UNIVERSIDAD TORCUATO DI TELLA

MBAV18

Blockchain como solución a la crisis del mercado de compra venta de inmuebles en Ciudad de Buenos Aires

Alumna Mariana Riquelme
Tutora Paz Cereijo
Año 2020
Buenos Aires, Argentina

UNIVERSIDAD TORCUATO DI TELLA

Agradecimientos

A Caro Collazo por guiarme y ayudarme durante este proceso.

A mi tutora, por ayudarme en todo este camino.

A mis padres, por acompañarme siempre.

A Caro, por su amor y paciencia infinita.

Índice de contenido

Resumen ejecutivo

El objetivo del presente trabajo fue analizar la factibilidad de que la tecnología blockchain brindara respuesta a las necesidades del mercado inmobiliario en Ciudad de Buenos Aires, que se encontraba casi paralizado ante la falta de respuesta sobre tres problemáticas bien definidas: posibilidad de fraude, altos costos de las transacciones y un mercado completamente dolarizado, en un contexto de escalamiento del dólar.

Mediante esta investigación exploratoria, se realizó una revisión de la literatura acerca de blockchain y se analizó su aplicación a este modelo de negocios. Luego se realizó un análisis sobre si los propietarios de inmuebles en CABA utilizarían un sistema de compra – venta de bienes inmuebles basados en la tecnología blockchain.

Como resultado del trabajo se mostró que la tecnología blockchain brindó una solución a los principales problemas que aquejan al sector inmobiliario argentino ya que aportó una alternativa innovadora, ágil y de fácil utilización para el ciudadano promedio.

En conclusión, el mercado inmobiliario de compraventa de inmuebles en la Ciudad de Buenos Aires se encontraba en un momento crítico debido a varias razones:

- ✓ Escaso acceso al crédito para quienes deseaban comprar una vivienda.
- ✓ Era un mercado dolarizado.
- ✓ Altos costos para realizar la transacción.
- ✓ Contexto desfavorable para alquilar un inmueble.

Ante esta situación, blockchain surgió como una alternativa viable ya que era una base de datos distribuida entre distintos participantes, que se encontraba protegida criptográficamente, organizada en bloques de transacciones relacionados uno con el otro matemáticamente, posibilitando que partes que no confiaban plenamente unas en las otras, lleguen a un acuerdo sobre la realización de una transacción. El consenso era la clave en este proceso. La red de manera eficiente certificaba que el movimiento (tanto la transferencia de propiedad y como contrapartida la entrega de dinero) se realizó, por lo cual, ya no era necesario contar con una inmobiliaria que realizara las certificaciones de dominio y de inhibición, como tampoco un escribano que certificara la transacción, reduciendo los costos que se pagaban para poder llevar adelante la transacción y los tiempos, y estaba garantizado que la operación era lícita para ambas partes.

Palabras claves

Blockchain, mercado inmobiliario, crisis.

Introducción

El comercio, como se lo conocía hasta el 2009, dependía de instituciones que servían como terceros confiables para garantizar que la transacción se ha realizado fehacientemente. Era necesario que "ese tercero" garantizara la operación, debido a que no existía confianza entre las partes. Esta necesidad de tener un intermediario para impedir el problema del doble gasto se traducía en mayores costos para realizar la operación (ya que existía una erogación monetaria por realizar esta intermediación) y, aun así, era aceptado que un porcentaje de las transacciones que se realizaban sean fraudulentas.

La tecnología blockchain, brindó una solución al problema descripto, ya que propuso que el sistema transaccional se basara en pruebas criptográficas en vez de tener como base la confianza entre las partes, lo que permitió suprimir cualquier tipo de intermediación. Se trataba de un libro mayor distribuido y digitalizado que registraba y compartía información de manera inviolable, así lo mencionó Satoshi Nakamoto en su manifiesto denominado Un sistema de Efectivo Electrónico de usuario a usuario. (Nakamoto, 2009)

La blockchain era conocida como la tecnología sobre la cual se desarrolla Bitcoin, pero con el paso del tiempo, se fueron descubriendo innumerables formas de aplicar esta tecnología lo que permitió optimizar procesos, reducir costos y aumentar la confianza entre las partes. En este sentido, uno de los conceptos más revolucionarios que brindó el desarrollo de blockchain fue en nacimiento de los Smart Contract.

Un contrato no era otra cosa que un acuerdo entre las partes, en el que se definía que se podía hacer, como se debía hacer y qué pasaría si no era cumplido, que por lo general se documentaban por escrito. En el caso de un contrato inteligente, el mismo era capaz de ejecutarse y hacerse cumplir por sí mismo, así lo mencionan Alex Preukschat en su libro Blockchain: La Revolución Industrial de Internet, donde detalló distintos usos que se le podían dar a la blockchain como medio para transformar las finanzas (Preukschat, 2017) .

Si se pensaba específicamente en el mercado inmobiliario argentino, se podía observar en los datos relevado por Reporte Inmobiliario, que muchos de los problemas que aquejaban al sector, quedaban resueltos y era más sencillo y menos costoso adquirir una vivienda si se hubiera utilizado, por ejemplo, un contrato inteligente para realizar la operación (Reporte Inmobiliario, 2021)

Posibilidad de fraude: Uno de los puntos que se utilizaban para justificar la "necesidad" de realizar este tipo de operaciones mediante una inmobiliaria y con un escribano "de confianza" es que de esta manera se disminuía el riesgo de ser estafados.

Altos costos para desarrollar la operación: Claramente, lo descripto en el punto anterior, sobre la necesidad de contar con varios intermediarios para disminuir el riesgo de fraude, genera sobre costos que se debían abonar al momento de realizar la operación tanto por parte del vendedor como del comprador (entre un 7% y 10% del total del valor de la escritura).

Mercado dolarizado: En Argentina existían una serie de restricciones por parte del Gobierno Nacional para poder comprar dólares (el máximo permitido por persona era de USD 200), a lo cual se le agregaban un 65% de impuestos (30% impuesto PAIS + 35% Impuesto a las ganancias) sobre el precio oficial. Este punto prácticamente empujaba a sus ciudadanos a adquirir dólares en el mercado ilegal (denominado "dólar blue"), lo que los dejaba expuestos a cualquier tipo de fraude sin posibilidad de defenderse ya que estaban cometiendo un ilícito.

Si bien era indispensable el apoyo gubernamental para que la cadena de bloques comience a ser utilizada y pudiera consolidarse en este mercado, lo expuesto anteriormente dejaba reflejado el gran potencial que tenía blockchain para transformar las transacciones que se realizaban en el mercado inmobiliario brindando seguridad y reducción de costos.

Para ello, la pregunta principal que se debía responder era la siguiente:

¿Esta tecnología ofrecía una alternativa a las problemáticas más importantes que presentaba la compra - venta de viviendas entre particulares, en el mercado inmobiliario de la Ciudad de Buenos Aires en 2021?

Para poder responder a esta pregunta principal, como guía de la investigación, se consideraron las siguientes preguntas:

1. ¿Qué es la cadena de bloques?
2. ¿Cuáles son sus principales características, fortalezas, debilidades?
3. ¿Cuáles son aquellos supuestos que deben darse para garantizar o fomentar la utilización de un sistema con estas características?
4. ¿Cuáles son las particularidades del mercado inmobiliario en la Ciudad de Buenos Aires?
5. ¿Cuáles son los puntos de dolor más importantes?

Para responder estas preguntas, en la presente investigación exploratoria, se realizó una revisión de la literatura acerca de blockchain y su aplicación a este modelo de negocios para luego realizar un estudio del caso, analizando si los propietarios de inmuebles en CABA utilizarían un sistema de compra – venta de bienes inmuebles basados en la tecnología blockchain.

El objetivo principal fue describir y entender las características de esta tecnología y analizar su aplicabilidad para regular el mercado de compra - venta de viviendas entre particulares en la Ciudad de Buenos Aires.

Esto se logró a través de los siguientes objetivos específicos:

- ✓ Revisión de la literatura existente sobre blockchain y su aplicación dentro del área de estudio.
- ✓ Descripción del proceso que se lleva adelante dentro de una blockchain.
- ✓ Análisis del proceso dentro de la blockchain y los Smart Contract.
- ✓ Retrato y problemática de la situación actual del mercado inmobiliario.
- ✓ Identificación de los puntos de dolor más importantes del sector.

El lector recorrió, de esta manera, la historia de esta tecnología, su definición, fundamentos que le dieron origen, sus obstáculos y posibilidades de mejora y el impacto que podría tener sobre el mercado inmobiliario en Ciudad de Buenos Aires bajo las características tan particulares del mismo.

Justificación y delimitación

Esta investigación fue exploratoria. Se realizó una revisión de la literatura acerca de blockchain y su aplicación a este modelo de negocios. Luego se realizó un análisis sobre si los propietarios de inmuebles en CABA utilizarían un sistema de compra – venta de bienes inmuebles basados en la tecnología blockchain.

Esta investigación fue no experimental, ya que se limita a observar los fenómenos tal como sucedieron en la realidad.

La población bajo estudio estaba conformada por los clientes dispuestos a consumir un sistema de intercambio de bienes inmuebles en la Ciudad de Buenos Aires basado en blockchain.

Marco Teórico

Capítulo 1 – Un poco de historia sobre Blockchain

El 31 de octubre de 2008, Satoshi Nakamoto utilizó la lista de correo de criptografía en wetzdown.org para darles a conocer a los cypherpunks (subgénero de la ciencia ficción en un entorno futurista distópico que combinaba una baja vida y alta tecnología con logros tecnológicos y científicos avanzados, como inteligencia artificial y cibernética , yuxtapuestos con un grado de ruptura o cambio radical en el orden social) que utilizaban esta red que se había desarrollado un sistema de efectivo electrónico Peer to Peer, donde no era necesario que intervengan terceros para garantizar la realización de dichas operaciones. En ese mensaje también se mencionó que la explicación de todo este proceso revolucionario quedaba plasmada en un documento que estaba alojado en el sitio bitcoin.org. La primera moneda digital había nacido.

Bitcoin no era lo mismo que blockchain, ya que esta última, era la tecnología en la que se basaba la criptomoneda para existir. Por este motivo, si bien se lo conocía a Satoshi Nakamoto como el cerebro detrás de esta tecnología, la misma nació mucho antes: el criptógrafo David Chaum propuso por primera vez un protocolo similar a una cadena de bloques en su disertación de 1982 "Sistemas informáticos establecidos, mantenidos y de confianza por grupos mutuamente sospechosos" y en 1991 S. Haber y W. Scott dieron a conocer su primer trabajo que consistía en una cadena de bloques protegida criptográficamente en la que no se podía manipular las fechas de los documentos. Posteriormente le incorporaron a la misma los árboles de Merkle (estructura de datos en árbol, binario o no, en el que cada nodo que no era una hoja estaba etiquetado con el hash de la concatenación de las etiquetas o valores de sus nodos hijos. Esto permitió que un gran número de datos separados puedan ser ligados a un único valor de hash) para recopilar más documentos en un solo bloque. (Corebi, 2019)

La irrupción del Bitcoin en el mundo financiero fue el puntapié inicial que necesitaba la tecnología para poder ganar escalabilidad a lo largo de esta década. Bitcoin nació en 2008 como la primera aplicación de una blockchain. El 3 de enero de 2009, Nakamoto anunció que se creó el primer bloque (bloque génesis) de la blockchain de Bitcoin. A su vez, el 9 de enero de ese mismo año se anunció el lanzamiento de la primera versión del Bitcoin y día 11 fue realizada la primera transacción en dicha plataforma.

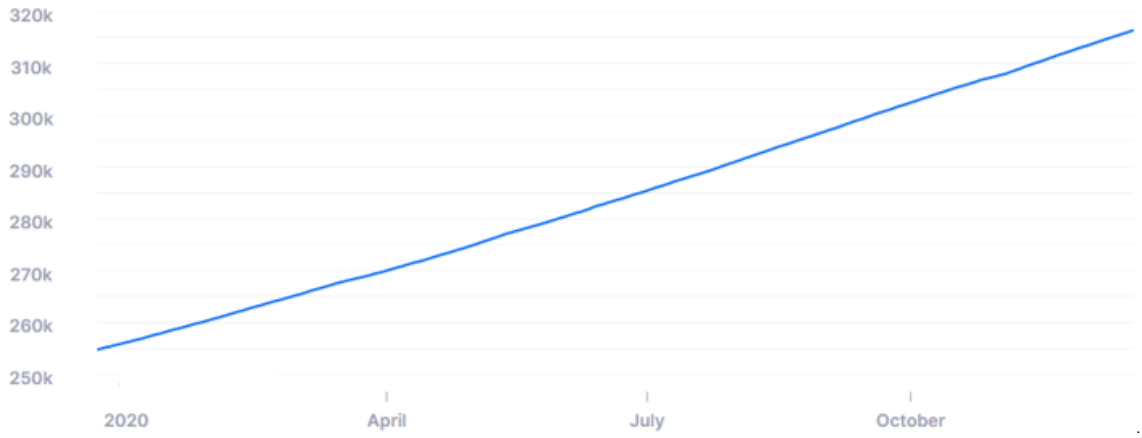
Este hito fue muy importante para el desarrollo posterior de la criptomoneda. En primer lugar, demostró que Bitcoin funcionaba, que era inalterable y que abría la posibilidad de desarrollar nuevas aplicaciones como los ya conocidos token o contratos inteligentes.

En el año 2013 nació Ethereum (una cadena de bloques descentralizada de código abierto que presentó una funcionalidad de contrato inteligente . El Ether fue la criptomoneda nativa de la plataforma y la segunda criptomoneda más grande por capitalización de mercado, después de Bitcoin), una nueva blockchain pública con funcionalidades adicionales a las Bitcoin, ya que esta nueva cadena de bloques tenía habilitada una función que le permitía a sus usuarios habilitar otros activos, como por ejemplo contratos, ampliando así su aplicación.

El crecimiento de la cadena de bloques Bitcoin fue exponencial a lo lago de los últimos años. En agosto de 2014, el tamaño del archivo de la cadena de bloques de Bitcoin, que contenía registros de todas las transacciones que se han producido en la red, alcanzó los 20 GB (gigabytes). En enero de 2015, el tamaño había creció a casi 30 GB, y de enero de 2016 a enero de 2017, la cadena de bloques de Bitcoin pasó de 50 GB a 100 GB de tamaño. El tamaño del libro mayor superó los 200 GiB a principios de 2020 (ver figura 1).

FIGURA 1

TAMAÑO DE LA BLOCKCHAIN BITCOIN EN MB DURANTE 2020

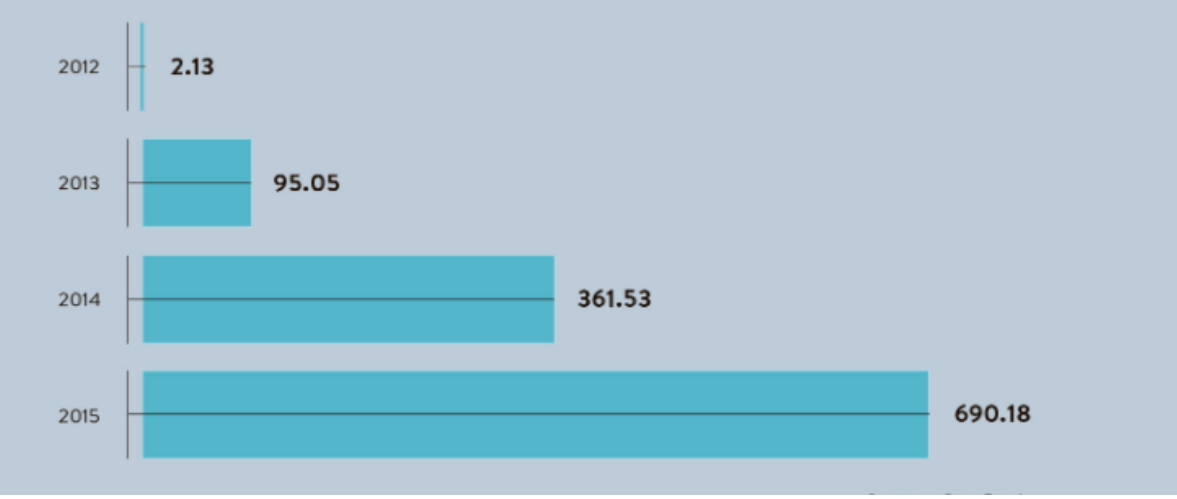


Nota: Crecimiento exponencial de Bitcoin durante 2020, ya que pasó de los 255 GiB a comienzo de 2020 para llegar a los 320 GiB a finales de ese mismo año. Fuente: https://www.criptonoticias.com/tecnologia/tamano-blockchain-bitcoin-aumento-25-en-2020/

Con respecto a la financiación global de capital de riesgo, creció un 91% en 2015 en comparación con el año anterior, o un increíble 726% en los últimos dos años. Se invirtieron USD 216 millones en blockchain en el primer trimestre de 2016 y fue la primera vez que blockchain y los startups híbridos recaudaron más dinero que los startups de Bitcoin (ver figura 2). (Allidina, 2016).

