuo que desea participar con una pequeña porción de su capital, sin tener que pasar por toda la intermediación que supondría hacer la compra de por ejemplo acciones de una empresa como Apple o Amazon en la que cualquier tipo de participación de sus accionistas nunca supone tener poder en la toma de decisiones. Las DAO se auto-organizan, pero a un nivel global e incluso existen casos de uso que nos hacen fantasear con la idea de organizaciones que no requerirán en absoluto de la participación humana. Se hace crítico tener un sistema de gobierno acorde a esta nueva estructura que ayude con el problema de tener a tantas personas con el poder de tomar decisiones, esto lo hace mucho más difícil ponerlos de acuerdo, pero tal vez esto no sea un problema si no una ventaja, ya que podría requerir de un consenso real entre las partes interesadas.

Habiendo participado personalmente en la pre venta de los tokens de la primera organización autónoma descentralizada (The DAO)[1], parece interesante escribir al respecto pues es un caso relevante dentro del ecosistema blockchain y de las criptomonedas, batió el record como el proyecto que logró recaudar la mayor cantidad de dinero hasta el año 2016 por la vía del crowdfunding[2] (aproximadamente 160 millones de dólares en una criptomoneda llama ether). The DAO sufrió ataque a tan sólo a un par de semanas de haber sido lanzado y tuvo consecuencias devastadoras, fue abandonado y muchas personas perdieron grandes cantidades de dinero.

Fue evidente que al ecosistema le falta evolución y todavía no está lo suficientemente listo para que una solución como esta sea implementada en este momento en el mundo real. Por estos motivos, consideramos la relevancia de la presente investigación académica y los hallazgos que pueda descubrir, manteniéndonos agnósticos ya que cualquier suposición sería tal vez muy prospectiva y difícil de sustentar. Además, vale la pena investigar sobre estas nuevas soluciones que ya están disponibles para su utilización y hacer una descripción del ecosistema para brindar una vista holística de soluciones disponibles que pueden ejercer un papel importante en el presente y futuro del management empresarial.

3 OBJETIVOS

El objetivo general del presente estudio es describir la tecnología de los smart contracts, determinar el actual grado de adopción y analizar las fortalezas y debilidades que presenta detallando sus posibles oportunidades y amenazas.
El trabajo contempla los antecedentes tecnológicos y económicos que dan origen a

[1] https://en.wikipedia.org/wiki/The_DAO_(organization)
[2] https://en.wikipedia.org/wiki/List_of_highest_funded_crowdfunding_projects

los smart contracts, la situación actual del ecosistema y los principales drivers necesarios para alcanzar la masa crítica que permita la vinculación a largo plazo con la comunidad y las organizaciones.

Como objetivos específicos planteamos:

a. Describir la tecnología de los smart contracts analizando los cambios que presenta este proceso de innovación en la economía y en los negocios.
b. Describir el alcance, posibilidades y mejoras en los modelos de negocio que permiten desarrollar los smart contracts.
c. Definir el estado de situación de los smart contracts y los desafíos para la adopción y difusión a nivel global.
d. Describir y evaluar los principales casos de uso que utilizan smart contracts dentro de su core business.
e. Describir respecto al proceso de adopción de los smart contracts, cuáles serán los posibles escenarios donde mayormente serán utilizados en el corto, mediano y largo plazo.
f. Realizar un análisis FODA de los smart contracts
g. Esbozar un roadmap para la tecnología de los smart contracts.

4 HIPÓTESIS

La creación de los smart contracts, dentro de las cadenas de bloques descentralizadas con mayor índice de adopción, han permitido ofrecer un cambio en el paradigma económico y empresarial mediante nuevos modelos de negocio que facilitan los mecanismos de intercambio en operaciones complejas.

5 PREGUNTAS DE INVESTIGACIÓN

¿Qué tipo de innovación tecnológica representan los smart contracts en la economía y los negocios?

¿Cuáles son las distintas posibilidades y mejoras que ofrecen los smart contracts?

¿Cuáles son las fortalezas, oportunidades, debilidades y amenazas que plantean los smart contracts?

¿Cómo se describen los nuevos modelos de negocio mediante los smart contracts?

¿Cuál es el estado de situación de los smart contracts respecto el grado de adopción tecnológica y el nivel de difusión a escala global?

¿Cuáles son los principales casos de uso de los smart contracts dentro de su core business?

¿Cuál es el roadmap de los smart contracts de acuerdo a las opiniones de los distintos referentes de la industria tecnológica?

6 METODOLOGÍA

El paradigma de la tesis es cualitativo, cuantitativo y se utiliza triangulación metodológica. Si tenemos en cuenta las características de ambos paradigmas, podemos determinar que el paradigma cualitativo es el más indicado para este trabajo, sin embargo, realizamos esfuerzos metodológicos a fin de cuantificar las características principales del modelo mediante un marco de trabajo académico que se ajusta a la economía y administración de negocios.

Es un proyecto de investigación exploratorio destinado a comprender:

- La tecnología de los Smart Contracts
- El estado de adopción
- Planificación del desarrollo, sus beneficios y debilidades haciendo uso de herramientas propias del management y la economía.

Se utilizarán las siguientes fuentes como mecanismo de triangulación para dinamizar los objetivos planteados:

- Marco teórico y reseña bibliográfica
- Información de tendencias y estadísticas
- Análisis y descripción de casos de negocio
- Entrevistas a los principales referentes académicos y expertos de la industria

7 MARCO TEÓRICO

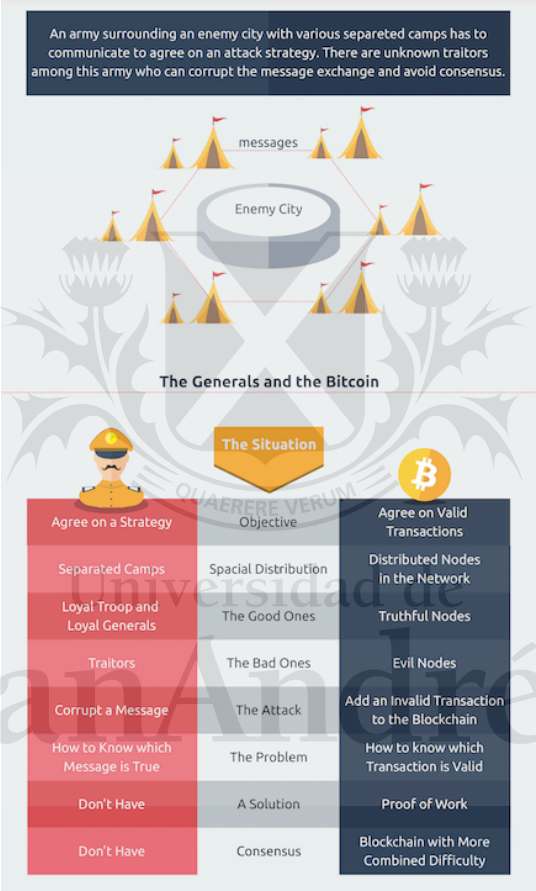
7.1 Bitcoin

A continuación, describimos una breve historia sobre el origen del Bitcoin y de la plataforma tecnológica Blockchain que permite la utilización del mismo.

El bitcoin es una moneda digital descentralizada concebida en el 2009. El término bitcoin se aplica tanto al software como a la red o protocolo de intercambio que utiliza. Las transacciones que se realizan prescinden de intermediarios y utiliza software de código abierto mantenido por la comunidad. La moneda no está respaldada por una institución central, está soportada por una red distribuida peer-to-peer (p2p) donde la estabilidad y confiabilidad del sistema recae en el uso de técnicas criptográficas y algoritmos que aseguran la veracidad de las transacciones.

El mayor avance tecnológico de la criptomoneda consistió en haber alcanzado el hito de crear un elemento digital escaso, con esto resuelve el problema del doble gasto en un sistema descentralizado gracias a un método llamado Proof-of-Work

que a su vez resuelve a lo que se le llama el problema del general bizantino. Este término proviene de la descripción de una situación donde las partes involucradas deben llegar a un acuerdo acerca de una misma estrategia para no fallar pese a que algunas de las partes pueden ser corruptas y/o deseminar falsa información o simplemente no son de confiar.



Fuente: Patrícia Estevão[3]

Es decir, que imposibilita el gasto del mismo bitcoin más de una vez por la misma persona (dando lugar por ejemplo a la falsificación). La solución radica en la utilización de un servidor de tiempo distribuido, por parte de la red de intercambio, que identifica y ordena secuencialmente las transacciones e impide su modificación.

[3] https://www.bitcoindesigned.com/infographics/bitcoin-and-the-byzantine-generals-problem/

En este sentido, se puede comparar la transferencia de una moneda digital con el endoso de un cheque: una persona escribe en el dorso el destinatario y la cantidad de dinero, y este puede a su vez endosarlo nuevamente. Además, es posible determinar la trazabilidad, es decir, conocer si la persona emisora del cheque era su dueño o receptor de endosos previos.

La analogía del cheque es posible de replicarla mediante firmas digitales y funciones hash criptográficas. En el momento que una persona transfiere dinero digital a otra, se crea una transacción, con una firma digital y un hash criptográfico (el sistema almacena un historial de transacciones realizadas con ese dinero) y la clave pública del destinatario. Luego, el destinatario verifica la firma digital contra la transacción utilizando el hash suministrado. Esto permite al destinatario determinar si el emisor era realmente es el dueño del dinero y a su vez habilitarlo a realizar nuevas transferencias con su clave privada.

El historial de todas las transacciones de bitcoins permanece almacenado en la cadena de bloques (conocida como blockchain), una base de datos distribuida que mantiene el registro de todas las transacciones en cada uno de los múltiples nodos que integran la red. Estos nodos son computadoras ejecutando el software de bitcoin en todo el mundo, conectadas entre sí por medio de Internet. El esquema descentralizado de comunicación P2P de la red Bitcoin impide establecer un control centralizado de todo el sistema. Esto imposibilita el aumento arbitrario de la base monetaria (la cantidad de bitcoins en circulación) y cualquier otro tipo de manipulación del valor por parte de una autoridad centralizada (Nakamoto, 2008; Antonopoulos, 2017; Belt, 2018; O'Keeffe, 2018).

7.1.1 Direcciones

Los usuarios que participan en la red Bitcoin poseen una billetera electrónica que contiene pares de llaves criptográficas. Las direcciones Bitcoin visibles corresponden a las llaves públicas de cada usuario que funcionan como puntos de emisión y recepción para todos los pagos. En cambio, las llaves privadas asociadas a cada llave pública sirven para que el usuario autorice pagos (transfiera bitcoins)

desde su billetera. Las direcciones públicas no tienen ninguna información sobre sus dueños, a su vez, éstas aparecen como secuencias aleatorias de números y letras de 33 ó 42 caracteres dependiendo de su formato (Nakamoto, 2008).

7.1.2 Transacciones

Cuando un usuario transfiere bitcoins a otro, el emisor renuncia a su posesión de una determinada cantidad de bitcoins, agregando la llave pública del destinatario y firmando la combinación resultante con su llave privada. Luego, la información generada se transmite a toda la red P2P como una nueva transacción. No obstante, la transacción es aceptada una vez que el resto de los nodos de la red verifican el número de bitcoins involucrados y la autenticidad de las firmas criptográficas (Nakamoto, 2008).

7.1.3 Cadena de bloques

La cadena de bloques es una lista mantenida colectivamente que contiene todas las transacciones realizadas y se encarga de agregar nuevas transacciones entre nodos. Por su parte, los nodos generadores de bitcoin se encargan de recoger todas aquellas transacciones que todavía no han sido confirmadas en un archivo llamado bloque candidato. Este archivo contiene la referencia a dichas transacciones y al último bloque válido conocido por ese nodo. Entonces, los nodos generadores compiten entre sí tratando de encontrar un hash de ese bloque, es decir, un código aleatorio que representa un esfuerzo computacional que demanda cantidades predecibles de prueba y error. Cuando un nodo encuentra la solución del bloque se transmite a toda la red. El resto de los nodos reciben al nuevo bloque solucionado, lo verifican y es agregado a la cadena.

Todas las transacciones realizadas quedan almacenadas en la cadena de bloques, esto representa una base de datos de libre acceso que contiene el historial de posesión de todas las monedas (o fracciones de monedas), desde la dirección creadora hasta la dirección del actual dueño, y se encuentra en todas las computadoras que ejecutan el software de Bitcoin.

La cadena de bloques es un registro totalmente transparente ya que cualquier usuario tiene la facultad de examinarlo en cualquier momento. Es posible analizar cualquier transacción que se haya realizado desde el lanzamiento de Bitcoin así como monitorear las nuevas transacciones en tiempo real.

De modo que, todo este proceso mencionado tiene como objetivo evitar el doble gasto que se produce cuando un usuario pretende transferir nuevamente monedas gastadas ya que la red detecta este evento y rechaza la transacción (Antonopoulos, 2017).

7.1.4 Generación de los bitcoins

Los bitcoins se generan aproximadamente cada 10 minutos y son distribuidos por la red para todos aquellos que encuentren nuevos bloques ejecutando el software de creación de bitcoins. El concepto de generar de bitcoin es conocido como minar haciendo referencia a la minería de metales preciosos.

El primer nodo generador en encontrar la solución al problema criptográfico que presenta el bloque-candidato es el que obtiene un nuevo lote de bitcoins. La probabilidad de que un usuario reciba un lote de bitcoin depende del poder computacional con el que contribuye a la red en relación al poder computacional de todos los otros nodos combinados. Los "mineros" también pueden unirse por medio de Internet para generar bitcoins en grupo, formando un "pool minero".

La cantidad de bitcoins generados por lote durante los primeros 4 años de funcionamiento de la red era de 50 BTC cada diez minutos, al cabo de 4 años pasó a ser una recompensa de 25 BTC cada 10 minutos y en el período que nos encontramos ahora 12.5 BTC y así sucesivamente hasta alcanzar la emisión de los 21 millones de bitcoin en el año 2140. A este proceso se le demonina "halfing"
Los premios o recompensas otorgados por minar están programados para que se disminuyan con el paso del tiempo, reduciendo el incremento de la base monetaria. A su vez, la cantidad de bitcoins a generarse está limitado, por diseño, a 21 millones de bitcoins. El protocolo actualiza cada dos semanas la dificultad del problema que

todos los nodos generadores están intentando resolver, ajustándola al poder computacional de toda la red.

Ante la dificultad actual para minar bitcoins mediante una computadora se crean clusters o grids de computadoras conectadas que conforman pool de minería. Por otro lado, hoy en día, la mayoría de los usuarios obtienen sus cripto-monedas en diversos marketplace a cambio de los productos que venden o en sitios de trading (O'Keeffe, 2018).

7.1.5 Economía

La base monetaria de Bitcoins está limitada ya que la cantidad total a generar es de 21 millones. Sin embargo, cada Bitcoin puede ser dividido hasta 8 decimales por lo que la oferta final de unidades comercializables es de 2,1 trillones. Se estima que el sistema dejará de producirlos hacia el año 2140.

Los costos crecientes asociados a la complejidad algorítmica para minar la moneda hasta finalmente alcanzar la oferta total de 21 millones producen una disminución en la tasa de crecimiento de la base monetaria. No obstante, el aumento en el uso del bitcoin a nivel global genera un desequilibrio monetario producido por el lado de la demanda que vuelve deflacionaria a la divisa criptográfica. Por último, las contraposiciones de ambos factores presentados provocan volatilidad en el precio del bitcoin (O'Keeffe, 2018).

7.1.6 Los determinantes del precio del Bitcoin

De acuerdo a O'Keeffe, el precio del Bitcoin y su volatilidad dependen, en gran medida, de 5 factores enumerados a continuación:

- La oferta monetaria.
- La dimensión de su alcance: el valor de toda divisa depende, en parte, de cuantos consumidores, productores y vendedores se encuentran dispuestos a aceptarla. A mayor uso, mayor su demanda y, consecuentemente, mayor su valor. Por el otro lado, a menor volumen de uso, mayor la posibilidad de que el

valor fluctúe más violentamente ya que pocos usuarios o tenedores de la moneda definen su precio.

- Las condiciones institucionales que gobiernan la comunidad virtual. En el caso del Bitcoin, el protocolo que delimita su marco de trabajo. Si una comunidad virtual brinda reglas y procedimientos claros y transparentes al mismo tiempo que ofrece medidas de seguridad efectivas, aumenta la confianza en ella y, por lo tanto, crece el valor de su moneda.
- La confianza que los usuarios tienen con su creador/emisor debido a que los pagos que se realizan a través de una moneda virtual no involucran el uso de ninguna institución financiera que actúa como intermediaria.
- Las expectativas sobre el valor futuro de la divisa y el historial de sucesos negativos (como por ejemplo la quiebra de plataformas de intercambio de las divisas criptográficas, estafas, ciberataques, etc.

Enumeramos, de forma resumida, una recopilación de ventajas que presenta la tecnología bitcoin según por los principales expertos en la materia (Tapscott, 2016; Antonopoulos, 2017; Lakhani, 2017).

