UNIVERSIDAD DE SAN ISIDRO, DOCTOR PLÁCIDO MARÍN

LICENCIATURA EN ADMINISTRACIÓN DE NEGOCIOS

REVOLUCIÓN DIGITAL**: BLOCKCHAIN Y LOS SMART CONTRACT COMO UNA SOLUCIÓN A LOS CASOS DE ESTAFAS Y FRAUDES DIGITALES**

TESIS DE GRADO

Zaida Lissett Sanchez Quispe

TUTOR:

Federico Fernandez

Juan Silva

ÍNDICE

AGRADECIMIENTOS

El presente trabajo de tesis es fruto de extensas e intensas horas de formación en las que me sumergí por varios años de mi vida, quiero agradecer en primer lugar a Dios por haberme dado la oportunidad de formarme en un importante institución, con valores humanos loables, agradecer a cada maestro que he conocido en estos años de estudio, ya que cada uno de ellos ha ido dejando en mí una valiosa enseñanza. Agradecer a mi maestro de proyecto final, Sergio, gracias por tu exigencia y guía en este último paso de la carrera.

Doy un especial agradecimiento a mis tutores de proyecto, Federico y Juan, gracias por sus consejos, gracias por compartir conmigo sus conocimientos y expertise profesional.

Le doy gracias a este maravilloso país, Argentina, que me abrió las puertas y me brindó muchas oportunidades de crecimiento y desarrollo personal y profesional. Agradecer a una de las personas mas importante de mi vida, a ti madre gracias por permitirme nacer, gracias por haberme cuidado con amor y esmero, a ti te dedico mi felicidad y logros futuros, aunque ya no este mas es este mundo, eres mi mas preciado recuerdo de amor. Le doy gracias a mis hijos por ser el motor que impulsa mi vida, y es para ellos que deseo dejar una huella positiva en mi paso por esta vida.

Agradecer a mi gran amigo de la vida, gracias a ti soy la mujer que volvió a soñar y creer en sí misma. gracias por tu paciencia, gracias por tu confianza y sobre todo gracias por devolverme la fe en la humanidad.

1. INTRODUCCIÓN

En los años setenta en Estados Unidos se desarrollaba el Internet de la información a partir de un proyecto militar, desde su irrupción, su uso se masificó en todo el mundo hasta el día de hoy, internet ha permitido conectar personas e instituciones sin importar las distancias. La tecnología ha cambiado drásticamente la forma en que nos relacionamos, la forma en que operamos dia a dia, es casi inconcebible pensar en realizar un trámite o transacción de manera presencial es decir yendo a un lugar físico, ya que desde de la irrupción de internet en la década de los 90 nuestra vida, nuestros hábitos, y costumbres, se han ido modificando, llevándonos cada vez más cerca a una economía digital, hoy todo es más accesible más sencillo, podemos comprar, trabajar, estudiar, socializar, realizar transacciones, casi todo a tan solo un clic, utilizando un dispositivo móvil o una computadora y lo podemos hacer desde cualquier lugar del mundo, siempre y cuando se disponga de una conexión a internet.

La tecnología juega un papel muy importante en nuestras vidas, ya que ha contribuido al desarrollo y progreso humano, en múltiples dimensiones, ha facilitado de alguna forma el trabajo y los esfuerzos enfocados al desarrollo e innovación, están dando como resultado nuevas tecnologías que emergen en pos del beneficio de la humanidad.

En el presente trabajo de investigación abordaremos la tecnología blockchain y los contratos inteligentes (smart contract), sus múltiples aportes al desarrollo tecnológico, y sobre todo el gran impacto que está teniendo en diversas industrias, en especial en el sector financiero, aunque, cabe recalcar que se trata de una tecnología relativamente nueva que se encuentra en pleno desarrollo y sobre la cual se ejecuta los smart contract . Los contratos inteligentes (smart contract) son programas computacionales que se ejecutan sobre la red blockchain, él término fue acuñado por primera vez en 1994 por el criptógrafo Nick Zsabo, no pudiendo desarrollarse en esa época debido a la inexistencia de la tecnología adecuada para ejecutarlos o llevarlos adelante.

La digitalización ha traído consigo múltiples problemas aparejados ya que cada vez son más las actividades que realizamos a través de celulares, computadoras o tablets, prácticamente toda nuestra vida se está mudando al entorno digital, por una parte las innovaciones tecnológicas hacen que nuestra vida sea mas comoda y confortable pero por otra parte son las causantes de otros males que podrían resolverse gracias a la red Blockchain pues por tratarse de una red descentralizada hace que no dependamos de una red central para realizar operaciones entre 2 o más partes, ya que estos entes centralizados actúan como árbitros garantizando que los acuerdos se cumplan pero están propensos a procesos

burocráticos, altos costos y errores humanos y por no mencionar los escandalos de las grandes corporaciones por el manejo de forma antiética de la información personal, pues los datos personales son considerados el nuevo oro negro de la época, con lo cual estas grandes corporaciones lucran.

Los smart contract pueden tener múltiples aplicaciones ya que al tratarse de programas computacionales funcionan mediante un lenguaje de programación que puede ser aplicado a cualquier industria pues mediante ellos se garantiza que lo pactado se cumpla es de decir si sucede X se ejecuta Y tan simple como eso y en la actualidad existen diversas plataformas que están ofreciendo el servicio así de esta forma no se tendrá la necesidad de contratar un programador especializado si deseamos ejecutar un smart contract.

Cabe mencionar que la globalización digital borró las fronteras entre países y son cada vez más las personas interesadas en trabajar para otros países sin tener la necesidad de mudarse, haciendo trabajo freelance, pero corren el riesgo de ser estafados porque por lo general consiguen los trabajos por medio de páginas webs. Pero las plataformas no garantizan la veracidad de los contratantes es decir ellas no garantizan si el trabajador freelance recibirá el pago pactado por el trabajo realizado, es hay donde los Smart contract ofrecen una soluciòn ya que estos contratos inteligentes son programados con ciertos requerimientos y se ejecutarán una vez se haya cumplido el plazo establecido y una vez ambas partes hayan cumplido con lo pactado, dejando de esta forma fuera cualquier intento de fraude.

Lo mismo sucede con los negocios en el ecosistema digital ya que empezamos hacer operaciones comerciales con personas que no conocemos, ¿cómo nos aseguramos que no estamos frente a un posible fraude? pues muchos delincuentes han aprovechado las vulnerabilidades que ha ocasionado la expansión de internet, para cometer delitos. Blockchain y los smart contract son una posible solución a dichas problemáticas en el ecosistema digital.

2. HIPÓTESIS

"BLOCKCHAIN Y LOS SMART CONTRACT REPRESENTAN UNA POSIBLE SOLUCIÓN A LOS CASOS DE FRAUDES Y ESTAFAS DIGITALES"

Esta tecnología es la nueva realidad y en los últimos años viene cambiando la manera en que gestionamos la información, blockchain puede compararse con la aparición de internet por el gran cambio disruptivo a nivel global que está generando

La hipótesis es una suposición de algo posible o imposible para sacar de ello una consecuencia (Real Academia Española 2014)

Según Izcarra (2014) una hipótesis es una tentativa de solución a través de preposiciones que intenta dar respuesta al fenómeno investigado, una hipótesis merece la pena ser abordada con una mente abierta para así dar lugar al conocimiento sin sesgos predeterminados y no necesariamente una hipótesis se valida como verdadera, puede que el resultado arroje una validación errónea , no significando que se haya tratado de una pérdida de tiempo o un trabajo infructífero, al confirmar que una hipótesis es nula se hace una contribución al conocimiento.

Cabe aclarar que la primera parte de un trabajo de investigación no es la hipótesis sino el planteamiento de la problemática para su posterior abordamiento basado en aportes previos realizados por otros autores, una vez empapados de la bibliografía previa, se procederá al planteamiento de la hipótesis que puede usarse como una medida provisional sin la necesidad de ser validada estrictamente o puede ser una predicción que debe ser verificada por el método científico. Existe una relación muy estrecha entre la revisión de la bibliografía, el planteamiento del problema y la hipótesis, un acercamiento inicial a la literatura para familiarizarnos con el problema nos lleva al planteamiento del problema para la posterior formulación de la hipótesis.

3. PROBLEMÁTICA

La confianza y la seguridad son una de las principales problemáticas a la hora de hacer transacciones o negocios a través de internet ya que necesitamos de un ente central que se encargue de garantizar que los acuerdos se cumplan tal como se pactaron. Sin embargo un ente centralizado no garantiza totalmente que los acuerdos puedan cumplirse, además están propensos al error humano, corrupción y sobre todo son vulnerables a ser víctimas de un ciberataque, por parte de agentes malintencionados. De darse un ataque a la base de datos del

ente central, dicha información podría ser utilizada para un fin delictivo. Además de representar una pérdida financiera.

La pandemia de covid 19, que venimos enfrentando desde finales de 2019, aceleró el proceso de digitalización que se venía dando en diferentes sectores de la economía, esto hizo de alguna forma sumergirnos en la llamada economía digital, la cual tiene características empoderadoras para los países a nivel global pero también tiene una cara negativa. ya que según noticias de los últimos años también hizo que se incrementen los hechos delictivos que se realizan dentro del ecosistema digital.

4. JUSTIFICACIÓN

Blockchain marcará un antes y un después de la sociedad que hoy conocemos como tal, ya que todo nuestro sistema financiero, económico, social y cultural se encuentran centralizados en un ente, con un poder enorme, sobre diferentes aspectos de nuestras vidas, ya sea en forma de Estado o como grandes corporaciones privadas, que están de alguna forma tomando decisiones por nosotros, lo que Blockchain viene a cambiar es esa centralización y darnos una mayor libertad pues gracias a su red descentralizada hace que sea inmutable, segura, transparente y privada casi imposible de falsificar muy contrario a las redes centralizadas que están propensas al error y corrupción humana.

5. OBJETIVOS

- Demostrar como blockchain está trayendo un cambio de paradigma en la forma actual que operamos como sociedad y su impacto a nivel global
- Los grandes desafíos en el sector empresarial y económico que se vendrán dando ya que Blockchain está abriendo paso a un ecosistema de negocios descentralizados basados en una tecnología relativamente nueva.
- Investigar la eficiencia y limitaciones de los smart contract
- Investigar casos de éxitos y fracasos de los smart contract
- Investigar el desarrollo de blockchain en Argentina

6. PREGUNTAS DE LA INVESTIGACIÒN

¿Que es blockchain y cuales son sus características?

¿Porque Blockchain va mucho más allá de las criptomonedas?

¿Por qué blockchain puede ser considerada una tecnología disruptiva?

¿Todas las empresas pueden beneficiarse de blockchain?

¿Qué nuevos modelos de negocios está generando Blockchain?

¿Qué son los smart contract

¿En qué tecnología están basados los smart contract?

¿En qué ámbitos pueden ser aplicados?

¿Puede la blockchain y los smart contract ser una solución a los casos de fraudes y estafas digitales?

¿Qué nuevos modelos de negocios utilizan Smart contract?

¿Cuáles son las ventajas de uso de los smart contract?

¿Cuáles son las limitaciones de los smart contract?

7. METODOLOGÍA DE LA INVESTIGACIÓN

El método científico se entiende como el conjunto de postulados, reglas y normas para el estudio y la solución de los problemas de la investigación que son institucionalizados por la denominada comunidad científica reconocida. En un sentido más global el método científico se refiere al conjunto de procedimientos que, valiéndose de los instrumentos o las técnicas necesarias, examina y soluciona un problema o un conjunto de problemas de investigación. (Bernal, 2006)

Según Cerda, el método tiene que ver con la metodología que se examina desde dos perspectivas; metodología de investigación cuantitativa y metodología de la investigación cualitativa.El método cualitativo o método no tradicional, se orienta a profundizar casos específicos y no a generalizar, su prioridad no es necesariamente medir, sino cualificar y describir el fenómeno a partir de rasgos determinantes, según sean percibidos por los elementos mismo que están dentro de la situación estudiada.

El presente proyecto de tesis será abordado desde la metodología de la investigación cualitativa, ya que el estudio e investigación de la tecnología blockchain en profundidad, podría revelar interesantes aspectos y posibles usos, para dar una respuesta efectiva a algunos de los problemas derivados de la globalización digital. Es de suma importancia garantizar aspectos como la confianza y seguridad dentro del sistema de la economía digital, puesto que pueden ser consideradas ejes transversales que permiten movilizar una economía hacia el desarrollo sostenible.

MARCO TEÓRICO

8. TECNOLOGÍA BLOCKCHAIN

ANTECEDENTES

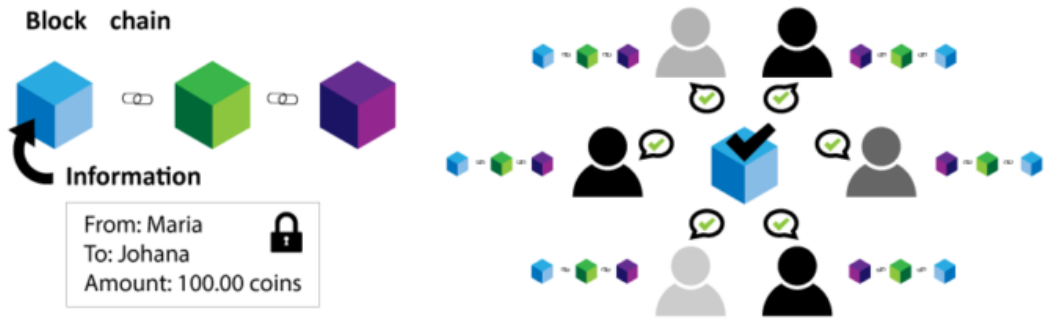
Blockchain surge en 2008, cuando una persona o un grupo de personas bajo el seudónimo de Satoshi Nakamoto, hacen la publicación de un documento, "white paper" dando origen, así, al proyecto Bitcoin. El origen del dinero digital fue posible gracias al desarrollo de un sistema de seguridad prácticamente impenetrable, este sistema se desarrolló combinando la tecnología de redes ya existentes (P2P) con técnicas criptográficas avanzadas

Blockchain puede definirse como un libro digital compartido que abarca una lista de bloques conectados y almacenados en una red distribuida, descentralizada y protegida mediante criptografía, sirviendo como un depósito de información irreversible e incorruptible. Las transacciones registradas, que pueden involucrar cualquier tipo de valor, dinero, propiedad o votos (Beck & Muller-Bloch, 2017, p 5390) no pueden modificarse retroactivamente sin alterar todos los bloques subsiguientes; de hecho los nuevos bloques son validados por pares en la red , otorgando credibilidad y evitando actividades maliciosas (Wringh &De Filippi , 2015, p 8-9)

Si bien la primera cadena de bloques vino de la mano de la criptomoneda Bitcoin, actualmente se ha extendido esta tecnología, existiendo cadenas públicas, cadenas privadas y cadenas híbridas, Las plataformas públicas que operan en un marco descentralizado, permiten a cualquiera agregarse a la red, leer transacciones, transferir activos y participar en el proceso de consenso, las privadas de naturaleza centralizada y con estricta autorización se caracterizan por ser más rápidas, permitiendo operar solo a ciertos miembros autorizados, siendo sus principales funciones la auditoría y gestión interna (Leonard, 2017, p 3;Garzik & Bitfury Group, 2015, pp 10-11). Las híbridas se caracterizan por ser todas las transacciones públicas, pero los nodos participantes son invitados (Legeren Molina, 2019, p 180).

En términos simplificados, la blockchain es un registro distribuido e indeleble, su funcionamiento se da a través de nodos que son computadoras participantes que están por voluntad propia a las blockchain abiertas o por invitación a las blockchain cerradas, estos nodos se consideran iguales entre sí , comparten un consenso o un protocolo, bajo el cual se realizan las transacciones, se van registrando la información y se va generando la cadena de bloques.

[1]



Fuente IBM

8.1 BENEFICIOS DE LA BLOCKCHAIN

8.1.1 INMUTABLE

Inmutabilidad significa que algo no puede ser cambiado o alterado, esta es una de las características de blockchain que ayuda a garantizar que la tecnología se mantenga como un red inalterable. La tecnología blockchain funciona ligeramente diferente a la del sistema bancario tradicional, en lugar de confiar en las autoridades centralizadas, la confianza está distribuida a través de una colección de nodos.

Cada nodo del sistema tiene una copia digital del registro, para agregar una transacción cada nodo necesita verificar su validez. Si la mayoría piensa que es válido, entonces se agrega al registro, esto garantiza la transparencia y la hace a prueba de corrupción.

Por lo tanto, sin el consentimiento de la mayoría de nodos, nadie puede agregar bloques de transacciones al registro, otro hecho, respalda las características de la blockchain, es que una vez que los bloques de transacciones se agreguen al registro, nadie puede cambiarlo. por ende ningún usuario de la red podrá cambiarlo, editarlo o eliminarlo.

[1]

8.1.2 DESCENTRALIZADA

La red está descentralizada, lo que significa que no posee ninguna autoridad que lo gobierne o una sola persona que ejerce control total en lugar de eso una red de nodos mantiene la descentralización .

Esto es una de las características más importantes de la tecnología blockchain que funciona perfectamente, es decir blockchain coloca a los usuarios en una posición directa. El sistema no requiere ninguna autoridad de gobierno .

Se puede almacenar cualquier cosa desde criptomonedas, documentos importantes, contratos u otros activos digitales valiosos, con la ayuda de blockchain se tiene control directo sobre ellos usando la llave privada, por ende la estructura descentralizada le está dando a la gente el poder sobre sus activos.

¿POR QUÉ ES TAN ÚTIL?