FIGURA 2

INVERSIONES DE CAPITALES DE RIESGO EN BITCOIN/BLOCKCHAIN EN MILLONES DE DÓLARES



Nota: A comienzo de 2012 el Bitcoin comenzó a recibir capitales y a medida que la confianza de los inversores fue creciendo, aumentaron las inversiones privadas. Fuente: https://elanalistaeconomicofinanciero.blogspot.com/2019/05/grafico-de-financiacion-de-capital.html

En mayo de 2018, la consultora de tecnología Gartner (firma global de investigación y asesoría que brinda información, asesoramiento y herramientas para líderes en TI, finanzas, recursos humanos, servicio y soporte al cliente, comunicaciones, legal y cumplimiento, mercadeo, ventas y cadena de suministro) descubrió que solo el 1% de los CIO indicaron algún tipo de adopción de blockchain dentro de sus organizaciones, y solo el 8% de los CIO planificaron o miraron experimentación activa con blockchain para el corto plazo. La investigación, contenida en la “Encuesta CIO 2018”. Por su parte, también se encontró que el 77% de los CIO dijeron que su organización no tenía interés en la tecnología y / o no habían planificado ninguna acción para investigarla o desarrollarla. Esta noticia fue un llamado de atención que dejaba en manifiesto la gran cantidad de discusión que era necesaria sobre el uso de la blockchain, ya que dicha tecnología aportaba capacidades muy valiosas y significativas, especialmente porque existieron problemas en torno a la confianza y la permanencia del registro de datos. (Wikipedia, 2020)

Asimismo, aun con algunas llamadas de atención en cuanto a su gran volatilidad, el número de transacciones de la blockchain Bitcoin no dejó de crecer (ver figura 3).

FIGURA 3

NÚMERO DE TRANSACCIONES BITCOIN DESDE 2009 A 2017

Nota: Las inversiones en Bitcoin se fueron multiplicando a medida que pasa el tiempo y gana valor entre los inversores como resguardo de valor. Fuente: https://www.bitcoin.com.mx/el-volumen-de transacciones-de-bitcoin-se-acerca-de-nuevo-a-su-cumbre/

Capítulo 2 – Decodificando la blockchain

Desde su creación las blockchains fueron creadas en tres partes que, al combinarse, aseguraban la trazabilidad de una operación y eliminaban el problema del doble gasto de una moneda:

2.1 - Criptografía: era un procedimiento donde se utilizaba un algoritmo con clave (clave de cifrado), para transformar un mensaje de tal forma que sea incomprensible, o al menos, difícil de comprender, a toda persona que no tenía la clave secreta (clave de descifrado) del algoritmo empleado. Era responsable de proveer un mecanismo infalible para la codificación segura de las reglas del protocolo que regían el sistema. Por otro lado, también era fundamental para evitar la manipulación, hurto o introducción errónea de información en la cadena de bloques, así como era la responsable de generar firmas e identidades digitales encriptadas.

2.2 - La cadena de bloques: era la base de datos diseñada para el almacenamiento de los registros realizados por los usuarios. Todas las blockchains tenían que actuar bajo las mismas reglas o protocolos para dar validez al bloque (y a la información reunida) e incorporarlo a la cadena de bloques. Una vez realizada esta tarea, la cadena continuaba con la emisión del siguiente bloque, permaneciendo inalterable la información registrada a través de la criptografía. Esto eliminaba la necesidad de un tercer ente de confianza.

2.3 - El consenso: su base era un protocolo común que verificaba y confirmaba las transacciones realizadas y aseguraba la irreversibilidad de estas. Este consenso debía proporcionar a todos los usuarios una copia inalterable y actualizada de las operaciones realizadas en la blockchain.

Una blockchain era una base de datos distribuida entre distintos participantes, que se encontraba protegida criptográficamente, organizada en bloques de transacciones relacionados uno con el otro matemáticamente, posibilitando que partes que no confiaban plenamente unas en las otras, llegaran a un acuerdo sobre la realización de una transacción. El consenso era la clave en todo este proceso.

Esta tecnología estaba conformada por distintos elementos relacionados entre sí:

2.4 - Protocolo: se utilizaba un protocolo estándar, en forma de software informático, para que una red de ordenadores (nodos) puedan comunicarse entre sí.
2.5 - Nodo: todos los ordenadores debían tener el mismo software (protocolo) para comunicarse entre ellos. Sin este software no podían participar de la blockchain.
2.6 - Red entre pares (P2P): en todas las blockchain, los nodos se encontraban conectados directamente entre sí, sin necesidad de intermediarios.

2.7 - Sistema descentralizado: eran todos los nodos conectados los que controlan la red, ya que son todos iguales entre si (no había una jerarquía entre los mismos).

Con lo cual, se pudo redefinir el concepto blockchain para decir que era un conjunto de ordenadores (nodos), que se encontraban conectados a una red y utilizaban el mismo sistema de comunicación para almacenar y validar la misma información registrada en una red P2P. Esta información, no se podía modificarse ya que complejos algoritmos criptográficos, sumadas a la capacidad colectiva de la red, contribuían a asegurar la irreversibilidad de las transacciones registradas (ver figura 4).

La blockchain podía ser clasificada de la siguiente manera:

2.8 - Blockchain Públicas: eran las blockchain que se encontraban accesibles desde internet públicamente. En este tipo de blockchain, se mantenía abierto al público sus datos, el software y su desarrollo, de forma tal que cualquier persona pudiera auditarlo, desarrollarlo o mejorarlo. Cualquiera podía formar parte de esta, el funcionamiento de la red era transparente y abierto, no existían entidades centralizadas y el mantenimiento económico de la blockchain dependía del sistema. (Oroyfinanzas, 2015)

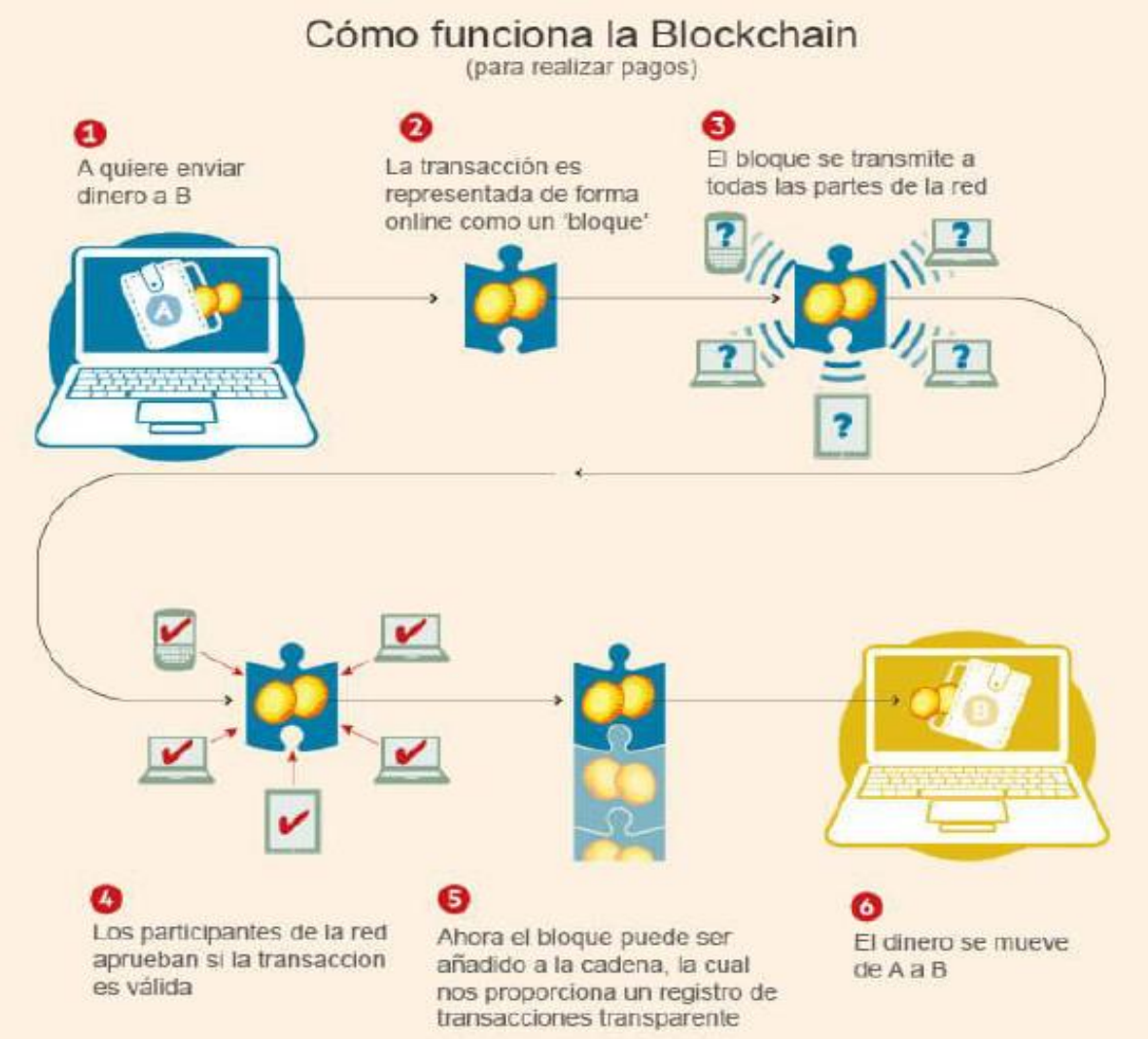
2.9 - Blockchain Privada: En este tipo de cadenas, era necesario un permiso para poder participar de ellas, donde el control lo ejercía una única entidad que se encargaba de mantener a la misma, darle permisos a los usuarios que querían participar, proponer transacciones y aceptar los bloques.

En estas, el acceso a la red se encontraba restringido, el acceso al libro de transacciones era privado, el mantenimiento económico dependía de la empresa que lo haya integrado.

2.10 - Blockchain Híbrida: No se encontraban abiertas al público en general y la gestión correspondía a varias entidades. No tenían una criptomoneda asociada y no recompensaban el minado de bloques.

FIGURA 4

FUNCIONAMIENTO DE BLOCKCHAIN



Nota: Funcionamiento de una blockchain, en este caso, para realizar pagos. Fuente: https://www.miethereum.com/blockchain/

Existían tres características principales que se podía distinguir en cualquier blockchain pública:

- **Abiertas**: cualquier persona podía convertirse en usuario y participar del protocolo común si contaba con unos mínimos conocimientos técnicos.
- **Descentralizadas**: no existía un usuario que tenga más poder que otro en la red y todos los nodos eran iguales entre sí.
- **Pseudoanónimas**: los propietarios de las transacciones no eran identificables personalmente, pero sus direcciones sí eran rastreables debido a su carácter público. Por este motivo, la mayoría de blockchain públicas no podían ser anónimas, excepto aquellas expresamente diseñadas para ser anónimas.

Existían tres características principales que distinguían a cualquier blockchain privadas:

- **Cerradas**: solo las personas o entidades que eran invitadas a participar adquirían la condición de usuarios o podían registrar transacciones. El protocolo predeterminado podía incluir distintos niveles de acceso a los usuarios, de modo que unos podían tener la capacidad de registrar información y otros no. El diseño que podía adquirir iba siempre en función de los fines perseguidos.
- **Distribuidas**: en número de nodos de los que se componía la blockchain privada podía estar limitado al número de participantes o a cierto número de ellos, de cualquier manera, todos los nodos se conocían. La fortaleza de una blockchain se basaba en gran medida en la cantidad de los nodos que la protegían y en los incentivos que estos podían recibir por cumplir ese papel ya que, a mayor número de nodos operativos, menor era la posibilidad de sufrir ataques. Pero, a diferencia de las blockchains públicas, donde el mantenimiento de los nodos dependía de la voluntad de los usuarios, en las privadas eran los participantes quienes se comprometían a mantener la estabilidad del sistema.
- **Anónimas**: una blockchain privada podía establecer el nivel de anonimato que quería para realizar o proteger transacciones. Los usuarios que registraban anotaciones podían estar o no perfectamente identificados.

Los usuarios de una blockchain privada estaban sujetos a un protocolo predeterminado que los podía capacitar, según se estableciera, para participar en el registro de las anotaciones y/o verificar los cambios introducidos en la cadena. En este sentido, una blockchain privada podía estar más centralizada y el número de nodos que componían la red podía limitarse al número de usuarios necesarios establecidos por los promotores. Por otro lado, la blockchain privada era distribuida, en el sentido de que era una base de datos repartida en varios nodos, mientras que la pública era descentralizada, porque en ella no se controlaba quien participa de la misma. (Preukschat, 2017)

2.11 - Aplicaciones descentralizadas

Este término surgió a partir del desarrollo de la tecnología blockchains. Una aplicación descentralizada, también denominada DApp o dApp, era una aplicación o pieza de software con una interfaz gráfica, que era ejecutada y administrada por múltiples usuarios en una red descentralizada. Es decir, no dependía de una autoridad o sistema central que regule y controle su funcionamiento. Como no estaba controlada por una entidad única, la posibilidad de fallos o caídas del sistema se reducían significativamente. Además, se podía optimizar el uso de la energía necesaria para hacer los cómputos necesarios para la ejecución del software. Los usuarios que contribuían al mantenimiento y operación del sistema aportando capacidad computacional, se beneficiaban con distintos tipos de recompensas. Este esquema existió desde la aparición de las redes de persona a persona (P2P), pero las criptomonedas y la blockchain permitieron que esta idea se explote por completo.

La incorporación de la tecnología blockchain, que permitía descentralizar prácticamente cualquier idea en el mundo tecnológico e informático, facilitó el desarrollo de estas aplicaciones inteligentes. Por otro lado, la incorporación de las criptomonedas proveyó el activo financiero que regía el sistema y se solía utilizar para recompensar a los participantes en el esquema descentralizado. Los administradores de las DApps se beneficiaban con pagos en la criptomoneda que respalda el proyecto. Así se obtenían beneficios similares a una acción de una gran empresa.

- ¿Cómo funcionaban?

El funcionamiento de una aplicación descentralizada estaba estrechamente relacionado con el software como tal. Cada DApp utilizaba una infraestructura distinta para lograr un objetivo concreto. Lo que compartían es el esquema conceptual. Para convertirse en una aplicación descentralizada, la gestión y administración se debían llevar a cabo de forma descentralizada. Para que un software sea considerado como una DApp, debía cumplir los siguientes requisitos (Buterin, 2014)

- ✓ Ser de código abierto.
- ✓ funcionar de forma autónoma.
- ✓ Todo cambio debía ser decidido por consenso de sus usuarios.
- ✓ Los datos y registro se debían almacenar criptográficamente.
- ✓ La aplicación debía usar un token criptográfico.
- ✓ Debía generar a estos últimos de forma automática.
- ✓ Las operaciones realizadas debían ser almacenadas en bloques por lo que verificaban mediante protocolos basados en algoritmos de prueba de trabajo (PoW) o prueba de participación (PoS).

Existían distintos tipos de DApps dependiendo de si poseían su propia blockchain o si utilizaban la cadena de bloques de otra DApp.