7.1.7 Ventajas del Bitcoin

- Global: no pertenece a ningún estado o gobierno y se puede utilizar en todo el mundo, independientemente de las barreras geográficas y políticas de forma descentralizada. Se podría decir que es una moneda privada pues no es emitida por ningun gobierno.
- Ajeno al sistema fiduciario: no se puede crear deuda con él, su valor no depende de la intervención de un banco central.
- Descentralizado e inconfiscable: probablemente sus mejores propiedades
- Anonimato: nadie está obligado a revelar su identidad, lo que hace al bitcoin especialmente útil para su uso en países donde gobiernan regímenes totalitarios.
- Límite de emisión: el aumento decreciente y predecible de la base monetaria, le permite mejorar el poder adquisitivo de los usuarios.

- Moneda divisible: actualmente se puede utilizar hasta con 8 decimales
- Transacciones en tiempo real: en menos de una hora puede estar realizada la transacción.
- Irreversibilidad de las transacciones: No existe manera de anular una transacción una vez incluida en un bloque pues no hay un tercero en medio que tenga estos permisos. De todos modos, existen servicios que custodian los bitcoins hasta que la parte que los recibe ha cumplido con su parte del acuerdo.
- Muy poco probable de falsificar: tal como está definido no se puede construir un bitcoin falso ni efectuar un doble gasto sin que la red lo detecte.
- No hay un regulador: ningún comité de "expertos" controla el destino del bitcoin. Hay unas reglas previamente fijadas por el protocolo ideado por Satoshi Nakamoto que ha de aceptar libremente quien quiera utilizar el bitcoin.
- Económico: el bitcoin tiene menores costes de transacción que la utilización de tarjetas de crédito, transferencias o Paypal. Realizando un pago con bitcoin se eliminan intermediarios no deseados.
- Seguro: el bitcoin cuenta con un fuerte respaldo criptográfico que lo protege de falsificaciones y se puede guardar en múltiples localizaciones simultáneamente. La tecnología en la que se basa el protocolo del bitcoin es varias veces más segura que la que utilizan los bancos y las tarjetas de crédito.
- Transparencia: todas las transacciones quedan grabadas en un registro de libre acceso.
- Micropagos: dado su divisibilidad y sus bajos costes de transacción es una moneda ideal para realizar micropagos.
- Funciona las 24 horas al día: para las operaciones en bitcoins no existen horarios ni días festivos.

- Se acumula en un espacio ínfimo: podría guardarse una fortuna enorme en una memoria USB, que puede ser guardada o trasladada sin depender de terceros.
- Escalabilidad: Nuevos desarrollos de segunda capa podrían darle al protocolo de bitcoin otras capacidades más allá de las actuales.

7.1.8 Desventajas y desafíos que presenta

- Volatilidad: desde su creación ha tenido grandes subidas de precio. El 2013 lo empezó a 10,2 EUR/BTC y lo cerró a 579,9 EUR/BTC, llegando cerca de los 900 EUR/BTC, lo que hace del bitcoin una moneda atractiva para la especulación. Con el tiempo lo normal es que el porcentaje de variación se reduzca y tenga una cotización más estable.
- Garantía de aceptación: aunque cada vez hay más establecimientos que los aceptan todavía son una minoría. Es utilizado fundamentalmente por freelancers o personas interesadas en adquirir contenidos digitales en internet.
- No hay un regulador o una entidad respaldatoria: el que no tenga un respaldo detrás de gobiernos y bancos centrales para muchos puede ser una clara desventaja ya que se sentirían más cómodos con el apoyo de un regulador.
- Anonimato: al igual que en el punto anterior, la enorme ventaja que supone el que las transacciones sean anónimas es una desventaja para muchos que temen que sea utilizada para actividades ilícitas y para no cumplir con las obligaciones tributarias.

7.2 Arquitecturas Distribuidas

Una de los conceptos más importantes a tener en cuenta en las criptomonedas y cadenas de bloques es el tipo de arquitectura distribuida. Una arquitectura distribuida está diseñada para eliminar la centralización quitando la dependencia de un servidor centralizado.

Los tipos de arquitecturas más importantes son:

- Arquitectura Centralizada: Toda la estructura está gestionada por un sólo nodo y sus usuarios pertenecen a la misma comunidad. Se utiliza principalmente en servicios web, alojadas en un servidor centralizado por el que tienen que pasar todas las personas que quieran acceder a ella (Wikipedia, Airbnb, Github).
- Arquitectura Federada: está dividida en varios nodos operativos que funcionan como su propia estructura centralizada fragmentando el servidor central en pequeños servidores distribuidos. Cada uno de estos tiene su propio dueño y su comunidad. A pesar de esto, cualquier usuario de la estructura puede acceder a los datos de otros independientemente del nodo al que pertenezcan (GNU Social, Buddycloud, Diaspora).
- Arquitectura P2P (Peer to Peer): Es una estructura totalmente distribuida, particionando los trabajos y la información entre los usuarios de la red llamados "peers". Cada uno de estos tienen los mismos privilegios en la infraestructura. Cada usuario controla su aporte a la red distribuida y generalmente todos pertenecen a la misma comunidad (BitTorrent, Bitcoin, Ethereum, Napster).

7.3 Blockchain

7.3.1 Definición y origen

Blockchain o cadena de bloques es, en esencia, un libro contable, descentralizado (En el caso de que más del 50% de los ordenadores que forman esa red blockchain no sean de la misma persona o empresa, podemos decir que la red está descentralizada ya que no tiene un centro de emisión, control o poder) y que puede ser público, privado o federado donde se registran todas las transacciones criptográficas. Técnicamente, es una base de datos distribuida, y puede utilizarse para mucho más que sólo para registrar la trazabilidad de las transacciones financieras de una criptomoneda. Es decir, Blockchain es un concepto mucho más amplio que Bitcoin, dado que también se pueden registrar activos físicos o electrónicos. Las ideas sobre Blockchain son más antiguas que la creación de

Bitcoin, dado que provienen de un trabajo de Haber y Stornetta en 1991. Su propósito era crear un método de timestampting seguro de documentos digitales, en lugar de un esquema de dinero digital (Narayanan, Bonneau, Felten, Miller & Goldfeder, 2016).

El blockchain registra bloques completos que se enlazan a bloques anteriores utilizando un sellado de tiempo confiable que evita la modificación de un dato luego después de haber sido publicado. Cada nodo, como puede ser una computadora conectado a la red, obtiene una copia de la cadena de bloques, que se descarga automáticamente. La cadena de bloques permite a los participantes del mercado realizar un seguimiento de las transacciones de la moneda digital sin necesidad de llevar un registro centralizado.

Una de las maneras clave de eliminar el control central mientras se mantiene la integridad de los datos es tener una gran red distribuida de usuarios independientes. Esto significa que los equipos que componen la red se encuentran en más de una ubicación. Estas computadoras se denominan a menudo nodos completos o "full nodes".

A fin de evitar que la red se corrompa, además de descentralizar las cadenas de bloque, a menudo se utiliza una criptodivisa. Una criptodivisa es un token o ficha digital que posee un valor de mercado y opera de forma similar a las acciones bursátiles en los mercados financieros.

Si bien cada criptodivisa funciona de modo diferente para cada cadena de bloques, en esencia, se pretende que el software pague el hardware con el objetivo de operar la red. El software corresponde al protocolo de cadena de bloques mientras que el hardware consiste en los nodos completos que están asegurando los datos en la red. Los protocolos de cadena de bloques más populares hoy en día son Bitcoin, Ethereum, Ripple, Hyperledger y R3CEV, entre otros.

Las cadenas de bloques están siendo utilizadas en una variedad de aplicaciones comerciales ya que es un método eficaz para digitalizar, codificar e insertar

prácticamente cualquier documento en la cadena de bloques. Al hacerlo, se crea un registro indeleble que no puede ser modificado. Además, la autenticidad del registro puede ser verificada por toda la comunidad utilizando la cadena de bloques en lugar de una única autoridad centralizada. Este concepto se la conoce como tecnología de libro distribuido por sus siglas en inglés DLT (Drescher, 2018).

7.3.2 Características generales del Blockchain

Las características generales del blockchain son:

- Consenso: se puede replicar la base de datos en varios servidores. De esta forma, si un servidor falla, la información aún estaría accesible en alguna de las réplicas. Sin embargo, como la transmisión de datos no es inmediata, y las fallas pueden ocurrir en cualquier momento, es posible que en ciertas ocasiones exista más de una versión de la base de datos. Esto hace necesario definir unas reglas que permitan saber cuál es la versión aceptada de la base de datos cuando aparezcan discrepancias, en otras palabras, que puedan establecer el consenso de la red alrededor de una versión de la información.
- Transparencia: toda la información en Blockchain es pública, no puede ser modificada y es fácilmente auditable. Cualquier persona tiene el potencial de controlar el acceso a los registros personales y saber quién los ha accedido.
- Desintermediación: la eliminación de los intermediarios como bancos o sociedades colectivas de las transacciones, disminuyen los costos de transacción y los riesgos asociados a su presencia

Por otro lado, una Blockchain se diferencia de una base de datos tradicional, por dos motivos, el control de acceso de escritura y lectura de datos está verdaderamente descentralizado, a diferencia de otras bases de datos distribuidas donde está centralizado lógicamente, y la capacidad de asegurar transacciones sin necesidad de terceros de confianza en un entorno competitivo (Drescher, 2018).

7.3.3 El ciclo de vida del Blockchain

La primera red de Blockchain se originó con la creación del Bitcoin como mecanismo para asegurar las transacciones de la criptodivisa. La cadena de bloques cuenta con más de 5000 "full nodes" y están distribuidos globalmente. Se utiliza principalmente para realizar operaciones de intercambio y comercializar el Bitcoin. Sin embargo, la comunidad detrás del bitcoin vio el potencial de realizar nuevas funcionalidades y aplicaciones con la red debido a su tamaño y seguridad comprobada a lo largo de todo este tiempo.

La red Ethereum es una segunda evolución del concepto de cadena de bloques. Toma la estructura tradicional de la cadena de bloques y añade un lenguaje de programación que permite extender sus funcionalidades. Al igual que el Bitcoin, cuenta con más de 5000 "full nodes" distribuidos globalmente. Ethereum se utiliza principalmente para comercializar su criptodivisa Ether, realizar smart contracts (contratos inteligentes), crear organizaciones autónomas descentralizadas (DAOs) y aplicaciones descentralizadas.

7.3.4 Funcionamiento de técnico del Blockchain

La estructura de la Blockchain, desde el punto de vista de ingeniera de software, puede entenderse como un árbol de bloques, donde dos bloques pueden tener el mismo padre, dando lugar a ramificaciones. La Blockchain tiene una cadena principal, llamada main chain, que es la cadena con mayor dificultad total, es decir, la suma de dificultades de todos los bloques que la componen. Los bloques que no pertenecen a la main chain son llamados bloques stale o huerfanos.

La raíz de la Blockchain es un bloque especial llamado Bloque Génesis. En el blockchain de Bitcoin, este bloque fue minado el 3 de enero de 2009. Uno de los campos minados contenía un titular del diario *The Times* de esa fecha, con el fin de manifestar la prueba que ese bloque fue creado ese mismo día; día en que los bancos de inglaterra fueron rescatados por mal manejo de recursos.

A la blockchain se agregan bloques que contienen transacciones. El número de un bloque es la altura del bloque dentro de la blockchain. Si un bloque contiene transacciones cuyos inputs hacen referencia a outputs que ya fueron gastados en un bloque de menor número dentro de su cadena, el bloque es inválido. De esta forma, en una cadena no se pueden agregar bloques que hagan double spending.

Cualquier full node de la red puede construir bloques, se les denomina nodo minero. Al recibir un bloque, los nodos lo validan y lo agregan a su blockchain. Es posible que cambien su cadena principal, si el nuevo bloque pertenece a una cadena previamente stale y esta ahora tiene mayor dificultad total que la cadena principal. Para que un bloque sea válido y aceptado por los nodos de la red, debe contener una prueba de trabajo (siglas en inglés PoW), que valide que el nodo minero hizo uso de CPU para poder construir el bloque.

Una de las partes intervinientes en el proceso, llamémosle A desea hacer una transacción a B. Esa transacción de dinero cuando vaya de A hacia B, A necesitará la confirmación de B de la recepción del dinero.

El dinero que en términos digitales son datos y que son representados en números, palabras e imágenes que fluyen de un punto hacia otro, siempre van con una capa de seguridad mediante una encriptación en la red de blockchain.

El monto es almacenado en un bloque y representado por un *hash***.** Este *hash* contiene toda la información relacionada al envío. Es en si, un el resultado de un algoritmo matemático que convierte determinados datos en una serie de caracteres.

La información es distribuida entre los participantes, que posean máquinas de computación o nodos, y son ellos los que validan que cada pieza de la información concuerde entre lo que se requirió y se envió.

El bloque validado se une a la cadena que está secuenciada por eventos previos que contienen su hash inmodificable que lo identifica.

En resumen, Iansiti (2017) precisa que el funcionamiento en un sistema de cadenas de bloques consiste en que cada registro réplica en gran número en bases de datos idénticas y ellas son constantemente mantenidas por diferentes partes involucradas. Eso refiere a que cualquier cambio que se introduzca en una copia, todas las demás copias identificarán lo mismo en simultáneo. Esto asegura que las transacciones y por ende los historiales de los activos intercambiados estén registrados en la base de datos.

7.3.5 Algoritmo del blockchain

a. La Blockchain es un árbol de bloques que cuenta con una cadena principal. El bloque raíz se conoce como bloque génesis.
b. Los bloques que no pertenecen a la cadena principal son bloques stale o huérfanos y no son tenidos en cuenta al momento de validar transacciones.
c. Un nuevo bloque se agrega a continuación de algún bloque de la Blockchain. En este caso el bloque forma parte de la cadena principal. Las transacciones que agrega este bloque ocurren después de todas las transacciones que fueron agregadas en bloques anteriores en su cadena.
d. Los inputs de las transacciones de un bloque hacen referencia a outputs de transacciones anteriores que todavía no fueron gastados.
e. Un nodo minero agrupa transacciones para crear un nuevo bloque, teniendo que hallar una prueba de trabajo (en inglés proof of work o conocido por sus siglas PoW) para que este sea válido.
f. Al hallar un nuevo bloque, el minero lo propaga por la red, y el resto de los nodos al recibirlo y validarlo también lo propagan.
g. Todos los nodos de la red tienen una copia de la Blockchain, que se usa para validar transacciones y bloques. Actualizan su copia con cada bloque válido recibido.

7.3.6 Arquitectura y taxonomía del Blockchain

En la tecnología blockchain, es posible encontrar tres tipos de arquitecturas predominantes: pública, privada y federada o de consorcio.

Las blockchain de tipo público se encuentran abiertas a cualquier persona en el mundo y por ende cierta parte de la información transaccional puede encontrarse disponible en los bloques. Cualquier persona puede contribuir con mantener el acuerdo transaccional en la red, es decir; generar los bloques dentro del blockchain. (Morabito, 2017). En el blockchain público el proceso de consenso determina qué bloques son añadidos a la cadena y qué estados actuales poseen, para eso hay una evaluación técnica como también de contexto de la información que ha sido transaccionada. Estas personas que resuelven los problemas computacionales en la transacción se denominan *miners* o mineros y juegan un papel importante en el establecimiento de la confianza. Estos por tal accionar son retribuidos principalmente por dos tipos de incentivos o conceptos conocidos como *proof of work* (en español prueba de trabajo) o *proof of stake* (prueba de participación) (Bambara et al.; 2018).

La prueba de trabajo es un concepto que se introdujo en 1993, por Cynthia Dwork y Moni Naor como mecanismo o protocolo de seguridad en una red. Este concepto consiste en realizar un tipo de trabajo costoso de realizar por una computadora como la factorización de números primos con el objetivo de servir para cumplir con prerrequisitos muy particulares. Por eso cada transacción implica también un coste extra por parte de la misma tecnología utilizada. Ejemplo de esto podemos encontrar en el Bitcoin.

Por el otro lado, la prueba de la participación se trata de un esquema basado en cálculos menos costosos y procesos de aleatoriedad. En lugar de depender de cálculos costosos el esquema de prueba de participación depende de las entidades que tienen participación dentro de la red (Morabito, 2017).

El blockchain abierto tiene por regla ser totalmente descentralizado, no posee un propietario y los bloques están bajo un criterio compartido de seguridad tanto por el algoritmo del software, como por los aportantes que certifican el orden y el concierto de la información desde sus nodos.

El tipo de blockchain privado se enmarca en las limitaciones del otorgamiento de accesos de edición y el derecho de crear nuevas transacciones en un grupo preseleccionado de usuarios o de nodos. (Drescher, 2017). Esta tecnología privada tiene gran parte de su desarrollo en el sector privado donde pequeñas redes empresariales implementadas con la tecnología blockchain ingresan, almacenan, coordinan y controlan la información de los libros distribuidos.

El blockchain de consorcio es una red de libros distribuida donde el proceso de consenso es controlado por un grupo pre selecto de usuarios o de nodos. (Bambara et al.,2018). Este tipo de blockchain es el preferido del sector privado en especial de la industria financiera, su cualidad de rapidez, que atraen mayor escalabilidad y proporcionan seguridad y privacidad en cada transacción.

7.3.7 Tipos de Blockchain

Las blockchains pueden ser permisivas o autorizadas, y dentro de estas categorías también podemos encontrar dos más en cada una de ellas, que son públicas y no públicas.

El primero (público permisivo) significa que cualquiera puede participar para leer o escribir en la cadena de bloques y el privado significa que sólo las partes designadas pueden decidir qué datos entran en la cadena de bloques o, según lo vemos, en la base de datos distribuida.