- MENOS FALLO: Blockchain está completamente organizado y como no depende de cálculos humanos es altamente tolerante a fallos por lo tanto las fallas accidentales no son un caso habitual
- CONTROL DE USUARIO: Con la descentralización, los usuarios tienen más control sobre el control de sus activos por ende no tienen que depender de terceros para acceder el manejo de sus propiedades
- MENOS FALLAS: Gracias a su descentralización le otorga una ventaja a cualquier ataque malicioso, esto se debe a que atacar el sistema es más caro para los piratas informáticos por lo tanto es menos probable que ocurra.
- SIN TERCEROS:La naturaleza descentralizada de la tecnología la convierte en un sistema que no depende de empresas como intermediarios, sin terceros, sin daño añadido
- CERO ESTAFAS: Gracias a que el sistema de ejecuta en algoritmos, no hay posibilidad que sus usuarios sean estafados es decir la red no puede ser manipulada sin el consenso de todos los nodos participantes
- TRANSPARENCIA: La naturaleza del sistema hace posible crear un perfil transparente de cada participante , cada cambio en la blockchain es visible y lo hace un sistema robusto.

8.1.3 SEGURIDAD MEJORADA

A medida que se elimine la necesidad de una autoridad central. No se puede cambiar simplemente cualquier característica de la red para beneficio propio, el uso del cifrado garantiza otra capa de seguridad para el sistema.

La criptografía establece otra capa de protección para los usuarios, la criptografía es un algoritmo matemático bastante complejo que actúa como un firewall para ataques, toda la información en la blockchain se ha cifrado criptográficamente, cualquier dato de entrada pasa por un algoritmo matemático que produce un diferente tipo de valor, pero la longitud siempre es fija.

Podría ser considerada como una identificación única para cada dato, todos los bloques en el registro vienen con un hash único y contienen el hash del bloque anterior, por lo tanto cambiar todas las identidades de hash es algo imposible, se tendrá una llave privada para acceder a los datos pero también una clave pública para realizar transacciones

8.1.4 TRAZABILIDAD

Se puede seguir el rastro de cualquier transacción realizada, ya que las transacciones son públicas, esto permite auditar y seguir cualquier transacción, este es precisamente el parámetro que hace que las criptomonedas como Bitcoin o Ethereum no sean óptimas para las actividades ilícitas.

8.1.5 PRIVACIDAD

No se almacena información alguna de los usuarios que operan en la red. Se confunde muchas veces privacidad con el anonimato, algo que la tecnología blockchain no ofrece, porque el anonimato sería la imposibilidad de rastrear transacciones, haciendo imposible conocer el emisor y receptor de los fondos, dentro de la red blockchain de Bitcoin o Ethereum se puede saber quien es el emisor y el receptor.

8.1.6 OPEN SOURCE (Código abierto)

El código de la tecnología blockchain es accesible a todo el mundo ya que está a disposición de todos, cualquiera puede trabajar sobre el código, editarlo, modificarlo.

8.2. CUADRO COMPARATIVO ENTRE SISTEMA CENTRALIZADO Y DESCENTRALIZADO

Características	**Sistema centralizado**	**Blockchain**
Administración de la información	Existe un administrador de la información	La información se encuentra descentralizado
Sistema de seguridad	El administrador debe implementar un sistema de seguridad con la fiabilidad de proteger la información La estructura de los mecanismos de seguridad está en manos del administrador o de un tercero señalado por el ente, sin que por ello, el administrador deje de ser responsable.	Existe un sistema criptográfico, el cual puede variar a través de los mecanismos de clave pública y privada
Transparencia	El administrador establece los mecanismos por los cuales los participantes accedan a la totalidad de la información dentro de los protocolos establecidos.	Los participantes del sistema tienen la posibilidad de acceder a la información y verificarla por medio de la cadena de bloques
Costos	Requiere de mantenimiento tanto la estructura tecnológica, como en materia de ciberseguridad por parte del administrador del sistema.	Hay una reducción de costos, ya que el manejo de la información es reemplazada por códigos algorítmicos, los cuales a través de los nodos, procesan y verifican la información de forma independiente de cada transacción
Alterabilidad de la información	Depende del sistema tecnológico de ciberseguridad con que cuenta el administrador, los cuales no son inmunes a ataques cibernéticos.	Al existir una descentralización de la información, la cual está organizada y distribuida en cadena de bloques, la manipulación y la alteración de la información es poco probables que ocurra

Fuente: Elaborada sobre la base de Preukschat (2017)

8.3 ELEMENTOS DE LA BLOCKCHAIN

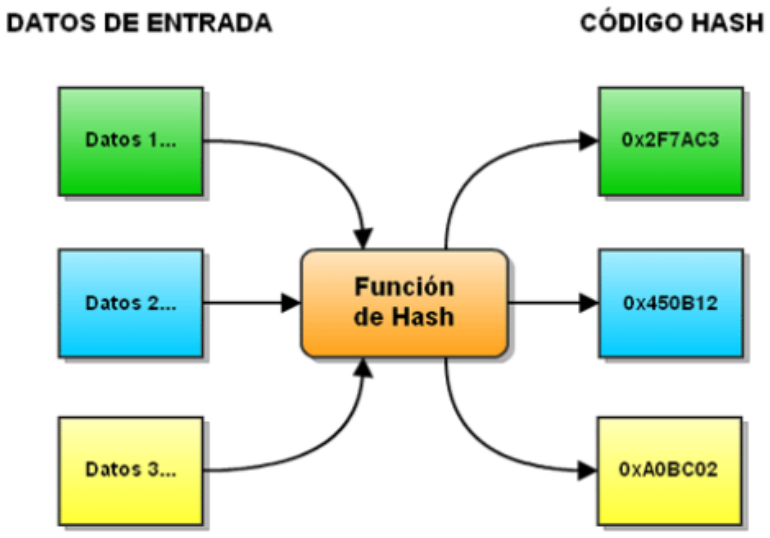
Para entender mejor la blockchain es necesario conocer los elementos que la componen.

8.3.1. FUNCIONES HASH

Una función hash es una función matemática con algunas propiedades especiales, sin embargo, como cualquier otra función, cumple con un objetivo específico. La función hash recibe una entrada y produce una salida, también llamado valor hash.

No es obligatorio que la entrada sea un número, puede ser cualquier tipo de información , desde un solo carácter hasta un archivo pesado como un video, la salida de una función hash tiene una extensión constante sin importar la entrada hay muchos tipos de funciones hash y la mayoría incluye en su nombre la extensión de la salida que producen, una de las funciones hash más utilizadas es SHA-256 (secure Hash Algorithm 256). El número indica que la salida siempre tendrá 256 bits sin importar la extensión de la entrada.

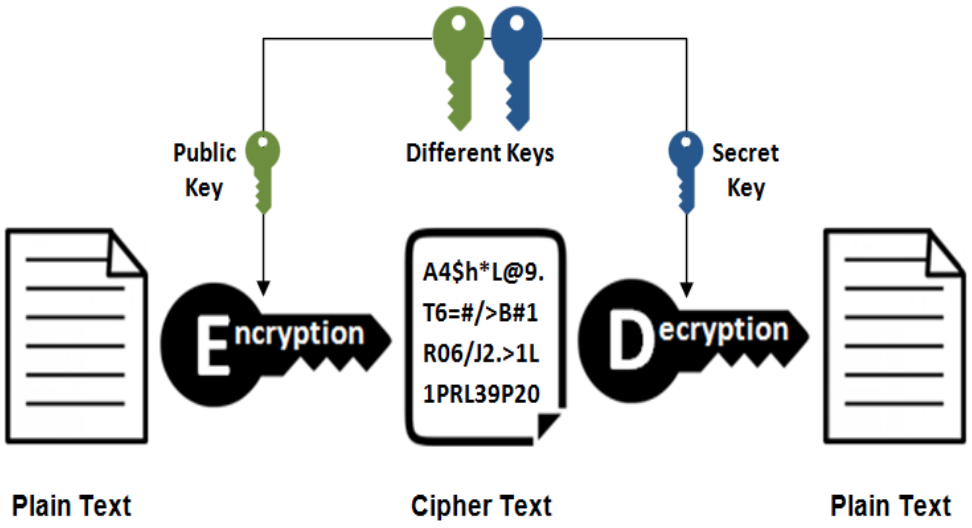
El valor hash funciona como la huella digital de la información, es posible que el usuario verifique la integridad de los archivos o que detecte si difieren entre sí.



Fuente IBM

8.3.2. CRIPTOGRAFÍA DE LLAVE PÚBLICA Y LLAVE PRIVADA

La criptografía de llave pública o también conocida como criptografía asimétrica, recibe su nombre del hecho que las llaves siempre están emparejadas, si el usuario ha encriptado información con una de las llaves, necesitará la otra llave para desencriptar y viceversa. Estas llaves son la llave pública y la llave privada o secreta, las llaves del usuario se traducen a su identidad en la cadena de bloques, por lo puede recibir fondos con su llave pública y enviarlos con la privada. La criptografía de llave pública es también el origen del término criptomoneda.

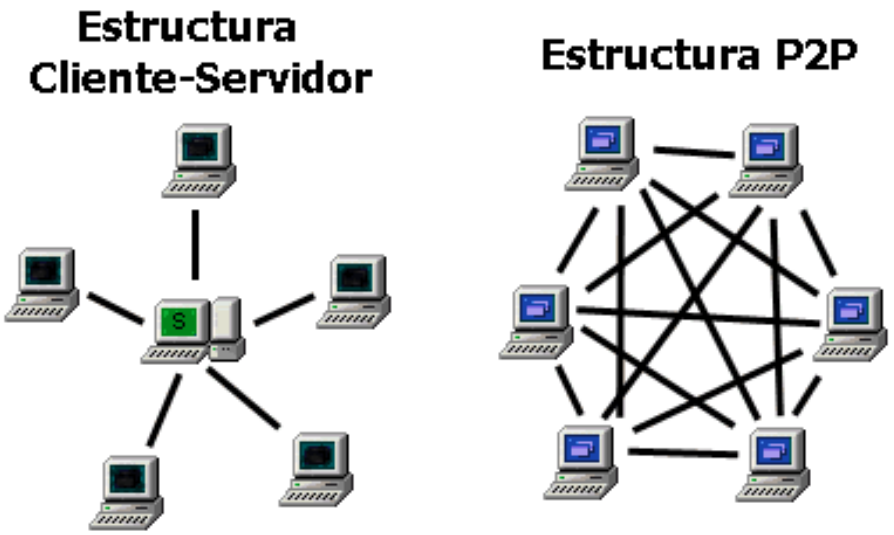


Fuente IBM

8.3.3 REDES PAR A PAR (P2P)

El consenso de una red par a par (P2P) es bastante común, en especial en el contexto de servicios de intercambio de archivos como BitTorrent. En una red descentralizada, los usuarios no se conectan a un servidor o entidad central para acceder al servicio, sino al resto de sus pares. Los pares son otros participantes de la red que se proporcionan al servicio entre si. Las redes P2P son resilientes, pues no existen puntos individuales expuestos a fallas, las cadenas de bloques las emplean regularmente, otra de las razones que la hacen robustas.

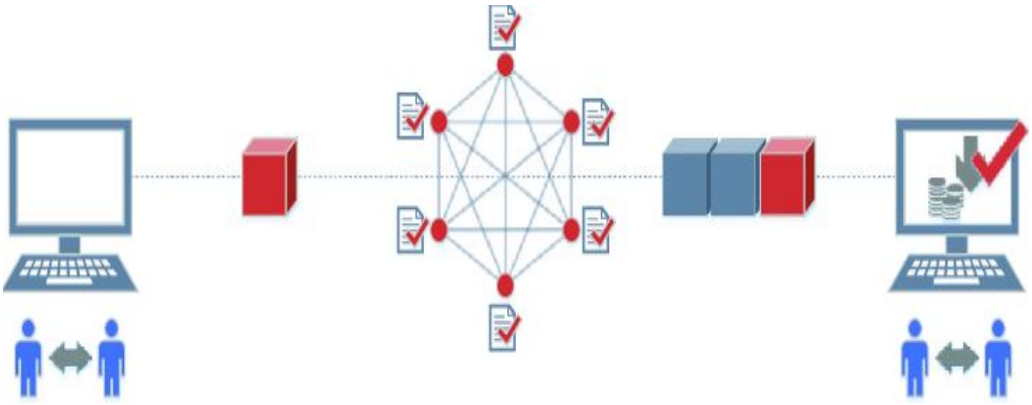
Para que el usuario cree una transacción o consulte su saldo le pide a los demás pares (nodos) de la red que conservan una copia de la cadena de bloques que le compartan la información que poseen. (Bitme. 2022)



Fuente: Cointelegraph

8.3.4 MECANISMOS DE CONSENSO

Si el usuario desea crear una especie de moneda digital en una red P2P con muchos participantes, se verá obligado a llegar a un consenso con todos sobre el orden de las transacciones. Si un usuario tiene un Bitcoin y crea dos transacciones distintas que gastan la misma moneda simultáneamente, habrá unos pares que reciben primero la versión A, la red debe llegar a un acuerdo sobre cuál transacción ocurrió primero, el mecanismo de consenso es lo que permite que una multitud de entidades que no se conocen ni se tienen confianza lleguen a un acuerdo sobre lo ocurrido

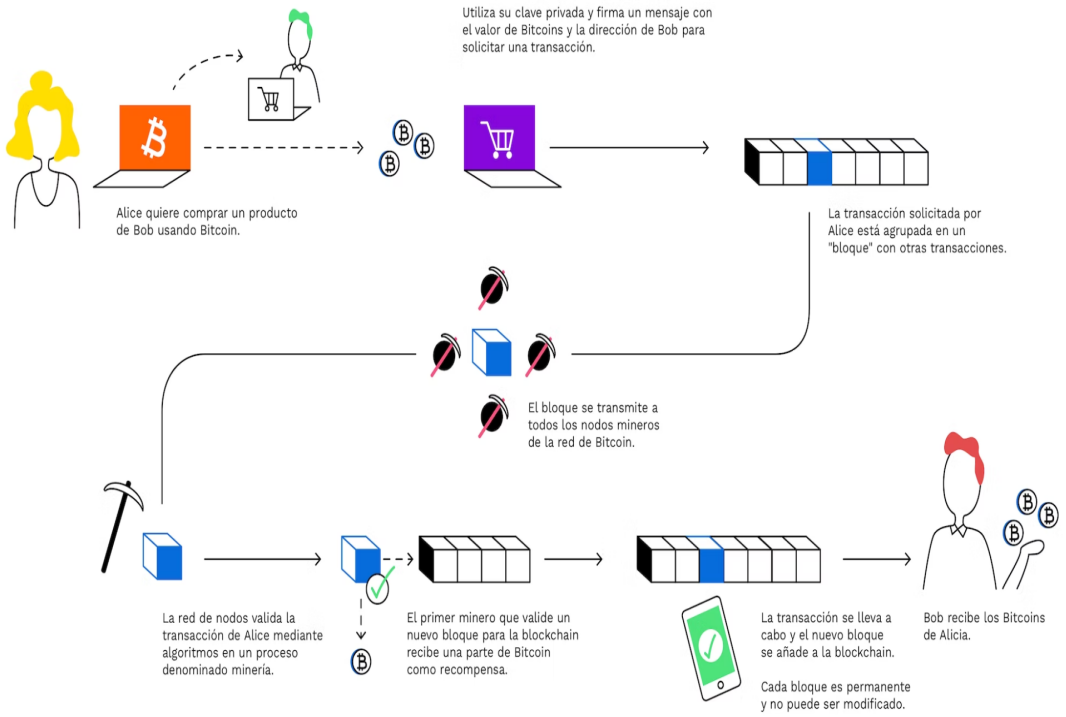


Fuente: Cointelegraph

8.3.5 PROOF OF WORK

Existen muchos mecanismos de consenso, el original o aquel que utilizan Bitcoin y muchas otras criptomonedas es el mecanismo de prueba de trabajo (proof of work). El concepto de minar una criptomoneda es bastante común, la prueba de trabajo lo realizan los mineros que compiten por crear bloques nuevos repletos de transacciones procesadas, el ganador comparte el nuevo bloque con el resto de la red y gana algunas criptomonedas minadas recientemente. El ganador de la carrera será el ordenador del minero que consiga resolver el problema matematico con más rapidez, esto produce el enlace criptográfico entre el bloque actual y el anterior, resolver este acertijo se le denomina prueba de trabajo, una de las características que deberá tener el ordenador que desee minar es un gran potencial computacional que estos a su vez consumen una gran cantidad de energía eléctrica

Los mineros son participantes de la red que tienen un papel fundamental en cualquier sistema de criptomonedas ya que son los responsables de validar y agrupar en bloques, transmitir y registrarlas, emplean un alto poder computacional necesario para resolver un puzzle criptográfico que se requiere al validar cada bloque. (IBM. 2021)



Fuente: IBM

8.3.6 PROOF OF STAKE (POS)

Recientemente la blockchain de Ethereum se ha trasladado al mecanismo de consenso, llamado prueba de participación (POS) desde la prueba de trabajo (POW). La prueba de participación es un tipo de mecanismo de consenso que usan las redes descentralizadas de blockchain para lograr consensos distribuidos.

Esto requiere que los usuarios participen con sus ETH (moneda nativa de Ethereum) para convertirse en un validador de la red, al igual que los mineros, los validadores son los responsables durante la prueba de trabajo deben ordenar las transacciones y crear nuevos bloques para que todos los bloques puedan coincidir con el estado de la red, la prueba de participación incluye una serie de mejoras para sistema prueba de trabajo.

- Mejor eficiencia energética, no necesitas usar mucha energía para minar los bloques.
- Barreras de entrada bajas, no se necesita un hardware del primer nivel para tener la oportunidad de crear un nuevo bloque.
- Mayor descentralización, la prueba de participación debería contribuir a la creación de nuevos bloques.
- Una mejora clave en la escalabilidad de la red Ethereum.

8.4 TIPOS DE REDES DE BLOCKCHAIN

En la actualidad existen distintos tipos de blockchain cada una con sus características y capacidades únicas que son adaptables a distintas necesidades. Estas clasificaciones de blockchain son la pública, la privada y la híbrida o federada.