- Según este criterio, existieron tres tipos de DApps:
  - ✓ Tipo 1 - Las que poseían su propia blockchain, por ejemplo, Bitcoin.
  - ✓ Tipo 2 - Las que utilizaban la blockchain de una DApp de tipo 1. Eran protocolos y tenían sus propios tokens necesarios para su funcionamiento, pero no contaban con una cadena propia, por lo que realizaban una equivalencia entre el token de la DApp de tipo 1 y sus propios tokens.
  - ✓ Tipo 3 - También eran protocolos y utilizaban tokens propios que eran necesarios para su función, pero no actuaban directamente sobre las de tipo I sino que utilizaban funciones de tipo II que permitían un desarrollo más rápido y sencillo.

- Ventajas de la DApps frente a las Apps

Realizar una aplicación descentralizada, aportaba bastantes ventajas frente a las tradicionales aplicaciones web:

- ✓ **Procesamiento de pagos y cobros**

En las webs tradicionales era muy común encontrar integraciones con distintas entidades de pago para poder recibir las erogaciones de los usuarios que navegan a través de ella. En una DApp no era necesario hacer integraciones adicionales, ya que era posible para el usuario enviar o recibir fondos de una forma directa, sin la figura de un intermediario.

- ✓ **Cuentas de usuario**

Era común para los usuarios tener que crear muchas cuentas de usuario con contraseñas diferentes, lo que podía hacer que, con el paso del tiempo, estas se olviden y tengan que recurrir al proceso de recuperar contraseña. Esta situación con las DApps no ocurría ya que los usuarios no necesitaban registrarse. Creaban una sola cuenta con su llave pública y su llave privada que contenía sus datos, y podían vincularla con cualquier DApp.

- ✓ **Base de datos**

En el sistema tradicional, los datos eran almacenados a través de discos duros, mediante servicios en la nube o personales. Ambas eran opciones que tenían sus riesgos: en el caso de los discos duros personales, estos podían ser hackeados y los datos salían a la luz; en el caso de servicios en la nube, una cuenta podía ser hackeada también si se hackeaba a la empresa que proporciona ese servicio. Por otro lado, si esta empresa desaparecía, los datos de los usuarios también lo hacían. Con las DApps, al almacenar datos en una blockchain, hacía que estos datos permanecieran inmutables, es decir, una vez que se registraban esos datos ya no se podían borrar. El registro en una DApp funcionaba de forma parecida a cómo funcionaban los inicios de sesión con las cuentas

de Facebook, Google o LinkedIn: se podía usar una cuenta creada en estas redes sociales para registrarte en otros sitios web sin necesidad de poner tus datos otra vez ya que los mismos permanecían en la cadena de bloques de forma encriptada, es decir, eran ilegibles para cualquier persona excepto para sus propietarios. Además, el carácter distribuido de la blockchain hacía que esos datos residiesen en cada ordenador, por lo que, si desaparecían de un ordenador, existían muchas otras "copias de seguridad". Como único punto negativo se podía decir que almacenar una gran cantidad de datos en una cadena de bloques podía resultar bastante costoso y además aumentaba de forma considerable el tamaño de esta en Megabytes.

- ✓ **Confianza**

Cuando un usuario utilizaba una aplicación web, este podía ver el código que se había usado a través de las herramientas de inspección del navegador. De esta forma, el usuario podía verlo desde el frontend (parte del software que interactúa con el usuario). Sin embargo, la interacción de ese frontend con el backend (parte que procesaba la entrada desde el frontend) es algo que no se podía ver a simple vista. Con las DApps, los usuarios estaban tranquilos ya que les permitía inspeccionar tanto el código del frontend como el código del contrato inteligente, que funcionaba como backend o servidor. De esta manera se podía verificar que el código no tenía fallo alguno por el cual se pudieran robar fondos o información que estaba depositada en la DApp. Esto hizo crecer el sentimiento de confianza y seguridad de los usuarios. (MiEthereum, 2018)

- DAO/DAC

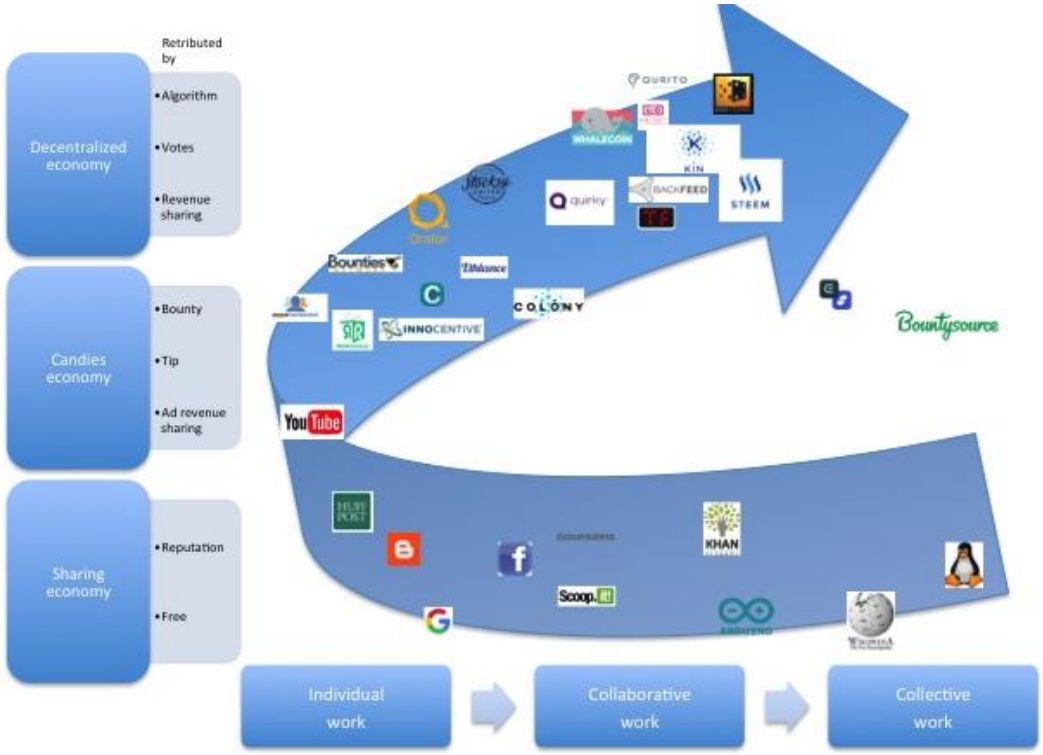
Una Organización Autónoma Descentralizada o DAO, también llamada Empresa Autónoma Descentralizada (en inglés Decentralized Autonomous Corporation) o DAC, era una organización que estaba dirigida a través de reglas codificadas en programas de ordenador llamados contratos inteligentes. Un registro de transacción financiera de una DAO, así como dichas reglas, estaban gestionadas a través de un blockchain. Existieron varios ejemplos de este modelo empresarial. El ejemplo más famoso ha sido The DAO, una DAO para fondos de capital riesgo, que se puso en marcha con $150 millones en crowdfunding en junio de 2016 y el cual fue inmediatamente pirateado y despojado de $50 millones de dólares americanos en criptomoneda. Dicho hackeo fue revertido unas semanas después, y el dinero fue recuperado al completo, gracias a una versión del blockchain de Ethereum.

La esencia conceptual de una organización autónoma descentralizada fue la capacidad de la tecnología de blockchain para proporcionar un libro mayor digital seguro que realizaba un seguimiento de la interacciones financieras a través de Internet, a prueba de falsificaciones gracias al sellado de tiempo confiable y a la diseminación de una base de datos distribuida. De este modo se eliminaba la necesidad de implicar a una entidad externa acordada por ambas partes (tercera

parte confiable) en cada transacción financiera, y por tanto simplificando la operación. Los costes tanto de una transacción habilitada vía blockchain como de poner a disposición de las partes los datos asociados a dicha transacción podían llegar a ser sustancialmente menores al eliminar la tercera parte confiable y la necesidad del registro repetitivo de intercambios de contrato en registros diferentes: por ejemplo, los datos incluidos en el blockchain podían, siempre y cuando las organizaciones reguladoras lo permitiesen, reemplazar documentos públicos como acciones y títulos. Este enfoque usando blockchain, permitió a múltiples usuarios colaborar a través de la computación en nube, en contratos inteligentes punto-a-punto (ver figura 5). (Wikipedia, 2020)

FIGURA 5

ECONOMÍA DESCENTRALIZADA



Nota: Economías descentralizadas y su interacción con el mundo laboral. Fuente: https://www.miethereum.com/smart-contracts/dapps/#toc17

- Lanzamiento de una DApp

Para realizar el lanzamiento de una DApp era necesario seguir cuatro pasos fundamentales:

- ✓ **Creación del Whitepaper**: En el mundo de las criptomonedas, el Whitepaper hacía referencia al documento que explicaba de forma clara, las intenciones, los objetivos y los problemas que la DApp deseaba resolver. El Whitepaper también era usado algunas veces como herramienta de marketing para persuadir a clientes potenciales y promocionar la DApp.

- ✓ **Establecer una hoja de ruta flexible**: Presentado el Whitepaper, también era necesario explicar los pasos que se iban a dar y cómo estaban divididos en fases o etapas. Estas no debían ser estrictas ya que podía haber situaciones que obligaran a tomar otro camino, en cuyo caso, los inversores de un proyecto podían señalarlos de estafadores al no seguir la hoja de ruta marcada al principio. Se aconsejaba discutir sobre el plan a seguir y escuchar a la comunidad creada en torno a la DApp. Era muy importante revisar los planes marcados después de escuchar la retroalimentación entre los desarrolladores de la DApp y los usuarios, ya que eran ellos los que utilizaban la herramienta.

- ✓ **Realizar una 'Crowd-sale' a través de una ICO**: El término Crowd-sale en el mundo blockchain, hacía referencia a la venta masiva de la criptomoneda propia de ese proyecto, en este caso, de esa DApp. Esto se llevaba a cabo a través de la llamada oferta Inicial, más conocida como una ICO. Una ICO, era un método de financiación a través del cual se ofrecía a los inversores una cantidad de esa nueva criptomoneda propia de la DApp a cambio de otras criptomonedas más conocidas como pueden ser Bitcoin o Ether. Este paso era necesario para poder cubrir los costes iniciales del lanzamiento y creación de la aplicación descentralizada. A cambio, los inversores recibían estas nuevas criptomonedas que conservaban con el objetivo de apoyar el proyecto y multiplicar su inversión inicial con el tiempo.

- ✓ **Comenzar a desarrollar la DApp**: Una vez que era explicado todo lo relevante a la DApp, marcados los pasos en la hoja de ruta y recibidos los fondos a través de la ICO, el paso siguiente era que el equipo de desarrolladores de la DApp utilice los recursos económicos recibidos para empezar la creación de esa aplicación descentralizada. (MiEthereum, 2018)

Capítulo 3 - Entorno blockchain y la seguridad

Se podía pensar que blockchain era una tecnología para gestionar y realizar pagos a través de Internet utilizando moneda virtual, pero eso era sólo el principio del ecosistema y de las posibilidades. Lo que permitía básicamente blockchain era la generación de un entorno de confianza entre pares que eliminaba la necesidad de intermediarios y que era soportada por toda la comunidad. Este entorno de confianza permitía el intercambio de activos de cualquier tipo, no sólo moneda virtual. Bitcoin, la primera aplicación desarrollada para blockchain, permitió el intercambio de un token o moneda virtual denominada Bitcoin, pero hubo otras aplicaciones que permitieron el intercambio de otros activos como nombres de dominio, propiedades, oro, etc. El intercambio venía definido por un sentido de la propiedad totalmente definido ya que todo quedaba almacenado en los blockchain particulares que una vez escritos resultaban inalterables, pero que permitían de forma permanente, la lectura pública de sus datos (Pérez, 2016).

Se pudieron identificar las siguientes tres generaciones del desarrollo de la cadena de bloques: blockchain 1.0 como moneda digital, blockchain 2.0 como economía digital y blockchain 3.0 como sociedad digital (Efanov & Roschin, 2018). Curiosamente, blockchain 1.0 tomó unos pocos años para madurar a partir de 2008, blockchain 2.0 y 3.0 han surgieron casi en paralelo de manera explosiva en 2015. (J. Leon Zhao, 2016)

3.1 - Blockchain 1.0

Blockchain 1.0 fue el desarrollo de la moneda, ya que implicó el despliegue de criptomonedas en aplicaciones relacionadas con el efectivo, como los sistemas de transferencia de moneda, remesas y pagos digitales (Swan, 2015). Fue la primera generación de aplicaciones de tecnología blockchain, básicamente y fue pensada para las transacciones económicas y pagos (Lérida & Pérez, 2016). Se refirió a la plataforma de tecnología subyacente (minería, hashing y el libro mayor público), protocolo de superposición (es decir, software de habilitación de transacciones) y la moneda digital (Bitcoin u otras) que representaron un almacén de valor y proporcionaron valor al protocolo por sí mismo. Bitcoin fue un caso raro en el que la práctica parece estar por delante de la teoría. Las principales ventajas de Bitcoin fueron:

- ✓ Ofreció la posibilidad de tarifas de transacción considerablemente reducidas para compras en línea.
- ✓ Proporcionó mayor anonimato que las tarjetas de crédito. Las cuentas eran seudoanónimas y el protocolo estaba diseñado para fomentar el uso de nuevos números de cuenta para cada transacción.
- ✓ El diseño descentralizado de Bitcoin y otras monedas digitales protegía contra la inflación. Las monedas tradicionales dependían de un banco central para regular el suministro de

dinero, introduciendo dinero nuevo en circulación según sea necesario. Bitcoin, por el contrario, utilizó la criptografía para garantizar un suministro de dinero relativamente fijo, que se permitió crecer a intervalos regulares.

3.2 - Blockchain 2.0

Significó el paso de las criptomonedas al mundo de las aplicaciones reales. Estaba pensada para la gestión y transferencia de activos y cualquier otro tipo de bien que pudiera estar en un registro público. Igualmente se podía utilizar para gestión y transferencia de activos físicos siempre que los mismos pudieran ser codificados de alguna manera.

Blockchain 2.0 se refería a la amplia gama de aplicaciones económicas y financieras existentes más allá de simples pagos, transferencias, y transacciones. Dichas aplicaciones incluyeron instrumentos bancarios tradicionales, como préstamos e hipotecas, complejos instrumentos del mercado financiero como acciones, bonos, futuros, derivados, además instrumentos legales tal como títulos, contratos y otros bienes y propiedades que pudieran ser monetizados. El sistema de compensación de pagos y los sistemas de información de crédito bancario pudieron ser escenarios apropiados de la aplicación blockchain. Un caso de uso emergente clave de la tecnología blockchain involucró contratos inteligentes. Estos contratos Inteligente eran básicamente programas de computadora que pudieron ejecutar automáticamente los términos de un contrato. Cuando se cumplía una condición preestablecida en un contrato inteligente entre entidades participantes, las partes involucradas en el acuerdo contractual podían realizar pagos automáticamente según el contrato de manera transparente.

Parte de la terminología que se refirió ampliamente al espacio blockchain 2.0 podía incluir Bitcoin 2.0, protocolos Bitcoin 2.0, contratos inteligentes, propiedad inteligente, Dapps (aplicaciones descentralizadas), DAO (organizaciones autónomas descentralizadas) y DAC (corporaciones autónomas descentralizadas).