Fuente: Elaboración propia con datos elaborados por Pavel Kravchenko

Para clasificarlos podríamos usar dos criterios importantes y estos son:

- El anonimato de cada validador.
- El nivel de confianza de un validador específico.

Una cadena de bloques pública permisiva como Bitcoin, utiliza la Proof-of-Work como mecanismo de consenso que proporciona el anonimato de los validadores, pero aún así, las cadenas de bloques públicas con permiso pueden usar un mecanismo de consenso diferente como Proof-of-stake y aun así proporcionar cierto nivel de anonimato para los validadores. La diferencia entre estos dos, es que con la PoW no se puede confiar pero al mismo tiempo no hay necesidad de hacerlo, pero con PoS, se debe tener cierto nivel de confianza en los actores que tienen participación en el sistema y para participar en el consenso, se debe tener una porción de monedas para hacer parte de la red.

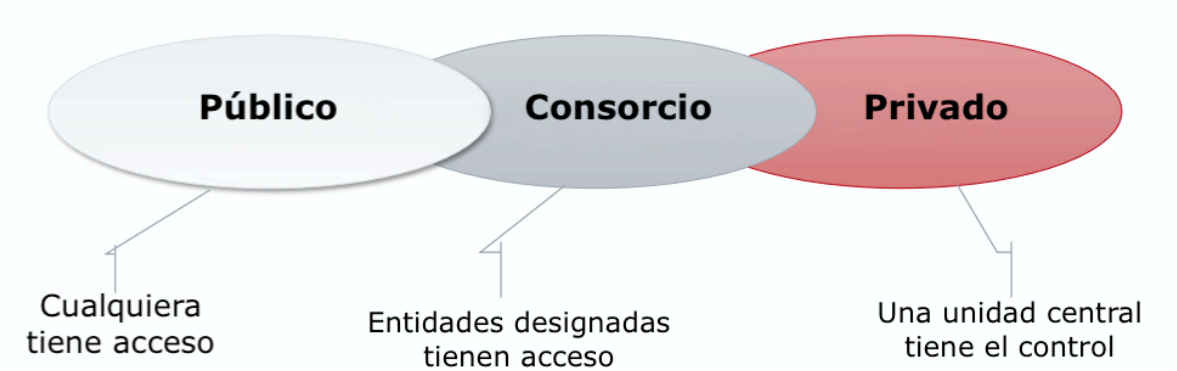
Si tenemos un blockchain público/sin permiso que usa PoW, el anonimato del usuario es alto, la inmutabilidad de los datos es alta, pero el inconveniente es que su capacidad de escala es baja.

Para las blockchains autorizadas/públicas que usan PoS como mecanismo de consenso, el anonimato de los usuarios también es alto, pero la inmutabilidad y escalabilidad es moderada.

Existen otros tipos de blockchains públicas/sin permiso, y la diferencia se basa en el mecanismo de consenso que utilizan, por ejemplo: los miembros de un comité de construcción donde cada propietario es elegible para votar estableciendo un nodo y participar en el consenso para tomar decisiones, el nivel de confianza en los validadores es bajo porque ya los conocemos. La PoS no serviría mucho aquí porque cada validador tiene igual poder de voto; por lo tanto, esto se vuelve adecuado para las cadenas de bloques de consorcios que utilizan el consenso de FBA (Acuerdo Bizantino Federado).

El último tipo de blockchains son autorizadas/privadas, donde el anonimato del usuario es bajo, la inmutabilidad también es baja, pero la escalabilidad es alta debido a la posibilidad de tener procesos centralizados. Dentro de esta categoría los nodos necesitan algún tipo de licencia para participar o ser parte de un grupo pequeño. Aquí es donde se requiere la BTF (Tolerancia a Fallos Bizantina) porque la inmutabilidad depende de tener acuerdos entre validadores y el uso de este mecanismo de consenso no implica restricciones para los participantes e incluso podría tolerar no tener reglas sobre el tipo de comportamiento que puede tener un nodo. Si no tuviéramos BFT, un nodo podría transmitir y publicar transacciones falsas, anulando así su inmutabilidad. Si se hace correctamente, este tipo de blockchains puede ayudar a las partes que confían cuando todas las partes en el proceso se conocen entre sí y si no cambian con frecuencia. Estos sistemas tienen la ventaja de brindar algún tipo de rastreabilidad, flexibilidad y ayuda con la eficiencia de corporaciones, grupos federados o un grupo limitado de personas; pero aún así la palabra blockchain realmente no encaja aquí (Swan, 2015; Drescher, 2017).

Se pueden categorizar de la siguiente manera:



Fuente: Elaboración propia

7.3.7.1 Blockchains Publicas

Las redes de blockchain públicas son aquellas a las que cualquier persona tiene acceso. En general estas redes son transparentes y los usuarios son anónimos. Ningún participante tiene más derechos que los demás, por lo cual no hay administradores de la red. Las redes públicas más conocidas son Bitcoin, Bitcoin Cash, Ethereum y Litecoin, que además tienen una criptomoneda asociada.

El procedimiento para participar es descargarse la aplicación correspondiente y conectarse de forma automática con un determinado número de participantes o nodos a los que se les solicita la versión más actualizada de la cadena de registros, lo que puede tomar minutos u horas dependiendo de su funcionamiento y hasheo en la red. Una vez que el usuario se hace con la copia actualizada de toda la cadena, tiene los mismos derechos y deberes que el resto de los participantes a la hora de proponer y validar transacciones.

La forma de validar las transacciones es mediante lo que se conoce como protocolos de consenso. De forma aleatoria se elige un participante cada vez para proponer un nuevo bloque. Si el elegido propusiese un bloque con información errónea, el resto de los participantes podrían rechazarlo. Para incentivar a los nodos para que propongan bloques válidos, muchas redes dan recompensa en forma de criptomoneda al nodo que propone un bloque cuando éste es aceptado. Los nodos

que compiten por validar los bloques, encontrando el hash válido del bloque, se conocen como mineros. La labor del minado en las redes públicas es el corazón que las mantiene vivas. Es la responsabilidad de los usuarios o nodos mineros seguir realizándolo.

7.3.7.2 Blockchains Federadas o de tipo Consorcio

Las redes de blockchain federadas son las más solicitadas a la hora de construir soluciones compartidas para gobiernos, empresas, y asociaciones. En general no son abiertas a la participación del público, sino que a un número determinado de organizaciones, entidades o compañías se encargan de administrar la red en conjunto y mantener copias sincronizadas del registro. El acceso mayoritario es mediante una interfaz web que los administradores ponen a disposición del usuario medio, en lugar de compartirles una copia de la cadena como en las redes públicas.

Una red de blockchain federada puede ser, por ejemplo, una buena opción para industrias como salud y finanzas, donde tienen lugar grandes volúmenes de transacciones entre distintas entidades con una alta necesidad de confianza. A la hora de diseñar e implementar una solución de este tipo, es fundamental acompañar a la herramienta blockchain con un plan estratégico adecuado consistente en definir desde quiénes y cómo van a administrar la red hasta qué información se les va a mostrar a los usuarios vía interfaz web. En muchos casos el usuario que accede vía web puede no tener interés ni conocimiento sobre blockchain, pero sí necesitar una plataforma que involucre entidades diferentes, necesidad de confianza y transparencia. Es importante señalar que al ser su acceso vía web y no como "nodos" de la red -es decir, que no tienen una copia de la cadena-, los usuarios comunes tendrán acceso a tanta información como los administradores decidan mostrarles a través de la misma. Se tendrán entonces opciones que varíen desde un gran nivel de transparencia hasta una transparencia nula.

Al contrario de las redes públicas, las redes federadas no recompensan al usuario para la creación del hash a través del minado de bloques y ni siquiera tienen una criptomoneda asociada. Los propios administradores o entidades a cargo de la red

proporcionan los recursos computacionales necesarios que cumplan con el propósito de generar el hash.

Aunque las redes de blockchain federadas no tienen un modelo de participación abierto al público, el software que las respalda sigue siendo en general de código abierto, lo que permite a la comunidad desarrolladora reutilizar código en muchos casos. Algunos de los softwares más comunes de código abierto utilizados para crear redes federadas son Hyperledger, Corda, EFW o Multichain, que permiten descargar la aplicación de blockchain y programar la cadena a tu gusto, decidiendo quién quieres que participe y bajo qué reglas se regulan las transacciones. También es posible y común crear entornos federados haciendo un fork de una red pública, generando así tu propia red customizada. (Bambara, 2018; Mougayar, 2016; Morabito, 2017, Drescher 2017).

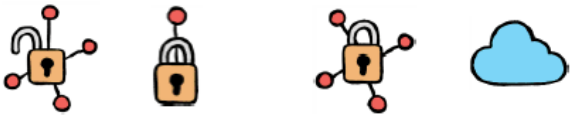
7.3.7.3 Blockchain Privadas

Una cadena de bloques totalmente privada es una donde los permisos de escritura se mantienen centralizados dentro de una organización. Los permisos de lectura pueden ser públicos o restringidos en una medida arbitraria. Las aplicaciones probablemente incluyan la gestión de la base de datos y la auditoría interna de una sola empresa, por lo que la legibilidad pública puede no ser necesaria en muchos casos, aunque en otros casos es deseable la audibilidad pública. Las blockachains privadas podrían brindar soluciones a los problemas de las empresas financieras, incluidos los agentes de cumplimiento de regulaciones tales como la Ley de responsabilidad y portabilidad de seguros de salud (HIPAA), las leyes contra el lavado de dinero (AML) y de conocimiento de clientes (KYC). El proyecto Hyperledger de la Fundación Linux y la red Gem Health son proyectos de blockchain privados en desarrollo.

Diferencias entre Blockchain Público, Consorcio y Privado:

Público	Consorcio	Privado
- En este tipo de *blockchain* se despliega una protección para los usuarios por parte de algunos desarrolladores que no tienen autorización de realizar ciertas acciones. - Los métodos al ejecutar un consenso despliegan criterios para detectar y eliminar entradas maliciosas o falsas.	- El consenso es un trato fácil al identificar a todos los participantes. - El costo de la transacción se reduce ya que se divide entre las empresas consorciadas	- *Blockchain* funciona solamente dentro de una organización especifica. - El *blockchain* privado limita el acceso de lectura y el derecho a realizar transacciones en pre selecto grupo de usuarios o nodos. - El operador del blockchain puede cambiar las reglas de juego.

Fuente: Elaboración propia basado en Bambara, 2018; Mougayar, 2016; Morabito, 2017, Drescher 2017



	Públicos Bitcoin, Ethereum, Litecoin	Privados Hyperledger, Corda, Quorum	Federados Hyperledger, Corda, Quorum	*Blockchain as a Service* IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	~	~	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA
No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart *Contracts*	✓	✓	✓	NA
Existe recompensa por minado de bloques	~	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	~	NA
Seguridad basada en protocolos de consenso	✓	✗	~	NA
Seguridad basada en funciones *hash*	✓	~	~	NA
Provee servicios en la nube	NA	NA	NA	✓

✓ Sí ✗ No ~ A veces NA No Aplica

Fuente: BBVA Research 2017

7.3.8 Extensiones del Blockchain

Utilizando la banca tradicional como una analogía, la cadena de bloqueos es como un historial completo de las transacciones de una institución financiera, y cada bloque es como un estado de cuenta bancario individual. Sin embargo, debido a que es un sistema de base de datos distribuida, que funciona como un libro mayor electrónico abierto, una cadena de bloques puede a su vez simplificar las operaciones comerciales para todas las partes. Por estas razones, la tecnología

está atrayendo no solo a instituciones financieras, sino que también a diversos actores del sector musical, aseguradores, mineras y el campo de estudio del Internet de las cosas (IOT). A su vez, mediante la tecnología DLT se están desarrollando variadas aplicaciones que facilitan las tareas administrativas como sistemas de votación, registros de armas o vehículos para gobiernos nacionales, registros médicos en clínicas médicas o incluso para confirmar la propiedad de antigüedades u obras de arte en aseguradoras (Bambara, 2018).

7.3.9 Obstáculos en la adopción de la tecnología

Los obstáculos a la tecnología además de ser técnicos son de índole jurídico legal en cuanto aprobaciones regulatorias o cuestiones políticas.

Entre los problemas que aún deben abordarse figuran los siguientes.

El blockchain debe interactuar perfectamente con otras partes de los procesos operativos, en otras palabras, permitir una configuración más rápida y reducir el tiempo de resolución de problemas. Lograr los aumentos de eficiencia debe ser lo suficientemente fácil y económico como para que todas las partes implicadas puedan beneficiarse.

La seguridad también sigue siendo motivo de preocupación. Varios bancos centrales, entre ellos la Reserva Federal, el Banco de Canadá y el Banco de Inglaterra, han iniciado investigaciones sobre monedas digitales. Según un informe de investigación del Banco de Inglaterra de febrero de 2015 declara que "Habría que seguir investigando para diseñar un sistema que pudiera utilizar la tecnología de bases de datos distribuidas sin comprometer la capacidad del banco central de controlar su moneda y asegurar el sistema contra ataques sistémicos".

El software de código abierto del blockchain obliga a mantener un control estricto y una revisión continua sobre el sistema ya que los hackers pueden aprovechar posibles vulnerabilidades al tratarse de un código de libre acceso. El ser un sistema de código abierto por un lado permite abrir y democratizar su uso, sin embargo, por el otro genera resistencias en su adopción. Ejemplo de este tipo son las instituciones

bancarias y los gobiernos cuando deben tratar cuestiones sensibles como ser la protección de datos personales.

La regulación también es fundamental para crear un entorno digital abierto para el comercio y las transacciones financieras. Los certificados físicos actuales deben digitalizarse para obtener todos los beneficios de un sistema completamente electrónico.

7.3.10 Ventajas que presenta el Blockchain

La consultora de servicios tecnológicos KPMG (2018) identificó las siguientes ventajas que ofrecen las cadenas de bloques.

- Los sistemas con tecnología DLT (Distributed Ledger Technology, en inglés) permiten a las empresas y a los bancos simplificar las operaciones internas, reduciendo drásticamente los gastos, errores y retrasos causados por los métodos tradicionales de conciliación de registros.
- Los libros contables electrónicos son más económicos de mantener que los sistemas de contabilidad tradicionales; en las oficinas la nómina de empleados administrativos puede reducirse considerablemente.
- Los sistemas con DLT, son en gran parte completamente automatizados, reducen considerablemente los errores y eliminan los pasos de confirmación redundantes.
- Minimizar las demoras de procesamiento también significa que se deja en riesgo menos capital en espera debido a transacciones pendientes de realizarse.
- Mayor transparencia y facilidad de auditoría permiten ahorrar en los costes en el cumplimiento normativo contra el blanqueo de dinero.

7.4 Smart Contracts

Una vez analizado el bitcoin, su tecnología, los tipos de redes de intercambio y las cadenas de bloques procederemos a detallar el concepto del contrato inteligente tema central del presente trabajo de investigación.

Un contrato inteligente (en inglés smart contract) es un programa informático que opera de forma autónoma permitiendo celebrar y ejecutar contratos entre dos o más partes. El software puede operar dentro de una cadena de bloques facilitando el proceso de cumplir digitalmente la negociación o el cumplimiento de un contrato.

En términos sencillos, un contrato inteligente es un contrato escrito que se ha traducido en código de software mediante sentencias y estructuras lógicas de programación. Estos contratos digitales pueden verificar de manera automática que se hayan cumplido las condiciones necesarias para la ejecución de sus órdenes. A su vez, los contratos inteligentes operan de forma autónoma permaneciendo inalterables a una posible manipulación desde el exterior, gracias a la red de consenso establecida en la blockchain.

La tecnología Blockchain permitió la existencia de contratos inteligentes ofreciendo la permanencia y las resistencias incorruptible provistas en el pasado por la tinta, el papel y una autoridad confiable que cerificaba el cumpliento del contrato.

El concepto de contrato inteligente fue acuñado por Nick Szabo en 1994 donde diseña la idea de un algoritmo capaz de auto-ejecutar, auto-cumplir, auto-verificar y auto-restringirse de acuerdo a las reglas de cómo había sido codificado. El concepto fue retomado con la aparición de Bitcoin junto a su red y bases de datos blockchain ya que hasta ese momento no existía una plataforma funcional que permitiera mecanismos criptográficos para evitar la inalterabilidad de los datos y una red de consenso distribuido (Gord, 2016).

Luego, con la creación del protocolo Ethereum, permitió extender las características funcionales de las cadenas de bloques agregando más lógica de programación. Esta lógica de programación es la que permite crear contratos inteligentes con un amplio conjunto de reglas y condiciones y luego almacenar el código fuente en su Blockchain. Permitiendo la posibilidad de crear infinidad de programas que serán ejecutados en cada computadora de la red y que tendrán todos los beneficios de la tecnología Blockchain.

El jurista, experto en tecnología blockchain, Lance Koonce afirma "… un contrato inteligente es un acuerdo que "vive" en un sistema que no está controlado por ninguna de las partes ni por los agentes de esa parte. Idealmente, tanto el activo digital que se transfiere como la moneda / activos utilizados para la compra también viven en ese sistema. El contrato en sí es una transacción autoejecutable entre las partes, desencadenada por eventos que pueden determinarse definitivamente como que han sucedido o no. Por ejemplo, llega el 7 de abril, se transfiere un monto de pago. Cuando la cantidad transferida es igual a una cierta cantidad, el activo subyacente se transfiere. No hay otras partes involucradas: el libro distribuido asegura que todas las transacciones sean verificadas por múltiples participantes, y sólo se confirmaran las transacciones que siguen las reglas del contrato inteligente" (Koonce, 2016).