8.4.1 **Blockchain pública**

Fué el primer tipo de blockchain que existió y se refiere a las blockchain que están públicamente accesible desde internet. A manera de ejemplo podemos nombrar a la red Bitcoin, Ethereum, Dash, Monero o Zcash. todas ellas mantienen abierto al público sus datos su software y su desarrollo a modo que cualquier persona puede revisar, auditar, desarrollar o mejorar los mismos (Bitme, 2022)

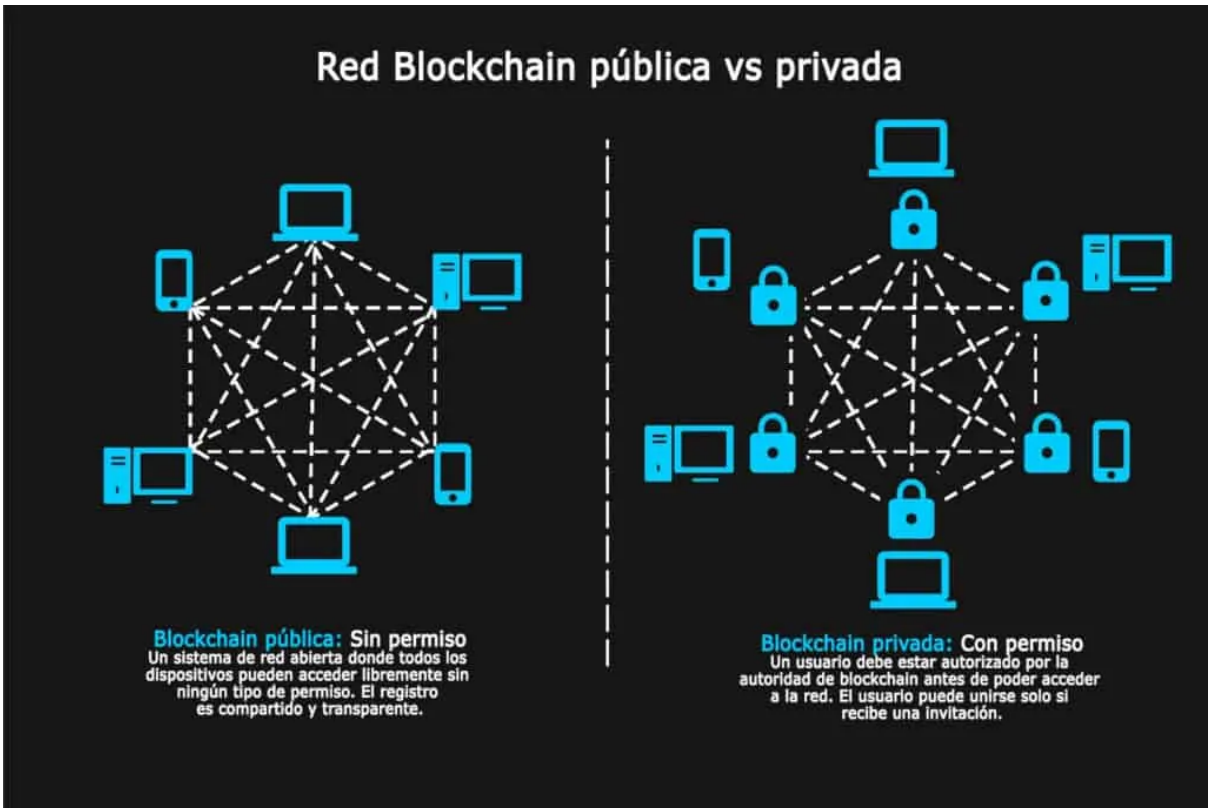
Para lograr eso, las blockchain públicas tienen medidas de seguridad que garantizan que ningún actor malicioso puede fácilmente alterar el funcionamiento de la misma. Es ahí donde entran en acción la tolerancia a las fallas Bizantinas en la programación, protocolos de consenso robustos, procesos DDos o contra ataques del 51% o el doble gasto. En pocas

palabras cualquier medida que ayude a mejorar la seguridad de la red es implementada en la misma, el objetivo es mantener la red funcionando y preservar su descentralización

CARACTERÍSTICAS DE LA BLOCKCHAIN PÚBLICA

Entre sus principales características podemos mencionar:

1. Las blockchain públicas permiten que cualquier persona pueda formar parte de la red, bien sea como usuario, minero o administrador de un nodo así que las personas pueden formar parte de la red sin restricción alguna
2. El funcionamiento de la red es completamente transparente y abierto. Los datos de la blockchain desde sus inicios están disponibles para todos sin restricciones, cualquier persona puede revisar o auditar el funcionamiento de la red y su software.
3. No existen autoridades centralizadas. las redes públicas son completamente descentralizadas y no existe autoridad central que regule su funcionamiento
4. El mantenimiento económico de la blockchain depende del sistema integrado de la misma. Generalmente este sistema depende de la minería y el cobro de comisiones por cada transacción de la red



Fuente: Bitme.academy

8.4.2 BLOCKCHAIN PRIVADA

con la evolución de la tecnología blockchain y su rápida expansión, muchas empresas se vieron interesadas en ella, esto trajo el desarrollo de soluciones blockchain privadas, por lo general cuentan con los mismos elementos que una blockchain pública pero a diferencia de estas, las blockchain privadas dependen de una unidad central que controla todas las acciones dentro de la misma.

Esta unidad central es la que permite dar acceso a los usuarios, además de controlar sus funciones y permisos dentro de la blockchain, normalmente son opciones de desarrollo del tipo de software privativo, aunque también hay desarrollo de software libre. Uno de los desarrollos de blockchain privada más importantes del mundo criptográfico es Hyper Ledger, este proyecto iniciado por la fundación Linux y varias empresas del sector tecnológico es el mayor ejemplo de blockchain privadas, también podemos mencionar el caso Corda de R3 o Quórum de Jp Morgan.(Bitme, 2022)

CARACTERÍSTICAS DE LAS BLOCKCHAIN PRIVADAS

Entre las características principales podemos mencionar

1. El acceso a la red está restringido a elementos que solo pueden ser autorizados por la unidad de control central
2. El acceso al libro de transacciones o cualquier otro medio de información generado por la blockchain es privado
3. El mantenimiento económico de la blockchain depende normalmente de la empresa que sostiene el proyecto. Con frecuencia, las blockchain privadas no cuentan con criptomonedas ni se realizan acciones de minería

8.4.3 BLOCKCHAIN HÍBRIDA O FEDERADA

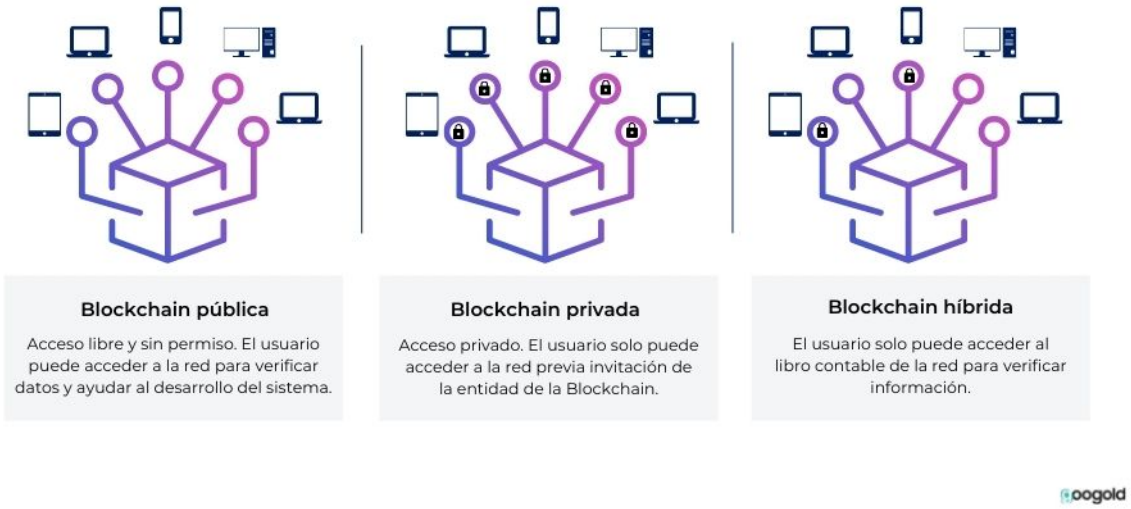
Este tipo de blockchain es una fusión entre las blockchain públicas y privadas. Es un intento de aprovechar lo mejor de ambos mundos. En esta red la participación en la red es privada, es decir el acceso a los recursos de la red es controlado por una o varias entidades, sin embargo el libro de registros es accesible de forma pública, significa que cualquier persona puede explorar bloque a bloque todo lo que sucede en la blockchain.

Por ejemplo, este tipo de redes son útiles para gobiernos u organizaciones empresariales que deseen almacenar o compartir datos de forma segura. Un perfecto caso de uso está sucediendo en el sector sanitario, donde se empieza a usar blockchain para almacenar los datos de sus líneas de producción de medicamentos, los datos almacenados

pueden ser revisados por las autoridades competentes con el fin de controlar la calidad, tanto a nivel de la misma empresa como de gobierno, el objetivo de la aplicación de este modelo es mantener la transparencia y la confianza. (Bitme, 2022)

CARACTERÍSTICAS DE LA BLOCKCHAIN HÍBRIDA

1. El acceso a la red está restringido a elementos que solo pueden ser autorizados por el resto de las unidades de control.
2. El acceso al libro de transacciones o cualquier medio de información generado por la blockchain es público.
3. No existe minería ni criptomonedas, el consenso de la red se da por otros medios que aseguran que los datos son correctos.
4. Es parcialmente descentralizado lo que conlleva a un mejor nivel de seguridad y transparencia.



Fuente: Googold (2022)

9. PRINCIPALES REDES BLOCKCHAIN

I. SOLANA

Solana es un proyecto de código abierto altamente funcional que implementa una nueva blockchain de capa 1, sin permisos y de alta velocidad. Creada en 2017 por Anatoly Yakovenko, un antiguo ejecutivo de Qualcomm, Solana tiene como objetivo escalar el rendimiento más allá de lo que suelen lograr las blockchain más populares, manteniendo los costos bajos, implementa un innovador modelo de consenso híbrido que combina algoritmo único de proof of history y proof stake , gracias a ello la red Solana puede procesar más de 710.000transacciones por segundo. (Cointelegraph. 2002)

La arquitectura de blockchain de tercera generación de Solana está diseñada para facilitar el desarrollo de smart contract y la creación de aplicaciones descentralizadas, además el proyecto es compatible con una serie de plataformas de finanzas descentralizadas, así como un mercado de tokens no fungibles

El ambicioso diseño de Solana pretende resolver el trilema de las blockchain,un concepto propuesto por el creador de Ethereum. Este dilema describe un conjunto de 3 grandes retos a los que se enfrentan los desarrolladores cuando construyen blockchain: Descentralización, seguridad y escalabilidad

La opinión generalizada es que blockchain se construye de tal manera que obliga a los desarrolladores a sacrificar uno de los aspectos en favor de otros dos, ya que actualmente solo se pueden beneficiar de dos de los tres beneficios, su moneda nativa SOL

II. CARDANO

Cardano es un blockchain de tercera generación que ha sido construida en base a estudios revisados por pares, lo que la ha llevado a ser considera la primera blockchain científica del criptomundo

Es uno de los proyectos más interesantes cuyo objetivo es brindar escalabilidad y seguridad, para lograr estos objetivos, Cardano ha estado avanzando en avances tecnológicos muy prometedores, que le ha permitido alcanzar importantes objetivos y demostrar la gran capacidad de la tecnología blockchain para hacer frente a los retos presentes, su moneda nativa es AdA.

III. BITCOIN

Una persona o un grupo de personas bajo el seudónimo de Satoshi Nakamoto creó el protocolo Bitcoin en 2008 para descentralizar el control del dinero cuando las entidades centralizadas habían fracasado en el mundo (crisis financiera del 2008) una publicación llamada el libro blanco de Bitcoin esboza un conjunto de reglas computacionales que determinaban un nuevo tipo de base de datos descentralizada, la red se puso en marcha en 2009.

La criptomoneda más conocida es Bitcoin y es para la que se creó la tecnología blockchain. Bitcoin es una moneda de intercambio digital que utiliza seguridad criptográfica.

IV. ETHEREUM

Ethereum es una tecnología para construir aplicaciones y organizaciones, tener activos, hacer transacciones y comunicarse sin ser controlada por una autoridad central. No hay necesidad de entregar datos personales para utilizar Ethereum, tiene su propia moneda llamada Ether, que se utiliza para pagar ciertas actividades en la red de Ethereum. (*¿Qué Es Ethereum? | Ethereum.org*, n.d.)

Blockchain permite hacer transacciones sin una autoridad central o intermediario, pero que es un intermediario, un intermediario o autoridad central puede ser un banco o gobierno que interviene una transacción entre el remitente y el receptor. Una autoridad central tiene el poder de afirmar, censurar o revertir transacciones y puede compartir los datos confidenciales que recopila con terceros, además dictamina que servicios financieros se pueden acceder.

Ethereum fue lanzada en 2015, se basa en la tecnología de Bitcoin pero tiene algunas diferencias grandes. Ambos permiten utilizar dinero digital sin proveedores de pago o bancos. Pero Ethereum es programable, es decir también puede utilizarse para construir aplicaciones descentralizadas sobre su estructura.

Ser programable significa que se pueden construir aplicaciones que usen la cadena de bloques para almacenar datos o controlar lo que su aplicación puede hacer, esto da como resultado una cadena de bloques de propósito general que puede ser programada para cualquier cosa . Que no haya límites para lo que Ethereum pueda hacer, significa una gran innovación en la red de Ethereum.

Mientras que Bitcoin es solo una red de pagos, Ethereum se parece más a un mercado de servicios financieros, juegos, redes sociales y otras aplicaciones que respeten la privacidad y no pueden censurarse

Actualmente las 2 principales redes de blockchain son Bitcoin y Ethereum. El presente trabajo de investigación está centrado en la blockchain de Ethereum ya que es considerada una red más inteligente puesto que no solo se puede generar transacciones de monedas digitales sino que se pueden programar proyectos descentralizados y smart contract. Al referirnos a Ethereum no podemos dejar de mencionar a su creador o desarrollador Vitalik Buterin, nacido en Rusia en 1994, se dice que fué un cripto activista en sus comienzos, cofundó la revista Bitcoin y posteriormente Ethereum.

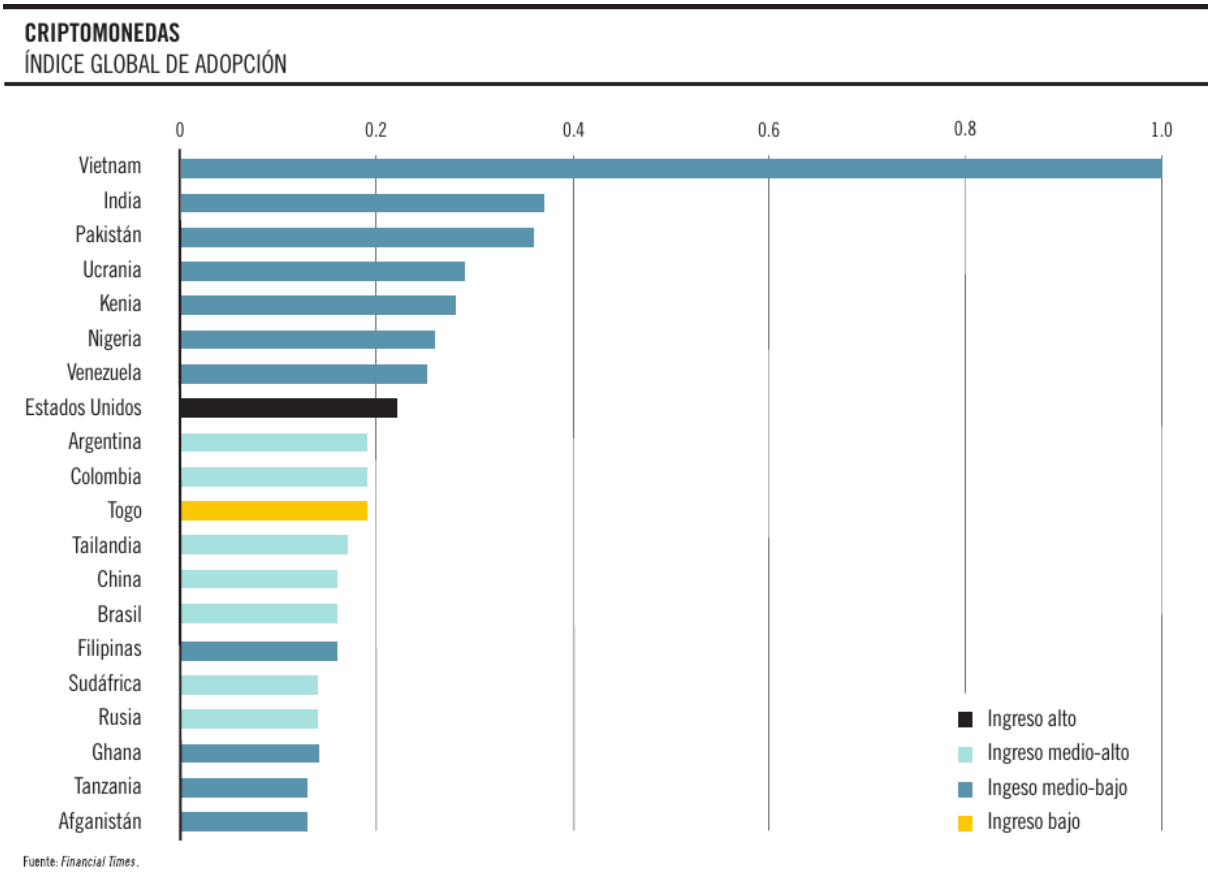
Con el objetivo de corregir fallas que ha su juicio detectó en proyectos como la red Bitcoin, Buterin comenzó a desarrollar Ethereum y en 2013 publicó su whitepaper. Luego de el avance inicial, Gavin Wood, cofundador se Ethereum publicó el libro técnico de Ethereum, en este se describe el funcionamiento de la ETHEREUM VIRTUAL MACHINE (EVM) es la principal tecnología de Ethereum, sobre la que el lenguaje de scripting muestra su pleno potencial (Buterin, 2022)