3.3 - Blockchain 3.0

Eran aplicaciones de blockchain que iban más allá de la moneda, las finanzas y los mercados, especialmente en las áreas de gobierno, salud, ciencia, alfabetización, cultura y arte. Correspondían al desarrollo de nuevas tecnologías basadas en la identidad, la libertad, la democracia y la contabilidad de activos de cualquier tipo. Blockchain 3.0 trató de solucionar las restricciones que actualmente existían en los mercados a nivel local, regulatorio y de entornos macroeconómicos. Es decir, mientras que blockchain 2.0 estaba tratando de migrar aplicaciones del mundo digital utilizando la trazabilidad y posibilidades de contabilidad en mercados masivos, blockchain 3.0 trató de cambiar el statu quo establecido utilizando la potencia, la deslocalización y la ubiquidad que generan las tecnologías blockchain. Si se pudo hablar de blockchain 2.0 como una evolución, en el caso de

blockchain 3.0 habló de revolución. (Lérida & Pérez, 2016). Blockchain 3.0 se refirió a una gran variedad de aplicaciones que no involucraban dinero, divisas, mercados financieros u otra actividad económica. Tales aplicaciones incluyeron arte, salud, ciencia, identidad, gobernanza, educación, bienes públicos y diversos aspectos de la cultura y la comunicación. La aplicación más prometedora de la tecnología blockchain estaba relacionada con las smart cities (Una ciudad inteligente era un área urbana que utiliza diferentes tipos de métodos electrónicos y sensores para recopilar datos . Los conocimientos adquiridos a partir de esos datos se utilizaban para gestionar activos, recursos y servicios de forma eficiente; a cambio, esos datos fueron utilizados para mejorar las operaciones en toda la ciudad. Esto incluía datos recopilados de ciudadanos, dispositivos, edificios y activos que luego se procesaban y analizaban para monitorear y administrar los sistemas de tráfico y transporte, centrales eléctricas, servicios públicos, redes de suministro de agua, desechos, detección de delitos, sistemas de información, escuelas, bibliotecas, hospitales y otros servicios comunitarios.), que involucró elementos horizontalmente acumulativos, como la gobernanza inteligente, la movilidad inteligente, la vida inteligente, el uso inteligente de recursos naturales, ciudadanos y economía inteligentes.

3.4 - El problema del 51%

Todo el mecanismo de una DApp para su funcionamiento tenía un punto débil que se conocía de antemano y era difícil resolución: el problema del 51%. Cuando más del 51% de la tasa de hash estaba controlada por un solo nodo (un minero o grupo de mineros), la cadena de bloques se podía distorsionar maliciosamente. En un denominado “ataque del 51%” existían dos bloques conflictivos compitiendo para la misma adición a la cadena de bloques. Si se modificaba un bloque en medio del blockchain, los enlaces hash no coincidían y se debían crear nuevamente. Para esto, los bloques posteriores debían ser re-minados para incluir los nuevos hashes que se volvían a calcular. En el caso entonces que un atacante quería modificar un valor para beneficio e intentaba reconstruir la cadena modificada calculando los hashes, debía tener el control de al menos el 51% de los recursos que utilizaba el protocolo de consenso, para que pudiera reconstruir la cadena a una velocidad superior a la que ésta se generaba. Esta vulnerabilidad afectaba principalmente a las plataformas que utilizaban prueba de trabajo o prueba de participación, pero aun así era una situación difícilmente realizable, dado que significaba tener el 51% de la potencia computacional o el 51% de las cryptomonedas (medio digital de intercambio que utilizaba criptografía fuerte para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido) de toda la red.

3.5 - Doble gasto

La tecnología blockchain resolvió un importante problema informático que había sido una barrera para tener un sistema monetario digital funcional durante años: el problema del doble gasto dado

que el dinero solo debía gastarse una vez, a diferencia de un archivo, que podía ser copiado arbitrariamente muchas veces.

El doble gasto ocurría cuando alguien hace más de un pago usando un mismo fondo. Esto era posible en una red peer-to-peer porque podía haber retrasos cuando los pagos pendientes se transmitían a la red o a las redes y los nodos recibían transacciones no confirmadas en diferentes momentos. Blockchain abordó este problema requiriendo que los nodos mineros resuelvan un problema matemático complejo para verificar la transacción. La complejidad del cálculo se ajustó de modo que, en promedio, se necesitaba 10 minutos para resolver un problema utilizando los poderes de procesamiento de los mineros.

Solo bloques con respuestas correctas al problema matemático se podían agregar a la cadena, con lo cual uno entre los pagos múltiples era aceptado y registrado en la blockchain, por lo que era casi imposible para las partes gastar fondos doblemente. Los sistemas centralizados de almacenamiento y administración de datos eran susceptibles de piratería, intrusión e incumplimientos, pero el mecanismo de consenso distribuido blockchain evitó el hackeo. Cada transacción debía ser verificada por la comunidad de mineros, dejando transacciones fraudulentas que no pueden pasar la verificación colectiva y validación porque blockchain era constantemente monitoreada por toda la red de nodos, cada uno de los cuales mantenían una copia de la cadena de bloques, los usuarios maliciosos no tienen forma de insertar bloques fraudulentos en el libro de contabilidad público sin ser notado inmediatamente por otros. Por lo tanto, era imposible comprometer la integridad de los registros en el blockchain.

3.6 - Claves privadas

Un aspecto clave en la seguridad era la gestión y almacenaje de claves privadas. Sin estas claves privadas no era posible realizar transacciones con las direcciones, por ello la perdida de estas era sinónimo de perder los fondos. Si las claves se perdían o destruían, no había forma de recuperarlas y los fondos asociados a esas direcciones nunca se podrán utilizar. Si las claves eran obtenidas por un tercero, este podía hacer uso fraudulento de todos los fondos asociados. En consecuencia, todos los activos que esta persona poseía en el blockchain desaparecían, y era casi imposible identificar al ladrón. Las consecuencias podían ser más devastadora que el robo de identidad en el mundo fuera de línea, donde las instituciones de terceros (por ejemplo, compañías de tarjetas de crédito) o las autoridades centrales resguardan transacciones, controlaban riesgos, detectaban actividades, o ayudaban a encontrar culpables.

Capítulo 4 - Fundamentos de blockchain

Esta tecnología nació a partir de la necesidad de encontrar respuesta al problema del doble gasto como piedra angular, y se basó en los siguientes principios:

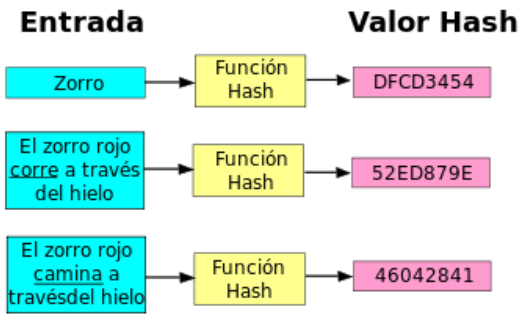
4.1 - Integridad

En internet no se podían realizar transacciones directamente sin intermediarios por la simple razón de que el dinero no era como otros bienes: este debía salir de la cuenta del pagador de una transacción e ir a la cuenta de la otra parte que intervenga en la transacción. El mismo dinero no podía existir en dos sitios al mismo tiempo. Esto que se describió, es lo que se conocía como el problema del doble gasto. En una blockchain el sistema registraba el momento en que se hacía la primera transacción en la que se gastaba una unidad monetaria concreta y rechazaba las transacciones subsiguientes en las que se intentaban gastar esa misma unidad, lo que impedía que sea gastada dos veces. Quienes participan de la red, ejecutaban los nodos de Bitcoin operativos, los llamados mineros reunían operaciones recientes, las registraban en forma de bloque de datos y repetían el proceso cada 10 minutos. Para tener validez, todos los bloques debían referirse al bloque anterior y también era necesario que se almacenara la blockchain completa en cada ordenador, por ello, los protocolos incluían un método que reservaba espacio en el disco de cada nodo utilizado. Por último, todo el mundo podía ver las transacciones que se realizaban en el mismo momento en que sucedían. Nadie podía esconder nada. Como era imposible basarse en la identidad de los mineros para decidir quién creaba el siguiente bloque, se armó un acertijo difícil de resolver, pero que era fácil de verificar para llegar al consenso. Este mecanismo era conocido como prueba del trabajo: los participantes decidían de común acuerdo que el primero que resolvía el acertijo creaba el siguiente bloque y los mineros empleaban una gran cantidad de recursos (hardware informáticos y electricidad) para encontrar el hash (es el resultado de una función hash, la cual era una operación criptográfica que generaba identificadores únicos e irrepetibles a partir de una información dada) correcto que resolvía el acertijo y así recibían los Bitcoins que el sistema les otorgaba como premio. El acertijo se generaba matemáticamente para que sea imposible resolverlo mediante un atajo. Este proceso, en el que el minero descifra el acertijo, tenía una distribución de Poisson (en teoría de probabilidad y estadística, era una distribución de probabilidad discreta que expresaba, a partir de una frecuencia de ocurrencia media, la probabilidad de que ocurra un determinado número de eventos durante cierto período de tiempo) por lo que estadísticamente debía ocurrir cada diez minutos (podía quedar resuelto en un minuto y la próxima vez podía tardar una hora, pero la media era de 10 minutos) Pero ¿cómo lograban los mineros esto? Primero reunían todas las transacciones pendientes que encontraban en la red y procesaban la información mediante una función criptográfica llamada algoritmo de hash seguro que daba como resultado un valor de hash de 32 bits. Si el valor de este hash se encontraba por debajo de cierto objetivo (establecido por la red y ajustado cada 2016 bloques), el minero había encontrado la resolución del acertijo y resolvía el bloque. Si el

valor no era correcto, el minero ajustaba la información entrante y lo intentaba de nuevo. Cada intento producía un valor de hash completamente distinto. Los mineros debían intentarlo muchas veces para dar con la solución por lo que para el minero encontrar el valor de hash correcto era muy costoso y difícil en el caso de Bitcoin (ver figura 6).

FIGURA 6

EJEMPLO VALOR DE HASH



Nota: A través de una función hash definida, se codificaba un mensaje para que sea indescifrable para cualquier otra persona que no conociera dicha función. Fuente: https://www.miethereum.com/smart-contracts/dapps/#toc17

¿Existían otros mecanismos para llegar al consenso en una blockchain? Sí, por ejemplo, la primera versión de la blockchain de Ethereum también utilizaba la prueba de trabajo, pero quienes la desarrollaron tenían la intención de sustituirlo por el mecanismo de la prueba de participación. En este mecanismo los mineros tenían que invertir y quedarse con algún depósito de valor y de esta manera gastaban energía en votar. Otro mecanismo era el de la prueba de actividad que combinaba el mecanismo de la prueba de trabajo y el de la prueba de participación. En este mecanismo, un número al azar de mineros debía suscribir el bloque usando una clave cifrada antes de que el bloque sea oficial (la prueba de destrucción requería que los mineros enviaran monedas a direcciones sin salidas en las que no se pueden convertir. A cambio de destruir estas monedas, los mineros participaban de una lotería en la que, en principio, ganaban más de lo que habían destruido. No era un mecanismo de consenso sino un mecanismo de confianza). Por otro lado, el mecanismo de la prueba de capacidad requería que los mineros asignaran al minado un espacio considerable de sus discos duros. Por último, existía lo que se conoce como el mecanismo de la prueba de almacenamiento que era similar a la anterior pero que requería que los mineros asignaran y compartieran espacio del disco en una nube distribuida.

Lo del almacenamiento era algo de relativa importancia ya que los datos de las blockchains diferían de los datos de internet en una cosa fundamental que era que, en internet, la mayor parte de la

información era maleable y fugaz y las fechas y horas exactas de su emisión no eran esenciales para la información pasada o futura. En una blockchain el movimiento de Bitcoins por la red quedaba registrado en todo momento y para que este sea válido, tenía que remitirse a su propia historia y a la historia de la blockchain, en consecuencia, la cadena debía preservarse en su integridad.

Satoshi Nakamoto combinó una red distribuida entre ordenadores que tenían igual jerarquía junto a criptografía inteligente para crear un mecanismo de consenso que pudo resolver el problema del doble gasto tan bien o mejor que un tercero fiable. De esta manera, en lugar de delegarle a grandes compañías y gobiernos la verificación de la identidad de la gente y su reputación, la misma se realizaba en la propia red. Era la primera vez que se disponía de una plataforma que garantizaba transacciones seguras y cantidad de información grabada sin que importe como actuaba la otra parte. La confianza era la condición *sine qua non* de la economía digital y una plataforma que permitía la colaboración segura y fiable de mucha gente, encerraba grandes posibilidades de conseguir una nueva forma de organización social.

4.2 - Descentralización

El poder se encontraba distribuido por todo el sistema que, a su vez, se encontraba constituido por una red de iguales, sin que existiera un ente o punto de control. De esta manera, ninguna de las partes que lo componían podían apagar el sistema por sí solas y de existir una autoridad central (como podía ocurrir en el caso de las blockchains privadas) que lograba inhabilitar o expulsar a un individuo o a un grupo, el sistema sobrevivía.

Durante la primera atapa de internet, las grandes instituciones con bases de usuarios bien asentadas, (ya sean de empleados, ciudadanos, clientes u organizaciones) hicieron poco por su contrato social ya que existía un ente superior que los iba a regular para evitar un fraude. Pero a lo largo del tiempo, una y otra vez estos entes reguladores demostraron su falta de voluntad para cumplir su objetivo y su capacidad de pasar por alto a los usuarios, almacenando y analizando sus datos, suministrando información al gobierno sin su consentimiento y realizando cambios importantes sin que estos estuvieran debidamente informados.

Una de las críticas que se le hacía a esta tecnología, era que se necesitaba mucha energía para poder sostener al sistema, pero los costos energéticos de controlar una blockchain superaron los beneficios. Satoshi Nakamoto ideó un método denominado prueba del trabajo, que exigía que los usuarios utilizaran mucha capacidad de procesamiento para defender la red y generar nuevas monedas. Este mecanismo se inspiraba en Hashcash (era un sistema de prueba de trabajo que se utilizaba para limitar el correo no deseado y los ataques de denegación de servicio , y más recientemente se hizo conocido por su uso en Bitcoins (y otras criptomonedas) como parte del algoritmo de minería): solución que encontró el criptógrafo Adam Back para reducir el spam o correo

basura y los ataques denominados de negación del servicio donde se requería que los remitentes hicieran una prueba de trabajo cuando enviaban un correo electrónico, así el sistema marcaba el email como correo especial para señalar la relevancia que el mensaje tenía para su remitente (ya que quien lo enviaba había gastado una gran cantidad de energía para enviarlo, el correo no era basura).

Cualquier persona podía descargarse gratis el protocolo Bitcoin y tener una copia de la blockchain de manera muy sencilla, ya que el protocolo utilizaba la técnica del bootstrapping (proceso donde un sistema simple activa otro sistema más complejo para servir al mismo propósito), que permitía instalar el programa en el ordenador o dispositivo móvil del usuario siguiendo unas sencillas instrucciones que hacían funcionar el resto del programa. Esto protegía la red del control del estado, ya que la red estaba en todos lados, porque la blockchain residía en todas partes y esto permitía obviar a los intermediarios. Los usuarios mantenían la cadena actualizando sus copias y prestando las unidades de procesamiento que le quedaban libres para las operaciones de minado. No existía posibilidad de cometer fraude ya que todas las operaciones y transacciones se difundían por la red para su verificación y validación. No había terceros ni servidores que centralicen ni almacenen nada.

Satoshi distribuyó también la facultad de emisión de monedas vinculando la acuñación de Bitcoins con la creación de un nuevo bloque en este gran sistema de registro, con lo que puso la capacidad de emitir monedas en mano de la blockchain mediante el siguiente mecanismo: el minero que primero resolvía el acertijo y se sometía a una prueba de trabajo recibía cierta cantidad de Bitcoins nuevos. De esta manera, no había reservas federales ni bancos centrales ni haciendas públicas que controlaran la circulación de moneda. Por otro lado, todos y cada uno de los Bitcoins contenían enlaces directos que llevaban al bloque donde se registró su creación y a todas las transacciones subsiguientes.

Los intermediarios no eran necesarios ya que el sistema funcionaba mejor con la colaboración de los usuarios y, por otro lado, la red les daba la posibilidad a estos de tener poder sobre sus datos, propiedades y su nivel de participación.

4.3 - El valor como incentivo

El sistema hacía coincidir los incentivos de todos los participantes ya que Satoshi programó el software para que premiara a los que trabajan en él y para que perteneciera a los que lo poseían y usaban sus monedas.