Por lo tanto, los contratos inteligentes se prestan a condiciones definibles, y una lógica bastante simple "Si X luego Y". Una vez que una condición o "entrada" queda sujeta a cualquier tipo de juicio por el que se pueda necesitar un ser humano, los contratos inteligentes dejan de ser una solución viable (al menos en la actualidad; uno puede imaginar un futuro donde los agentes de inteligencia artificial crean esas llamadas).

Cuando se escribe un Smart contract, el programador puede escribir en líneas de código y de manera explícita la secuencia de pasos lógicos de ejecución del acuerdo para producir lo que se espera obtener al final, el programador tiene que escribir lo que debe ser realizado y cómo realizarlo; dentro del Smart contract se incluirá una secuencia de instrucciones que actualizarán los estados de las normas y cláusulas contractuales (obligaciones, prohibiciones y permisos) dependiendo de cuales tareas deben ser realizadas y de su estado actual. El programador juega un papel importante puesto que a modo de código es difícil estipular los pasos secuencialmente tal y como aparecen en un acuerdo impreso en papel por lo que no refleja lo que se encuentra escrito en lenguaje natural, sino que refleja la manera

en la que debe ser ejecutado el acuerdo de manera lógica y que pueda ser interpretado por lenguaje de computadora (Idelberger et al. 2016).

Este tipo de contratos inteligentes representan la implementación de un acuerdo contractual en el que los requerimientos legales han sido formalizados en código de computadora, de esta manera las partes involucradas en el pacto pueden estructurar sus relaciones de manera más eficiente ejecutándose de manera autónoma sin la ambigüedad de las palabras. La confianza en el código permite modelar el rendimiento del acuerdo y simular su ejecución y rendimiento previo al inicio de las actividades contractuales (Wright and De Filippi 2015).

Como cualquier tipo de acuerdo, los Smart contracts requieren de negociación entre las partes para su perfeccionamiento. En un sistema basado en blockchain debe existir acuerdo entre las partes acerca de la manera en la que el código se debe comportar antes de desplegarlo dentro del sistema; una vez en ejecución, el Smart contract establece las relaciones legales entre las partes en concordancia con las normas de la ley por las son regidos o decidieron ser regidos. Comúnmente el pacto es expresado primero en lenguaje natural y después es traducido a Smart contract pero no necesariamente debe realizarse de esta manera.

Existen acuerdos que no requieren de mucha formalidad, como lo son los orales o aquellos que se cierran con un apretón de manos, pero normalmente su grado de complejidad y la necesidad de mantener un récord de lo acordado obliga que se escriba lo que fue acordado, que sea guardado de manera segura y a su vez certificado para cumplir con leyes que apliquen; comúnmente los acuerdos pueden ser certificados por un tercero o por un notario (Idelberger et al. 2016)

En este sentido, Idelberger (2016) afirma "Aquí juega un papel disruptivo esta tecnología pues remplazaría la necesidad de un tercero y a su vez pasa de ser guardado en una sola máquina a pertenecer a toda una red de entidades que verifican continuamente su validez; esto brinda un seguimiento de ejecución fehaciente y en tiempo real". Al no haber restricciones en la estructura de datos que

se pueden alojar en un blockchain los Smart contracts pueden ser alojados en este tipo de plataformas, ya que utilizan un tipo de lenguaje programación que es familiar con las herramientas de compilación que actualmente usan los programadores tales como javascript, go, c#, c++, node js, etc.

7.4.1 Evolución del Contrato Inteligente

En lo que concierne a los contratos legales tradicionales, los mismos suelen ser creados usando plantillas de procesamiento de texto personalizadas por abogados y otros profesionales legales, los cuales contienen lenguajes legales estandarizados que especifican términos y condiciones. Además, los contratos basan su operatividad mediante terceros para su interpretación y ejecución. En caso de surgir algún conflicto, se recurre a un tribunal con el objetivo de remediar el conflicto. En consecuencia, este proceso consume tiempo, dinero y hasta en ocasiones resulta redundante al pasar por diferentes instancias judiciales.

Como respuesta a esta problemática, la solución fue desarrollar el contrato inteligente. Este es un programa de computadora capaz de llevar a cabo el contrato entre las partes. Por ejemplo, el framework de desarrollo de Smart Contracts Solidity, para la cadena de bloques Ethereum, es capaz de ejecutar de forma autónoma los términos y condiciones de un acuerdo. El código del contrato define los términos y condiciones como un conjunto de silogismos lógicos, de la misma manera que lo haría un documento legal. Las condiciones pueden ser validadas y confirmadas por las llamadas RPC (llamada a procedimiento remoto en computación distribuida) a otros contratos inteligentes o inicialmente a Oráculos (externos a la cadena de bloque). De este modo, el código del contrato inteligente se puede ejecutar automáticamente en la cadena de bloques.

De acuerdo a la consultora KPMG, adoptar el desarrollo de contratos inteligentes mediante la tecnología Blockchain presenta los siguientes beneficios o atributos relevantes:

- Confiabilidad y accesibilidad: la cadena de bloques reside en miles de nodos, distribuidos por todo el mundo; por lo tanto, es seguro desde un único punto de falla. Si un nodo falla, todos los otros nodos continúan funcionando. Cada nodo mantiene una copia de la cadena de bloques.
- Transparencia: todo el mundo puede ver todas las transacciones que residen en la cadena de bloques.
- Irrevocabilidad: las transacciones pueden ser irrevocables.
  Inmutabilidad: No se pueden producir alteraciones no detectadas en los datos de la cadena de bloques.
- Asegurado digitalmente: los documentos y los activos pueden protegerse criptográficamente.

KPMG afirma, "Los contratos inteligentes que utilizan atributos de blockchain, pueden desarrollarse para garantizar que: a) las transacciones sean auditables; b) los activos siempre se pueden verificar a través de una cadena de custodia; c) los registros de transacciones no pueden ser alterados; y d) las personas maliciosas y corruptas no puedan disputar la veracidad de los registros".

7.4.2 Funcionamiento técnico del Contrato Inteligente

Una persona se suscribe a un contrato o firma uno entre una o más contrapartes. Este contrato está codificado bajo un código de software donde persistirá dentro de una cadena de bloques.

Luego, cuando un evento ocurre, como puede ser, el vencimiento de una fecha, un resultado esperado o precio de un bien alcance cierto límite el contrato es ejecutado de acuerdo a los términos especificados en el código de software. Es necesario considerar que los individuos involucrados son anónimos, sin embargo, el contrato es de carácter público.

Detallamos los elementos que son necesarios a considerar al momento de desarrollar un contrato inteligente.

- Objeto del contrato: El software debe tener acceso a bienes o servicios bajo contrato para bloquearlos y desbloquearlos automáticamente.
- Firmas digitales: Todos los participantes inician un acuerdo donde firman el contrato con sus claves privadas.
- Términos del contrato: Los términos de un contrato inteligente toman la forma de una secuencia exacta de operaciones. Todos los participantes deben firmar estos términos.
- Plataforma descentralizada: El contrato inteligente se despliega en la cadena de bloques de una plataforma y se distribuye entre todos los nodos de la red.