CAPITALIZACIÓN DE MERCADO DE LAS PRINCIPALES CRIPTOMONEDAS

	#	Nombre	Precio	1h %	24h %	7d %	Cap. de Mercado	Volumen (24h)	Acciones en circulación	Últimos 7 días
☆	1	Bitcoin BTC	$19,577.96	0.16%	1.69%	2.91%	$374,732,262,243	$27,426,132,546 1,403,917 BTC	19,182,181 BTC	
☆	2	Ethereum ETH	$1,337.05	0.46%	2.56%	4.82%	$163,048,805,000	$9,387,650,796 7,045,762 ETH	122,373,863 ETH	
☆	3	Tether USDT	$1.00	0.00%	0.00%	0.01%	$68,446,625,245	$36,661,147,542 36,658,970,025 USDT	68,442,559,805 USDT	
☆	4	USD Coin USDC	$1.00	0.00%	0.01%	0.01%	$44,758,193,078	$2,972,531,613 2,972,301,409 USDC	44,754,726,833 USDC	
☆	5	BNB BNB	$275.30	0.05%	1.10%	2.31%	$44,384,471,855	$596,543,338 2,168,431 BNB	161,337,261 BNB	
☆	6	XRP XRP	$0.4803	0.08%	1.02%	2.08%	$23,900,195,664	$1,484,932,904 3,099,508,981 XRP	49,887,015,710 XRP	
☆	7	Binance USD BUSD	$0.9996	0.03%	0.09%	0.08%	$21,643,371,815	$6,457,496,580 6,452,940,278 BUSD	21,628,100,611 BUSD	

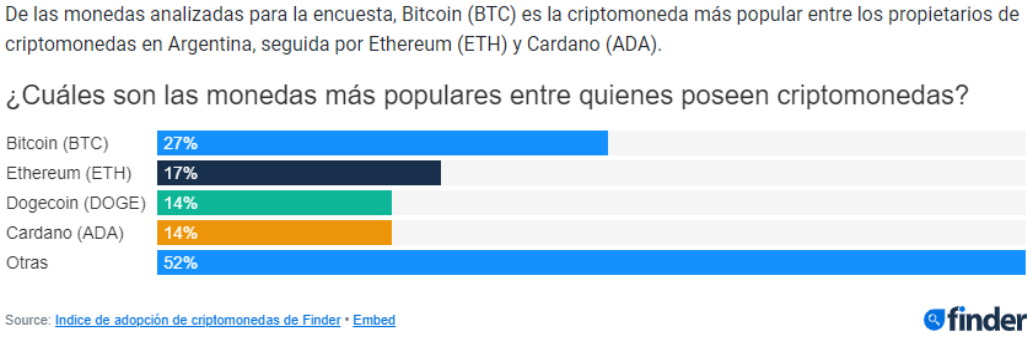
Fuente: Coinmarketcap, octubre 15 2022

ÍNDICE GLOBAL DE ADOPCIÓN DE CRIPTOMONEDAS



Fuente: Financial times, 2022

CRIPTOMONEDAS MÁS POPULARES EN ARGENTINA



Fuente: Finder, 2022

DIFERENCIAS ENTRE LA BLOCKCHAIN DE BITCOIN Y DE ETHEREUM

CARACTERÍSTICAS	BLOCKCHAIN	ETHEREUM
Creador	Satoshi Nakamoto	Vitalik Buterin
Financiación	Sin financiación	ICO en 2014, 18 millones de $ recaudados
Nivel de descentralización	Alto	Medio (muchas decisiones dependen de un pequeño grupo de personas
Precio de moneda	Alto, su precio se consolida por una política deflacionaria, aceptación y confianza	Medio, su precio fluctúa debido a la emisión inflacionaria y la presión al alza del bitcoin
Emisión total de monedas	Limitada (aprox. 21 millones de monedas)	Ilimitada (La emisión total no está limitada , la emisión anual se mantiene en 18 millones de Ether, la ETH 2.0 la llevara a 2 millones anuales
Minería	Mecanismo de consenso POW (proof of work)	Actualmente algoritmo POS (proof of stake)
Escalabilidad	Actualmente 6-8 transacciones por segundo	Entre 16-20 transacciones por segundo. Con el cambio a ETH 2.0 se podrá llegar hasta las 100.000 transacciones por segundo
Smart contracts	Limitado, de momento no hay Turing completo	Avanzado. Soporte Turing completo y un lenguaje de programación flexible para facilitar la codificación

9. BLOCKCHAIN COMO INNOVACIÓN DISRUPTIVA

Blockchain es una revolución perfectamente comparable a la aparición del ordenador portátil o al desarrollo y popularización de internet, es posiblemente uno de los cambios más importantes y fundamentales que vayamos a ver en nuestras vidas, con ese potencial de cambiarlo todo (Tapscott and Tapscott 11)

Una de las ventajas de esta tecnología es que es adaptable a múltiples aplicaciones en nuestra vida desde un registro de tierras en algún lugar en África hasta la creación de un protocolo de seguridad para los dispositivos conectados a internet, a la vez une otros detalles a su capacidad disruptiva, una de ella es las barreras de entrada sumamente bajas, que permite prácticamente a cualquier empresa indistintamente de su tamaño o capacidad económica pueda plantearse a construir sobre ella .

"*A estas alturas, con más de 26 años trabajando en innovación creo que sé reconocer una disrupción cuando la veo. Y si blockchain no es una revolución es que nunca hemos visto ninguna"* (Tapscott and Tapscott 12)

Las aplicaciones que podría tener blockchain se encuentran en proceso de desarrollo debido a los potenciales que representa dicha tecnología (Government Office for Science, 2016). Así tanto el sector público como el privado están incursionando en la aplicación de dicha tecnología, en escenarios tales como la contratación, administración, cadena de suministro, procesos de flujos de productos y servicios a través de la cadena de bloques (Naranja Tan, krause & Gradstein, 2017)

Tapscott y Tapscott determinan lo siguiente:

> ¿Qué pasaría si existiera un internet del valor en el que las partes de una transacción pudieran almacenar e intercambiar valor sin la necesidad de intermediarios tradicionales? En pocas palabras, eso es lo que ofrece la tecnología blockchain. El valor no se guarda en un archivo en algún lugar; se representa mediante transacciones registradas en una hoja de cálculo global o libro mayor, que aprovecha los recursos de una gran red peer-to-peer para verificar y aprobar transacciones. Una blockchain tiene varias ventajas. Primero, es distribuido: se ejecuta en computadoras proporcionadas por voluntarios de todo el mundo, por lo que no existe una base de datos central para piratear. En segundo lugar, es público: cualquiera puede verlo en cualquier momento porque reside en la red. Y tercero, está encriptado: usa encriptación de alto rendimiento para mantener la seguridad (2017, pp. 10-11).

La blockchain es considerada la revolución industrial de internet, o su paso posterior, ya que a partir de ella, se pasa desde una etapa de internet de la información a un internet del valor (Preukschat, 2017)

9.1 CARACTERÍSTICAS DE UNA TECNOLOGÍA DISRUPTIVA

- Simplicidad
- Accesibilidad
- Asequibilidad
- Trazabilidad

La integridad de los datos, la descentralización y los smart contract, son elementos transversales que impactan a la mayoría de industrias.

Según Preukschat (2017), la blockchain tiene una infinidad de usos que afectan de manera particular a diversas industrias como la banca, las aseguradoras, telecomunicaciones, sector energético, salud, pymes, juegos en línea, industria 4.0, etc. Así como también otros sectores como la música, las smart cities, la participación ciudadana entre otros

Sin duda el sector financiero es la industria en donde mayor impacto está teniendo la blockchain, estamos ante el auge de ecosistemas de finanzas descentralizadas, llevadas a cabo por medio de proyectos interesantes pero vale la pena aclarar que la tecnología actual es aún incipiente, ya que se puede evidenciar algunas vulnerabilidades en el sistema. Sin embargo no cabe duda que blockchain llegó, y llegó para quedarse, podemos afirmar entonces, que blockchain está cimentando las bases para un sistema financiero diferente al que conocemos hoy día.

2

[2] Según el informe más reciente sobre registros distribuidos de la firma consultora PricewaterhouseCoopers (PwC), la expansión de blockchain se enfocaría en 12 países en la próxima década, encabezados por **China y Estados Unidos, seguidos de Alemania, Japón, Reino Unido, India y Francia**. (INCP. 2020)

10. USOS Y APLICACIONES DE BLOCKCHAIN

10.1 SMART CONTRACT

En estos últimos años, tras la creación de Bitcoin y el lanzamiento de su primera versión en 2009, han sido muchos los proyectos interesantes que han ido apareciendo aportando ideas y soluciones descentralizadas a muchos procesos o aplicaciones centralizadas que todos usamos en la actualidad.

Una de las innovaciones que se fueron dando en la red blockchain son los smart contract que tienen como objetivo eliminar intermediarios para simplificar procesos y con ello ahorrar costos, producto de dicha operación.

Para entender un smart contract, primero tenemos que recordar que significa un contrato. Un contrato es un acuerdo entre dos o más partes que se definen mediante términos a supuestos escenarios, es decir, unas reglas de juego que permitan que todas las partes que lo acepten entender en qué va a consistir la interacción que van a realizar

Hasta el momentos los contratos han sido documentos verbales o costosos documentos escritos, estos documentos están sujetos a las leyes de jurisdicciones territoriales, y en ocasiones requieren de escribanos, eso se transmite es un encarecimiento del mismo y un aspecto más controversial aún es que pueden estar sujetos a la interpretación según la conveniencia de alguna de las partes.

En cambio un smart contract o contrato inteligente es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin la presencia de intermediarios ni mediadores. Evitan el problema de la interpretación al no ser verbal o escrito en el tipo de lenguaje coloquial. Los smart contract se tratan de script (códigos informáticos) escrito en lenguaje de programación, quiere decir que los términos del contrato son puras sentencias y comandos en el código que lo forman

Un smart contract puede ser creado por personas físicas o jurídicas, pero también por máquinas u otros programas que funcionan de manera autónoma, un smart contract tiene validez sin la necesidad de depender de autoridades. Su código es visible para todos y no se puede modificar al estar asentado sobre la tecnología blockchain, esto le confiere un carácter descentralizado, inmutable y transparente.

10.2 GESTIÓN DE LA PROPIEDAD INTELECTUAL

La tecnología blockchain está teniendo gran impacto sobre los derechos de propiedad intelectual e industrial, y no podemos obviar su estrecha relación con los activos intangibles, su utilización en este ámbito es cada vez más común pues permite conocer a tiempo real quien es propietario de los derechos de explotación y brinda un sello inalterable de titularidad. Entre los beneficios que puede brindar esta tecnología se puede destacar la capacidad de generación de evidencia, que puede ser utilizada en la lucha contra la pirateria y las falsificaciones, también permite una más ágil gestión en los registros de los activos

Para obtener la propiedad mediante derecho de autor es requisito indispensable que se pueda demostrar su autoría, para ello la ley de propiedad intelectual,configura un registro de propiedad intelectual.

Un aspecto interesante entre la vinculación de la propiedad intelectual y blockchain se presenta en el entorno de la música, como ejemplo podemos citar a Open Music Initiative, una iniciativa sin fines de lucro que crea un protocolo de código abierto para la identificación de creadores y titulares de derechos musicales.

Otro ejemplo de vinculación de esta tecnología y la propiedad intelectual es copyrightLY una aplicación descentralizada que aprovecha la potencia de la tecnología blockchain y web semántica para facilitar la gestión de los derechos de autor de los creadores que suben su contenido al almacenamiento descentralizado y usan un hash de contenido resultante para registrar reclamos de autoría en la cadena que vincula el contenido a sus identidades y una marca de tiempo.

10.3 CADENA DE SUMINISTROS

En 1956, el propietario de una transportadora en los EE UU, Malcolm McLean se reunió con el ingeniero Keith Tantliner para elaborar algo que revolucionará el comercio mundial: el moderno container de transporte marítimo. Poco después de 60 años con procesos y suministros cruciales y cada vez más complejos, la cadena de suministro global está a punto de dar otro paso adelante , esta vez con la ayuda de la tecnología blockchain. (*Cómo Blockchain Fortalece Las Cadenas De Suministro?*, n.d.)

Blockchain suministra un mecanismo más eficaz y definitivo para rastrear datos en cadenas de suministro multicompleja. De esta forma aumenta la eficiencia, reduce los errores humanos y esclarecer las responsabilidades y obligaciones a largo de la cadena. Por ejemplo una carga puede transmitir desde Bangladesh hasta Canadá con todos los detalles rastreados, como la temperatura de los almacenes hasta los puertos en todo el mundo, si hubiere una

intervención de esta cadena en cualquier lugar, esa información seria registrada y suministrada a las partes interesadas

Blockchain podría suministrar una custodia segura de los ítems conforme avancen por la cadena de suministro, eliminando cualquier argumento y suposición de la cuestión. Además reduciría significativamente el costo de los productos de tránsito por cuenta de menores gastos de documentación, para los próximos años, Meyrick estima que el costo máximo de la documentación comercial necesaria para procesar y administrar estos productos es de 1/5 de los costos de transporte. Si las empresas pudiesen reducir su carga administrativa utilizando blockchain , esta eficiencia adicional podría aumentar el comercio mundial en un 15 % (Collosa, 2022)

10.4 SECTOR PÚBLICO

En la actualidad ya son muchos los países que recurren a la tecnología blockchain para mejorar la calidad de los servicios y procesos del sector público ya que desean brindar servicios más eficientes, transparentes, confiables y trazables. Pero también blockchain tiene el potencial para ayudar a reducir la corrupción en procesos especialmente vulnerables.

BENEFICIOS DE USAR BLOCKCHAIN EN EL SECTOR PÚBLICO

- Respaldar la digitalización de los organismos públicos, facilitando una infraestructura descentralizada y altamente eficiente. Una infraestructura capaz de garantizar la privacidad, el cumplimiento y el intercambio de datos optimizado
- Ayudar a los gobiernos a construir un ecosistema donde la tecnología refuerce la confianza, permitiendo la interoperabilidad institucional, los datos se pueden compartir entre varias entidades de forma segura y transparente, de esta forma se garantiza el respaldo en tiempo real y la auditabilidad de los datos confidenciales
- Para reducir la burocracia y la corrupción, las instituciones pueden usar blockchain para vincular identidades del mundo real a documentos e identificaciones digitales verificadas y encriptadas. Impulsar la confianza y el compromiso de los ciudadanos al cambiar la manera en que los ciudadanos interactúan con las instituciones. (Collosa, 2022)

A. CASO DE USOS EN EL SECTOR PÚBLICO

Identidad digital: Se trata de una piedra angular de la interacción de los servicios públicos. La blockchain puede colaborar con la resolución de fallos actuales. Para citar un ejemplo,en Argentina, DIDI es el primer proyecto de identidad digital auto soberano a través de la blockchain. el objetivo es mejorar el acceso a bienes y servicios de calidad de poblaciones de barrios vulnerables así de esta forma blockchain les confiere características potentes que podrían ayudar a reducir la asimetría de la información y generar inclusión financiera

Licitaciones públicas: estos procesos pueden hacerse más transparentes si se utiliza blockchain. Destacan los casos de uso de la sociedad informática de Vasco que en 2017 adjudicó la licitación para uso de blockchain en el registro de contratista, también los casos de Chilecompra, donde su plataforma de contrataciones públicas inició un proyecto piloto para el uso de la blockchain en adquisiciones públicas. Lo mismo está sucediendo en Perú, en Colombia destaca una exitosa experiencia de contratación para el programa de alimentación en la ciudad de Medellín. EStados unidos ha utilizado blockchain para contratación pública de emergencia para hospitales durante la pandemia

Incentivos comunitarios tokenizados

En Viena en 2020 se inició un proyecto llamado Kultur Token, tenía una propuesta de valor muy sencilla pero potente, acceso gratis a actividades culturales a cambio de conductas medioambientales responsables

Presupuesto participativo/votaciones; El municipio madrileño de Alcobendas (España) utiliza la blockchain de Ethereum para registrar con un sello de tiempo el voto decreto perro trazable de los ciudadanos en el uso de fondos del presupuesto participativo

Programa de transferencias sociales: Los programas de emergencia son vulnerables al fraude y la corrupción. Blockchain tiene el potencial de mitigar los riesgos haciendo más transparente el proceso y evitando el desvío de fondos. El programa mundial de alimentos estimó un ahorro con el uso de blockchain humanitario a través del proyecto Building Blocks, asimismo ha invitado a otras agencia de la onu y a actores humanitarios a colaborar en una red blockchain neutral, el objetivo es mejorar la cooperación, reducir la fragmentación y reforzar la eficiencia de las intervenciones para el desarrollo.

11. SMART CONTRAT

Una vez analizado la tecnología blockchain y sus múltiples ventajas, se procederá a abordar el tema central del presente trabajo de investigación, los" Smart Contract"

Contrato inteligente: un conjunto de promesas, incluidos los protocolos dentro de los cuales las partes cumplen otras promesas. Los protocolos generalmente se implementan con programas en una red informática o en otras formas de electrónica digital, por lo que estos contratos son «más inteligentes» que sus antecesores en papel. El uso de inteligencia artificial no está implicado.(Nick Szabo, 1995)

Un contrato inteligente (smart contract por su traducción en inglés) es un programa informático que opera de manera automática, permitiendo celebrar y ejecutar contratos entre dos o más partes. El software opera dentro de la cadena de bloques facilitando el proceso de cumplir digitalmente la negociación o el cumplimiento del contrato.

Con la seguridad de blockchain los contratos inteligentes pueden ejecutarse automáticamente, lo que elimina la necesidad de supervisión, todo lo que se necesita es un programa de computadora para reconocer un evento que desencadene la ejecución.

Las reglas programadas no se pueden modificar una vez que el contrato inteligente entre en vigor, cada parte debe comprenderla y aceptarla, luego cada acción o cláusula se almacena en la cadena de bloques.