En la primera era de internet, las empresas concentraban una gran cantidad de poder que, combinada con su gran tamaño y complejidad, les permitía sacar cantidades desproporcionadas de valor de las mismas redes que las dotaron de derechos para que lo hicieran. Un buen ejemplo de esto fueron los grandes bancos que explotaron el sistema financiero hasta el límite debido a que las

estructuras de incentivos estaban diseñadas para que la mayoría de los altos ejecutivos y mucho de los encargados de los préstamos actuaran con falta de visión y mucho riesgo. Se dieron malos incentivos a la gente, por ese motivo, se comportaron mal. Por otro lado, según un estudio que realizó la consultora Ernst & Young, casi las dos terceras partes de los directivos encuestados dijeron que recababan información de los consumidores para hacer negocios y casi el 80% reconoció haber aumentado sus ganancias gracias al aprovechamiento de esa información. Paradójicamente, cuando piratas informáticos atacaron esas empresas y robaron datos de las tarjetas de crédito e información bancaria de los consumidores, fueron ellos los que pagan ante la justicia. No sorprendió entonces que, según la misma encuesta, casi la mitad de los consumidores dijeran que habían negado el acceso a sus datos en los siguientes cinco años, y más de la mitad mencionara que proporcionó menos datos, incluso habiéndose censurado a sí mismos en los medios sociales, que en los cinco años anteriores.

Satoshi entendía sobre la Teoría de Juegos (rama de la matemática y de la economía que estudiaba la conducta de los individuos), por lo que esperaba que los participantes actuaran en interés propio. Sabía que las redes sin protección eran vulnerables y con anterioridad habían recibido ataques llamados Sybil que hicieron que los nodos forjaran múltiples identidades, los derechos desaparecieran y el valor de la reputación se depreciara. La integridad de la red de iguales y la reputación de sus usuarios se vio menoscabada cuando no fue claro tanto si se estaba tratando con tres partes, como si se estaba tratando con una parte que usa tres identidades. Por eso, se programó el código fuente de la blockchain Bitcoin para que, por muy egoístamente que actuaran los participantes, sus acciones beneficiaran al sistema en su conjunto y aumentaran su reputación. La exigencia de recursos que necesitaba el mecanismo de consenso, unida a la idea de que se premiaba con Bitcoins a los mineros, persuadían a los participantes a comportarse correctamente y a ser fiables en el sentido en que se esperaba. De esta manera, los ataques Sybil (donde el atacante pervertía el sistema de reputación de un servicio de red ya que creaba una gran cantidad de identidades seudónimas y las usaba para obtener una influencia desproporcionadamente grande. Llevaba el nombre del tema del libro Sybil, un estudio de caso de una mujer diagnosticada con trastorno de identidad disociativo) eran económicamente inviables.

Por norma, la primera transacción de un bloque era una transacción especial que daba comienzo a una nueva moneda que pertenecía al creador del bloque. Esto constituía un incentivo para que los propios nodos sostengan la red. Bitcoin ofrecía premios para que los mineros crearan un bloque y lo vincularan con el bloque anterior. Los primeros que completaban un bloque se llevaban cierta cantidad de Bitcoins por su esfuerzo. El protocolo de Satoshi premiaba a los primeros que lo hicieron generosamente: durante los primeros cuatro años, los mineros recibieron 50 Bitcoins (BTC) por cada bloque. Cada cuatro años el premio fue disminuyendo a la mitad: 25 BTC, 12, 5 BTC y así sucesivamente. Como ahora ellos tambien poseían Bitcoins, tenían un incentivo para garantizar el

éxito duradero de la plataforma, por lo cual compraron los mejores programas para ejecutar operaciones de minado, gastaron energía lo más eficientemente posible y mantuvieron el registro. De esta manera, Bitcoin no solo los incentivó para participar en la labor de minado y en las transacciones con otros participantes, sino que le dio derecho a la propiedad de la plataforma misma. Las cuentas de usuarios distribuidas son el elemento más básico de la infraestructura criptográfica de la red, ya que poseyendo y usando Bitcoins estamos financiando el desarrollo de la cadena.

Satoshi decidió que el grupo económico que financie la red fueran los propietarios de capacidad procesadora. Con lo cual, se requería que esos mineros consumieran un recurso externo a la red, principalmente electricidad, si querían participar en el sistema de premios. Podía suceder que varios mineros encontraran dos bloques igualmente válidos de igual extensión y los demás mineros debían elegir uno para seguir construyendo la cadena. Normalmente se elegía el que se creía que ganaría y no los dos, pues si se elegía a los dos se verían obligados a dividir su capacidad procesadora entre las dos cadenas, lo que significaba una pérdida de valor. La paradoja de estos esquemas de consenso es que, actuando en interés propio, se estaba sirviendo a la red de iguales, lo que a su vez afectaba a la reputación como miembros del grupo económico.

Otra forma de preservar valor era la política monetaria que se encontraba programada en el software. Todas las monedas que utilizó la humanidad han sigo inseguras por distintas razones. Esta inseguridad se manifestó de muchas maneras desde la falsificación al robo, pero la más problemática de todas fue seguramente la inflación. Por esta razón, Satoshi Nakamoto impuso un techo a la cantidad de Bitcoins que se podían emitir, que es de 21 millones, para evitar una inflación arbitraria. Dado que cada 4 años el número de Bitcoins minados en un bloque se reducía a la mitad y el ritmo de minados era de 6 bloques por hora, esos 21 millones de Bitcoins debían estar en circulación en 2040. De esta manera, no podía haber hiperinflación ni devaluaciones.

Por otro lado, a diferencia de las monedas tradicionales, cada Bitcoin podía dividirse en ocho lugares decimales. Esto permitía a los usuarios combinar y dividir valor a lo largo del tiempo en una sola transacción de esta manera, los usuarios podían establecer contratos inteligentes para medir el uso de un servicio y realizar pagos en pequeñas fracciones a intervalos regulares (ver figura 7).

FIGURA 7

TRANSACCIONES DE UNA BLOCKCHAIN.

Nota: Ejemplo gráfico de cómo es una blockchain haciendo un paralelismo con un libre diario contable. Fuente: https://www.miethereum.com/smart-contracts/dapps/#toc17

4.4 - Seguridad

Las medidas de seguridad se encontraban integradas en la red y no solo garantizaban la confidencialidad, sino también la autenticidad de todas las transacciones realizadas y la imposibilidad de que fuera denegado realizar operaciones a cualquier usuario que así lo deseaba. Necesariamente todo el que quería participar de esta red, debía usar criptografía (no era posible optar, por el contrario, era obligatorio) y las consecuencias de portarse mal solo las sufría la persona que se comportaba mal.

Existían varias actividades que atentaban contra la seguridad del individuo en la red: Pirateo, robo de identidad o de información, fraude, ciberacoso, correo basura, programas maliciosos. La primera era de internet, en lugar de brindar transparencia y reducir estas infracciones, hizo poco para aumentar la seguridad de las personas, las instituciones y la actividad económica. El usuario normal de internet recurría casi siempre a débiles contraseñas para proteger su correo electrónico o sus cuentas porque los proveedores de servicios no le ofrecían nada mejor. Si la siguiente etapa de la revolución digital suponía el traspaso de dinero directamente entre pares, ese traspaso debía poder hacerse sin riesgo de pirateo informático. Por este motivo, Satoshi requirió que los participantes de la red usaran infraestructura de clave (PKI) para crear plataformas seguras. PKI era una forma avanzada de criptografía asimétrica por la que los usuarios disponían de dos claves que no desempeñaban la misma función: una era para encriptar y la otra para desencriptar. Por ese motivo eran asimétricas. La plataforma Bitcoin constituyó el mayor despliegue de PKI del mundo y el segundo de EE. UU. después del sistema de acceso común del departamento de defensa.

Creada en los años setenta, la criptografía asimétrica cobró fuerza en los 90 en forma de programas de encriptación de correo electrónico que eran bastante seguros y también bastante complicados de usar porque requerían que todos los miembros de la misma red lo usen y que tomen nota de sus dos claves, así como de las claves públicas de los demás. No existía posibilidad de cambiar una contraseña. Si es olvidada, había que empezar desde el principio. Estos sistemas fracasaron porque no tenían incentivos y la gente nunca consideró la privacidad un incentivo lo bastante fuerte como para proteger esos sistemas.

La cadena Bitcoin resolvió estos problemas porque dió incentivos para adoptar PKI en todas las transacciones de valor, no solo en el uso de Bitcoin sino también en los protocolos Bitcoin compartidos. No existía la preocupación por si los firewalls son débiles, o por empleados ladrones o piratas informáticos. Si dos personas usaban Bitcoin, si podían almacenar e intercambiar Bitcoin con seguridad, entonces podían almacenar e intercambiar información confidencial y activos digitales con seguridad en el sistema blockchain.

El funcionamiento era el siguiente: la moneda digital no se almacenaba en un archivo propiamente dicho. La representaba una serie de transacciones indicadas por un hash criptográfico. Los usuarios tenían las criptoclaves de su dinero y lo intercambiaban directamente entre sí. Esta seguridad traía consigo la responsabilidad de mantener privadas las claves. La blockchain Bitcoin funcionaba con el conocido y asentado SHA-256 (Era un conjunto de funciones de hash criptográficas que fueron diseñadas por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y publicadas por primera vez en 2001), publicado por el Instituto Nacional de Procesamiento de la Información. Las muchas repeticiones de ese cálculo matemático que se necesitaban para encontrar la solución de un bloque obligaban al dispositivo informático a consumir una considerable cantidad de electricidad para resolver el acertijo y ganar un Bitcoin nuevo (otros algoritmos, como el de la prueba de participación, gastaban menos energía). Por último, la cadena más larga solía ser la más segura. La relativa antigüedad de la blockchain de Satoshi y su ya asentada base de usuarios y mineros de Bitcoins aumentaban su seguridad. Atacarla requería más capacidad procesadora que atacar cadenas cortas.

4.5 - Privacidad

Respetar el derecho a la privacidad no era exactamente lo mismo que respetar la privacidad. La gente debía poder controlar sus propios datos, decidir sobre su identidad y como cuando y cuanta compartir con los demás. Al eliminar la necesidad de confiar en los otros, Satoshi eliminó la necesidad de conocer la verdadera identidad de esos otros para interactuar con ellos.

La privacidad era un derecho humano fundamental en una sociedad libre. En los últimos veinte años de internet las bases de datos centrales, tanto del sector público como del privado, acumularos toda

clase de información confidencial sobre individuos e instituciones, a veces sin conocimiento de estos. Las empresas sondeaban el mundo digital en busca de esa información y creaban lo que se podría llamar ciberclones de esos individuos e instituciones. Esto representaba atentados contra la privacidad por partida doble, primero por reunir y usar los datos personales sin el conocimiento ni permiso de los propios usuarios, y segundo porque no protegían ese tesoro de los piratas informáticos.

Satoshi no incorporó ningún requisito de identidad en la capa de red misma, con lo que nadie tenía que proporcionar nombre, dirección de correo electrónico ni ninguna otra información personal para descargarse y usar el programa de Bitcoin. La blockchain no necesitaba saber la identidad del usuario y Satoshi no necesitaba recabar información de nadie para comercializar otros productos. Su software de código abierto era el último grito en el mercado de liderazgo intelectual. Las capas de identificación y verificación estaban separadas de la de transacción, lo que significaba que la parte A emitía la trasferencia de Bitcoins desde la dirección de la parte A a la de la parte B. No había referencia alguna a la identidad de nadie en esa transacción. Entonces la red confirmaba que la parte A no solo controlaba la cantidad de Bitcoins especificada, sino que también autorizaba la transacción y luego registraba la cantidad emitida por la parte A como una cantidad no gastada asociada a la dirección de la parte B. Solo cuando la parte B se disponía a gastar esa cantidad comprobaba la red que era esa parte quien la controla en ese momento.

En el sistema blockchain los participantes podían elegir mantener cierto grado de anonimato en el sentido de que no necesitaban asociar ningún otro detalle a su identidad ni guardar esos detalles en una base de datos central, por lo que en el sistema blockchain no había tesoros de información personal. De esta manera los protocolos de este sistema nos permitían elegir el nivel de privacidad que se quería en cada transacción o entorno y de esa manera ayudaba a administrar mejor la identidad y las interacciones con el mundo.

4.6 - Derechos preservados

Los derechos de propiedad eran transparentes y legítimos y las libertades individuales estaban reconocidas y debían ser respetadas. Todos nacían con una serie de derechos inalienables que debían ser protegidos.

En la primera fase de la economía digital la cuestión era buscar la manera de ejercer esos derechos más eficazmente. Internet se convirtió en un medio para desarrollar nuevas formas de arte, información y entretenimiento para establecer derechos de autor, pero se debía confiar en intermediarios que controlaban las transacciones y que podían denegarlas, retrasarlas, retener el dinero en sus propias cuentas o autorizarlas para luego revertirlas. También, se daba por sentado que un porcentaje de la gente engañaría y que cierto grado de fraude era inevitable. En esta realidad,

los derechos legítimos fueron dejados de lado, no solo los derechos de privacidad y seguridad sino también los de libre expresión, reputación y participación equitativa. Los intermediarios podían criticar, difamar y bloquear a los usuarios con poco costo.

En una blockchain, la prueba de trabajo que se requería para acuñar moneda también registraba el momento en el que se hacen las transacciones, de manera que solo se autorizaba la primera vez que se gastaba una moneda. Este desarrollo combinado con PKI, no solo impedía el doble gasto, sino que también confirmaba la propiedad de todas y cada una de las monedas en circulación y cada transacción era inmutable e irreversible. En otras palabras, no era posible negociar con lo que no era propiedad de esa persona, fuera una propiedad real, intelectual o un derecho de la persona, como tampoco se podía negociar con aquello a lo que no se estaba autorizado a negociar en nombre de otra persona, en calidad de agente, como abogado o director de una empresa.

En internet no siempre se podía hacer valer los derechos contractuales o ver si se respetaban. A partir del desarrollo de la tecnología blockchain, para el caso de transacciones más complejas en las que intervenían muchos derechos y muchas partes, existían los denominados contratos inteligentes, que eran códigos especiales que ejecutaban conjuntos complejos de instrucciones en blockchain.

Un contrato inteligente (programa informático o protocolo de transacción que estaba destinado a ejecutar, controlar o documentar automáticamente eventos y acciones legalmente relevantes de acuerdo con los términos de un contrato o acuerdo. Los objetivos de los contratos inteligentes eran la reducción de la necesidad de intermediarios confiables, arbitrajes y costos de ejecución, pérdidas por fraude, así como la reducción de excepciones maliciosas y accidentales) permitía, por ejemplo, que una parte cediera derechos de uso a otra parte. El código del contrato podía incluir el término o duración de la concesión, la cantidad de dinero que pasaría de la cuenta del editor a la del compositor en concepto de derechos de autor y algunas cláusulas de rescisión del contrato. Para hacer que este contrato inteligente entrara en vigor, el compositor y el editor firmaban usando claves privadas. También permitía que los propietarios de activos unieran sus recursos y crearan una sociedad en la blockchain. El contrato incluía codificadas, unas cláusulas de admisión que especificaban claramente los derechos de esos propietarios. Nadie podía apoderarse del contrato, suspenderlo o redirigirlo a una dirección de Bitcoin diferente. Solo había que transmitir la transacción firmada a cualquiera de los nodos de la red desde cualquier parte y por cualquier medio.

4.7 - Inclusión

La economía funciona mejor cuando funciona para todos, para ello era imprescindible eliminar obstáculos que dificulten la participación. Significaba crear nuevas plataformas que hicieran posible el capitalismo distribuido, no simplemente un capitalismo redistribuido.

La mayoría de la población mundial seguía estando excluida, no sólo del acceso a la tecnología sino también del acceso al sistema financiero y a las oportunidades económicas. Además, la promesa de que internet traería prosperidad para todos era una deuda pendiente, aunque ha ayudado a las empresas del mundo desarrollado a dar trabajo a millones de personas de economías en vías de desarrollo, que ha facilitado la empresa y ha dado a los más desfavorecidos nuevas oportunidades y acceso a información básica.

Pero no fue suficiente. Seguía habiendo muchas personas sin una cuenta bancaria y en el mundo desarrollado la prosperidad disminuiría a la vez que la desigualdad social aumentaba. Y, en las economías en vías de desarrollo, el celular era muchas veces el único medio de conectarse al que las personas podían acceder. La mayoría de las instituciones disponían de aplicaciones de pago para celulares que combinaban cámaras y códigos QR, sin embargo, las comisiones que eran necesarias para mantener a estos intermediarios hacían que el acceso a estas tecnologías desde los sectores más vulnerables fuera poco factible.