En la siguiente imagen podemos observar un contrato básico con sus sentencias de código que fue escrito en la cadena de bloques Ethereum.

```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

Fuente: Blockgeeks

Aplicación de la lógica empresarial de los Smart Contracts:

Fuente: BBVA Research

7.5 Contratos Ricardianos

Un contrato ricardiano coloca los elementos que definen un acuerdo legal en un formato que puede expresarse y ser ejecutado en software. La clave es hacer que el formato sea legible por una máquina para que pueda ser extraído para propósitos computacionales, y legible como un documento de prosa ordinaria tal que los abogados y las partes contratantes puedan leer lo esencial del contrato sin inconvenientes.[4]

Los contratos ricardianos se implementan en varios sistemas, algunos de ellos son:

- Diseñado en la década de 1990 por Ian Grigg de la compañía Systemics.
- Utilizado en contratos de transacciones abiertas, construido por Chris Odom, desde 2010.

[4] http://iang.org/papers/ricardian_contract.html

- Utilizado en Open Bazaar para realizar transacciones de ofertas y ofertas, desde 2014.
- Y finalmente, en 2016, se anunció su uso en Corda como una palanca de legitimación para contratos inteligentes.

7.6 Oráculos

Los oráculos son programas informáticos que permiten actualizar el estado del contrato inteligente con la incorporación de información externa. Estos permiten desencadenar las órdenes programadas dada una situación específica en el mundo real. La información externa que es consumida mediante un servicio RPC puede informar diversos tipos de datos o valores como la cotización de una moneda, la ejecución de un pago, el cambio en un precio o el aumento de una temperatura.

Los proyectos de software, más relevantes en la actualidad, en relación a Oráculos son Orisi y Oraclize. Estos se tratan de sistemas que recogen toda la información de distintos proveedores externos y determinan el dato más fiable en función de lo que la mayoría indica. De esta forma, se descentraliza también el proceso de validación de información externa certera y real evitando tener que introducir un actor o tercera parte que interviniente (Swan,2015; Gord,2016).

7.6.1 Desafíos de los Contratos Inteligentes

A continuación, detallamos los principales desafíos que deben superar los contratos inteligentes que operan dentro de las cadenas de bloques.

- Rendimiento: los recursos informáticos y el rendimiento requeridos para el procesamiento de transacciones, validación y detección de fraudes determinarán a qué servicios bancarios, financieros y de pago se puede aplicar mejor. Actualmente, la cadena de bloqueos no es lo suficientemente eficaz como para manejar miles de transacciones por segundo.

- Interoperabilidad: garantizar la interoperabilidad entre las diferentes implementaciones de la cadena de bloques para que puedan comunicarse entre sí.
- Escalable: cada nodo de la red de la cadena de bloques debe conocer cada una de las transacciones que se producen a nivel global, lo que puede crear un arrastre significativo en la red. El objetivo es realizar todas las transacciones con una mayor eficiencia, pero de una manera que no sacrifique la descentralización y seguridad que proporciona la red.

7.6.2 Riesgos de los Contratos Inteligentes

Los riesgos potenciales del uso de los Contratos Inteligentes incluyen aspectos tales como la gobernanza del despliegue, la gestión de riesgos regulatorios y legales. Estos riesgos y la forma en que se gestionan apuntalan fundamentalmente a la confianza del mercado en la tecnología. Para ser eficaz, la cadena de bloqueo y los contratos inteligentes requieren normas o estándares, es decir, un conjunto de reglas comunes por las que todos los participantes operan, con el fin de garantizar precisión y fiabilidad.

El modelo descentralizado plantea desafíos cuando es necesario cambiar las reglas, porque esos cambios deben ser acordados y aceptados por todos los participantes para que funcionen de manera coherente. Se requerirá un marco de gobernanza para implementar y operar la cadena de bloqueos como una aplicación legal y debe tener en cuenta las funciones de supervisión y monitoreo, el establecimiento de reglas y la gestión del control de aceptación y cambio.

La gobernanza en general será un requisito no sólo para las tecnologías jurídicas, sino también para todas las tecnologías que gestionan la información. Esta transformación a algunas reglas comunes de gobierno de la información no sólo es crítica para la cadena de bloqueo, sino también para otras actividades como el descubrimiento electrónico y la ciberseguridad. Las normas de gobernanza en torno a la cadena de bloques contribuirán a fomentar la confianza del mercado en la

tecnología y en el entorno jurídico-reglamentario. De este modo se aceleraría la adopción y el éxito del contrato inteligente (Swan, 2015).

7.6.3 Desafíos legales de los Contratos Inteligentes

Las principales consultoras de tecnología afirman que uno de los desafíos más importantes que enfrenta el Contrato Inteligente está relacionado con su validez jurídica. En este sentido, la naturaleza híbrida actual de un contrato inteligente combinado con un contrato tradicional no programado o manual, por ejemplo, un documento Word con términos y condiciones, crea algunos nuevos problemas en cuanto a su validez. Como, por ejemplo, si un contrato inteligente es legalmente vinculante dependerá de varios factores, incluyendo el caso de uso específico, el tipo de contrato inteligente que se utilice y la ley aplicable. Los desafíos mencionados por Lance Koonce (2016) son los siguientes:

- Aplicabilidad: cuando un contrato inteligente tiene un efecto contractual jurídicamente vinculante, la tecnología en la que se utiliza puede ocasionar a veces problemas en relación con la exigibilidad legal. Puede que no exista una autoridad administrativa central para resolver una disputa. Los mecanismos de solución de controversias podrían abordar la aplicabilidad y las variaciones jurisdiccionales. La inserción de un mecanismo de resolución de disputas en un contrato inteligente será pro formativa para abordar los temas relacionados con la aplicabilidad y las variaciones jurisdiccionales.
- Transparencia: el Blockchain puede implicar cierto nivel de transparencia. Pero, ¿qué pasa si las partes no quieren que se divulguen los detalles? ¿Cómo mantener partes del contrato en privado y otros beneficios de la cadena de bloques?
- Cambios: la incapacidad de poder desbloquear transacciones que no deberían haber sucedido, ya sea por ilegal o por infringir requisitos regulatorios.
- Limitaciones de codificación: los contratos a menudo tratan con lo desconocido y tienen cláusulas que no se reducen fácilmente al código o que pueden ejecutarse automáticamente como un simple "si esto, entonces ese"

procedimiento. La fuerza mayor es un buen ejemplo. Los contratos a menudo incluyen conceptos de juicio subjetivo, razonabilidad y actuar de buena fe. En la actualidad, estos conceptos no pueden traducirse fácilmente en afirmaciones lógicas. Dicho esto, habrá servicios de código que pueden proporcionar pruebas de "razonabilidad", que se han utilizado en el comercio de valores durante años.

En relación al avance de los contratos inteligentes en materia jurídica, podemos citar el ejemplo del estado de Arizona, en Estados Unidos, donde recientemente aprobó legislación que reconoce tanto al contrato inteligente como las cadenas de bloques.

Arizona en 2017 aprobó la Ley de Transacciones Electrónicas de Arizona (AETA), HB-2417, cuyo fin es el evitar cualquier incertidumbre legal en torno a las transacciones del Blockchain y los contratos inteligentes relacionados con ciertos activos digitales. Dicha ley incluye una definición muy específica de la tecnología de cadena de bloque como distribuida, un libro de contabilidad descentralizado, compartido y replicado, que puede ser público o privado, autorizado o con un permiso menor, o impulsado por una economía de criptografía simbólica o con un permiso menor y establece que los datos en el libro de contabilidad están protegidos con criptografía, son inmutables y auditables y proporcionan una verdad sin censura.

A su vez, la ley HB-2417 incluye una definición de contratos inteligentes como "un programa impulsado por eventos, con estado, que se ejecuta en un libro mayor distribuido, descentralizado, compartido y replicado que puede hacerse cargo de la custodia e instruir la transferencia de activos en ese libro mayor".

7.7 Plataformas de Smart Contracts

A continuación, detallamos las plataformas más importantes para realizar contratos inteligentes.

7.7.1 Ethereum

La plataforma Ethereum inicio su funcionamiento a mediados del 2015, logró recaudar aproximadamente 180 millones de dólares mediante crowdfunding a con bitcoins. Todos quienes participaron en su financiamiento colectivo o ICO (initial coin offering, lo que sería para las empresas públicas el initial public offering) recibieron 2000 ether por cada bitcoin que aportaban para el desarrollo de la plataforma.

Ethereum es una plataforma open source, descentralizada que permite la creación de contratos inteligentes entre pares. Ethereum se basa en el modelo blockchain con tecnología de contabilidad distribuida (DTL). A su vez, integra un lenguaje de programación Turing-complete que permite generar contratos inteligentes y aplicaciones descentralizadas denominado Solidity.

El propósito inicial del proyecto Ethereum consiste en descentralizar la web mediante la introducción de cuatro componentes como parte de la hoja de ruta de su Web 3.0: publicación de contenido estático, mensajes dinámicos, transacciones confiables y una interfaz de usuario integrada y funcional. Estos componentes están diseñados para reemplazar algunos aspectos de la experiencia Web que damos por sentado actualmente, pero haciéndolo de una manera completamente descentralizada y anónima.

Ethereum, cuenta con una criptomoneda propia llamada Ether, la cual permite impulsar la plataforma en la creación de contratos y aplicaciones distribuidas. El ether es utilizado por los usuarios de la red como medio de intercambio entre personas o máquinas para ejecutar las operaciones solicitadas. El ether constituye un modelo de incentivos que pretende recompensar a los desarrolladores en mejorar la calidad del código optimizando los recursos de la red y maximizando los beneficios de los usuarios (Buterin, 2014).

7.7.2 RSK

RSK (anteriormente conocida como RootStock) es una plataforma peer-to-peer enfocada a la creación y ejecución de contratos inteligentes sobre la cadena de

bloques Bitcoin. El objetivo de RSK es agregar valor y funcionalidad a la red central de Bitcoin implementando la utilización de contratos inteligentes mediante el desarrollo de una *sidechain* (en español cadena de bloques paralela). La RSK MainNet comenzó su funcionamiento el 2 de enero de 2018.

La plataforma de RSK facilita la creación de programas distribuidos complejos. Para lograr este propósito se apoya en Solidity, un lenguaje de programación del tipo Turing completo con una sintaxis similar a Javascript. El código generado tras su compilación se ejecuta directamente en la máquina virtual de RSK. A su vez, el código de RSK mantiene la compatibilidad con el de Ethereum.

La moneda nativa de RSK es el bitcoin. Mediante la creación de una vinculación bidireccional entre la cadena de bloques de Bitcoin y la de RSK, se consigue que cada bitcoin esté disponible en una sola cadena al mismo tiempo. A raíz de esto, la base monetaria global mantiene los valores establecidos en el patrón de emisión principal de bitcoins.

La seguridad del sistema de RSK está establecida a través de un sistema mixto. Primeramente, una federación de entidades de confianza que ayuda a transferir los bitcoins entre las dos cadenas de bloques, y después, una potencia de minería que recibe comisiones por las transacciones. La capacidad transaccional máxima para pagos simples está estimada en aproximadamente 400 transacciones por segundo.

En lo que a software respecta, el cliente de RSK está basado en el de Ethereum, por lo cual muchas funcionalidades son parecidas, como la compatibilidad de los contratos o la topología de la red.

RSK aprovecha el hecho de que existe una gran inversión de dinero en hardware específico para minar en Bitcoin, facilitando la adopción. Por un lado, obtiene poder de cómputo de forma sencilla y, por el otro, evita la necesidad de reinvertir dinero en hardware especial para minar RSK. Esto se logra mediante un proceso conocido como merged-mining que consiste en reutilizar los bloques de Bitcoin para proveer PoW (siglas de prueba de trabajo) para bloques de RSK (Lerner, 2015).

7.7.3 Counterparty

Counterparty es un protocolo meta-coin contruido sobre el blockchain de Bitcoin. En 2014 fue añadido soporte para Contratos inteligentes en la red de Ethereum, lo que quiere decir que cualquier smart contract que trabaja en Ethereum, podría trabajar en Conterparty también. Actualmente esta funcionalidad sólo está habilitada en testnet y es incierto su roadmap.

Los smart contracts aquí pueden ser escritos en Solidity (código similar al javascript) o Serpent (similar a phyton). La red corre bajo la cruptomoneda XCP, y transaccionar con un código es posible a través de la instalación de un cliente (software) en una computadora. Como todos los nodos reciben la misma solicitud en las transacciones, y como todos los clientes tienen el mismo contrato codificado en la blockchain de Bitcoin, los resultados de ejecución de código de todos los clientes de Counterparty serán exactamente los mismos.

Como hay una cantidad fija de XCP y ejecutar contratos inteligentes destruye estas monedas, Counterparty decidió que la cantidad de XCP que consumen los smart contracts decrecerá lentamente.

Existen otras plataformas de smart contracts como Cardano, EOS, NEO, Qtum, etc, que no serán examinadas dentro de este estudio.

8 ANÁLISIS DE CASOS

Una vez presentado el marco teórico de nuestro trabajo de investigación, proseguiremos a describir y analizar diversos casos relevantes que hacen uso tanto de la tecnología blockchain y como la de contratos inteligentes.

8.1 Caso The DAO

The DAO fue la primera organización autónoma descentralizada, fue constriuda sobre la blockchain de ethereum y obtuvo los fondos de tal manera que cualquier persona podía participar de manera alegal y sin intermediarios. Una vulnerabilidad

de código permitió a un hacker drenar los fondos de la DAO a tan solo dos semanas de estar funcionando y parece ser el caso de este tipo de mayor relevancia e impacto dentro del ecosistema de la blockchain y de las criptomonedas, pues fue la primera vez en que inversores no calificados podían participar en un crowdfunding de tal magnitud sin tener que pasar por regulaciones batiendo record como el projecto que logró recaudar la mayor cantidad de dinero hasta el año 2016 por la vía del crowdfunding[5] (aproximadamente 160 millones de dólares en una criptomoneda llama ether). The DAO tenía el objetivo de proveer un nuevo modelo de negocio descentralizado tanto para empresas comerciales como a las sin ánimo de lucro.[6]

No tenía una estructura convencional o mesa de directivos, durante el tiempo que funcionó fue manejada por votación de todo aquel que participó en la pre-venta de los tokens. The DAO no estaba ligada a ningún estado o gobierno, su código es open source, turing complete y vulnerable a errores como todo software, el hacker logró explotar estas características del smart contract y el proyecto fue abandonado demostrando la inmadurez de la industria.

Para tratar de recuperar algunos fondos, "la comunidad de la blockchain de ethereum decidió dividir la cadena de bloques y llegar a un consenso en el que los fondos de The DAO todavía permanecían en las manos de los inversores. Esto dividió a la comunidad entre quienes decían que fundamentalmente esta práctica iba en contra de las propiedades de la blockchain y en particularmente una de las más importantes que es la inmutabilidad. Por esta razón, una parte de la comunidad decidió permanecer en la cadena original donde el hacker todavía tenía la propiedad de los fondos robados, de esta manera nace la cadena de bloques de ethereum classic y desde entonces tanto la blockchain de ethereum como la de ethereum classic, tienen cada una su propio token y diferentes transacciones a partir del bloque 1920000.

[5] https://en.wikipedia.org/wiki/List_of_highest_funded_crowdfunding_projects
[6] https://en.wikipedia.org/wiki/The_DAO_(organization)

8.2 Caso Kleros

Kleros es una plataforma desarrollada mediante la tecnología blockchain con el fin de resolver disputas entre personas de forma descentralizada. El concepto de su desarrollo está basado en los principios de una organización descentralizada donde miembros de la misma comunidad intervengan como jurados para resolver los conflictos.

Kleros conecta a los usuarios que necesiten resolver sus disputas y los jurados con las habilidades necesarias para solucionarlas de forma justa. Nuestro protocolo de resolución utiliza la tecnología de blockchain y jurados en colaboración abierta y distribuida para adjudicar cada caso de forma rápida, segura y accesible.

La plataforma pretende ofrecer arbitraje rápido, seguro y accesible para virtualmente cualquier situación. En este sentido, Ferico Ast[7] el CEO y fundador de Kleros.io afirma "las disputas en una economía global, digital y descentralizada ocurren en áreas en las que ni los tribunales estatales ni los métodos tradicionales de resolución de conflictos pueden actuar. Para este propósito nosotros desarrollamos contratos simples y concretos del tipo Si o No en referencia a lo pactado. Son muy pocos los proyectos de Smart contracts que se ocupan de cuestiones legales y kleros es uno de ellos".

8.2.1 Funcionamiento de Kleros

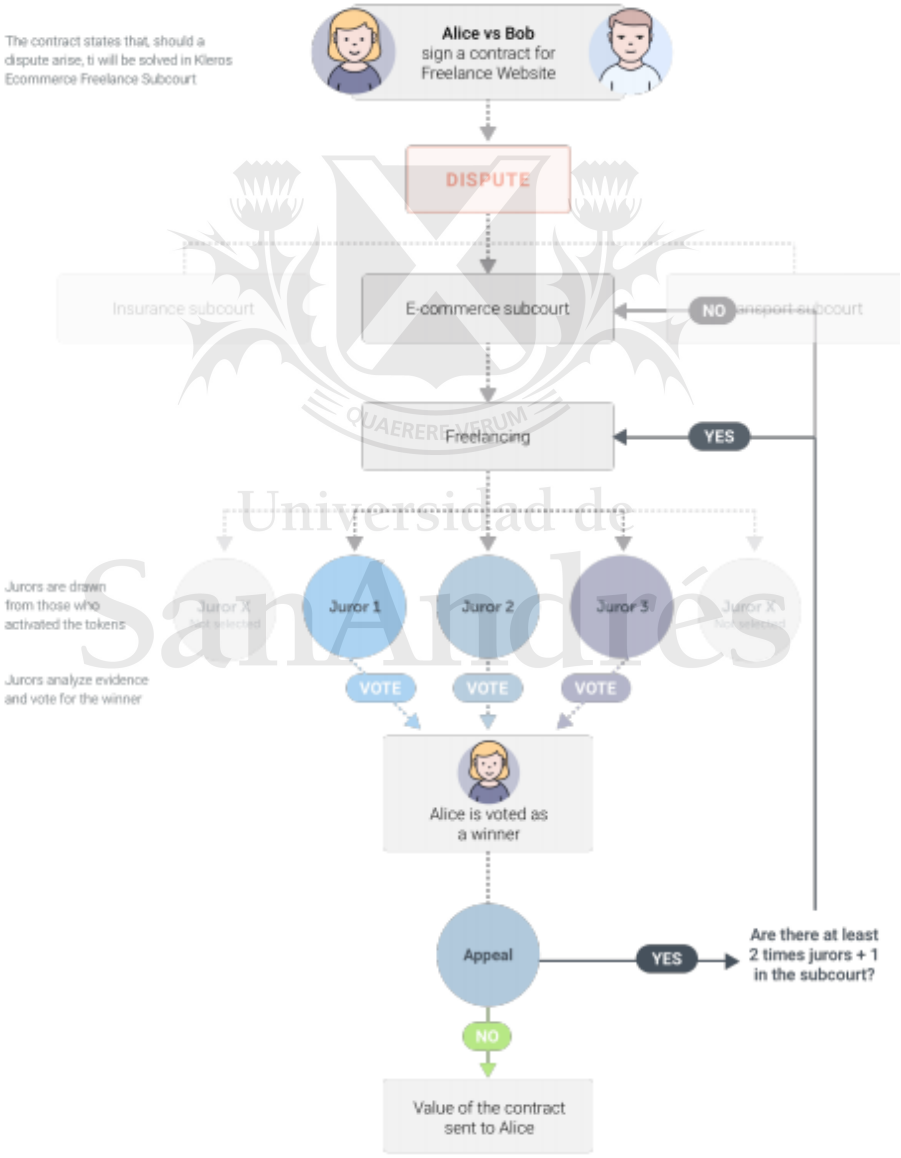
El funcionamiento desde una perspectiva a alto nivel, es el siguiente. Los usuarios crean un smart contract y eligen a Kleros como protocolo de resolución de conflictos. Toda la información relevante del caso es enviada de forma privada y segura a Kleros. El tribunal se forma a partir de jurados dispuestos a colaborar. Éstos evalúan la evidencia y emiten su voto. Finalmente, la decisión tomada por el tribunal es ejecutada por el smart contract.