Los smart contract también pueden funcionar como ecosistemas financieros tradicionales fuera de la red blockchain, las partes contratantes pueden agregar un oráculo, una fuente de información externa que se designa para actualizar la información clave en la cadena de bloques, verificar el cumplimiento del acuerdo y desencadenar las acciones correspondientes.

Un smart contract puede transformar las transacciones comerciales tradicionales, suponga que una empresa de alimentos congelados desea vender sus productos a una cadena de supermercados, no se encuentran en el mismo país y es la primera vez que hacen negocios, usan un contrato inteligente para garantizar que cada una cumpla con su parte del trato.

El oráculo puede ser la empresa de transporte, que registra la entrega en la cadena de bloques a través de un smart contract. una vez que lleguen los productos, la orden de pago se emitirá automáticamente, un dispositivo conectado al internet de las cosas (IOT) podría monitorizar la temperatura del contenedor y avisar de una ruptura de la cadena de frío, lo que desencadenaría la cláusula de penalización

La primera vez que se escuchó hablar de contratos inteligentes fue en 1993 cuando el criptógrafo Nick Szabo comenzó a utilizar este término. Szabo propuso el cambio de los contratos tradicionales a este sistema, pero no tuvo éxito debido a las limitaciones de la tecnología de ese momento, sin embargo en 2009 gracias a la aparición de Bitcoin y su tecnología subyacente blockchain, hizo posible la ejecución de los contratos inteligentes, pero cabe recalcar que los smart contract están programados en la blockchain de Ethereum que es considerada una blockchain más inteligente

El elemento clave para ciertas aplicaciones de la blockchain son los contratos inteligentes (smart contract) que, contra lo que se pueda deducirse, ni son contratos ni son inteligentes en absoluto. Se trata de unos programas informáticos que aplican determinadas cláusulas de un contrato que se almacenan en la blockchain, con una característica importante, se ejecutan de modo automático cuando se cumplen las condiciones especificadas en el contrato.

Esto quiere decir que el registro en la blockchain se automatiza en el marco de condiciones pre establecidas de esta manera ahorra tiempo, procesos burocráticos y costos, la mayoría de los smart contract están asentadas actualmente en la cadena de bloques de Ethereum, ¿que es exactamente ethereum? Ethereum es una plataforma global de código abierto para aplicaciones descentralizadas, en donde los programadores pueden escribir contratos inteligentes que controlan el valor digital. El lenguaje de programación utilizado es Solidity.

Conjunto de promesas especificadas en formato digital, incluyendo los protocolos por medio de los cuales se ejecutan dichas promesas.(Nick Szabo, 1999)

Programas de computación que operan sobre tecnologías de registro distribuida y cuya ejecución obliga automáticamente a dos o más partes de acuerdo con los términos predefinidos por los mismos (Ley italiana nº 12, 11/12/2019)

Se dice que desde remotas épocas de la humanidad, el hombre de ha valido de máquinas en favor de su propio desarrollo, tenemos evidencia escrita de las primeras máquinas expendedoras de agua diseñada por el ingeniero griego Herón de Alejandria para dispensar de agua bendita en los templos de Tebas y el alto Egipto, estas máquinas estaban ubicadas en la puerta de los templos y ya funcionaban con monedas que al introducirlas en la máquina proporcionaban agua para el lavado de manos y cara. Sin tener la necesidad de la existencia de un vendedor en el otro extremo de la máquina, así la operación se realizaba entre el hombre y la máquina. En 1920 aparecieron las primeras máquinas expendedoras de

bebidas consideradas las antecesoras de los smart contracts junto con las máquinas expendedoras de agua.

No todo smart contract es un contrato en términos de la ley ya que dijimos que también dan lugar a aplicaciones informáticas enfocadas en múltiples industrias, eso quiere decir que los smart contract están dando lugar a nuevos modelos de negocios basadas en un sistema descentralizado en su operación, a continuación detallaremos algunas de sus principales modelos.

Smart contract escrito en lenguaje de programación solidity

```
template FixedSupplyTokenProposal
    with
        owner: Party
        issuer: Party
        amount: Decimal
    where
        signatory issuer -- Issuer creates proposal

    controller owner can -- Proposed owner can choose to accept
        Accept : ContractId FixedSupplyToken
            do create FixedSupplyToken with owner, issuer, amount -- Which creates the token

template FixedSupplyToken
    with
        owner: Party
        issuer: Party
        amount: Decimal
    where
        Signatory issuer, owner
```

Fuente: Digital Asset

3

[3] En su artículo "*Trusted Third Parties Are Security Holes*", da su opinión. Para él, las partes de confianza traicionan lo que pretenden resolver. Las partes de confianza están diseñadas para mejorar la seguridad comercial. La seguridad comercial incluye la protección contra la violación de datos, la privacidad, la integridad y la propiedad. Nick está en contra de las partes de confianza. Además, considera que estas partes de confianza son demasiado caras y arriesgadas.

11.1. APLICACIONES DE LOS SMART CONTRACT

MODELOS DE SMART CONTRACT

1.1. MODELO EXTERNO

- No es contrato en términos jurídicos
- Funciona en términos tecnológicos
- Se combinan múltiples contratos para operar entre sí, lo que se conocería como aplicación descentralizada (DAPP) para cumplir con procesos y cálculos más complejos

Una de las disrupciones más notorias de la tecnología blockchain, sin duda son los smart contract, ya que está impactando directamente en el sistema financiero tradicional, dando lugar a ecosistemas completos de productos financieros descentralizados y así de este modo, modificando la forma en que estamos acostumbrados a realizar transacciones y comercio. Párrafos abajo detallaremos algunas propuestas interesantes, consideradas las más relevantes dentro del ecosistema descentralizado.

11.1.1 ¿QUÉ SON LAS APLICACIONES DESCENTRALIZADAS (DAPP)?

Dapp es el acrónimo de "Decentralized Applications" o "Aplicaciones descentralizadas". Es un tipo de aplicación, cuyo funcionamiento no depende de puntos de control o servidores centrales, ya que funciona en base a una red descentralizada. Una red donde el usuario tiene el control total del funcionamiento de la misma, las Dapps permiten que las personas puedan acceder a diferentes servicios de forma segura, estas apps pueden ser utilizadas en computadoras personales, smartphones o incluso ser accesibles desde una página web.

Pensemos en una app tradicional, por ejemplo youtube, Twitter o Instagram. En todos estos servicios, las decisiones se toman a unos servidores centrales, esto les permite a la empresa propietaria, tomar decisiones de censura, o alteración del comportamiento, incluso

beneficiar y perjudicar únicamente a determinadas personas, poniendo en constante tela de juicio la neutralidad e igualdad de las condiciones. (Bitme, 2020)

Estas son algunas de sus razones. Limitan la imaginación. Diseñar una tercera parte que se base en protocolos es fácil. Así que se limita la imaginación para idear los que no lo hacen. Las partes de confianza tienen agendas e intereses ocultos. Además, los costes de transacción son demasiado elevado (Nick Szabo, 1996

El concepto de Dapps no es nuevo. Las primeras Dapps se vieron en protocolos de compartición de archivos como BitTorrent o DC + + Ambas aplicaciones son sistemas peer-to-peer de compartición de archivos con alta resistencia a la censura. Sin embargo la primera Daap usando blockchain fue, el Bitcoin, esto es por que su estructura y funcionamiento describe con éxito la primera Dapp blockchain de la historia.

Sin embargo no fue hasta 2014 con la presentación de Ethereum, su lenguaje de programación solidity y la capacidad de ejecutar smart contract que las Dapps se masificaron, esto hace que blockchain pueda ser adoptada de manera masiva al permitir nuevas formas de interacción entre los usuarios, el mundo real y el ecosistema digital

A. DIFERENCIAS ENTRE UNA DAPP Y UNA APP TRADICIONAL

Las Dapp y las App tienen algunos elementos en común, sin embargo, su diferencia radica en cómo interactúan con dichos elementos. Ambos tipos de aplicaciones tienen 3 estructuras básicas que son: el frontend, el backend y la capa de almacenamiento de datos.

a. **Frontend**: La primera capa, el frontend, viene a ser la interfaz que los usuarios utilizan para interactuar con la aplicación. En este caso, tanto las Dapp como las App tradicionales, pueden hacer uso de los inmensos recursos gráficos existentes para ello. Desde interfaces web escritas en HTML hasta las más elaboradas. en framework como Qt o GTK. La finalidad de esta capa es simplemente, dar al usuario la capacidad de interactuar, recibir y enviar información a la aplicación que esté usando (Bitme, 2022)

b. **Backend:** Es la segunda capa hace mención a la lógica principal de la aplicación, esta logia es centralizada, a diferencia de las Dapps, el backend está relacionado a un smart contract que se ejecuta sobre una blockchain, es este caso la blockchain de Ethereum. De esta forma un smart contract tiene la programación que garantiza el funcionamiento de la Dapp, al ser los smart contract visibles y públicos, esto garantiza un alto nivel de transparencia y seguridad, así los usuarios están seguros que la Dapp no hará nada distinto a lo que especifica el smart contract. (Bitme, 2022)

c. **Almacenamiento de datos:** En una App tradicional, la capa de almacenamiento también es centralizada, normalmente los datos son almacenados en el computador del usuario o en servidores centrales controlados por terceros. Este sistema de trabajo tiene muchos fallos. Por ejemplo un usuario, puede perder la información de la aplicación si su computador se daña también puede suceder que los servidores queden fuera de servicio o sean bloqueados, acciones que impedirían que el usuario pueda acceder a la aplicación de forma correcta o incluso pierda la información.

En el caso de las Dapps, el almacenamiento de datos es completamente descentralizado, cada usuario de la Dapp almacena su historial completo de las acciones que se realizan en la red Dapp, además, las interacciones son almacenadas en la blockchain dentro de los bloques de las mismas, todo ello con una seguridad criptográfica.

B. FUNCIONAMIENTO DE UNA DAPP

Una Dapp funciona parecida a una red blockchain. En este caso cada usuario de la Dapp es un nodo dentro de la red. cada usuario, vela por el correcto funcionamiento y las operaciones que se realizan en la red

El canal de comunicaciones que usa la Dapp es la blockchain, en ella se deja registro de cada operación que pasa por el smart contract que controla la Dapp. La aceptación o no de las operaciones realizadas por los usuarios de la Dapp, va sujeta a la programación de dicho smart contract, de esta forma, se busca garantizar que todos los participantes actúen en el marco de lo especificado por el mismo.

El smart contract en este caso, es un punto intermedio que se encarga de corroborar la validez de cada interacción. Cada vez que hay una nueva operación Dapp, la información de la plataforma se actualiza en cada nodo, con ello se garantiza que la información quede almacenada en cada una de ellas. Así de esta manera cada usuario contribuye a mantener en pie la aplicación con los recursos de su ordenador. este tipo de estructura también garantiza que la plataforma siempre estará en servicio, esto por la imposibilidad de dar de baja a todos los nodos de la red al mismo tiempo.

En este punto las Dapp llevan un gran avance, pues al trabajar y ejecutarse sobre una blockchain, gozan de sus capacidades de seguridad, privacidad e incluso anonimato , adicionalmente, garantizan también que la data sea usada por la Dapp solo accesible por la persona que originó dicha información, con lo que los usuarios mantienen un control absoluto de sus datos en cada momento

C. BENEFICIOS

Las Dapps se construyen sobre redes de la blockchain de Ethereum y por lo general ofrecen los siguientes beneficios:

- Inmutabilidad: Nadie puede cambiar la información una vez que haya sido registrada en la cadena de bloques

- A prueba de manipulaciones: Los contratos inteligentes publicados en la cadena de bloques no se puede manipular sin alertar a todos los demás participantes en la cadena de bloques
- Transparente: Los contratos inteligentes que impulsan las Dapps son abiertos y auditables
- Disponibilidad: mientras la red Ethereum permanezca abierta las Dapps integradas permanecerán activas y utilizables

D. DESVENTAJAS

Es cierto que la blockchain ofrece múltiples beneficios pero también tiene muchas desventajas

- Inmutabilidad: sólo pueden ser erróneos por estar mal programados y es justo esta característica un gran potencial por convertir los errores humanos en algo más grande
- Transparente: los contratos inteligentes abiertamente auditables también pueden convertirse en vectores de ataques para los piratas informáticos, ya que pueden ver el código y encontrar vulnerabilidades
- Escalabilidad: en la mayoría de los casos el ancho de banda de una Dapp está limitado a la cadena de bloques en la que se aloja.

Dentro del ecosistema de las finanzas descentralizadas podemos encontrar diferentes aplicaciones pero en el presente trabajo de investigación nos vamos a enfocar en Dao y Defi

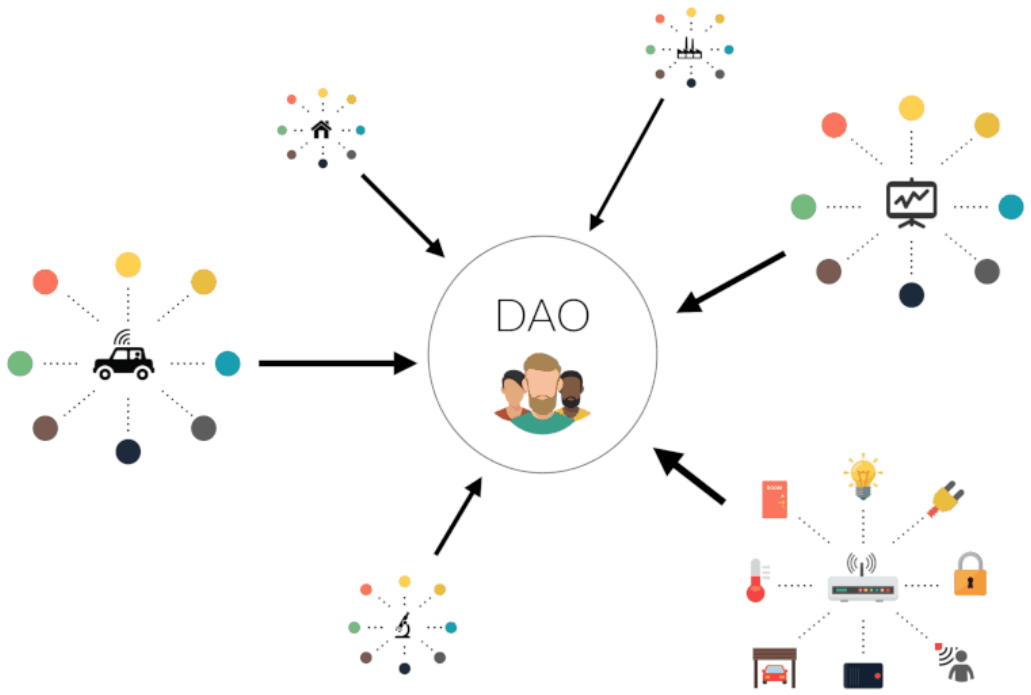
I. ORGANIZACIONES DESCENTRALIZADAS (**DAO)**

Una Dao es una organización totalmente autónoma que no está gobernada por una sola persona, sino que se rige por un código. Este código se basa en contratos inteligentes y permite que las dao reemplacen la forma en que normalmente se ejecutan las organizaciones tradicionales, como se ejecutan en código , estaría protegido de la intervención humana y operaria de forma transparente. No habría ningún efecto por ninguna influencia externa. Las decisiones o fallos de gobernanza se decidirán a través de la votación del token Dao.

Las siglas de DAO provienen del inglés Decentralized autonomous organization, que quiere decir Organización autónoma descentralizada. Hace referencia a un tipo de organización que es controlada en su totalidad por algoritmos computacionales, conocidos como smart contract y determinan las reglas de cómo deben cooperar las partes implicadas en la DAO

DAO no está vinculada a ninguna regulación o ley en particular debido a la naturaleza descentralizada donde se ejecuta el smart contract y que coordina la organización, la cadena de bloque (blockchain)

Los smart contract pueden ser tan simples o complejos como se haya decidido programar. Pero los mismos quedarán transparentes e inmutables en el momento que sean publicados en la cadena de bloques, de esta manera las partes interesadas puedan revisar su funcionamiento y las reglas que se han programado dentro, teniendo la seguridad de no podrá ser modificado en el futuro.



Fuente: Bitme academy

II. FINANZAS DESCENTRALIZADAS (DEFI)

Las finanzas descentralizadas o Defi es el movimiento que permite a los usuarios utilizar servicios financieros como préstamos y comercio sin la necesidad de depender de entidades centralizadas. Estos servicios financieros se brindan a través de aplicaciones descentralizadas (Dapp) en la mayoría de ellas se ejecutan en la blockchain de Ethereum.

Defi no solo es un producto o empresa, sino es un conjunto de productos y servicios que actúan como reemplazo a instituciones que van desde la banca. los seguros. los bonos y los mercados monetarios. Defi Dapps permite a los usuarios combinar servicios para abrir múltiples posibilidades.

Para el funcionamiento de las Defi Dapps normalmente requiere que la garantía se bloquee en contratos inteligentes, La garantía acumulada en Defi Dapps a menudo se le denomina Valor total bloqueado, según Defi Pulse el valor total bloqueado a principios de 2019 midió alrededor de $275 millones pero en febrero de 2020 alcanzó un máximo de $1.200 millones. El gran crecimiento de Total Value sirve como indicador del rápido crecimiento del ecosistema Defi.

El ecosistema Defi se encuentra en una rápida expansión que nos sería casi imposible cubrir todo lo que Defi tiene para ofrecer, por esa razón hemos seleccionado algunas categorías de Défi que creemos son importantes.

Si bien las DEfi pueden revolucionar los servicios financieros tradicionales al eliminar la necesidad de un ente centralizado, sin embargo debe tenerse en cuenta que Defi en su estado actual aún es incipiente y experimental, con muchos proyectos que se mejoran a diario. puede desarrollarse hasta convertirse irreconocible lo que es hoy, a continuación abordaremos las 8 categorías principales de Defi

1. MONEDAS ESTABLES

Es sabido que el precio de las criptomonedas son extremadamente volátiles, es común que tengan oscilaciones de más del 10 % para ofrecer un tipo de solución a esa volatilidad se crearon las monedas estables o stablecoin vinculadas a otros activos estables como el dólar USD.