Satoshi Nakamoto diseñó el sistema para que la blockchain de Bitcoin funcionara con los protocolos más elementales de internet (TCP/IP) pero también para que pueda funcionar sin internet si fuera necesario. Imaginó también que sería posible que las personas quisieran acceder mediante su teléfono celular a las blockchains, por ello utilizó lo que llamó verificación de pago simplificada (SPV) que puede ser utilizado por teléfonos móviles para activar esas cadenas.

De esta manera, para utilizar una blockchain no era necesario contar cuenta bancaria, ni certificado de ciudadanía, ni partida de nacimiento, ni dirección domiciliaria, ni moneda local estable. Este sistema, abarataba muchísimo los costos de utilizar dinero, facilitaba el acceso a una cuenta bancaria, obtener un crédito e invertir y fomentaba la empresa y la participación en el comercio global.

Esto era parte de la visión de Satoshi ya que entendía que para las personas de economías en vías de desarrollo la situación era crítica. Cuando los estados necesitaban fondos para ejercer su gobierno, sus bancos centrales o sus tesoros simplemente emitían más moneda para aprovecharse de la diferencia entre los costes de fabricación y el valor nominal de la moneda. El incremento de la masa monetaria devaluaba la moneda y si la economía del país decaía, estos organismos centrales podían congelar las cuentas de sus ciudadanos. Dada esta posibilidad, los ricos podían trasladar sus monedas a países con más seguridad jurídica y monedas más estables, pero los pobres no tenían esta posibilidad por lo cual, tuvieran la moneda que tuvieran, esta perdía su valor.

De esta manera, el potencial que tenía el uso del sistema blockchain para registrar propiedades en los países en vías de desarrollo, donde era una cuestión muy importante ligada a la pobreza, era incalculable ya que no existía una entidad de confianza que administre los títulos de propiedad de

tierras y por eso la gente podía decir “esta propiedad es mía” y lo usaban como aval para mejorar su situación personal y familiar. (Tapscott, 2016)

Capítulo 5 - Superando obstáculos

Como toda tecnología revolucionaria la blockchain tiene sus pros y sus contras que vamos a analizar en detalle a continuación:

5.1 - Es una tecnología selectiva

La mayoría de las personas solo tiene una vaga idea de lo que es Bitcoin la criptomoneda y muy pocos han oído hablar de la tecnología blockchain. El reto tiene varias facetas.

El primero es que la infraestructura está desigualmente distribuida. Para muchas personas, tener acceso a internet es algo cotidiano, sin embargo, en el mundo existen millones de personas que no tienen acceso a internet. Esta desigualdad en el acceso a internet y a las nuevas tecnologías se lo conoce como brecha digital y afecta a una parte muy importante de la población mundial. Según un informe elaborado por We Are Social junto con Hootsuite, el 67% de la población mundial utilizaba en 2019 un smartphone y el 57% tenía acceso a internet. Los usuarios se reparten de manera dispar, encontrándose la mayoría en Asia Pacífico, la región con más habitantes pero no con la mayor penetración de internet —un 48% frente al 89% de América del Norte, el 78% de Europa, el 62% de América Latina y El Caribe y el 32% de África y Oriente Próximo—. A su vez, según una estimación de la Enacom, Ente Nacional de Comunicaciones, en 2020 en Argentina 1 de cada 3 hogares todavía no tiene acceso a internet. El organismo estima que hay 8,8 millones de accesos de banda ancha fija para un total de 14 millones de hogares. Registrándose en los últimos 10 años una duplicación del porcentaje de hogares con acceso a internet fijo. (We are social, 2019)

En segundo lugar, esta tecnología carece de controles de seguridad necesarias para hacer frente a un uso tan masivo por lo que podría tener problemas de capacidad, fallos por virus, etc. lo que causaría grandes perjuicios a los usuarios técnicamente no preparados.

En tercer lugar, es necesario un cambio de comportamiento por parte de los usuarios para esta tecnología, sobre todo de los mayores, que no se encuentran acostumbrados a utilizar frecuentemente medios tecnológicos. Es necesario que se abran a la tecnología para poder adaptarse mejor a ella.

Por último, otro punto importante es la falta de recursos legales en un mundo que está migrando hacia las transacciones irrevocables y contratos inteligentes. Las empresas que apuestan por la tecnología blockchain siguen a la espera de una regulación que pueda acompañar su acelerado ritmo de innovación y desarrollo. La descentralización, la seguridad y la inmutabilidad de los datos son sus grades ventajas, y al mismo tiempo, los factores problemáticos a la hora de establecer una delimitación por parte de los organismos reguladores.

5.2 - Alto nivel de consumo de energía

En estos primeros días de la blockchain, el método de la prueba del trabajo ha sido fundamental para crear confianza en la gente. Pero hashear, que es el proceso de aplicar el algoritmo de hash seguro 256 a las transacciones pendientes para validarlas y resolver un bloque, gasta muchísima electricidad. El consumo de energía es necesario tanto para hacer funcionar la blockchain y poder validar la transacción, como para enfriar los dispositivos electrónicos y que no fallen.

Este punto es muy seguido de cerca por parte de los desarrolladores de Bitcoin ya que es una preocupación real y requiere una solución: si Bitcoin se convierte de verdad en una red global, hay que renunciar a la prueba del trabajo como única forma de hacerla segura. Afortunadamente, el carácter abierto del protocolo Bitcoin facilita esta iniciativa. Varias cadenas alternativas al Bitcoin han explorado otros algoritmos de consenso alternativos como, por ejemplo, la prueba de participación para hacer segura la red y que a la vez siga siendo descentralizada.

5.3 - Los gobiernos

La mayor amenaza que tiene una blockchain, por ejemplo, Bitcoin es que la regulen tanto que en algún momento aparezca un competidor más privado y anónimo, todo el mundo se pase a él. Si los gobiernos no entienden esta tecnología ni las implicaciones que tiene, están destinados a fracasar. El desafío no es menor ya que deben evitar, por un lado, desestimular la innovación reaccionando exageradamente ante los potenciales malos usos, y por otro lado, hacer un mal uso de nuevas aplicaciones como son las plataformas de gestión de la identidad basadas en blockchain y utilizarlas para restringir las libertades. Debe existir un equilibrio entre la regulación de la legislación y la seguridad jurídica para que los inversores sigan sosteniendo el desarrollo global de esta tecnología.

Por otro lado, los marcos legales en los que se desarrolla esta tecnología también son importantes ya que los contratos inteligentes definen y gestionan los derechos de propiedad. Su código no prejuzga la asignación de derechos y no puede usurpar ni transferir esos derechos. La verdadera lucha está en como adaptar rápida y eficazmente las viejas normas pensadas para la vieja tecnología de manera que esas normas sean reconocibles cuando esta nueva tecnología comience a usarla, pero a la vez estén muy desarrolladas cuando la tecnología triunfe.

5.4 - Las nuevas viejas empresas

En la primera generación de internet una serie de empresas poderosas se apropiaron de la tecnología y la usaron en sus vastos imperios privados para quedarse con la mayor parte del valor, acabando con las oportunidades de innovación para mejorar la experiencia servicio del cliente.

Ante el desarrollo de esta nueva tecnología, estas empresas se ven obligadas a adaptar o reemplazar su modelo de negocio tradicional. La razón principal del éxito de blockchain es que permite resolver el problema de la propiedad intelectual en una era digital, creando una mejor economía compartida, abriendo la fabricación y cambiando la colaboración empresarial, permitiendo a las empresas realizar transacciones de manera más eficiente, más transparente, más rápida, más barata y con un mayor nivel de seguridad. A cambio de estos beneficios para las empresas, esta tecnología ofrece a los usuarios disminuir el costo de transaccionar, ser más eficiente y otorgarles mayor seguridad a sus transacciones sin revelar ni utilizar su información.

5.5 - Beneficios inadecuados para la colaboración masiva distribuida

Los mineros están incentivados para mantener la infraestructura de Bitcoin porque, si la red falla, todos los Bitcoins no convertidos que han ganado (o podrían ganar) con el minado se perderían o no valdrían o estarían en peligro. En este sentido, el servicio que los mineros prestan no es validar transacciones, ya que cualquier nodo completo puede validar realizar esta actividad. Lo que hacen los mineros es preservar la distribución del poder: el poder de decidir qué transacciones incluir en cada bloque, de poseer monedas, de votar lo que es verdadero.

Cualquier cambio que se haga en el protocolo original de Bitcoin, ya sea para introducir una moneda alternativa, o para actualizar el sistema, debe ofrecer los debidos incentivos económicos para preservar la descentralización del minado, de manera que los mineros revaloricen la red a cambio de elevadas sumas de Bitcoins. Como el número de monedas acuñadas se reducen a la mitad cada cuatro años la pregunta que surge es, ¿qué pasará cuando la distribución baje a cero? Como el ciclo del minado depende del precio de mercado del Bitcoin, cuando el precio cae, algunos mineros mantienen sus reservas y esperan hasta que el precio aumenta. Otros no pueden permitirse esto y abandonan el minado o dedican su capacidad procesadora a otras monedas alternativas que podrían ser más rentables. Otros se unen a grupos de mineros y comparten su capacidad procesadora con otros nodos esperando aumentar sus probabilidades de conseguir al menos una fracción de ganancias.

Una alternativa para mantener a los mineros puede ser cobrar comisiones. Habrá comisiones por transacción y así los nodos (mineros) tendrán un incentivo para recibir e incluir todas las transacciones que puedan. De esta manera, cuando el total de monedas creadas alcance el límite predeterminado, los nodos serán recompensados solo por las comisiones. Pero esta propuesta generará otro inconveniente dado que habrá millones de micropagos y cada bloque tiene un tamaño máximo fijo, la cantidad de transacciones que un minero puede incluir es limitada. Como consecuencia, los mineros agregarán primero las transacciones con las comisiones más altas, dejando que aquellas con comisiones más bajas o nulas se disputen el espacio que quede. Si la comisión de nuestra transacción es lo bastante elevada, podemos esperar que algún minero la

incluya en el siguiente bloque, pero si la red está ocupada y nuestra comisión es baja, podrían pasar dos, tres o más bloques antes que un minero la registre en la cadena.

Como las comisiones representan el costo marginal de verificar una transacción, sin comisiones que incentiven a los mineros y dado que la retribución por bloque sigue disminuyendo a la mitad, el ritmo del hash caerá y si esto sucede, la seguridad de la red disminuye. Así, podrían construir una mayoría de mineros que secuestrara la creación de bloques e impusiera su versión de la verdad al resto de la cadena, lo cual sería un grave problema para la integridad de la cadena.

5.6 - La teoría del desempleo

En 2019 la oficina de Argentina de la Organización Internacional del Trabajo (es un organismo especializado de las Naciones Unidas que se ocupa de los asuntos relativos al trabajo y las relaciones laborales. Fue fundada el 11 de abril de 1919, en virtud del Tratado de Versalles con el doble objetivo de lograr la expansión global de los derechos de los trabajadores y atenuar las causas de las revoluciones obreras que sacudieron fundamentalmente a algunos de los países involucrados en la Primera Guerra Mundial). realizó una investigación a pedido de la Secretaría de Empleo del Ministerio de Producción y Trabajo, donde se analiza el cambio tecnológico y el futuro del trabajo, en el marco de las actuales competencias laborales y habilidades colectivas para construir una nueva matriz productiva en Argentina. Este estudio planteaba que, si bien actualmente se presentan múltiples desafíos para el país, también aparecen nuevas oportunidades. De esta manera se argumentaba que las empresas que introducen innovaciones tienden a generar más y mejor empleo. A su vez, aseguraba que las instituciones de formación son clave para impulsar la capacitación laboral que demanden los empleos del futuro. (Ente Nacional de Comunicaciones, 2019)

La sustitución de trabajadores por máquinas no es nueva y no necesariamente implica una reducción de los puestos de trabajo, sino más bien una reorganización de estos. En este sentido, las blockchains son una extraordinaria plataforma para la automatización radical del trabajo, en la que unos códigos informáticos y no los humanos hacen las tareas, gestionando recursos y personas.

En un mundo en vías de desarrollo el sistema blockchain y las criptomonedas podrían permitir a los empresarios conseguir financiación, proteger activos y la propiedad intelectual y crear trabajo incluso en las comunidades más pobres. Cientos de miles de personas podrían convertirse en microaccionistas de nuevas empresas y participar en el intercambio económico. La tecnología podría mejorar drásticamente la entrega y distribución de ayuda humanitaria, aumentar la transparencia del estado, reducir la corrupción y sentar las bases de un buen gobierno, que es la condición para crear trabajo en muchas partes del mundo.

Incluso en el mundo desarrollado las consecuencias son impredecibles. Una plataforma global que reduzca los costos transaccionales, en particular los costos de generar confianza y crear riqueza, podría atraer a muchos participantes.

5.7 - La dificultad de gestionar protocolos

A diferencia de internet, la comunidad Bitcoin aún no tiene organismo de control oficiales que anticipen sus necesidades y guíen su desarrollo. Esto conlleva a la incertidumbre. La gente que quiere que las blockchains sigan siendo descentralizadas, abiertas y seguras no se pone de acuerdo en cómo avanzar. Si no se soluciona el problema de su gestión, el movimiento podría desintegrarse en facciones enfrentadas y hundirse.

Bitcoin no es una moneda para que la gente rica especule con ella, es una red de pago. Si Bitcoin quiere convertirse en un mecanismo de pago global serio, debe prepararse para un uso masivo. No puede dejar de funcionar cuando de pronto el flujo de transacciones sobrepase la capacidad del sistema. Las comisiones que tendrían que pagar las personas que no quieran esperar meses o años para que sus transacciones se procesen, se dispararían. O quizás saldría algún poder central a defender al consumidor y se encargaría de procesar el exceso.

5.8 - Fomenta el lavado de dinero

Al principio, los detractores de la moneda Bitcoin la consideraron un instrumento para lavar dinero y comprar bienes ilícitos o realizar otro tipo de transacciones ya que como esta tecnología es descentralizada, veloz y distribuida, los delincuentes la explotarían. La realidad es que no hay nada especial en la tecnología de Bitcoin o de las blockchain que las haga más efectivas para los delincuentes que otras tecnologías. Por el contrario, las autoridades en general creen que las monedas digitales podrían contribuir a aplicar la ley al proporcionar un registro de actividades sospechosas e incluso al ayudar a resolver delitos cibernéticos ofreciendo desde servicios financieros hasta el internet de las cosas. Bitcoin y la tecnología blockchain podrían disuadir a los delincuentes a usarlas ya que, en primer lugar, deberían hacer públicas todas sus transacciones en la blockchain, con lo que la ley puede controlar los pagos en Bitcoin más fácilmente que en efectivo, que sigue siendo el medio de pago preferido por los delincuentes. (Tapscott, 2016)

Capítulo 6 - ¿Quién lideró la revolución blockchain?

La idea de descentralizar los sistemas informáticos no era nueva. En los años 90 esta idea derivó en el desarrollo de una red -internet- que dio lugar al surgimiento de una nueva sociedad: la digital. Muchos factores explicaban este cambio, pero el más importante fue la capacidad de esa misma red para transformarse y adaptarse a los nuevos hitos tecnológicos (desde la primera computadora personal hasta los dispositivos móviles) Esta revolución contó con diversos responsables, entre los que se destacaron los navegadores web, los creadores de contenidos, los buscadores, el e-commerce y hasta los ciberdelincuentes.