La colaboración abierta permite acceder a una comunidad global de jurados. Estos jurados que pueden estar especializados en diversos temas o áreas de interés

[7] Entrevista realizada en Buenos Aires, Argentina el día 17/7/2018

forman diferentes cortes en relación a la disputa. La tecnología de blockchain garantiza la integridad y transparencia a la hora de seleccionar a los jurados. La teoría de juego proporciona incentivos para una participación honesta. El sistema de votación garantiza un proceso democrático en la resolución de conflictos.

En la imagen siguiente podemos observar un diagrama del funcionamiento del Kleros.



Fuente: Esquema de funcionamiento de kleros.io

En relación con la tecnología Blockchain y los contratos inteligentes Federico Ast expresa "Considero que blockchain es como el internet del año 95, es decir, se encuentra en una fase inicial de early adopters. Actualmente, el tema más avanzado es el referido a remesas y pagos internacionales. A su vez, a los smart contracts todavía falta tiempo para que llegue a una maduración tecnológica donde sean utilizados por todas las personas. Además, falta explotarlo en cuanto casos de uso y proyectos ya que es necesario contar con un programa balanceado de incentivos entre los integrantes de la red con el fin de lograr los objetivos que persigue el proyecto. Por otro lado, el ecosistema que rodea a los contratos inteligentes se encuentra en una fase inicial del cual también falta maduración. En mi opinión el market place es lo más importante y necesario para mejorar la adopción de caras al usuario final. Ahora bien, la cantidad de blockchain, criptomonedas y smart contracts disminuirán a una pocas y no como la cantidad de cientos que hay hoy en día."

8.3 Caso Hyperledger Fabric

Encabezando la lista de los competidores de Ethereum, este proyecto que fue creado en 2015 por la Linux Foundation en co-desarrollo con IBM y es un blockchain privado con necesidad de autorización que facilita la ejecucióin de smart contracts o "cadenas de código". Es de código abierto y tiene el propósito manifestado de ayudar al desarrollo de bases de datos distribuidas basadas en blockchain.

Su desarrollo se basa en diferentes frameworks desarrollados bajo la sombrilla de Hyperledger; estos incluyen Hyperledger Burrow, Fabric, Orohan Sawtooth e Indy.

Así como Ethereum creó su propio lenguaje de programación, los desarrolladores de Hyperledger crearon un set de herramientas basadas en java, Go y otros lenguajes de programación comunes por medio de la instalación de módulos. De esta manera no tienen que depender de conocer un lenguaje en particular.

Al ser un blockchain privado en el cual se necesita autorización, todos los participantes de la red conocen las identidades de sus pares, esto hace que la

necesidad de confiar se elimine pues ya se conoce con quien se realiza las operaciones.

Ctualmente participan más de 200 compañías dentro del espectro de empresas tecnológicas como IBM, Intel, Cisco, entre otras, y otras instituciones financieras como Deutsche Börse Group, J.P. Morgan, SWIFT, además de nuevos de la industria como Digital Asset Holdings y R3CEV.

8.4 Caso Lisk

Lisk es una blockchain pública que corre aplicaciones descentralizadas, cada una de estas aplicaciones corre su propio sidechain y utilidad llamada Lisk Commander el cual puede ayudar a depurar los procesos. Pretenden proveer capacidad de escalabilidad y seguridad por medio de la designación de 101 validadores delegados elegidos, haciendo que requieran de un algoritmo de concenso proof-of-stake.

8.5 Marketplace – Bisq

Para dar más referencias de lo que podría contruirse con smart contracs, cabe mencionar Bisq, un marketplace especializado en el intercambio de criptomonedas y compra de las mismas con dinero fiat utilizando tecnología de smart contracts sobre una blockchain.

Es una casa de cambio peer-to-peer donde se puede intercambiar Bitcoin con cualquier otra criptomoneda soportada por la plataforma, incluso se puede comprar criptomonedas con dólares.

Bisq llama la atención por mostrar mayor descentralización de los otros casos de acuerdo a estas características:

- Utiliza un software que necesita estar online para enviar o recibir ofertas
- La comunicación funciona de manera p2p sin ningún servidor central
- No hay necesidad de registro previo o mostrar identificación para que las partes participen y realicen transacciones.

- En el momento en el que una oferta es aceptada por un crontrato inteligente que está distribuido sólo entre las partes, un hash del contrato inteligente es grabado en la blockchain de Bitcoin como una operación OP_RETURN.

8.6 Marketplace - Open Bazaar

Es un proyecto open source que pretende desarrollar un protocolo para el e-commerce, sus transacciones suceden de manera descentralizada pues utiliza pagos directos por medio de la red de bitcoin y utiliza esta moneda como medio de intercambio.[8]

Los smart contracts que permiten transaccionar e interacción entre las partes (comerciante, comprador y árbitro de la transacción) son construidos como contratos Ricardianos, y cada paso del intercambio es firmado criptográficamente para asegurar la autenticidad de la información y así prevenir la manipulación de los contratos.

Open Bazaar permite arbitraje de las transacciones cuando sucede una disputa por medio de sistema de firmas múltiples 2-de-3 que permite el arbitraje de las transacciones para que las partes poseean de manera individual una llave privada, haciendo innecesario la participación de alguien que pueda representar al marketplace.

8.7 Freelancing marketplace – Cryptogrind

Otro marketplace especializado, Cryptogrind es un marketplace descentralizado orientado al sector laboral, donde freelancers y clientes pueden encontrarse los unos a los otros, comunicarse y facilitar los pagos de manera segura y privada.

Se soporta en arbitraje a través de billeteras miltisig 2-de-3 donde una de las dos direcciones está reservada para la resolución de disputas que se realizan a través de Reddit. En este proceso, Cryptogrind toma el 4% de la transacción.

[8] https://www.openbazaar.org

9 CONCLUSIONES

- ¿Qué tipo de innovación tecnológica representan los smart contracts en la economía y los negocios?

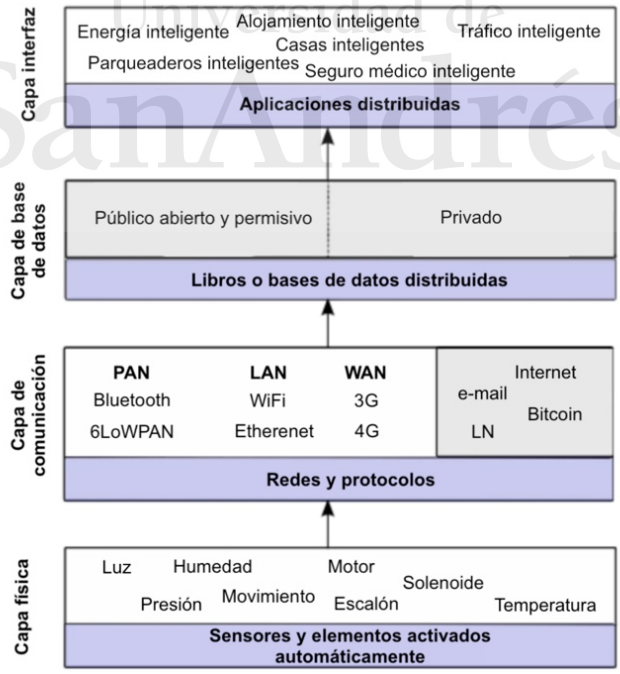
La blockchain no es una tecnología disruptiva clásica sino una tecnología fundacional como el TCP/IP que no irrumpió en alguna compañía o industria en particular sino que proporcionó una capa sobre la cual las personas realizaron desarrollos para casos de uso específicos de la tecnología. En sus inicios, TCP/IP no tenía mucho más caso de uso que el de mensajería binaria remota para permitir comunicación entre pocos en el mundo que la tenían a su alcance. En el caso de la blockchain, desde el día uno, tiene al menos un caso de uso aplicable a millones de personas y es el de mover valor económico de manera casi instantánea, de manera p2p en un ambiente donde no se requiere la confianza.

Con la blockchain y desarrollos de segunda capa como la lightning network, las reglas y restricciones de la organización definidas en contratos inteligentes serían en esencia, autosuficientes, más difíciles de romper, explotar, detener o denegar su servicio, ya que sus réplicas exactas se distribuirían a todos los participantes, sin autoridades centrales, pero con cada nodo de forma independiente realizando sólo acciones de validación. Una capa como esta que brinde mayor flexibilidad de programación sobre la blockchain y que permita correr smart contracts, aplicaciones distribuidas o simples programas de computadora donde la confianza no es necesaria, hace pensar en varias maneras en las cuales los smart contracts pueden ser usados para el beneficio económico empresarial. Por ejemplo, incluso aquellas empresas que funcionen dentro de blockchains privadas, recibirían un estímulo en la eficiencia, reduciendo costos e incrementando la velocidad de operación gracias a la automatización y desintermediación en los procesos.

Si esta tecnología logra abrirse paso como para impactar en la arquitectura corporativa, la gobernanza empresarial podría verse impactada por sus implicancias de descentralización tanto a nivel de una organización pequeña como algo más complejo de gestionar como Estados o Naciones. En este sentido, la blockchain puede ser útil no sólo para permitir la toma de decisiones de manera transparente, sino también para aumentar la participación pública en la economía mundial, lo que abre nuevos mercados a quienes sepan aprovecharlo.

Aplicaciones distribuidas de código abierto junto con la habilidad de enviar dinero e intercambio de valor de manera "instantánea" y programable no sólo entre personas sino también entre persona-máquina y máquina-máquina, entre dispositivos IoT que comparten información de manera peer-to-peer; tiene el potencial de irrumpir en la manera que se monetiza nuestra propia información, redistribuyendo y conservando valor donde pertenece.

Esta arquitectura podría verse de esta manera:



Fuente: Elaboración propia

No se pueden negar los beneficios de la evolución y proliferación de la automatización de procesos robóticos mediante la combinación de inteligencia artificial y robots de software, pero una gobernanza algorítmica cien por ciento pura, sería una distopía tecnocrática. Los beneficios de la transparencia en organizaciones descentralizadas "autónomas" podrían ayudar en numerosos problemas de los modelos de gobernanza contemporáneos, pero no debemos olvidar cuál sería el propósito de un gobierno algorítmico y preparar planes de contingencia a medida que los algoritmos adquieren terreno sobre los eventos cotidianos del mundo real.

- ¿Cuáles son las distintas posibilidades y mejoras que ofrecen los smart contracts?

Existen algunos aspectos que deben ser considerados cuando se discuten las maneras en las cuales se les puede sacar provecho a los smart contracts.

a. Contabilidad: los compromisos económicos de una empresa, tanto con sus proveedores como con sus accionistas y demás partes interesadas, si están definidas por reglas en contratos inteligentes, queda poco espacio para la duda o la ambigüedad. Con tal transparencia, hay pocas posibilidades de ocultar acciones corruptas o negar la responsabilidad. Las personas que autorizan cada gasto del presupuesto serían responsables de manera automática e indiscutible.
b. Costos de búsqueda de talento humano y clientes: más allá de las búsquedas en internet, respetar la privacidad de las personas por medio de la revelación selectiva de información.
c. Costos de contratación: encontrar acuerdos y reforzar los compromisos
d. De coordinación: la gestión interna empresarial de las personas y la distribución de la responsabilidad. Autoridad y poder es más fácil en una blockchain porque provee persistencia de la prestación del servicio de manera estable.

e. Costos de (re)construcción de confianza: preservarán la integridad pues la transparencia y confianza están codificadas en software.

Estamos rodeados de libros contables centralizados: para mantener los registros de la propiedad de tierras, cuentas de bancos, bases de datos de identificación personal, etc. Hasta ahora, no teníamos más opción que confiar en entidades que tienen estos libros centralizados bajo su custodia y control, por esto, estamos indiscutiblemente expuestos a: exclusión a través de censura o a ser inhabilitado por la competencia.

Bitcoin, desarrollos de segunda y poder usar smart contracts sobre esta red, posiblemente puedan dar una solución práctica a estos problemas con un acercamiento abierto, descentralizado y asegurado por criptografía. El libro contable es público y está distribuido, todos pueden inspeccionarlo y mantener una copia, todos los participantes tienen los mismos permisos y habilidades, no existe una entidad especial en la que se necesita confiar, como cada participante está verificando a los otros participantes entre ellos llegan a un acuerdo o consenso acerca de si el estado actual del libro es el que corresponde a el de la cadena de bloques más larga (siendo esta la más asegurada por la cantidad de trabajo agregado en su construcción). La tecnología de la blockchain, con esa implementación de una manera "trustless" de transferir valor entre pares, abrió la caja de pandora hacia un nuevo paradigma que podría impactar en la sociedad de manera fundamental.

La organización autónoma descentralizada es una organización que está completamente definida en línea, vive en el internet y se ejecuta con todas sus reglas de gestión escritas en contratos inteligentes. No depende de las personas para tomar decisiones, sino que "contrata" a las personas para que hagan las cosas que no puede hacer por sí misma, como interactuar con el mundo real. A modo de ejemplo, una DAO puede pagar a un contratista humano de su capital interno para realizar una tarea del mundo real, esta operación está determinada por las reglas

de la misma DAO, y a menudo, los participantes votan para decidir sobre lo que debe hacerse.

- ¿Cuáles son las fortalezas, oportunidades, debilidades y amenazas que plantean los smart contracts?

fortalezas: Compartir el conocimiento en una comunidad open source, la ética que de ahí deriva pues el código está bajo el escrutinio de toda la humanidad, esto permitiría un crecimiento orgánico y más estable para que sea expansible y adaptable. Una comunidad con un amplio terreno por explorar puede surgir con nuevas ideas de casos de uso por probar.

No todo es público en la vida real y lo mismo ocurre en el dominio digital, la protección de datos confidenciales tanto personales como de negocios es imperativa. Idealmente, desarrollos futuros nos llevarían a gozar de una dualidad entre privacidad y transparencia con blockchains públicas y contratos inteligentes que puedan correr sobre desarrollos de segunda capa sobre la red de Bitcoin. Idealmente tendríamos todos los registros de transacciones almacenados en una base de datos inmutable de forma cifrada, lo que protegería la privacidad y al mismo tiempo permitiría una auditabilidad perfecta; un gran apalancamiento para la regulación, pues nada sucedería en secreto y sólo los detalles necesarios serían revelados.

oportunidades: puede ser que ya estemos transicionando a la fase de ascenso dentro de la curva de adopción de esta tecnología en ciertas áreas. La naturaleza de los smart contracts hace de su implementación un desafío en diferentes escenarios; por un lado, tenemos smart contracts en blockchains privados que pueden ser ejecutados de manera rápida (consensuadamente optimizados para un flujo alto de transacciones) y económica (no se necesita gastar en gas para la ejecución y el spam no es un problema) - su problema más grande es más político: adopción, estandarización, responsabilidad.

Por otro lado, están los smart contracts en un blockchain público que tiene todo un set de desafíos tecnológicos, unos fundamentales y otros más persistentes como el de la escalabilidad.

debilidades: en este momento cuando los smart contracts son una tecnología de vanguardia dentro del ecosistema de la transparencia distribuida reforzada a través de la blockchain, hay algunas limitaciones y molestias para trabajar con ellos; se encuentran ahora dentro de la fase de investigación y desarrollo donde la competencia por ser la plataforma sobre la cual se correrán los smart contracts es grande y la posibilidad de fracaso puede ser mayor. I+D con alto riesgo de no lograrlo en el corto tiempo es costoso, no hay parámetros de mejores prácticas establecidas, tanto los usuarios como los desarrolladores no están familiarizados con el producto, la falta de pruebas es bastante obvia (evidente en el caso DAO) y un ecosistema que se expande por medio de la proliferación de diferentes plataformas se aleja de la estandarización y por su amplitud puede convertirse en un ecosistema resistente al cambio. En este punto de la tecnología, es una apuesta muy grande apostarle a utilizar aplicaciones críticas con contratos inteligentes.

amenazas: Existen factores que hacen que sucedan escenarios y eventos que afectan la curva de adopción con mayor o menor impacto, y en el caso del bitcoin y los smart contracts hay muchos de estos factores que hacen presión en contra de una adopción acelerada, esto sucede ya que los dos están incursionando en un ambiente que es altamente regulado; y estas áreas altamente reguladas tienden a desacelerar la adopción particularmente desde el lado corporativo y profesional.

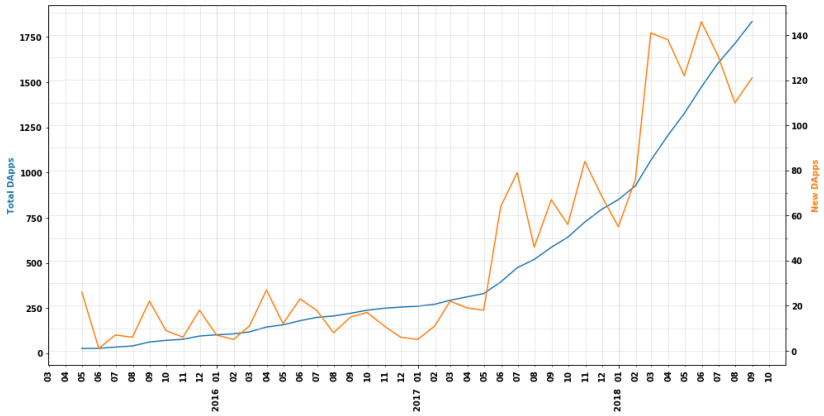
Los usuarios de las aplicaciones de software clásicas suelen tener un contrato legal con el proveedor de software (licencia) que les permite en algunos casos revisar el código fuente, compilarlo y usarlo. En el caso de los contratos inteligentes es diferente, ya que los contratos inteligentes están "vivos" en la red, se ejecutan automáticamente y el código fuente de un contrato inteligente implementado no es en realidad fácil de verificar.

- ¿Cómo se describen los nuevos modelos de negocio mediante los smart contracts?

Creemos que lo más efectivo sería enfocarse en áreas donde existe un beneficio para la corporación y el más probable de esta tecnología es el ahorro en los costos de intermediación. Esto significaría en un principio el establecimiento de blockchains privados para las corporaciones, blockchains B2B en los que los negocios pueden interactuar, en los cuales sucedería la liquidación de las transacciones y récord de operaciones de una manera más eficiente a como se viene realizando desde hace más de 30 años. Ahí se tiene un beneficio tangible como driver del comportamiento corporativo que empuja hacia la adopción entre organizaciones que tienen estructuras y formatos de datos similares.

- ¿Cuál es el estado de situación de los smart contracts respecto el grado de adopción tecnológica y el nivel de difusión a escala global?