Theater (USDT) fue una de las primeras monedas que se introdujo , cada USDT supuestamente está respaldada por 1$ en la cuenta bancaria del emisor. Sin embargo, una desventaja importante de esta moneda es que los usuarios deben confiar en que las reservas de USD están totalmente garantizadas. El objetivo de las stablecoin es resolver el problema de confianza y volatilidad a la que están sujetas las criptomonedas y además es uno

de los principales elementos en el ecosistema Defi ya que se necesita una elemento que sea intercambiable y a la vez se le asigne un valor. Si bien las stablecoin no son realmente una aplicación financiera en sí misma, son importantes para hacer que las aplicaciones Defi sean más accesible para todos al tener una reserva estable

2.. PRÉSTAMOS

Los sistemas tradicionales requieren que sus usuarios tengan cuentas bancarias para poder utilizar sus servicios, un lujo que 1.700 millones de personas en la actualidad no tienen, además los préstamos de los bancos vienen con otras restricciones, como tener un buen historial crediticio y sobre todo una garantía que convenza a los bancos que uo es digno de crédito y capaz de pagar un préstamo.

Los préstamos descentralizados eliminan esa barrera, lo que permite a cualquier persona garantizar sus activos digitales y utilizarlos para obtener préstamos y también obtener un rendimiento de sus activos y participar en el mercado de préstamos contribuyendo a los fondos de los préstamos y ganando interés sobre estos activos, con este tipo de modelo no es necesario tener una cuenta bancaria o una verificación de solvencia

3.. INTERCAMBIOS

Para intercambiar una criptomoneda por otra, se pueden utilizar intercambios como Coinbase o Binance. Los intercambios a través de estos sistemas son centralizados, lo que significa que actúan como intermediarios y custodios de los activos que negocian. Los usuarios no tienen control total de sus activos, esto puede convertirse en un peligro en caso que los intercambios sean pirateados o no puedan sus obligaciones.

Los intercambios descentralizados tienen como objetivo resolver este problema al permitir que los usuarios intercambien criptomonedas sin renunciar a la custodia de sus activos, sin almacenar fondos en intercambios centralizados es decir los usuarios no necesitan confiar en un intermediario para poder realizar transacciones y que estas sean seguras.

4. DERIVADOS

Un derivado es un valor cuyo valor deriva de otro activo. Como acciones, materias primas, divisas, activo subyacente, índices, bonos o tasa de interés

Los comerciantes pueden usar derivados para cubrir sus posiciones y disminuir su riesgo en cualquier operación. Por ejemplo, supongamos que eres un fabricante de guantes y quieres protegerte de un aumento inesperado en el precio del caucho, puedes comprar un contrato de futuros de su proveedor para entregar una cantidad específica de materia prima en una fecha específica a un precio acordado hoy.

Los contratos de derivados se financian principalmente en plataformas centralizadas. Las plataforma Defi están comenzando a construir mercados de derivados descentralizados

5. GESTIÓN DE FONDOS

La administración de fondos es el proceso por el cual se supervisa y administra flujo de efectivo para generar un rendimiento de sus inversores. Existen 2 tipos principales de administración de fondos; gestión de fondos activa y gestión de fondos pasiva. La gestión de fondos activa tiene un equipo de gestión que toma decisiones de inversión para superar un punto de referencia particular, como el S & P 500. La gestión de fondos pasiva no tiene un equipo de gestión, pero está diseñada de tal manera que imita el rendimiento de un punto de referencia particular, tanto como sea posible

En Defi, algunos proyectos han comenzado a permitir que la gestión de fondos se lleve a cabo de manera descentralizada, la transparencia de Defi facilita a los usuarios seguir cómo se administran sus fondos y comprender el costo que pagarán

6. PAGOS

En uno de los proyectos Defi tiene como objetivo cambiar la forma en que abordamos el pago reconfigurando los pagos como flujos en lugar de transacciones con la que estamos familiarizados.

El nacimiento de Defi y la tasa de innovación indudablemente introducirán nuevas formas de pensar sobre cómo funcionan los pagos para abordar muchas de las deficiencias del sistema actual

7. SEGUROS

El seguro es una estrategia de gestión de riesgos en la que una persona recibe protección financiera o una compensación de seguro contra las pérdidas de una empresa en

caso de un incidente, es bastante común que las personas aseguren sus autos, casas, salud y vida.

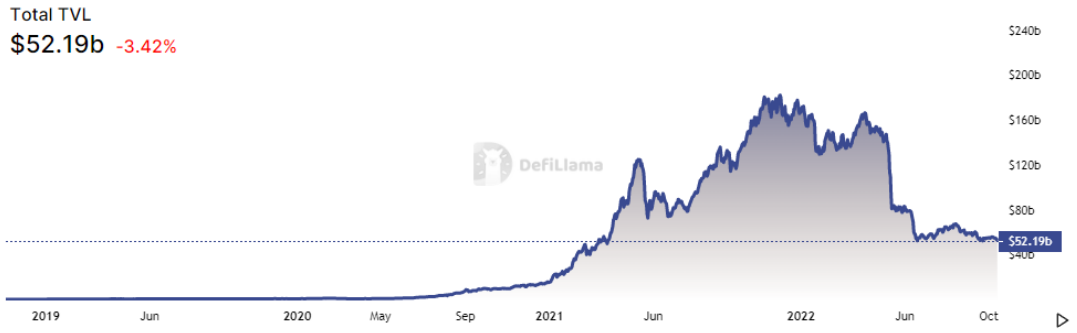
DIFERENCIAS ENTRE FINANZAS TRADICIONALES, FINTECH Y DEFI

CARACTERÍSTICAS	TRADICIONALES	FIN TECH	DEFI
Control del sistema	Gobierno y Bancos	Gobierno y Bancos	Red descentralizada, ejecutado sobre la blockchain y smart contract
Confianza	Bancos y terceros	Bancos y terceros	Sin intermediarios
Transferencia de dinero	Fiat	Fiat	Criptomoneda, tokens, stablecoin
Control de préstamos	Bancos	Bancos, grupos de préstamos	Deuda tokenizada
Mercados	Exchanges tradicionales	Exchanges tradicionales	Exchanges de criptomoneda (DEX y CEX)

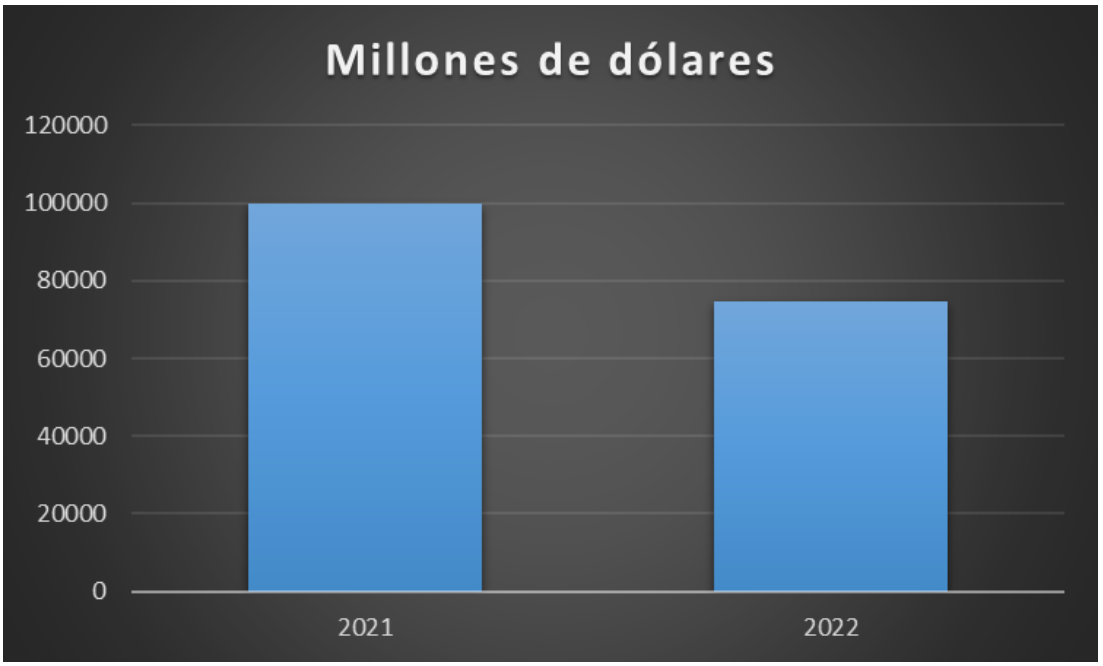
3. NICK SZABO**,** apuntaba, tal vez sin saberlo, al nacimiento de las DeFi cuando presentó su idea de los smart contracts en el año de 1995. Eso es 13 años antes de la creación del Bitcoin, una idea sin duda adelantada a su época. Sin embargo, no fue hasta la llegada de **Ethereum** en 2014, lo que supuso un cambio radical a esta idea. Ethereum y sus smart contracts permitían a los desarrolladores crear cualquier cosa que pudieran imaginar sobre una blockchain. Y justamente eso lo que empezó con un experimento ahora se está transformando en un movimiento por sí mismo, en un ecosistema financiero descentralizado que opera miles de millones de dólares cada mes.

Un ecosistema que durante los años 2018 y 2019 mantuvo un desarrollo constante, y durante los primeros meses de 2020 ha tenido un crecimiento sin precedente. Incluso ha llegado al punto que ha revalorizado los proyectos blockchain al permitir crear puentes entre las finanzas tradicionales y las **criptomonedas**. (BTME ACADEMY, 2022)

VALOR TOTAL BLOQUEADO EN DEFI (TLV)



Fuente: Cripto 247 (2021) billones de dólares



Market cap 2022: 74.270 USD
Market cap 2021: 100.000 USD

11.2. MODELO INTERNO

Los contratos ya no se redactan exclusivamente a través de palabras, sino de códigos informáticos, y su cumplimiento puede no depender de la voluntad de las partes, sino de un software. Esta forma de operar en él tràfico jurìdico no es ciencia ficciòn, sino una realidad a la que han dado lugar los smart contract o contratos inteligentes (Abad Ramòn, 2022)

Sin embargo por el momento, su aplicación aún no es masiva, aunque puede facilitarle las cosas a los bufetes de abogados a la hora de redactar un contrato y también puede automatizar procesos en algunos sectores empresariales.

No obstante el sector de los seguros es uno de los que más se pueden beneficiar de los smart contract, que se pueden utilizar para aumentar la velocidad en el pago de las indemnizaciones por siniestros y reducir costes y errores asociados con su procesamiento manual.

La multinacional de seguros Axa presentó en 2017 Fizzy, un seguro por retraso de vuelos basados en blockchain. Un smart contract, conectado a la base de datos globales de tráfico aéreo, activaba automáticamente la compensación tan pronto como observaba un retraso no justificado de más de dos horas. Según la compañía, el uso de este contrato agiliza el proceso de indemnización y mejoraba la relación entre la aseguradora y el cliente, aunque en 2019 cesó el proyecto debido a la baja adopción por parte de las industria del viaje.

- Funciona en términos jurídicos
- Se ejecuta a través de códigos de programación
- Genera una obligación contractual
- No necesita de un ente centralizado para generar confianza
- No hace falta intermediarios para garantizar su ejecución

13.2.1 ELEMENTOS MÁS IMPORTANTES

I. **La red**: Funcionan sobre un protocolo específico, sobre la blockchain

II. **Los términos**: Los términos están definidos mediante cláusulas ejecutivas, términos claros y precisos en su programación, por lo cual se definen las condiciones que darán lugar a la autoejecución del contrato.

III. El código: El lenguaje de la máquina ejecuta ciertas órdenes, se maneja por la lógica booleana, es decir si sucede x sucedera y, no existe forma de negociar los términos con la máquina ya que se ejecutará tal como fué programado, aquí podemos diferenciar dos tipos de elementos; la fuente, que sería el tipo de lenguaje más cercano al lenguaje coloquial, es decir al lenguaje que utilizamos las personas para comunicarnos y el otro elemento se trata del código objeto, este es un tipo de lenguaje máquina, es decir un tipo de código que es entendido por la máquina. En el caso de los smart contract programados en Ethereum, el lenguaje de programación utilizado es Solidity.

IV. Los oráculos: Es un protocolo o servicio para transferir información veraz y verificada a la blockchain para que pueda ser usada en aplicaciones. Consideramos al oráculo como un servicio de cloud para blockchain que proporciona información actualizada y confiable. Los oráculos hacen de puente entre el mundo exterior y la blockchain que alberga aplicaciones, sin un oráculo la aplicaciones no tienen forma de interactuar con información fuera de la blockchain

Se trata de herramientas de los que se valen los smart contract para recopilar información del exterior, es un elemento sumamente importante para la calidad de ejecución de los smart contract ya que si el oráculo no es una fuente fiable, el contrato no se ejecutará de la manera correcta y esto daría lugar a posteriores problemas.

Por ejemplo, un oráculo puede recopilar información en tiempo real acerca de los precios de las acciones en la bolsa de New York y hacer que estén disponibles para contratos inteligentes.

Además de los flujos de los datos institucionales. Los oráculos pueden importar información de dispositivos físicos como sensores antimanipulación o termómetros.Una aplicación DEfi que monitorea las cadenas de suministros de alimentos, podría por ejemplo poder importar información de los escáneres de códigos de barras (Nakamoto, n.d.)

ARBITRAJE DESCENTRALIZADO:

Este es un elemento que se utiliza ante la existencia de renegociar un contrato o una disputa jurídica, El mundo atraviesa un acelerado proceso de globalización y digitalización. Un número creciente de transacciones se realiza en línea entre personas de todo el mundo. Entre el 3 y el 5% termina en disputas, un total de más de 700 millones sólo en 2015 (Katsh y Rabinovich-Einy 2017: 67)

Los métodos existentes de arbitraje son exclusivamente lentos, costosos y poco confiables para un mundo en línea y en tiempo real. Kleros presenta el concepto de justicia descentralizada, un innovador sistema de resolución de disputas basado en la tecnología blockchain y la inteligencia colectiva, Kleros es el primer sistema funcional de justicia descentralizada.

Tomamos el siguiente ejemplo, Maria una emprendedora argentina, contrata por internet a Bob, un programador de sitios web de Guatemala. Acuerdan las características del producto y Bob empieza a trabajar, algunas semanas más

tarde, entrega el sitio web. Pero Maria no está satisfecha con el trabajo, ella alega que la calidad del trabajo es considerablemente de baja calidad ya que la calidad es inferior a lo que esperaba, a lo que Bob responde; solo hice lo que acordamos. Maria se siente frustrada ya que entrar en un litigio judicial le podría costar mucho dinero y tiempo.

Imaginense que al momento del acuerdo Maria y Bob hubiesen hecho el acuerdo mediante un smart contract, designando a un sistema de arbitraje descentralizado como Kleros.

4

[4] Kleros es una cooperativa que desarrolla un protocolo basado en la blockchain de Ethereum, en la que mediante aplicaciones descentralizadas resuelven disputas surgidas de cualquier tipo de contratos valiéndose del arbitraje de terceros, que son guiados por incentivos económicos para llegan a una decisión.(Wikipedia)

12. USOS DE LOS SMART CONTRACT

I. TOKENIZACIÓN DE ACTIVOS

Con el auge de la digital, la tokenización de activos en las empresas se ha convertido en un campo de experimentación para explorar nuevos modelos de negocios y a su vez desarrollar herramientas que le permiten atraer y fidelizar clientes

Tokenizar es el proceso por el cual las empresas pueden emitir su propio token, respaldada por sus propios activos tradicionales, por ejemplo; bonos, acciones, divisas y otros activos no financieros por ejemplo, el sector inmobiliario, sector del arte y la música, sector agrícola, etc.

Por tokenizar también se entiende como la acción de incluir los activos de una empresa en libros contables distribuidos que se ejecutan dentro de la blockchain o emitir activos en forma de token NFT (token no fungible) para su venta o distribución (*Tokenización De Activos, Qué Es Y Cómo Funciona | IFEMA MADRID*, 2022)

14.2 CLASES DE TOKEN

I. Utility tokens

Utility token o token de utilidad es empleado como una herramienta para la recaudación de capital u obtener financiamiento por parte de las startups, empresas y grupos de proyectos

Se utiliza como resguardo de participación en las ventas masivas para reunir capital en un proyecto, estos utility token nos permiten tener acceso a un futuro producto o servicio de una empresa. Es una forma de acceso a un determinado valor, aunque no está del todo garantizado, aquellos utility token no cuentan como inversiones ya que en muchos países no cuentan con un marco regulatorio para los mismos. (Bitme,2022)

- Vehículo para obtener financiación
- Activo que se representa digitalmente y fraccionado
- Herramienta de gestión, de derecho, asignado a un token
- Representa activos (digitales o físicos) o derecho de acceso a terceros poseedores
- Se puede utilizar para obtener liquidez, un token que representa un activo puede ser utilizado como garantía en préstamos Defi

VENTAJAS

- **Dominio fraccionado**; fraccionar un activo del mundo real en tantas partes sea necesario en forma de token, los cuales pueden ser adquiridos por cualquier sujeto, en cualquier lugar y en cualquier momento
- A**utomatización de pagos**; eliminación de riesgo de la contraparte, ya que está respaldado por un smart contract
- **Inversión automatizada**; pueden acceder tanto inversores institucionales como inversores minoristas

REGULACIÓN

- Regulación; falta de normativa específica
- Regulación de acuerdo a la jurisdicción
- Esquema Sandbox regulatorio; tiene como finalidad el crecimiento de las Fintech y otras empresas tecnológicas que buscan financiación a través del crowdfunding y así mismo trabajar dentro de la inclusión financiera. Cabe recalcar que el único país dentro de latinoamericana que cuenta con un sistema Sandbox es Colombia

CASOS DE USO EN ARGENTINA

I. OPENVINO

,OpenVino, pioneros en aplicar blockchain y tokenizar el vino en el mundo, cada Token está respaldado por una botella de vino.