6.1 - Los inicios de la red

Tim Berners-Lee (nació el 8 de junio de 1955, era un informático inglés mejor conocido como el inventor de la World Wide Web . Es profesor de Ciencias de la Computación en la Universidad de Oxford y profesor en el Instituto de Tecnología de Massachusetts (MIT). Berners-Lee propuso un sistema de gestión de la información el 12 de marzo de 1989, luego implementó la primera comunicación exitosa entre un Cliente y servidor del Protocolo de transferencia de hipertexto (HTTP) a través de Internet a mediados de noviembre) fue el responsable de que hoy cualquier persona pueda acceder a internet de manera simple, ya que fue el creador del lenguaje HTML y del sistema World Wide Web. A raíz de este desarrollo fue que nacieron, a mediados de los 90, los navegadores web. El más popular fue Netscape Navigator, y es gracias a este que se adoptó la palabra “navegar” para describir el viaje que los usuarios de la web hacían por la misma. En 1997 se lanzó al mercado el navegador de Microsoft, el famoso Internet Explorer y su exitoso sistema informático Windows, siendo el navegador estrella. Luego en 2004 la Fundación Mozilla presentó a Firefox, el cual utilizaba el código fuente de Netscape Navigator, que había sido liberado por sus desarrolladores. De esta manera se introdujo el concepto de código abierto, instando a los usuarios a compartir conocimiento para impulsar el crecimiento y la vitalidad de la red en sí misma. Con la llegada de los *smartphones*, las tiendas de aplicaciones (iTunes y Google Play, principalmente) asumieron un gran protagonismo. Según un informe de Hootsuite 2018, había más teléfonos móviles conectados a Internet que personas en el mundo. El estudio señalaba que existían 8.485 millones de dispositivos conectados a internet en el mundo. De ellos, más de la mitad (57%) correspondían a *smartphones,* es decir, 4.836 millones de móviles conectados a internet. Además, junto con los dispositivos móviles se vio multiplicada la oferta de navegadores, lo que permitió que Apple amplíe el número de usuario de su navegador Safari y Google hiciera lo propio con Chrome, de la mano del sistema operativo Android.

Sin embargo, no debe perderse de vista que fueron los propios usuarios de la red quienes también jugaron un rol protagónico como sujetos activos y creadores de contenidos originales. El auge de estos generó que internet fuera el mayor espacio de difusión de información que existía en el mundo. A su vez, la primera plataforma que permitió a los usuarios expresar sus opiniones y desarrollar

espacios personales para comunicar sus ideas fueron los blogs. Herramientas como Blogger, Tumblr y WordPress, ofrecieron la posibilidad de editar de manera rápida, sencilla e incluso barata para poder compartir contenidos.

Sin embargo, a pesar de que internet nació como un espacio descentralizado, la abundancia de sitios web convirtieron a los buscadores en las grandes estrellas, siendo Yahoo! la primera, quien luego tuvo que cederle su liderazgo a Google. Pero internet también se convirtió en la principal herramienta de comunicación social. Inicialmente, la aparición del correo electrónico (con su característica arroba) desplazó a la correspondencia tradicional. Su extensión se produjo de la mano de programas como Outlook y, sobre todo, de servicios como Hotmail, quien monopolizó el sector hasta que llegaron Google y su Gmail. Luego vendrían otras herramientas de comunicación como el chat, los servicios de mensajería instantánea y los foros, a los que luego les seguirían las redes sociales con Facebook y YouTube, primero y luego con la llegada de Instagram, Linkedin, Twitter, Google Plus, Snapchat y TikTok.

Junto con el crecimiento y evolución de la web, se dio el desarrollo del *e-commerce*, encabezado por plataformas como eBay, Amazon y Alibaba. A su vez en 2004, surgió el ciberdelito, con profesionales especializados en realizar estafas, así como robo de dinero y datos. En el primer semestre de 2020, según datos de Interpol, el sector financiero global reportó un crecimiento del 200% en el número de ataques cibernéticos. Según este organismo, la ciberdelincuencia creció a un ritmo muy acelerado, volviéndose más ágiles, utilizando nuevos métodos e incluso cooperando entre sí, de una manera nunca vista.

En este contexto se insertó el desarrollo de una nueva tecnología, la blockchain que combinaba el concepto código abierto y colaboración. Satoshi Nakamoto reconcilió los incentivos de las distintas partes codificando principios de poder distribuido, integridad, valor indiscutible, derechos de los participantes (como privacidad, seguridad y propiedad) e inclusión tecnológica. El resultado ha sido un gran desarrollo de la tecnología en los primeros años, fruto del cual son los ecosistemas que conocimos.

6.2 - En busca de un liderazgo

En su origen, Satoshi Nakamoto planteaba la no intervención, pero una especie de dios estaba empezando a crear tensiones. Como ocurrió con todas las tecnologías revolucionarias, hay ideas encontradas sobre el ecosistema blockchain. Incluso los desarrolladores de blockchain se dividieron en varios bandos, cada uno con su propio criterio. Sin embargo, el código era solo una herramienta. Para que esta tecnología siguiera avanzando y cumpliera con su promesa a largo plazo, tenían que liderarla los humanos. Era preciso que todas las partes implicadas se unieran y resolvieran algunas cuestiones fundamentales. Los problemas que esta tecnología presentaba constituyeron desafíos

que hubo que superar para que esta revolución triunfe, no razones para oponerse a ella. Lo que se necesitaba no son instituciones estatales (como los tradicionales que regulaban la actividad económica y social como el Fondo Monetario Internacional, la Organización Mundial de Comercio y la ONU, entre otros), sino que la sociedad civil, el sector privado, gobiernos y los individuos colaborarán en redes no estales. Estas redes para soluciones globales estaban proliferando, creando nuevas formas de cooperación, cambiando la sociedad e incluso produciendo valor público global. En este sentido, se necesitaba que todos los interesados colaboren globalmente y asuman el liderazgo.

6.3 - El ecosistema blockchain

Aunque la tecnología blockchain surgió de la comunidad de código abierto, enseguida atrajo a muchas personas, cada una con su formación, intereses y motivaciones. Desarrolladores, inversores, empresarios, gobiernos y organizaciones no gubernamentales tenían sus propias perspectivas y un papel que desempeñar. Empezaba a haber indicios de que muchos de los participantes principales veían la necesidad de liderarla y estaban dando un paso al frente. Entre los mismos se destacaron:

- ✓ Pioneros de la industria blockchain
- ✓ Inversores de riesgo
- ✓ Bancos y Servicios financieros
- ✓ El mundo académico
- ✓ Gobiernos y legisladores

Capítulo 7 - Atributos que consideró el comprador para adquirir una propiedad

Se identificaron cuales eran los atributos que el comprador de una vivienda valoraba a la hora de elegir una propiedad en la Ciudad de Buenos Aires. Los atributos eran los aspectos o cualidades en las que se podía seccionar o describir un bien o servicio al momento del consumo, estos podían ser aspectos deseables o indeseables del producto, pero, la combinación de estas en distintas magnitudes, hacían a la definición misma del producto final. Entonces se podía decir que el producto final era visto por el consumidor como una suma de atributos y que valoraba en mayor o menor medida los productos o servicios dependiendo de las proporciones en que estos atributos se presentaban en los mismos.

Según datos de la Cámara Argentina de la Construcción, el proceso de compra venta de un inmueble constaba de dos etapas solapadas, en la primera se seleccionaba la localización o barrio, con las características y atributos deseados, en el cual se iba a buscar el inmueble, mientras que en la segunda atapa, se seleccionaban las unidades habitacionales con las características deseadas (Inmobiliario, 2009)

7.1 - Selección de la locación o barrio

Los atributos relevantes al momento de la selección eran:

La accesibilidad

Este atributo hacía referencia al tipo de conectividad preponderante en el entorno. Constaba de cuatro niveles y cada uno de estos eran de utilidad para determinar la valoración que los compradores potenciales asignaban a cada uno de estos del tipo de transporte.

Los niveles que comprendían este atributo eran:

a) Acceso al subte (a menos de 10 cuadras).
b) Acceso a trenes (a menos de 10 cuadras).
c) Acceso a colectivos (a menos de 5 cuadras).
d) Acceso a avenida y tránsito rápido.

Densidad

La concentración poblacional podía ser un fastidio en términos de congestión, pero para otros las zonas poco concentradas podían profundizar los problemas de inseguridad, el efecto más fuerte dependía tanto del estado de ánimo de los individuos como de su percepción del problema.

Los cuatro niveles en los que se componía este indicador eran:

a) Alta (existencia de edificios entre medianeras).
b) Media alta (existencia de edificios entre medianeras y edificios con entorno perimetral).
c) Media (existencia de edificios y casas).
d) Baja (solo casas).

Cercanía a la zona comercial

Hacía referencia al tipo de entretenimiento o el ambiente que esto generaba en el entorno del inmueble.

Este atributo constaba de cuatro niveles:

a) Avenida comercial.
b) Shopping.
c) Cines, teatros o museos.
d) Bares y restaurantes.

Espacios verdes

Medía la valoración subjetiva de la distancia hacia algún espacio abierto por parte de los compradores. Los niveles utilizados aquí estaban medidos en distancias a la cual el espacio verde en cuestión puede estar.

Los atributos que se consideraban eran:

a) Localizado en frente.
b) A menos de dos cuadras.
c) Entre dos y cinco cuadras.
d) Entre cinco y diez cuadras.

Seguridad

Este atributo estaba pensado en términos de cuan inseguro podía ser un barrio, con lo cual, los niveles de este podían indicar situaciones de menor a mayor inseguridad:

Los atributos que se consideraban eran:

a) Calles iluminadas.
b) Seguridad extra (cámaras, garitas, etc)
c) Existencia de viviendas abandonadas/usurpadas
d) Cercanía de asentamientos ilegales.

7.2 - Selección de las unidades habitacionales

En la segunda etapa (selección de las unidades habitacionales con las características deseadas) los comprados tenían en cuenta las características descriptas a continuación para determinar qué aspectos aumentaban o disminuían la utilidad o el bienestar en el consumo de este y, por lo tanto, la probabilidad de compra del inmueble.

El precio, contrariamente al resto de los atributos, no solo permitía aumentar o disminuir la probabilidad de compra del inmueble, sino también, posibilitaba al analista determinar la reducción en el precio necesaria para compensar la variación en la utilidad del producto por la eliminación de un atributo deseado o el aumento en el mismo que posibilitaba la incorporación de un atributo deseado por la demanda, lo que contribuía a la cuantificación monetaria de la modificación de los distintos atributos.

Características de edificio

Este atributo hacía referencia a la existencia de diferentes estructuras edilicias, lo que pretendía determinar era cuál de ellas es la más deseada por los compradores.

En este sentido se clasificaron las estructuras en cuatro niveles:

a) Edificios en torres.
b) Edificios entre medianeras.
c) Edificios con departamentos en dúplex.
d) Edificios con departamentos en tríplex.

Amenities

Determinar cuál de ellos era el más valorado por los compradores permitía reducir costos o esfuerzos innecesarios de comercialización.

Los amenities considerados como relevantes eran:

a) Gimnasio / quincho / SUM
b) Cochera en el edificio
c) Parrilla
d) Pileta / solárium

Ubicación en el edificio

Era de utilidad para asignar en mejor medida el precio de venta de las unidades dentro del edificio, por lo que los niveles de este atributo son:

a) Al frente.
b) Al contra frente.
c) Interno lateral.
d) Último piso.

Tipo de unidad

Este atributo hacía referencia a los amenities de uso exclusivo existentes en la unidad, al igual que los amenities del edificio o de uso común, este atributo permitía aumentar el potencial de venta mediante la incorporación o no de los siguientes puntos:

a) Parrilla en la unidad.
b) Dormitorio principal en suite.
c) Cocina integrada.
d) Balcón aterrazado.

Precio

Este atributo no sólo era de interés en términos de conocer qué precio el mercado potencial consideraba como aceptable, sino también para dar valor al resto de los tributos ya que, al variar los atributos aumentaba o disminuía el precio por metro cuadrado que mantenían al comprador indiferente (Maximiliano Gómez Aguirre, Camara Argentina de la Construcción, 2020).

7.3 - Costos para realizar la transacción

Inmobiliarias

Las inmobiliarias eran las que realizan la gestión para la venta de un inmueble por parte del vendedor. Realizaban las publicaciones y la publicidad de la vivienda y eran quienes mostraban la propiedad a los interesados. El vendedor solía pagar entre un 1% y un 2% del valor de venta a la inmobiliaria.

Por su parte, los compradores pagaban entre un 3% y un 4% como comisión a las inmobiliarias por la tramitación de los certificados de dominio e inhibición. En el certificado de dominio, se informaba quiénes eran los titulares del dominio (dueños) y si el inmueble tenía algún embargo (medida cautelar) o algún derecho real (hipoteca, servidumbre, etc.), mientras que, el certificado de inhibición informaba si los titulares de dominio (dueños) tenían o no impedimentos (inhibición general de bienes) que no les permitía disponer de ese bien para su venta.

Entes recaudadores

Además de las inmobiliarias, estaban los gastos que se debían abonar a los entes recaudadores. Tanto los compradores como los vendedores debían enfrentar los pagos a la AFIP (La Administración Federal de Ingresos Públicos, es el servicio de impuestos de Argentina) y a la agencia recaudatoria que les correspondía por su domicilio.

En el caso de la Ciudad de Buenos Aires era la AGIP, mientras que en la Provincia de Buenos Aires sería ARBA (La Agencia de Recaudación Provincia de Buenos Aires era una entidad autárquica de derecho público en el ámbito de la provincia de Buenos Aires, Argentina, que tenía por objeto la recaudación de impuestos provinciales).

Por un lado, el vendedor tenía que pagar el Impuesto a la Transferencia Inmobiliaria (ITI), que era del 1,5%. Sin embargo, no lo hacía si era su única vivienda.

También existía el denominado impuesto a los sellos. Era un gasto del 3,6% del valor del inmueble que lo pagaban el comprador y el vendedor en partes iguales. Es decir que cada parte se hacía cargo del 1,8% del impuesto de sellos. Sin embargo, si el que estaba comprando no poseía otra propiedad, estaba exento de este pago hasta la suma de $ 975.000. Por lo tanto, dados los precios de mercado de ese momento, los que adquirían un departamento o una casa de más de un ambiente ya tenían pagar este impuesto.

Escribanos

Al costo de la inmobiliaria y los impuestos, había que sumarle los gastos de escrituración. El comprador se hacía cargo de la tasa de inscripción y el aporte notarial, que oscilaba entre un 0,6% hasta un 0,8%; mientras que la parte vendedora pagaba entre un 0,6% y un 1% por los certificados.

Por último, al comprador se le sumaban los honorarios del escribano. En términos generales era un 2% más IVA del valor del inmueble, aunque este porcentaje lo podían acordar entre el escribano y el cliente (Libre, 2018)

En resumen, cada parte tenían los siguientes costos para poder realizar la transacción, con el objetivo de que la misma no sea una estafa y, aun así, ese riesgo no está mitigado 100%:

Costos para el comprador:

- ✓ Comisión inmobiliaria: entre el 3% y el 4%.
- ✓ Impuesto a los sellos: 1,8%.
- ✓ Escrituración: del 0,6% al 0,8%.
- ✓ Escribano: 2% más IVA.

Costos para el vendedor:

- ✓ Comisión inmobiliaria: entre el 1% y el 2%.
- ✓ Impuesto a los sellos: 1,8%.
- ✓ Impuesto a la transferencia: 1,5%
- ✓ Escrituración: del 0,6% al 1%.

Por otro lado, tanto la inmobiliaria como el escribano estaban obligados a emitir factura y a cobrar su comisión en pesos (no en dólares estadounidenses) a tipo de cambio oficial, según lo establecido en el artículo 765 del nuevo Código Civil y Comercial Argentino.

Capítulo 8 - Blockchain y el mercado inmobiliario argentino

Teniendo en cuenta cómo funcionaba una blockchain y las complejidades que presentaba el estado del mercado inmobiliario argentino (ámbito donde se interrelacionaban la oferta y demanda de inmuebles, estableciendo cantidades y precios ofertados y demandados y cuando estos coincidían, se realizaban transacciones para él intercambio), surgió la pregunta sobre si esta tecnología podría transparentar las operaciones que se llevaban a cabo cada día. Para resolver este punto se aplicaron los beneficios que blockchain ofrecía y se detallaron una serie de punto a favor que resultaron de la aplicación de esta tecnología:

8.1 - Casi en tiempo real

La cadena de bloques permitió la liquidación casi en tiempo real de las transacciones registradas, eliminando la fricción y reduciendo el riesgo, pero también se limitó la capacidad de contra cargo por cancelar transacciones.