Con la necesidad de mayor flexibilidad para la escritura de código de los smart contracts, a parte de bitcoin, un número importante de plataformas alternativas han surgido en el último par de años, sea implementando criptomonedas o alguna forma de smart contracts.

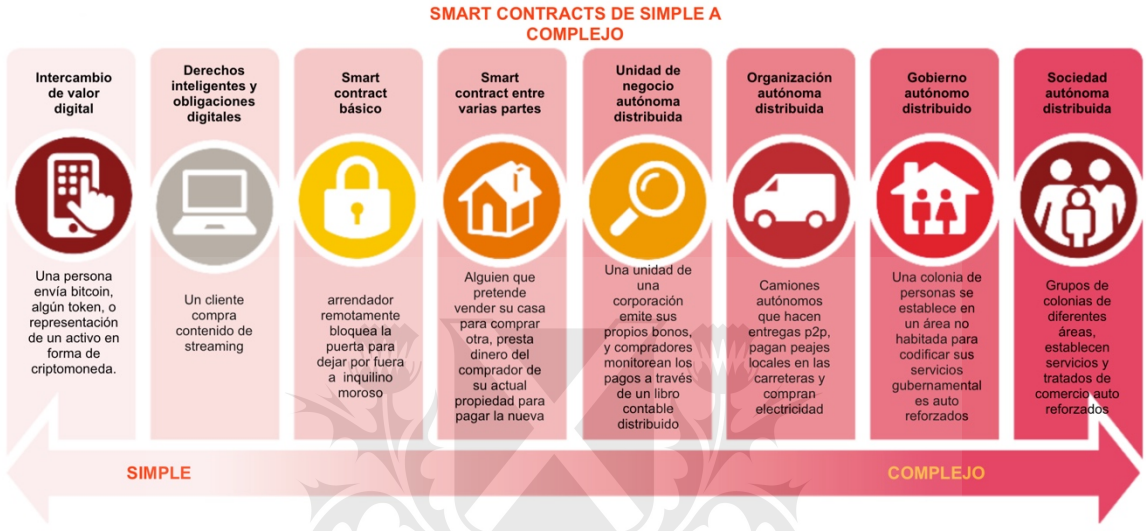


Fuente: Roman Storm[9]

[9] https://blog.stateofthedapps.com/why-dapps-are-here-to-stay-91b933b2a64a

- ¿Cuáles son los principales casos de uso de los smart?

Identificamos los siguientes casos de uso desde los más simples a los más complejos.



Fuente: Elaboración propia

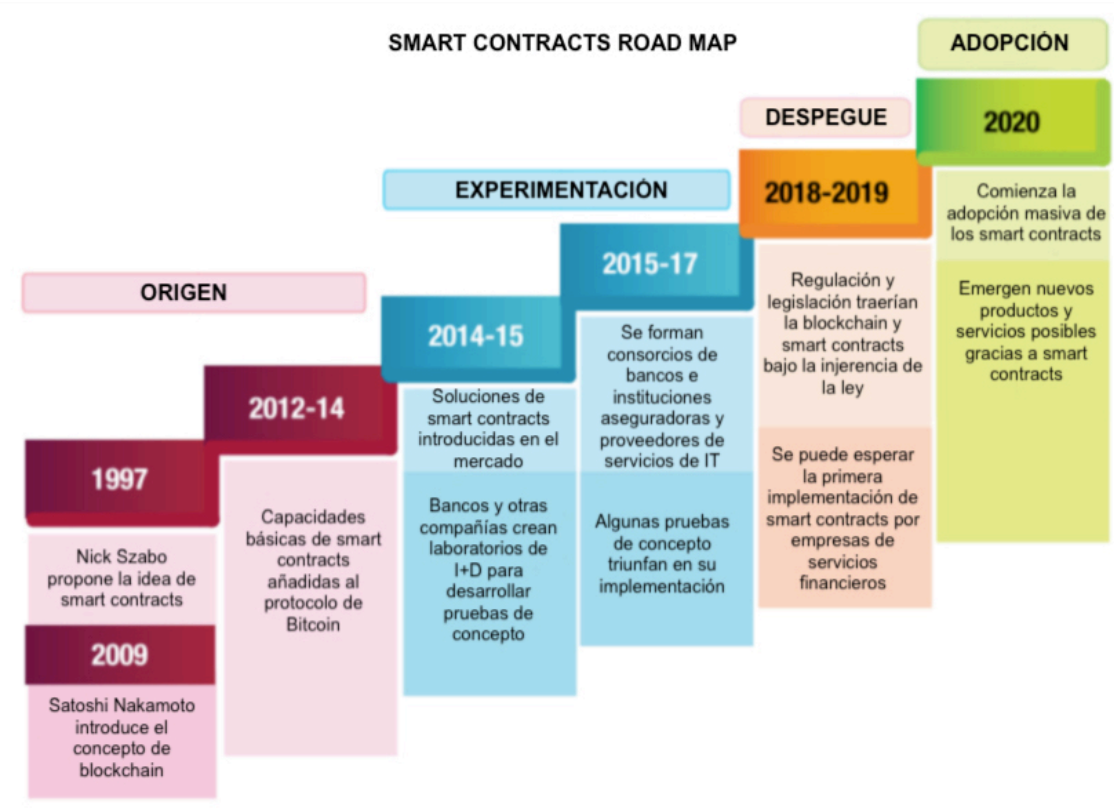
a. Intercambio de valor digital: Una persona envía bitcoin, algún token, o representación de un activo en forma de criptomoneda.
b. Derechos inteligentes y obligaciones digitales: Un cliente compra contenido de streaming.
c. Smart contract básico: arrendador remotamente bloquea la puerta para dejar por fuera a inquilino moroso.
d. Smart contract entre varias partes: Alguien que pretende vender su casa para comprar otra, presta dinero del comprador de su actual propiedad para pagar la nueva.
e. Unidad de negocio autónoma distribuida: Una unidad de una corporación emite sus propios bonos, y compradores monitorean los pagos a través de un libro contable distribuido.
f. Organización autónoma distribuida: Camiones autónomos que hacen entregas p2p, pagan peajes locales en las carreteras y compran electricidad.

g. Gobierno autónomo distribuido: Una colonia de personas se establece en un área no habitada para codificar sus servicios gubernamentales auto reforzados.
h. Sociedad autónoma distribuida: Grupos de colonias de diferentes áreas, establecen servicios y tratados de comercio auto reforzados.
i. Industria de seguros: una compañía de seguros podría evaluar una reclamación de una manera más confiable al utilizar los datos de IoT, como la hora exacta, el clima y el medio ambiente, e incluso detectar múltiples reclamaciones por un mismo accidente. Las reclamaciones no impugnadas podrían ser pagadas automáticamente. En general, sería un seguro más rentable con un menor riesgo de fraude, esto tiene un potencial enorme de ahorros en los miles de millones de USD.
j. Crowdfunding: ejecutadas con contratos inteligentes, las plataformas de crowdfunding podrían des intermediar al "proveedor" del servicio o al menos minimizar los costos operativos al permitir los pagos directos y el procesamiento descentralizado, manteniendo al mismo tiempo un alto nivel de transparencia.
k. Esquemas de pago y trading: la liquidación de transacciones complejas podría ser realizada entre las partes sin depender de terceros.
l. Cuentas bancarias inteligentes: en general las cuentas bancarias no son muy inteligentes, es posible ingresar y sacar dinero pero hay pocas cosas que se pueden realizar de manera dinámica; una cuenta más compleja podría desencadenar una transferencia a otra cuenta cuando se alcance un umbral o se podría programar ahorros mensuales adaptables.
m. Fabricación y cadena de suministro: los grandes fabricantes deben seguir miles y miles de piezas procedentes de todo el mundo; el seguimiento de cada parte desde su creación hasta su ensamblaje final es algo que se puede lograr mediante el uso de una blockchain, pero con contratos inteligentes se podría hacer un seguimiento de procesos y de procedencias de metadatos históricos acerca del elemento de manera automatizada en una base de datos distribuida. Por lo tanto tener información confiable que permita la mejor detección de errores y toma de decisiones oportuna al mismo tiempo que se reemplazan los

contratos hechos sobre papel con smart contracts que ayudarían a reducir documentación compleja para el seguimiento de los elementos, envío y sus movimientos.

n. Votaciones: tanto durante su recolección como acciones que se desencadenarían correspondiente a los resultados obtenidos
o. Distribución de dividendos: Pagos automáticos a stake holders de empresas, regalías a artistas y otro tipo de contribuidores.
p. Información del sector público: Mantener la información de los ciudadanos de manera segura y al mismo tiempo disponible a través de los servicios estatales.

- ¿Cuál es el roadmap de los smart contracts de acuerdo a las opiniones de los distintos referentes de la industria tecnológica?



Fuente: Elaboración propia

Los contratos inteligentes son, en muchos aspectos, una tecnología de vanguardia que conlleva todos los riesgos y posibles recompensas futuras. Seguramente ocurrirán fallas importantes como el incidente de The DAO. Todo emprendimiento con el potencial disruptivo de esta tecnología debe ir acompañado con cuidado y debida diligencia.

Son un enfoque prometedor para construir un puente entre el "código que se ejecuta de manera autónoma" y un dominio legal tradicional como son los contratos Circadianos, que se han investigado durante un par de años dentro de este espacio criptográfico y se están integrando lentamente en algunas plataformas de contratos inteligentes. Así, a medida que el conjunto de opciones para desarrollar contratos inteligentes aumenta con las nuevas plataformas, también hay intentos de hacer que este proceso sea más formalizado y verificable.

La blockchain de Bitcoin abrió ampliamente la puerta a la transparencia y este principio también se mantiene hasta cierto punto en otras cadenas de bloques públicas que permiten complejos contratos inteligentes. Casi se espera que cualquier proyecto que se base en esta tecnología tenga su código de manera abierta. Sin embargo, hay casos de uso que requieren la confidencialidad de las transacciones y sólo estamos al comienzo de nuevas capacidades en privacidad, por lo que podemos esperar que la privacidad sea priorizada en un futuro muy cercano. Esto ya está siendo implementado sobre desarrollos de segunda capa sobre la misma red de bitcoin con la lightning network.

- ¿Cuáles son los distintos desafíos tecnológicos que se le presentan a los smart contracts?

a. Inmutabilidad: hemos hablado de sus beneficios, pero es algo delicado; siempre que los contratos inteligentes interactúan con los humanos, pueden ocurrir errores que deben ser depurados, lo cual es difícil en un contexto inmutable.

b. Seguridad: escribir contratos inteligentes se supone que es tan fácil como actualmente se programa una aplicación que maneja transacciones financieras, pero en este caso es una espada de dos filos: un error y el dinero se pierde irrevocablemente.
c. Los usuarios no siempre son cuidadosos y los atacantes tienen todo el tiempo para escanear la cadena de bloques para encontrar contratos vulnerables. Eso, unido a la naturaleza inmutable, puede significar que tenemos formas limitadas de arreglar los agujeros de seguridad.
d. Confidencialidad: los contratos inteligentes en blockchains públicas pueden "mostrar demasiado", todo es transparente (tanto de datos como del core business), muchos se sentirían más seguros con cierto nivel de privacidad. Ya existen investigaciones e implementaciones para poder subsanar este problema en un futuro cercano, con la ayuda de hardware especializado, desarrollos en criptografía y desarrollos de segunda capa como el lightning network. Si todas las transacciones que suceden en una blockchain son visibles pero iniciadas por personas que utilizan plataformas donde es permitido usar sólo pseudónimos entre pares de los cuales sólo se conoce su dirección de billetera, no hay información personal compartida, por lo que en el futuro podríamos esperar que se implementen nuevos requerimientos de KYC dependiendo en como la regulación evoluciona al respecto. Algunas redes son creadas, cumpliendo con determinadas reglas.
e. Transparencia: la estructura y todas las funciones y privilegios de una DAO están escritas en smart contracts, su código es público y puede ser examinado en cualquier momento. De hecho son creadas abiertamente y corren abiertamente. No existen "cajas negras", pues cualquier cambio realizado en el contrato es realizado de manera abierta y todas las acciones que la DAO realiza son visibles en la blockchain, de esta manera nada está escondido. Aplicando esto a Gobiernos, una Agencia Autónoma Gubernamental Descentralizada llevaría la transparencia de los gastos públicos a otro nivel.

f. Responsabilidad: Cuando sucede un error de código la pregunta que surge es: ¿Quién es responsable? esto es un desafío para los reguladores, el determinar si el error fue necesariamente eso o fue algo deliberadamente puesto en el código para beneficio de los desarrolladores, creadores, algún participante o del smart contract si funciona como entidad. La formalización verificada de los smart contracts ayudará en cierta medida pero todavía podemos esperar muchos más errores futuros tal como sucedió con el incidente de la DAO. Por la pseudo-anonimidad de los participantes, probablemente será necesario diseñar algunos mecanismos de respaldo para minimizar las posibilidades de estafas.
g. Fuentes de datos de calidad: suponiendo que pueda existir una red auto contenida donde se encuentran los contratos inteligentes en vivo, se necesitaría un puente seguro hacia el mundo externo y sería crucial tener servicios honestos de oráculos y/o un consenso confiable de un grupo de oráculos sindicados.

Si bien la blockchain y los contratos inteligentes plantean muchas cuestiones legales y normativas, crear corporaciones enteras encima de ellos es aún más incierto. Las preguntas sobre su estado legal, cuando no existe una entidad gubernamental identificada aún no han sido respondidas. Tal vez un cierto nivel de identificación se convierta en una necesidad impuesta por los gobiernos en un futuro próximo.

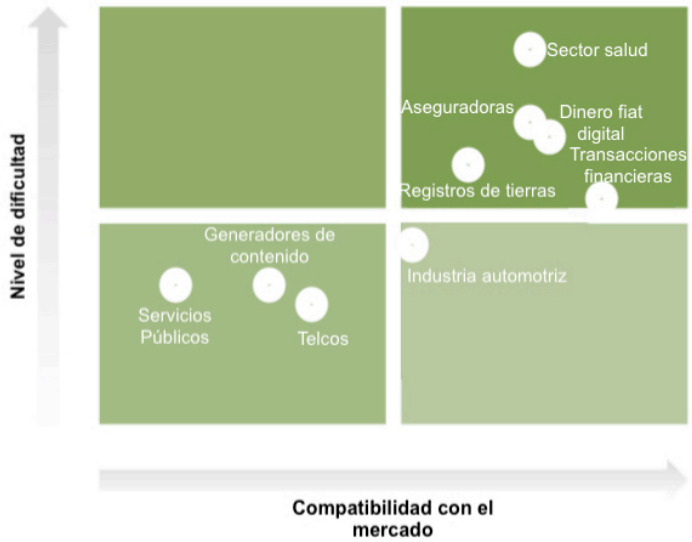
Desarrollos de código en un entorno que cambia tan rápido y que es tan inexplorado como este, no solo significa que cambian las herramientas de programación, sino también el lenguaje de programación subyacente y el entorno de ejecución. Aquí, la situación es diferente entre blockchains públicas y privadas, pero no consideramos las privadas, ya que pueden operar bajo las condiciones adecuadas para ellas y pueden ajustarse más fácilmente pues no son open source ni globales, mientras que las públicas son más generales y operan en un ambiente hostil.

Parámetros de mejores prácticas apenas se están formando, es una fase de prueba y error que ha demostrado evidencias de grandes posibilidades de encontrar vulnerabilidades de código que permiten explotar los errores de código.

Junto con el potencial que los contratos inteligentes brindan como innovación tecnológica, estamos experimentando los primeros choques de su interacción con el mundo real. Existen todavía brechas entre las características que habilita la tecnología y el dinero y otra brecha entre las posesiones de las personas que a veces están protegidas por la misma tecnología y el no tener la garantía de que estén en realidad seguras.

Desde el lado corporativo es posible que existan dos corrientes importantes, una es desde el lado emprendedor donde se ven intentos por brindarle al mercado algo innovador, diferente, orientado al cambio y que agregue valor en comparación con lo ya establecido. Pero desde el lado de las empresas establecidas y más específicamente para aquellas que son entidades financieras y bancarias; en adición a cumplir con las regulaciones, a las empresas podría preocuparles que la aplicación de monedas electrónicas pueda por ejemplo afectar sus ingresos gracias a su volatilidad y cambios abruptos de precios.

De acuerdo al nivel de dificultad de penetración en una industria y la compatibilidad de diferentes mercados, se traza el siguiente gráfico:



Fuente: Elaboración propia

10 CONCLUSIÓN FINAL

Adoptar un modo de operación autónomo descentralizado bien podría ayudar a las empresas y los gobiernos de alguna manera, pero si la eficiencia es una preocupación, no sugeriría usar este tipo de modus operandi, ya que tener una forma descentralizada de hacer las cosas significa que, por ejemplo, en el caso de las transacciones, cada una de estas debe ser validada por todos los participantes de una red lo que la hace tan eficiente como el menos eficiente de sus nodos. Es necesario que algunas cosas se hagan de manera centralizada si queremos que funcionen correctamente.

La transparencia, la confianza en la rendición de cuentas, la capacidad de auditoría y la seguridad, por otro lado, son beneficios que las organizaciones pueden obtener con la adopción de un modo de operación autónomo descentralizado.

Gobiernos, organizaciones, negocios o empresas deberían tener un acercamiento a esta tecnología de manera paulatina implementándola en partes de tus procesos y no pretender hacerlo en todas sus operaciones. Uno de los beneficios o ventajas de este tipo de estructura es que es altamente resistente a la corrupción ya que todas las acciones dentro del sistema son transparentes.

Si las transacciones son públicas, la auditoría se convierte en una tarea fácil, y dependiendo de la apertura del sistema, la información estaría disponible para el escrutinio de todo el mundo, o para ser más precisos, para quienes participan en el sistema. Con smart contracts, de manera generalizada, los participantes en la red pueden interactuar (enviar mensajes) con código de computadora lleno de habilidades que por si mismas pueden ser más, o menos estructuradas.

Gracias al incidente de la DAO, pudimos evidenciar que plataformas como la blockchain de ethereum, orientadas hacia facilitar casos de usos más complejos tienden a ser menos efectivas y sobre ellas tienden a construirse servicios secundarios. Es necesario un marco formal, dado que los errores en los contratos inteligentes tienen consecuencias económicas directas y en algunos casos

irreversibles. Con la facilidad y rapidez con la que pueden ser desarrollados, los programadores son propensos a cometer errores, por lo tanto, un marco de análisis formal para los errores en smart contracts es de gran importancia.

Confiar es importante, pero no tener la necesidad de hacerlo porque la confianza está dada por el sistema mismo es un cambio de paradigma por el que tendremos que cruzar, o no. Pero está claro que entre más nos valemos de algoritmos que van adquiriendo implicaciones políticas y sociológicas más profundas, esta nueva tecnología de la blockchain, llega prometiendo muchas cosas que pueden ser catalogadas como una esperanza ingenua, pero no se puede negar que esta red demuestra un crecimiento orgánico y resiliencia cada vez que se pone a prueba su anti fragilidad.

11 BIBLIOGRAFÍA

Antonopoulos, A (2017) Mastering Bitcoin. O´Reilly

Bambara, J.J.,Allen, P.R., Madsen, R., Lederer, S., Kedar Lyer, W. (2018) Blockchain: A Practical Guide to Developing Business, Law and Technology Solutions. McGraw-Hill

Belt, A., Kok, S. (2018) A reality check for blockchain commodity trading. The Boston Consulting Group

Berg, C., Davidson, S., Potts, J. (2017) The Blockchain Economy: A beginner´s guide to institutional cryptoeconomics. Recuperado en https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4

Brownworth, A. How Blockchain works. M.I.T Recuperado en http://blockchain.mit.edu/how-blockchain-works/

Buterin, and Vitalik. 2014. "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform," no. January: 1–36. https://github.com/ethereum/wiki/wiki/White-Paper.

Carson, B., Romanelli, G., Zhumaev, A., Walsh, P. (2018) Blockchain beyond the hype: What is the strategic business value? McKinsey&Company

Cuomo,J. (2018) Understanding blockchain: Debunking the myths of enterprise blockchain. Recuperado en https://www.ibm.com/blogs/blockchain/2018/05/understanding-blockchain-debunking-the-myths-of-enterprise-blockchain/

Drescher, D. (2017) Blockchain Basics. A Non-Technical Introduction in 25 Steps. Apress

Furlonger, D., Valdes, R., Kandaswamy, R. (2017) Hype Cycle for Blockchain Business, 2017. Gartner. ID: G00332628

Gartner (2017) Hype Cycle for Blockchain Business, 2017. Gartner.

Gartner (s.f) Gartner Hype Cycle. Recuperado en https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

Gilson, Ronald J, Charles F Sabel, and Robert E Scott. 2013. "Contract and Innovation: The Limited Role of Generalist Courts in the Evolution Novel Contractual Forms."

Gord, M., (2016) Smart Contracts Described by Nick Szabo 20 Years Ago Becoming Reality. Recuperado de https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/

Hileman, G., Rauchs, M. (2017) Global Blockchain Benchmarking Study. University of Cambridge

IBM (2017) Tomorrow's Value Chain How blockchain drives visibility, trust and eciency. The *Consumer Goods Forum and IBM.* Recuperado https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=REW03029USEN

Kandaswamy, R., Furlonger, D., (2018) Blockchain-Based Transformation: A Gartner Trend Insight Report. Gartner

Klappich, C., Tohamy, N., (2017) Hype Cycle for Blockchain Business, 2017. Gartner. Blockchain in Supply Chain. P25

Koens, T.,Poll, E., (2018) What Blockchain Alternative Do You Need? Recuperado en http://tommykoens.com/wp-content/uploads/2018/09/blockchain-alternative.pdf

Koonce, Lance, (2016) Let's Disintermediate All the Lawyers: Smart Contracts on the Blockchain

KPMG, (2018) Realizing blockchain's potential Introducing, KPMG blockchain technology risk assessment solution.

Lage S. O., (2017) ¿Es blockchain realmente inmutable? BBVA. Recuperado de: https://www.bbva.com/es/blockchain-realmente-inmutable/

Lakhani, K., Iansiti, M. (mayo, 2017) La verdad sobre Blockchain, *Harvard Business Review En español*. Recuperado de https://hbr.es/tecnolog/546/la-verdad-sobre-blockchain.

Idelberger, Florian, Guido Governatori, Régis Riveret, and Giovanni Sartor. 2016. "Evaluation of Logic - Based Smart Contracts for Blockchain Systems."

Lerner, Sergio (2015) RSK White Paper, Recuperado en https://docs.rsk.co/RSK_White_Paper-Overview.pdf

Mendez, D., (2015) Blockchain, la revolución tecnológica llega a la economía (parte 2) Recuperado en https://www.beeva.com/beeva-view/tecnologia/blockchain-la-revolucion-tecnologica-llega-a-la-economia-parte-2/

Morabito, V. (2017) Business Innovation through Blockchain. Springer

Mulligan, C., Zhu Scott, J., Warren, S., Rangaswami J.P., (2018)Blockchain Beyond the Hype A Practical Framework for Business Leaders. World Economic Forum