El presidente del Instituto Nacional de Vitivinicultura, Martin Hinojosa, firmó un acta compromiso con la empresa OpenVino, plataforma que tiene como objetivo unir la producción Vitivinícola con las nuevas tecnologías disruptivas basadas en un sistema de código abierto de software con tecnología blockchain y smart contract,

actualmente OpenVino cuenta con 3 módulos; transparencia, trazabilidad y tokenización.

(*OpenVino: Criptomonedas Para Bodegueros Respaldadas Con Vino - Noticias De Mendoza*, 2022)

CARACTERÍSTICAS DE OPEN VINO

- Empresa de código abierto, los servicios de la empresa web3 y los smart contract en blockchain, permiten a las bodegas iniciarse e implementar cripto economías para modelo de negocios sustentables, éticos y sustentables
- Token respaldada por una botella de vino,Openvino en 2018 presentó el primer criptoactivo del mundo respaldado en vino y su plataforma de negociación descentralizada, a partir del 2022 se abre a bodegas de Argentina y alrededor del mundo.
- Openvino utiliza IOT (internet de las cosas) y los acerca a viñedos y bodegas a través de sensores ambientales

II. AGROTOKEN

El ecosistema de los agronegocios cuenta con una nueva herramienta para obtener mayor liquidez a partir de la tokenización de los commodities agrícolas.

Una de las grandes novedades presentadas en Expoagro 2022 es AgroToken, la primera infraestructura de tokenización de commodities agrícolas, fundas por Eduardo Novillo Astrada y Ariel Scalites, la propuesta les permite a los agropecuarios convertir sus granos de soja, maíz y trigo en criptoactivos de manera simple, rápida y segura, es decir que un activo físico se transforma en activo digital o stablecoin. (Novillo & Scaliter, 2022)

¿CÓMO FUNCIONA EL SISTEMA?

Por cada tonelada de granos que se convierte en activos digitales o token, existe una tonelada de granos entregada a un acopio que lo respalda y certifica, luego

de ese proceso, el productor contará con token de , CORA o WHEA (soja, maíz y trigo)

Estos cripto activos ya se están utilizando para el pago de regalías, adquisición de insumos, camionetas, maquinarias, hacienda y combustible, entre otros, además las toneladas son validadas mediante PoGR (prueba de reserva de granos, por sus siglas en inglés) un sistema seguro, transparente, descentralizado y auditable en todo momento mediante la red blockchain Ethereum. (Novillo & Scaliter, 2022)

III. BITCOW

Bitcow cuya particularidad radica que está respaldado por vacas, el mundo de las economías digitales viene creciendo y el sector agropecuario no es la excepción.

Es un token que está respaldado por la ganadería, es este caso cada token esta respaldado por 1,2 (corresponden a una vaca preñada) vacas, es decir si se venden 100 Bitcow, en el campo ganadera tendría que haber 120 vacas preñadas, lo que se busca a través de Bitcoin es hacer partícipe a cualquier persona del rodeo ganadero, es decir que la gente pueda participar del negocio ganadero, que es muy conocido y de bajo riesgo pero no está al alcance de cualquier persona.

"La idea es que a medida que pase el tiempo el rodeo de vacas que se compraron vayan teniendo cría. Al principio hay una vaca preñada con garantía y a los cinco o seis meses ese rodeo empieza a tener los terneros. Lo que hacemos entonces es vender los terneros machos para solventar los gastos del sistema y las terneras hembras nos las quedamos para que se incorporen al rodeo principal. Entonces, si por ejemplo arrancamos con 100 vacas, al año siguiente deberíamos tener 120 o 130 vacas, con lo cual el inversor pasa a tener 20% o 25% más de bitcows. ***Esto es un negocio donde el inversor va teniendo cada vez más bitcows, por ende más vacas".*** (Bazán, 2021)

EMPRESAS MULTINACIONALES QUE ADOPTAN BLOCKCHAIN EN SUS OPERACIONES

CASOS FALLIDOS DE SMART CONTRACT

HACKEO THE DAO

The Dao era una organización autónoma descentralizada lanzada en 2016 en la red de bloques de Ethereum, después de recaudar 150 millones de dólares en ether a través de la venta de token. Thre Dao fué pirateada debido a vulnerabilidades en su base de código. La cadena de bloques de ethereum finalmente se dividió para restaurar los fondos robados, pero no todas las partes estuvieron de acuerdo con esta decisión , lo que dio como resultado que la red se dividiera en dos cadenas de bloques distintas; Ethereum y Ethereum classic. (company, n.d.)

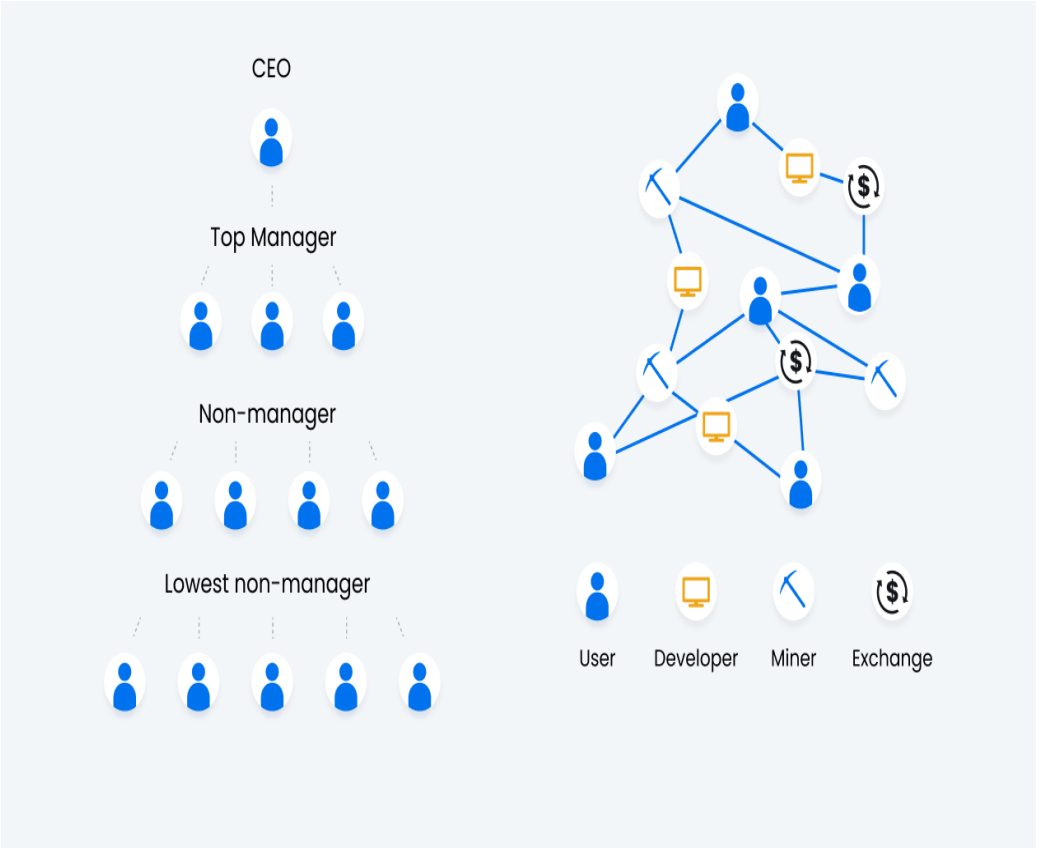
Lanzado en 2016 The Dao era un organización dirigida a inversores de capital de riesgo, elogiada como la primer organización descentralizada y autónoma, es decir su funcionamiento no iba requerir de procesos burocráticos, tampoco jerárquicos ya que todo los términos de su funcionamiento estaban automatizados a través de un smart contract. The Dao fue el primer proyecto y el más ambicioso desarrollado sobre la cadena de bloques de Ethereum ya que en ese entonces solo tenía un año desde su fundación. A tan solo 3 meses de su lanzamiento, The Dao sufrió un robo equivalente a 60 millones de Ether, lo que hizo replantearse algunas cuestiones relevantes referidas a la seguridad.

Después de muchos debates, se decidió que los fondos robados serían devueltos a los inversores, dueños de los fondos, dicha decisión ocasionó molestias entre los miembros de la comunidad de Ethereum lo cual derivó en una bifurcación de la red, es decir hubieron personas que no estuvieron de acuerdo con la decisión alegando que se iba en contra de los principios éticos de la blockchain y es así como la red quedó dividida en Ethereum y Ethereum classic.

Cabe aclarar que lo que fue hackeado, no fue la blockchain de Ethereum, este caso trata de un ataque en contra de las vulnerabilidades encontradas en el smart contract de The Dao, es decir el hacker encontró un error en el smart contract en el que estaba asentado The Dao y lo aprovechó, desviando 60 millones de ether a su billetera, pero una de las especificaciones del smart contract era que los fondos no podrían ser retirados antes de los 21 días. Los directores de Ethereum se replantearon asuntos importantes en cuanto a la seguridad de los smart contract y el refuerzo minucioso a las vulnerabilidades halladas. la lección de este caso se puede tomar desde el punto de vista de los errores que se comenten en

el proceso de desarrollo de nuevas tecnologías, en el principio pueden ser incipientes, vulnerables a ataques maliciosos pero de los errores se aprende y así como el desarrollo tecnológico ha ido evolucionando y lo seguirá haciendo con el paso de los años. Una tecnología no es mala, ni buena, todo depende del usos que se le pueda dar, pero no cabe duda que las bases en las que está cimentada la blockchain le otorga características revolucionarias que están impulsando un cambio de paradigma en el presente siglo.

DIFERENCIA ENTRE UNA ORGANIZACIÓN CENTRALIZADA Y UNA THE DAO



Fuente: Linkedln

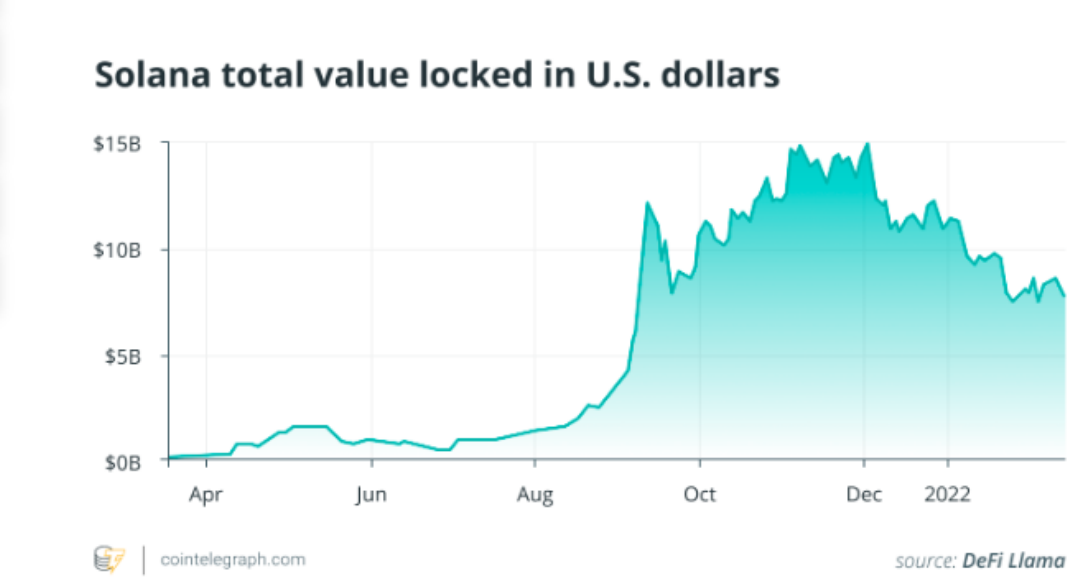
WORMHOLE: Caso de hackeo a la red Solana

Se trata del segundo mayor hackeo de las finanzas descentralizadas, podría hacer que se cuestione el ecosistema Solana y los protocolos cross-chain

¿Qué es un protocolo cross-chain?

Los cross-chain, son un tipo de intercambio de monedas que tiene lugar entre dos criptomonedas diferentes que se ejecutan en sus propias blockchain. Es decir es un mecanismo que permite a los usuarios intercambios de diferentes criptomonedas directamente entre dos partes. (Bitme, 2022)

CAPITALIZACIÓN DE MERCADO



Fuente: Cointelegraph (octubre 2022)

Solana se ha convertido en una de las redes blockchain de contratos inteligentes de más crecimiento desde su lanzamiento oficial en marzo de 2020. El valor total bloqueado en los protocolos Defi en la red, creció casi 152 millones de dólares en marzo de 2021.

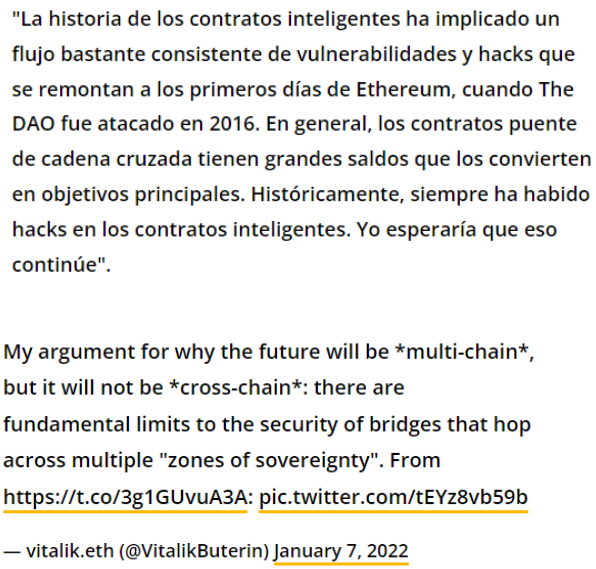
El puente de token Wormhole se vio afectado por un fallo de seguridad que culminó con la pérdida de 120.000 token de Ether, con una valorización actual de 159 millones de dólares al precio del ether actual.

Recientemente, el puente de tokens de Wormhole se vio afectado por un fallo de seguridad el 3 de febrero del presente año que culminó con la pérdida de 120.000 tokens de Ether (wETH) envueltos por valor de más de 375 millones de dólares al precio del Ether en ese momento.

Este exploit fue el mayor hasta en 2022 y el segundo mayor hackeo de Defi de la historia, wormhole es un protocolo de puente de tokens que conecta múltiples redes de blockchain como Ethereum, Solana, Terra, BNB smart chain, Polygon, Avalanche y Oasis. Permite a los usuarios enviar y recibir tokens entre cadenas de estas redes sin necesidad de un exchange centralizado o de tediosos procesos de conversión, mientras que el Ether envuelto (wETH) fue el único activo afectado por el exploit, Certik, una firma de auditoría de contratos inteligentes, mencionó que el puente de Wormhole a la red blockchain Terra podría verse afectado por la misma vulnerabilidad que el puente de Solana. (*El Hackeo De Wormhole Ilustra El Peligro De Los Puentes Cross-Chain De DeFi*, 2022)

Vitalik Buterin, cofundador de Ethereum, escribió en una sesión de Reddit AMA junto con el equipo de investigación de la fundación Ethereum donde dijo que el futuro de la tecnología blockchain es la multicadena y no la cadena cruzada, Vitalik ha razonado con respecto a las preocupaciones de seguridad de puentes y lo activos de tokens no nativos, con un enfoque de probabilidad de ataque del 51% dijo:

"*Siempre es más seguro tener activos nativos de Ethereum en Ethereum o activos Solana en Solana que tener activos Ethereum en Solana"* (Buterin, 2022)



Fuente: Cointelegraph (Buterin, 2022)

AXIE INFINITY

Un delincuente informático vulneró la seguridad de Ronin, una red que soporta al videojuego Axie Infinit, y extrajo más de 620 millones de dólares en Ethereum y USDC

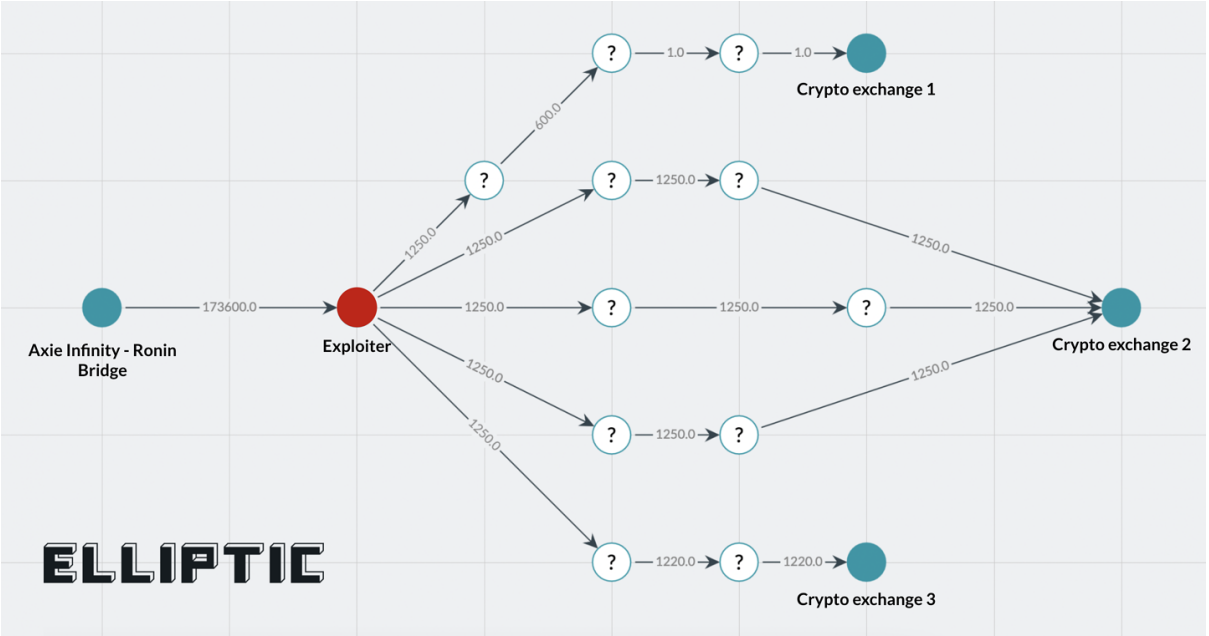
El proyecto Ronin, una blockchain que soporta a Axie Infinity, sufrió una intrusión masiva que derivó en este hurto, considerado el robo más grande de criptomonedas a la fecha

Axie Infinity es un juego basado en la blockchain en el que los jugadores compran tokens no fungibles (NFT) de monstruos similares a Pokemon para enfrentarnos en batallas, los jugadores pueden ganar un segundo token, llamado Smooth Love Potion (SLP), durante el juego y cambiarlo por dinero en una plataforma de intercambio. (Asmakov, 2022)

El informe oficial de la compañía señaló que los hacker lograron acceder a las claves privadas de los nodos validadores, como consecuencia pudieron acceder a los 5 nodos validadores que es el umbral estipulado para validar la transacción.