Nakamoto,S. (2008) Bitcoin: un sistema de dinero en efectivo electrónico peer- to -peer. Recuperado de https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

O'Keeffe, D. (2018) Understanding Cryptocurrency Transaction Speeds. Medium. Recuperado en https://medium.com/coinmonks/understanding-cryptocurrency-transaction-speeds-f9731fd93cb3

Peck, M.E. (2017) Do You Need a Blockchain? This interactive will tell you if a blockchain can solve your problem. IEEE SPECTRUM. Recuperado en https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

Popper, N., Lohr, S., (2017) Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter? The New York Times. DealBook

Roling, J., Peters, M., (2017) Blockchain for E&U Is it hype or reality? Recuperado en https://smartgrid.ieee.org/resources/94-resources/webinars/1014-demystifying-blockchain-for-energy-utilities. IEEE SmartGrid

Sreedhar, B., Bhatnagar, S. (2017) Blockchain Market, Global Forecast to 2022. MarketsandMarkets

Schneider, J., Blostein, A., Lee, B., Kent, S., Groer, I., Beardsley, E. (2016) Profiles in innovation, Blockchain putting theory into practice. Th Goldman Sachs Group, Inc.

Stewart Macaulay. 1974. "The Standardized Contracts of United States Automobile Manufacturers, The Impact of Large Scale Business Enterprise Upon Contract."

Swan, Melanie. 2015. Blockchain: Blueprint for a New Economy. https://books.google.com/books/about/Blockchain.html?id=RHJmBgAAQBAJ&pgis=1.

Wright, Aaron, and Primavera De Filippi. 2015. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia." Social Science Research Network. http://papers.ssrn.com/abstract=2580664.

Tapscott, D. (abril, 2018) Blockchain represents the second era of the internet, *52-Insights*.Recuperadodehttps://www.52-insights.com/don-tapscott-blockchain-represents-the-second-era-of-the-internet-interview/

Tapscott, D., Tapscott, A. (2016) Blockchain Revolution How the technology behind bitcoin is changing money, business, and the world. Penguin Random House LLC.

Tapscott, D., Tapscott, A. (2017) How Blockchain Is Changing Finance. HBR

World Economic Forum (2018) Annual Report 2017- 2018. Recuperado en https://www.weforum.org/reports/annual-report-2017-2018

Zach,C. (mayo, 2017). Blockchain, explained, MIT Management Sloan School. Recuperado de http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/?utm_source=mitsloantwitter&utm_medium=social&utm_campaign=blockchain

Zimmermann, Reinhard, and Simon Whittaker. 2000. "Good Faith in European Contract Law."

12 ENTREVISTAS

Entrevistados

- Matias Gallardo – CTO en Koibanx: Arquitecto Líder en Desarrollos de Software.
- Federico Ast – CEO y fundador de Kleros.io: PH.D. en Dirección de Empresas por IAE, Licenciado en Economía y Licenciado en Filosofía por UBA. Docente universitario, divulgador y periodista. Trabajó y fundó diversas startups tecnológicas.

- Maximiliano Del Hoyo – Desarrollador de negocios en RSK: Licenciado en Administración de Empresas por UBA, se especializa tecnología, finanzas, mercados emergentes y Bitcoin.
- Marcos Malamud – CEO Fundador de Malamud Consulting. Experto en tecnologías de alto impacto social enfocadas a brindar soluciones en el sector gobierno. Implementó de forma exitosa una blockchain basada en Ethereum que permite la trazabilidad de fondos públicos en el Municipio de Bahía Blanca.
- Lucas Jolias - Socio de Prince Consulting: Politólogo especializado en tecnologías de información y comunicación, y su impacto en la economía, el gobierno y la sociedad. Ha trabajado en proyectos de Blockchain, Smart Cities y gobierno digital en Argentina, Chile, Brasil, México y con organismos internacionales como el Banco Interamericano de Desarrollo y el Banco Mundial.
- Ariel Graizer - Presidente de la Cámara Argentina de Internet (ex CABASE): Especialista en Internet y regulaciones tecnológicas en Argentina. Participante del proyecto Blockchain Federal Argentina, representando al ámbito privado.
- Diego Angel Masini - Investigador e Ingeniero en Software en RSK: Especialista en implementación de proyectos de Blockchain e IoT.

Preguntas

¿Qué opinión tenés acerca de los smart contracts descentralizados?

Ventajas, desventajas, (Fortalezas, Oportunidades, Debilidades, Amenazas)

¿Qué proyectos de smart contracts descentralizados consideras más interesantes?

¿Conoces cuáles son los costos y tiempo que tiene un desarrollo de un proyecto con smart contracts que funcionen con una estructura descentralizada?

¿Crees que en un futuro los sc sean adoptados en el entorno legal?

¿Crees que en un futuro los sc sean adoptados en el ámbito de gobierno?

¿Qué opinión te merece la adopción tecnológica de los sc en una blockchain?

¿Crees que tienen futuro de manera descentralizada?

13 ANEXOS

Entrevista a Matías Gallardo Arquitecto de desarrollo Blockchain en Koibanx 4/7/2018

Respecto a los smart contracts tengo una posición intermedia no van hacer autónomos completamente, pero si transformarán en una herramienta eficiente, rápida fácil y transparente para operar con diversa cantidad de contratos.

Que una red de blockchain sea centralizada o descentralizada dependerá del caso de uso que se deba desarrollar. Creo que en el futuro la blockchain tenderá ser descentralizadas o a los sumo usar nodos federados.

La blockchain plantea un nuevo paradigma tecnológico y queda claro que es mucho más que un repositorio de datos compartidos de bajo costo o una herramienta de notariado de transacciones. Será necesario alinear los incentivos y controles para cada caso de uso.

Por el momento, el mayor costo de armar proyectos de desarrollo en blockchain o con smart contracts reside en el costo de capital humano. Aún es baja la cantidad de programadores con conocimientos para desarrollar proyectos con blockchain o smart contracts.

Los costos operativos que ofrece la tecnología blockchain son menores que los ofrecidos por las empresas líderes de servicios en la nube como Amazon o Google.

Por ejemplo, deployar un contrato en ethereum tiene un costo por única vez, que está determinado, por la complejidad algorítmica del contrato y la cotización de la moneda en ese momento. Luego cada contrato tiene un costo marginal de utilización por parte del consumidor.

Desarrollar en la blockchain permite aprovechar el servicio de ledger probado, contar con un sistema de backup automático y acceder a los datos en tiempo real en una red de alta disponibilidad con nodos en todo el mundo. Esto permite tener el core business del proyecto de software dentro de la blockchain.

Una amenaza que pueda surgir es que la tecnología no termine de adoptarse por el resto de la población por ser difícil de comprender para el usuario final. Los conceptos de minado, consenso distribuido, wallet o claves criptográficas son temas poco fáciles de abordar. Otra amenaza es el problema de la escalabilidad en sistemas completamente descentralizados.

Respecto a los hackeos que son noticia en los medios de comunicación, por lo general, están relacionados a robos en empresas de intercambio de criptodivisas que operan fuera de la cadena de bloques. La red de bitcoin o ethereum, que son descentralizadas y en la actualidad las más utilizadas cuentan con un sustento matemático y de arquitectura de software de buen diseño. Además las comunidades que están detrás de estos proyectos cuentan con fuertes incentivos de mejorar en caso de que surjan posibles bug o errores de programación inherentes a todo proyecto de desarrollo de software.

Los proyectos que me resultan más interesantes en el mundo blockchain son Plasma que pretende agregar escalabilidad a la red y Sharding con sus canales de pagos lighting network que permitiría acelerar los tiempos de transacciones entre los usuarios de la red.

Para que crezca la adopción de sistemas con blockchain es necesario crear más proyectos en la cadena de valor aumentando los actores en el ecosistema. Un ecosistema diverso permite generar mayor valor a la red. Por ejemplo, dentro de la blockchain de bitcoin las sidechains (especie de blockchain paralelas) están permitiendo desarrollar los primeros contratos inteligentes en bitcoin cuya red de bloques es la más popular.

La adopción de los smart contracts está todavía en sus inicios. Es necesario crear mayor cantidad de estándares, normalizaciones y buenas prácticas al momento de desarrollar contratos inteligentes. Con el tiempo se profesionaliza la creación de los contratos inteligentes. Por otro lado, la interoperabilidad y la creación de interfaces serán determinantes para aumentar la adopción tecnológica.

Una de las grandes ventajas de los contratos inteligentes, en una red que nace de la cultura open source, es que estos contratos son públicos lo cual permite que sean auditados y probados por todo una comunidad antes de ser utilizados.

La tecnología de blockchain ya tiene millones de dólares invertidos por una comunidad amplia y diversa que tiene como interés aumentar la adopción tecnológica por parte del usuario final.

Entrevista Federico Ast emprendedor y fundador de kleros.io 17/7/2018

Kleros.io es una plataforma para resolver disputas de forma descentralizada basadas en los principios de una dao como organización descentralizada. Es necesario contar con un programa balanceado de incentivos entre los integrantes de la red con el fin de lograr los objetivos que persigue el proyecto.

"Considero que blockchain es como el internet del año 95" Se encuentra en una fase inicial de early adopters. Actualmente lo más avanzado es el tema de remesas y

pagos internacionales. A los smart contracts todavía falta mucho para que llegue a una maduración tecnológica y además falta explotarlo en cuanto casos de uso y proyectos.

Considero que en un futuro cercano aparecerá una una killer app basada en smart contract donde la cuestiones legales se resuelvan todo desde esta plataforma.

Hoy kleros.io se ocupa de contratos concretos del tipo está o no esta lo pactado. Son muy pocos los proyectos de smart contracts que se ocupan de cuestiones legales y kleros es uno de ellos.

El ecosistema que rodea a los sc se encuentra en una fase inicial del cual también falta maduración. El market es lo más importante y necesario para mejorar la adopción de caras al usuario final.

Considero que en el futuro existirán tanto blockchain centralizadas como descentralizadas todas cumpliendo funciones específicas según su caso de uso. Ahora bien, la cantidad de blockchain, criptomonedas y smart contracts disminuirán a una pocas y no como la cantidad de cientos que hay hoy en día.

Me parece muy interesante la blockchain de Aragon que permite la creación de organizaciones descentralizadas (DAO) junto con modelos de gobernanza y Origin Protocol que ofrece una blockchain para servicios de sharing economy descentralizados similares a AirBNB o Uber.

Los gobiernos sin dudas en el corto tiempo van a empezar a adoptar la tecnología de blockchain para sus desarrollos y modelos G2B

Criptovalley Zurich Singapur BsAs y Berlin

Entrevista Maximiliano Del Hoyo de RSK 15/8/2018

La descentralización plena es una utopía

Hoy en día la tecnología de blockchain resulta lenta y cara. La mayoría de las aplicaciones son pruebas de concepto con muy pocas cosas productivas. La tecnología está en una fase de investigación pero avanzando de forma rápida.

Hoy el foco son la cantidad de transacciones por segundo.

Para la adopción a un mercado masivo todavía falta. Se requiere más ux que resulta un gran desafío y proyectos más amigables y madurar el ecosistema de servicios asociados.

Los casos y ejemplos de utilización con blockchain son los del tipo prueba de existencia como notarios patentamiento

Respecto a costos frente a la nube es necesario evaluar el caso de uso en particular. Por que el mercado está muy volátil y ecosistema en sus primeras fases.

Ventajas Fortalezas de los SC

Los SC son algoritmos con lógica de negocio que reemplazan la confianza por verdad matemática. Logran desintermediación en la cadena de valor de aquellos actores que no agreguen valor. En el futuro permitirán ahorrar en tiempos y costos en los procesos de negocios

Problemas

Se trata de software código y si esta mal escrito así como si tuvieran bug resulta un problema. La auditoría es importante.

Debilidad: Si el contrato no está bien escrito es propenso a ser hackeado

La consultoría, auditoría y seguridad está creciendo mucho (Zeppelin y Coinfabric)

Proyectos interesantes
CIVIC de identidad
Oraclise servicio de oráculos
Proyectos de storage distribuido storj
Servicios de directorios
Proyectos de lightning network Lumino
Cadenas de suministro supply chain (no hace falta confiar en el otro)

En gobierno Argentina tiene el boletín oficial en blockchain. Por otro lado, RSK y BID armaron una wallet para la villa 31 de identidad digital para dar servicio de serivicio financiero.

(NOTA: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/)

Este proyecto permite consumir un montón de servicios que tienen costos asociados importantes, otorga identidad digital y construcción de una reputación que levanta restricciones para ofrecer créditos.

LA MAYORÍA DE LAS COSA SON ANUNCIOS TODAVÍA LE FALTA A ESTA TECNOLOGÍA

El fenómeno es que se están reemplazando los procesos tradicionales por blockchain con sc permitiendo automatizar todo.

TODO SE ESTÁ REINVENTANDO

Entrevista Marcos Malamud de Malamud Consulting 20/8/2018

Hoy el blockchain es un hype poné un tema de agenda y atrae las moscas (hace ruido)

Hay algo de exuberancia irracional.

Es una tecnología interesante que permite descentralizar, distribuir con mecanismos criptográficos seguros. Es una herramienta más disruptiva en transparencia y estabilidad

Debilidades problemas de implementación, adopción (pocos desarrolladores), costos volátiles.

Amenazas vulnerabilidades en la construcción de SC como bugs o fallas de diseño en el sistema

La blockchain no existe sin una dapp

En sistemas de gestión el feature mas interesante es la inmutabilidad

Hoy una de las utilidades más real del blokchain es la de notariado.
En mi opinión crece más rápido el hype que la tecnología ya que todavía están en desarrollo y no ha tenido un apoyo fuerte por las grandes compañías tecnológicas (Amazon, Google, Facebook)

Amenazas
Robo de las ICO
Hay intereses de grandes players financieros que no tienen interes en que crezca la tecnología
Cuestiones de regulaciones que impidan el uso para algunos casos de uso

Debilidad

La red es lenta y los costos son muy volátiles

Los costos de mantenimiento (revisar el nodo actualizarlo, volatilidad del precio complica la automatización) Un airdrop en eht descalabro todo, saturó la red.

Los desarrollos en blockchain hoy son interesantes dependiendo del impacto que tiene el proyecto. Faltan grandes player sponsoreando.

SC reglas de negocio ejemplo de importación y el pago a cada uno de los actores en la cadena de valor

Entrevista Lucas Jolias de Prince Consulting 31/10/2018

Blockchain permite la eliminación de los intermediarios.

Es una tecnología disruptiva tanto en el plano económico y gobierno.

Ofrece una arquitectura tecnológica nueva para construir consenso.

El ledger de blockchain con su consenso ofrece confianza y resuelve conflictos.

Permite la **construcción de una verdad** así como fue el registro escrito.

Blockchain es una tecnología con un sistema de reglas y mecanismos de consenso que ofrecen un mecanismo de gobernanza unicos que incentivan a la desintermediación.

Smart Contracts la evolución en las cadenas de bloque permite casos como notariado digital, tokenización

Se busca siempre generar un valor agregado real y no usar blockchain por una cuestión de hype tecnologico. Esos son los proyectos que tendrán exito.

Blockchain y los SC generan cambios en los modelos de negocio. Ejemplo, en los bancos o en el Estado repensando los servicios que ofrecen. Sin embargo, no creo que blockchain mate a los bancos o al estado.

Ejemplo, la burocracia estatal fue creada para generar confianza, es decir, la necesidad de incluir un tercero en un proceso o transacción. Ahora bien, con Blockchain y su desintermediación bajan los costos de transacción asociados.

Confianza, consenso, cambios en las reglas de juego, cambio de fase o paradigma.

Entrevista Ariel Graizer de CABASE, Javier Días UNLP y Luciano MINUCHIN ARIU 31/10/2018

En Argentina se está desarrollando la blockchain federal argentina (BFA, https://bfa.ar/) inciativa organizada entre ARIU, CABASE y NIC. (Toda la información técnica en https://gitlab.bfa.ar/blockchain/docs/wikis/home).

La BFA ofrece procesos de auditoría mediante la verificación de información, certidumbre en fechas, inmutabilidad de los datos ingresados, acceso público.

La capa de servicios tiene timestamp, votación y contratos inteligentes.

Es una red semipública, permisionada de modelo liviano, sostenida por los miembros sin una criptomoneda asociada.

Proyectos actuales

- Notariado del Boletín Oficial de la República Argentina en blockchain (ver https://www.boletinoficial.gob.ar/#!estatica/certificacionBlockchain)

- Certificado de título universitario del sistema informatico universitario SIU

Proyectos futuros con smart contracts

- Registro del automotor
- Registro de la propiedad
- Salida de buques para la agencia de Prefectura

Entrevista Diego Masini RSK 31/10/2018

El Blockchain no es más que un registro distribuido con grandes capacidades de auditoría.

Ofrece una internet del valor.

Transacciones instantáneas

Costos marginales decrecientes con baja fricción.
Reserva valor (como el oro)
Contrato inteligente con lógica, automatico y consenso distribuido

Canales de pago

Capa de servicios como puede ser almacenamiento distribuido, dapps o frameworks.

El futuro de la blockchain trata los siguientes temas:
Servicios de nombre (equivalente a un dns para que las nros de wallet se acorten)
Canales de pago

Oráculos

Almacenamiento distribuido (sidechains)

Ver https://educate.rsk.co/ y https://ambassadors.rsk.co/

Blockchain cambio de paradigma en las reglas de confianza siendo abierta y descentralizada. Es necesario mejorar la experiencia de usuario para tener mayores de niveles de adopción en la gente. Además. debe haber un marco legal que acompañe a la tecnología.