El ataque tuvo lugar el 23 de marzo del presente año y se descubrió una semana después, cuando los piratas informáticos que los perpetraron utilizaron los fondos robados para vender un corto Axie Infinity (AXS) y Ronin (RON). Los hackers esperaban ganar más dinero con su hazaña, pensando que la noticia del mayor hackeo de criptomonedas, sin embargo, fueron liquidados antes de que se conociera la noticia. (*Las Consecuencias Del Hackeo De USD 650 Millones De Axie Infinity*, 2022)

El puente de Ronin fué cerrado después de lo sucedido con todos los fondos retenidos hasta que se lleve a cabo una investigación y determinar e identificar los posibles fallos, a su vez la empresa ha pedido ayuda a varias bolsas de criptomonedas y a al grupo de análisis de criptomonedas Chainalysis para poder rastrear el camino de los fondos hackeados y poder recuperarlos. La vulneración al puente de Ronin fué similar a lo ocurrido con el puente Wormhole de Solana, donde los hackeadores lograron salirse con la suya.



Fuente: Elliptic, 2022 (movimiento de los fondos robados del Ronin Bridge)

15. DESAFÍOS LEGALES DE LOS SMART CONTRACT

Por su naturaleza descentralizada, compartida, consensuada y por su inmutabilidad, blockchain permite la operación y alojamiento de los denominados Smart contract o contratos inteligentes de la forma en que Nick Szabo lo había conceptualizado en 1994

El modo autónomo en que se ejecutan los smart contract o contratos inteligentes han traído consigo un escenario con diversidad de retos desde el punto de vista jurídico, pues gracias a blockchain se resuelven algunos de los problemas que presentan los contratos electrónicos(manipulación en la redacción o confirmación de emisión y recepción) cabe recalcar que existen diferentes tipos de smart contract, siendo dos de ellos los smart contract code y los smart contract legal.

Se espera que los contratos inteligentes reúnan las ventajas de la cadena de bloques y de los procesos automatizados o autónomos, para proporcionar una formación de contratos validada y de igual a igual sin necesidad de verificación independiente (Bellamy y Hill, 2016)

En el ámbito de la informática, un smart contract es, en términos simples, una secuencia de código y datos que efectúa la operación para la cual fue programada; bajo esta óptica no sería un contrato en términos jurídicos; una definición legal sobre un smart contract sería la de un programa informático con instrucciones ejecutables codificadas, donde el código puede, entre otras opciones programadas, contener las que tengan relación al cumplimiento de las cláusulas y en donde exista un acuerdo de voluntades, concurriendo así su relación en el mundo legal.

- No todo smart contract es un contrato en términos de la ley, ya que tendría que reunir todos los requisitos que la ley prevé
- No se encuentra una clara definición en el código civil y comercial Argentino
- Redacción, trabajo conjunto entre abogados y programadores
- Identificación de las partes, en blockchain no es necesario compartir información personal para poder negociar, basta con un alias para poder hacerlo
- Capacidad, como probar que la persona es capaz en términos de la ley
- Consentimiento
- Cláusulas predispuestas
- Contratación sin la intervención del componente humano
- Idoneidad e imparcialidad del oráculo
- Actividades reguladas
- Nulidad

- Ley y jurisdicción aplicable

  Blockchain al tratarse de una tecnología no se encuentra bajo la regulación de ningún país, lo que sí están regulando algunos países son los servicios financieros que se están formando en el ecosistema blockchain. A continuación se muestra la lista de algunos países que contemplan y regulan la circulación y operación de los activos digitales.

REGULACIÓN DE CRIPTOMONEDAS EN EL MUNDO

Estados Unidos: A pesar de existir una gran cantidad de inversores en criptomonedas y empresas de blockchain, aún no ha desarrollado un marco regulatorio claro para dicha clase de activos. La Comisión de Bolsa y Valores (SEC) considera a la criptomoneda como un valor, mientras que la Comisión de Comercio de Futuros de Commodities llama a Bitcoin un commodity y el Tesoro lo llama moneda. Los intercambios de criptomonedas se encuentran bajo el alcance regulatorio de la Ley de Secreto Bancario y deben registrarse en la Red de Ejecución de Delitos Financieros. También están obligados a cumplir con las obligaciones contra lavado de activos (AML) y la lucha contra la financiación del terrorismo (CFT). Mientras tanto, el Servicio de Impuestos Internos clasifica las criptomonedas como propiedad a efectos del impuesto federal sobre la renta.

Canadá: Se convirtió en el primer país en aprobar un fondo cotizado en bolsa de Bitcoin en febrero de 2021. Además, los Administradores de Valores y la Organización Reguladora de la Industria de Inversiones han aclarado que las plataformas de comercio de criptomonedas y los distribuidores en el país deben registrarse con los reguladores provinciales. Además, Canadá clasifica a las empresas de inversión en criptomonedas como empresas de servicios monetarios y requiere que se registren en el Centro de Análisis de Informes y Transacciones Financieras. Desde el punto de vista fiscal, Canadá trata las criptomonedas de forma similar a otros commodities.

Reino Unido: Considera la criptomoneda como propiedad pero no como moneda de curso legal. Además, los intercambios de criptomonedas deben registrarse en la Autoridad de Conducta Financiera del Reino Unido (FCA) y tienen prohibido ofrecer operaciones con derivados. Además, el organismo regulador ha introducido requisitos específicos de criptomonedas relacionados a "Conoce a tu cliente" (KYC), AML y CFT. Aunque los inversores todavía pagan impuestos sobre las ganancias de capital del comercio de criptomonedas, la tributación depende del tipo de actividad realizada y de quién participa en la transacción.

Japón: Reconoció a las criptomonedas como propiedad legal bajo la Ley de Servicios de Pago. Mientras tanto, los exchanges en el país deben registrarse en la Agencia de Servicios Financieros (FSA) y cumplir con las obligaciones AML y CFT. Japón trata las ganancias comerciales generadas por las criptomonedas como "ingresos varios", gravando así a los inversores.

Australia: Clasifica las criptomonedas como propiedad legal, por lo que posteriormente las somete al impuesto sobre las ganancias de capital. Los exchanges son libres de operar en el país, siempre que se registren en el Centro Australiano de Análisis e Informes de Transacciones y cumplan con obligaciones específicas AML y CTF. En 2019, la Comisión Australiana de Valores e Inversiones introdujo requisitos reglamentarios para las ofertas iniciales de monedas (ICO) y prohibió los exchanges que ofrecen monedas privadas.

Singapur: Clasifica la criptomoneda como propiedad pero no como moneda de curso legal. La Autoridad Monetaria de Singapur (MAS) otorga licencias y regula los exchanges como se describe en la Ley de Servicios de Pago. Singapur, en parte, obtiene su reputación como refugio seguro de las criptomonedas porque las ganancias de capital a largo plazo no están sujetas a impuestos. Sin embargo, el país grava a las empresas que realizan transacciones habituales en criptomonedas, tratando las ganancias como ingresos.

Corea del Sur: No considera las criptomonedas como moneda de curso legal o activos financieros. Como tal, las transacciones en moneda digital evitan el impuesto a las ganancias de capital. El Servicio de Supervisión Financiera de Corea

del Sur supervisa la regulación de exchanges de criptomonedas, y los operadores están sujetos a estrictas obligaciones AML y CFT. A partir de septiembre de 2021, los intercambios de criptomonedas y otros proveedores de servicios de activos virtuales deben registrarse en la Unidad de Inteligencia Financiera de Corea, una división de la Comisión de Servicios Financieros.

China: No clasifica las criptomonedas como moneda de curso legal; sin embargo, las clasifica como propiedad a los efectos de determinar las herencias. El Banco Popular de China prohíbe que los exchanges operen en el país. Binance, el mayor exchange del mundo, se lanzó inicialmente en China, pero trasladó su sede a las Islas Caimán en 2017 tras los cambios regulatorios en criptomonedas. Además, China prohibió la minería de Bitcoin en mayo de 2021, lo que obligó a muchos que participan en la actividad a cerrar sus operaciones o reubicarse en jurisdicciones con un entorno regulatorio más favorable. Suiza: El Parlamento aprobó la Adaptación de la Ley Federal a los Desarrollos en la Tecnología de Registros Electrónicos Distribuidos (2020), que establece un marco ampliado para regular blockchain y DLT basado en la taxonomía de tokens y ICOs (2018). La Ley AML (2020) requiere que las empresas de blockchain verifiquen la identificación del cliente y la informen a la Oficina de Denuncias de Lavado de Dinero. La Administración Federal de Impuestos de Suiza ha establecido una guía sobre el tratamiento fiscal de las criptomonedas, que establece que la riqueza privada generada a partir de las criptomonedas no incurre en impuestos. Sin embargo, los ingresos obtenidos de la minería y el comercio sí están sujetos a impuestos

CONCLUSIONES

Blockchain es posiblemente la tecnología más disruptiva en los últimos tiempos, que está cambiando poco a poco el mundo de los negocios ya que permite registrar transacciones de manera permanente dentro de una red descentralizada, la cual utiliza un registro distribuido, lo que significa que todos sus participantes son dueños de la información, esto es un red blockchain cuya información se guarda segura por medio de una código criptográfico.

Las empresas pueden lograr importantes ventajas competitivas con esta tecnología, de esta manera las organizaciones tienen acceso a una herramienta confiable para transacciones financieras y comerciales. Comparto algunos beneficios que aporta blockchain a las empresas:

La digitalización: Todos los datos en la plataforma están basados en tecnología de registro distribuido. lo participantes de la red pueden tener acceso de manera inmediata a documentos o transacciones, a la vez este registro inalterable crea una huella auditable, que por su característica inmutable es inmanipulable, "crea una sola verdad"

Menor riesgo operativo: Al ser un proceso descentralizado e incorruptible reduce los riesgos operacionales en las empresas que se genera a través de los contratos inteligentes

Reducción de pérdidas: La creación de información basada en esta red, considerada inmutable, permite reducir el número de conciliaciones, dado que cada bloque contiene su información y la información del bloque anterior por lo tanto blockchain facilita la automatización de conciliaciones y reduce notablemente errores en dichos procesos

Ahorro en costos: Está tecnología mejora la eficiencia operativa, reduce el costo del capital, genera menores costes de cumplimiento de riesgos administrativos

Creación de nuevos mercados: Con la llegada de blockchain se abre el mercado del internet del valor ya que permite representar algún elemento del mundo real a través de un representación digital.

Hoy en día es en el sector financiero, el área donde más se investiga y se prueban proyectos, ya que por sus características promete brindar mayor seguridad, transparencia, eficiencia, automatización y ventajas competitivas en las operaciones

Ya son muchas las industrias que están implementando esta tecnología, debido a que directivos e instituciones han aceptado su potencial. Pero su adopción no ha cumplido con lo pronosticado hace años anteriores cuando apareció por primera vez.

Cabe reconocer que a pesar de sus múltiples beneficios, aún es una tecnología que se encuentra en pleno proceso de adopción y expansión. Por estar íntimamente ligados al

ecosistema de las criptomonedas, muchas personas piensan que Blockchain y Bitcoin son lo mismo, pero realmente no son lo mismo ya que bitcoin es solo uno de sus tantos usos. Blockchain es más que una criptomoneda. Es una tecnología con características realmente revolucionarias que podría aportar grandes beneficios para la sociedad actual, su pasado con el bitcoin puede hacer que no parezca confiable debido a que la volatilidad es una de las características más relevantes de las monedas digitales.

RECURSOS A UTILIZAR

Para el presente trabajo de investigación se estará usando recursos encontrados en páginas de internet así como videos conferencias que abordan el impacto de Blockchain como una tecnología disruptiva e innovadora dadas a través de plataformas de video como Youtube así como la búsqueda de información en trabajos de tesis de diferentes autores, ya que tratándose de una nueva tecnología, que esta en plena evolución y desarrollo, amerita recopilar información actualizada y relevante desde diferentes puntos de vistas, entre ellos desde una mirada técnica, una mirada legal pues los smart contract no dejan de ser contratos utilizados para el cumplimiento de acuerdos entre partes interesadas, el presente trabajo de tesis estará centrado en demostrar las múltiples ventajas de los smart contract frente al desafío de la globalizaciòn digital que trae aparejado problemas que deben ser abordados de una forma eficiente, algunos de los beneficios que ofrece blockchain en cuanto a seguridad, inmutabilidad y reducción de costo, pueden ser aprovechados en el sector empresarial, A continuación se detalla cada uno de los recursos a utilizar en el presente trabajo, tanto lecturas así como también videos que fueron recopilados a través de páginas web y bibliotecas digitales.

CLASE MAGISTRAL; BLOCKCHAIN Y CONTRATOS INTELIGENTES, UCA, 202O
https://youtu.be/ggjvuc8Yo8M

CONTRATACIONES DIGITALES, LEGAL TECH 2020
https://youtu.be/UQysKoXWeM4

¿QUÉ SON LOS CONTRATOS INTELIGENTES?
https://youtu.be/oDNl9QbhFb0

HOW SMART CONTRACT WILL CHANGE THE WORLD
https://youtu.be/pA6CGuXEKtQ

ETHEREUM 2020
https://youtu.be/YpUG1VFEiZE

SMART CONTRACT, Ethereum.org
https://ethereum.org/en/smart-contracts/

¿QUÉ SON LOS SMART CONTRACT? Bitme academy, 2021
https://academy.bit2me.com/que-son-los-smart-contracts/

INTRODUCCIÓN A LOS SMART CONTRACT
https://solidity-es.readthedocs.io/es/latest/introduction-to-smart-contracts.html

SMART CONTRACT EN ETHEREUM, Udemy academy
https://www.udemy.com/course/smart-contracts-en-ethereum-para-principiantes-solidity/

CREANDO SMART CONTRACT, Paradigmadigital.om
https://www.paradigmadigital.com/dev/creando-smart-contracts-en-ethereum/

LOS CAMBIOS DE ETHEREUM, Academia Platzi
https://youtu.be/XnHBmwjpaxk

METODOLOGÍA DE LA INVESTIGACIÓN, Uca, 2020
/https://www.uca.ac.cr/wp-content/upl

DECENTRALIZED FINANCE
https://docs.ethhub.io/built-on-ethereum/open-finance/what-is-open-finance/

¿QUÉ SON LAS FINANZAS DESCENTRALIZADAS?
https://platzi.com/blog/que-son-finanzas-descentralizadas-defi/?gclid=Cj0KCQjwvZCZBhCi

FINANZAS DESCENTRALIZADA
ARIsAPXbajsWEHN60gJi8BAXCOoPrDXbWmDEAYNE3l2VvPFXmLAGIC73adMzbJYa

¿WHAT IS THE DEFI?
AslKEALw_wcB&gclsrc=aw.ds

FINANZAS DESCENTRALIZADAS, Ripio.com
https://launchpad.ripio.com/guias-capitulos/finanzas-descentralizadas-defi

PORQUE BLOCKCHAIN VA MÁS ALLÁ DE LAS CRIPTOMONEDAS
https://eleconomista.com.ar/cryptos/por-blockchain-va-mucho-mas-alla-criptomonedas-n50772

BLOCKCHAIN ELEMENTOS BÁSICOS
https://search.abb.com/library/Download.aspx?DocumentID=9AKK107046A1240&L

EN EL BLOCKCHAIN NADA PUEDE SER BORRADO
https://www.infobae.com/america/colombia/2022/09/18/en-el-blockchain-nada-puede-ser-bor

USO DE BLOCKCHAIN
ider-en-el-uso-de-esta-herramienta/

EL ROBO DE CRIPTOMONEDAS
https://www.iprofesional.com/tecnologia/359865-criptomonedas-revelan-el-robo-mas-grande-de-la-historia

EL SISTEMA SWIFT Y LAS FINANZAS
https://www.lanacion.com.ar/economia/comercio-exterior/el-sistema-swift-y-las-fintech-nid2232762/#:~:text=SWIFT%20

WHAT IS ETHEREUM
https://blockgeeks.com/guides/ethereum/

CUÁLES SON LAS SOLUCIONES QUE BLOCKCHAIN PUEDE APORTAR
https://www.forbesargentina.com/innovacion/cuales-son-soluciones-blockchain-puede-aportarles-empresas-argentinas-n22306

QUE ES ETHEREUM GAS
https://blockgeeks.com/guides/ethereum-gas/

TECNOLOGÍA BLOCKCHAIN
https://es.cointelegraph.com/news/blockchain-technology-can-change-the-world-and-not-just-via-crypto

MARKET CAP RONIN
https://www.coinbase.com/es/price/ronin

LAS CONSECUENCIAS DEL HACKEO A RONI
https://es.cointelegraph.com/news/the-aftermath-of-axie-infinity-s-650m-ronin-bridge-hack

INTERNET DE LAS COSAS
https://www.came-educativa.com.ar/news/internet-de-las-cosas-inteligencia-artificial-y-blockchain-catalizadores-de-la-transformacion-digital/

WHAT ARE SMART CONTRACT
https://blockgeeks.com/guides/smart-contracts/

HACKEO DE WORMHOLE
https://es.cointelegraph.com/news/wormhole-hack-illustrates-danger-of-defi-cross-chain-bridges