8.2 - Entorno sin confianza

La tecnología blockchain estaba basada en pruebas criptográficas, lo que les permitía a ambas partes realizar las transacciones directamente entre sí, sin la necesidad de un tercero de confianza.

8.3 - Libro mayor distribuido

La red distribuida *Peer-to-Peer* registraba el historial público de transacciones que era conservado en un seguro código fuente que servía de prueba de que la transacción ocurrió.

8.4 - Irreversibilidad

La cadena de bloques contenía un registro seguro y verificable de cada transacción, lo que mitigaba el riesgo de doble gasto, fraude, abuso y manipulación de transacciones.

8.5 - Resistente a la censura

La economía criptográfica que se encontraba incorporada en el modelo blockchain proporcionaba incentivos para que los participantes continuaran validando bloques, reduciendo la posibilidad de que malas influencias modificaran los registros de transacciones previamente registrado

Entonces, ¿cómo podían las blockchains innovar en el mercado inmobiliario argentino en la compra/venta de un inmueble?

I. **Búsqueda de propiedades a través de un servicio de cotización múltiple que se encontraba habilitado por blockchain**

El comprador y el vendedor o sus respectivos corredores enumeraban sus requisitos en un servicio de cotización múltiple y transparente, lo que permitía a todas las partes ver los listados disponibles según sus requisitos.

II. **Visita e inspección de la propiedad**

Los corredores discutían los requisitos de sus clientes y organizaban las visitas e inspección a la propiedad.

III. Negociación y firma de la carta de intención

Ambas partes negociaban los términos y el valor de la transacción. El comprado enviaba la carta de intención al vendedor, expresando su interés en la propiedad.

IV. Preacuerdo mediante el uso de identidades digitales

Utilizando identidades digitales de individuos y activos basados en blockchain, el vendedor verificaba la identidad del comprador y este último podía conocer las transacciones anteriores que realizó el vendedor y los gravámenes que afectaban a la propiedad.

V. Preparación del acuerdo

Se preparaba la documentación del acuerdo, que contenía todas las cláusulas y términos acordados entre las dos partes, que era verificado por los equipos legales de ambos lados.

VI. Venta de un inmueble mediante contratos inteligente

Los términos clave del acuerdo se registraban en la cadena de bloques y esto se convertía en el contrato inteligente que iniciaba el pago de la transacción a través de billeteras Bitcoin o cuentas bancarias que utilizaban una interfaz de pago hacía la cadena. El vendedor luego transfería la posesión de la propiedad al comprador así, el acuerdo de transacción se registraba oficialmente.

VII. Análisis de datos en tiempo real

Como varios pagos y transacciones se registraban en la cadena de bloques junto con las identidades digitales de individuos, propiedades y organizaciones, el comprador podía realizar un análisis de datos en tiempo real utilizando herramientas analíticas.

Capítulo 9 - Oportunidades de mejora

9.1 - Mejorar el proceso de búsqueda de propiedades

Desafío existente: el proceso de búsqueda de propiedad era ineficiente debido a que los datos se encontraban fragmentados.

Los corredores, propietarios, inquilinos, compradores y vendedores a menudo usaban múltiples portales o sitios de inmobiliarias para acceder a los datos de las propiedades como ubicación, precios de ventas y otras características. La precisión y el detalle de los datos de las propiedades era completamente dependiente de las preferencias que tenían los corredores, debido a la falta de procesos estandarizados. Esto podía generar que la información sea inexacta, errónea o incompleta. Además, el proceso en sí tendía a ser ineficiente, ya que los datos, en general, estaban fragmentados en múltiples plataformas. Como resultado, existían retrasos en la toma de decisiones por parte de propietarios e inquilinos, y bajos niveles de confianza en la calidad de la información disponible.

9.2 - Acelerar el proceso de validación de la documentación previa al arrendamiento / negociación y evaluación financiera

Desafío existente: Agilizar el proceso de evaluación y verificación de la documentación

En una transacción de arrendamiento o de compra/venta de un inmueble, generalmente se dedicaba un tiempo significativo a las actividades relacionadas a la revisión financiera, ambiental y legal para evaluar el precio de un inmueble. Esto se debía principalmente al uso de documentos físicos para probar la posesión de una propiedad, documentos que a menudo se almacenaban en lugares aislados y no eran lo suficientemente flexibles para satisfacer diversas necesidades. Por otro lado, el proceso de verificación era manual, por lo que aumentaba las tareas administrativas y era propenso a la pérdida de información y errores. Además, la participación de numerosos proveedores de servicios externos tendía a alargar el proceso de validación de la información, y aumentaban el costo relacionado con la transacción.

La oportunidad blockchain: impulsar la eficiencia y precisión en el proceso de verificación de la documentación y mejorar la toma de decisiones

Los participantes del mercado de inmobiliario debían considerar el desarrollo de identidades digitales para que una propiedad pueda ser comercializada mediante transacciones digitales. Como su nombre indicaba, la identidad digital con respecto a una propiedad inmobiliaria implicaba un identificador digital que consolidaba información como perfil del propietario, información financiera y legal en formato digital. Una combinación de tecnología blockchain junto con identidad digital podía aliviar los desafíos discutidos anteriormente de las pruebas de identidad física y acelerar algunas de

las transacciones previas como suscripción, evaluación financiera, obtención de un compromiso hipotecario, etc.

Un informe de la consultora Deloitte (multinacional de servicios profesionales) titulado “Un plan para la identidad digital: el papel de las instituciones financieras en Building Digital Identity” mencionaba que el desarrollo de una identidad digital les permitiría a las instituciones financieras desempeñar actividades con mayor precisión sobre la que ofrece la identidad física, y simplificar parcial o totalmente muchos procesos. La integridad de los datos era fundamental para alcanzar identidades digitales que sean precisas. Pero los datos iniciales serían tan buenos como el usuario los registre. Para garantizar la precisión, diferentes participantes tales como inquilinos, inversores, fuentes de financiación y asesores, etc. debieron validar los datos para brindar mayor seguridad. Adicionalmente, las empresas desarrollaron soluciones para abordar los desafíos de la integridad de los datos consideraron el uso de la identidad digital de la propiedad y las personas, para tener como resultado un poderoso impacto en la reducción de las ineficiencias e inexactitudes actuales.

9.4 - Mayor facilidad para alquilar y/o administrar las propiedades y su flujo de efectivo

Desafío existente: alta complejidad en la gestión de contratos de alquiler en curso, operaciones inmobiliarias y flujos de efectivo

Existían muchas complejidades en la administración de una propiedad debido a las dependencias entre propietarios, inquilinos e inmobiliarias. Desde el inicio de un contrato de arrendamiento, existían numerosos servicios que debían pagarse y transacciones que debían ejecutarse, rastrearse y registrarse de forma regular. También existían varios controles sobre los mismos datos. Como resultado, las empresas inmobiliarias tenían necesidades rigurosas para contabilizar los pagos, para asegurar el cumplimiento y gestión del flujo de efectivo y costos relacionados.

La oportunidad blockchain: los contratos inteligentes permitían una gestión más fácil, transparente y eficiente de propiedades y flujos de efectivo

La ejecución de un arrendamiento de bienes raíces mediante contratos inteligentes podía abordar muchos de los desafíos asociados con la propiedad y gestión del flujo de caja. Según Nick Szabo (era un informático, jurista y criptógrafo conocido por su investigación en contratos digitales y moneda digital . Se graduó de la Universidad de Washington en 1989 con una licenciatura en ciencias de la computación y recibió una licenciatura en derecho de la Facultad de Derecho de la Universidad George Washington. Era profesor honorario de la Universidad Francisco Marroquín), un destacado líder de pensamiento de blockchain y smartcontrats, un contrato inteligente era un conjunto de promesas, especificadas en forma digital, que se encontraban incluidas en los protocolos dentro de los cuales las partes cumplen estas promesas. Para el sector inmobiliario, el contrato de arrendamiento tradicional podía transformarse en un contrato de arrendamiento inteligente. El uso

de este en una plataforma blockchain permitía la transparencia en términos de arrendamiento y transacciones. El contrato podía utilizar alquileres o bonos para pagos automatizados a propietarios, administradores de propiedades y otras partes interesadas, junto con una reconciliación casi en tiempo real.

9.5 - Toma de decisiones más inteligente

Desafío existente: la ausencia de datos enriquecidos en tiempo real afectaba la capacidad de toma de decisiones de la administración

Muchos sistemas y procesos del mercado inmobiliario estaban aislados y, en consecuencia, la información se dispersaba en diferentes puntos. Esta falta de interoperabilidad daba como resultado redundancias de datos, duplicación de registros y opacidad. Como tal, las decisiones de la gestión de una emergencia se basaban con frecuencia en conjuntos de datos que no proporcionaban una vista en tiempo real de las actividades en marcha.

La oportunidad blockchain: el tejido conectivo entre diversos sistemas de tecnología definía la calidad de los datos, análisis y toma de decisiones

La tecnología blockchain podía ser el tejido conectivo entre los sistemas tecnológicos de las empresas que se desenvolvían en el mercado inmobiliario y el resto de los participantes de una transacción de alquiler o venta, ya que proporcionaba una base de datos más abierta y compartida para todos. Como resultado, los interesados podían abordar algunos de los problemas de interoperabilidad utilizando el análisis predictivo de datos para obtener información más inteligente y casi en tiempo real de los datos de blockchain. Si bien los jugadores podían usar sus propias capacidades para analizar datos internos, también podían contratar a terceros proveedores de blockchain como intermediarios para analizar datos agregados de la industria.

9.6 - Gestión de títulos de propiedad transparente y relativamente más económicos

Desafío existente: existían altos costos para realizar estas transacciones debido a la posibilidad de fraude en el registro de títulos de propiedad y engorroso proceso de autorización.

Los sistemas de registro de los títulos de propiedad estaban basados en papel, por lo cual, tenían varias desventajas. Por ejemplo, era muy común que en las transacciones inmobiliarias haya al menos un defecto en el título que debía corregirse antes de realizar la transferencia de este. Como resultado, los propietarios solían gastar dinero y tiempo para arreglar estas inconsistencias. En consecuencia, esto podía derivar en un aumento en los costos de la operación, tanto para vendedores como para compradores.

La oportunidad de blockchain: redujo el fraude y simplificaba el proceso de registros de títulos

Una identidad digital de una propiedad basada en blockchain podía incluir su historial, ubicación y detalles del título. Los compradores y los bancos podían confiar potencialmente en esta identidad digital de la propiedad para la evaluación del título, ya que cualquier cambio en los datos tenían que hacerse a través de un consenso en varios nodos de blockchain que se encontraban distribuidos. La naturaleza encriptada y a prueba de manipulaciones de la cadena de bloques dificultaba que los perpetradores cometan fraude. Este aumento de la seguridad y la transparencia podía reducir tanto el riesgo de fraude como los costos al simplificar el proceso de verificación del título. Un proceso más digitalizado y transparente también podía acelerar la ejecución de la transferencia del título, el uso del título como garantía y reducir el tiempo total de transacción. De hecho, algunos gobiernos de todo el mundo planeaban utilizar blockchain como plataforma para un impacto social más amplio, ya que los registros de títulos de propiedad tenían el potencial de reducir la corrupción y mejorar transparencia sobre la propiedad de la tierra.

9.7 - Permitir un procesamiento más eficiente de financiamiento y pagos

Desafío existente: los mecanismos de financiación y pagos eran lentos, costosos y opacos, especialmente en transacciones transfronterizas

Los pagos y transferencias de dinero para transacciones de propiedad eran costosos y requerían mucho tiempo debido a la participación de socios de múltiples canales y documentación extensa. Esto era quizás más pronunciado cuando el comprador financiaba una compra a través de una hipoteca o cuando la transacción era transfronteriza. El tiempo típico para cerrar una hipoteca comercial era de aproximadamente tres meses y el proceso de aprobación de financiamiento implicaba un papeleo extenso. A menudo había menos coordinación entre las distintas partes, y la falta de datos estandarizados aumentaba el riesgo para el prestamista hipotecario. En una transacción transfronteriza, los cargos por cambio de divisas y la participación de múltiples intermediarios generalmente aumentaban tanto el plazo de entrega del pago como los costes de transacción.

9.8 - La oportunidad blockchain: sistemas de pago y financiamiento más rápidos, económicos, seguros y simplificados

Las identidades digitales y los contratos inteligentes habilitados por blockchain podían reducir potencialmente las ineficiencias y aumentar la transparencia en los procesos de financiamiento y pagos. Para comenzar, blockchain podía simplificar el proceso de financiamiento durante la solicitud del préstamo, la documentación y etapas de servicio. La identidad digital de una propiedad reducía tanto el tiempo para validar la información como la documentación del préstamo y tal vez incluso las

preocupaciones sobre la integridad de los datos. El contrato de préstamo inteligente era accesible para todas las partes legales involucradas. Además, la ejecución de contratos inteligentes en plataformas blockchain heredaba todos los beneficios de blockchain, incluido una serie de registros completos, inmutables y rastreables, que ofrecían información para la auditoría de las transacciones como eran el historial, flujos de caja de la propiedad y pagos de hipotecas. El comprador también podía rastrear la hipoteca en tiempo real. En transacciones inmobiliarias transfronterizas, blockchain podía proporcionar una red común para que las partes en la transacción interactuaran y compartirán información sin intermediarios como los bancos. La información compartida en la red común podía incluir detalles del remitente y el destinatario, tarifas de transacción, tipos de cambio, tiempo de entrega, y muchos otros. Además, el proceso de liquidación podía ser más fluido ya que los libros de contabilidad de las partes en el lado de la transacción estaban conectados a través de una red abierta. La robustez del proceso había sido mejorada a través de un software que verificaba criptográficamente la disponibilidad del fondo y facilitaba la transferencia simultánea de fondos. De esta manera, la tecnología podía ayudar en la liquidación en tiempo real en todos los libros mayores, al tiempo que minimiza la liquidación, riesgo y retrasos en los pagos. (Preukschat, 2017)

9.9 – Nuevos horizontes

Esta tecnología fue creada para eliminar a los intermediarios en las transacciones económicas. Por este motivo, eliminaba tanto intermediarios como el intercambio de datos, es decir, permitía un movimiento totalmente anónimo, con una privacidad total de los datos de los interesados. (Martín, 2019)

Una de las principales aplicaciones de blockchain, y por la cual ha recibido el mayor de los focos en los últimos años, es sin lugar a duda el Bitcoin, lo que le permitió a pequeñas y grandes economías albergar un modelo descentralizado y aplicarlo en distintos ámbitos de la sociedad. El uso de blockchain estaba cada vez más afianzado en algunas industrias como las finanzas y las telecomunicaciones ya que había ganado terreno a fuerza de su principal característica: la transparencia.

Por otro lado, un campo que parecía tan ajeno y complejo de mejorar, como era el de la suplantación y robo de identidad, gracias a los controles biométricos y la aplicación de cifrado en cadena que ofrece blockchain se lograron grandes avances en la protección de datos de los usuarios.

Las empresas que buscaban generar negocios y ahorrar dinero se enfocaron a esta tecnología digital como palanca estratégica. La blockchain era un elemento clave en los nuevos modelos de negocio porque permitía compartir datos de forma segura y sin intermediarios, con lo cual se reducía el impacto económico de las integraciones de datos y se innova en procesos.

Según las proyecciones que realizó la consultora Gartner se indicaba que a partir de 2021 la blockchain empezaría a despegar de forma masiva. La proyección de crecimiento era exponencial, para 2025 se preveía un volumen de negocio alrededor de la cadena de datos de 176 millones de dólares y de 3 billones en 2030. Para llegar a estos resultados, era necesario que se la comience a utilizar masivamente cuanto antes.

Hay países que comenzaron a apostar a esta tecnología, porque la consideraron superadora, tal es el caso de Malta que con un marco legal que acompañaba, logró que las empresas emergentes tomen a la cadena de bloques como base para su actividad. Además de las inversiones que suponía para la economía, sus ciudadanos también estaban experimentando como los afectaba la transformación digital. (Ortín, 2019). El uso de estas nuevas tecnologías planteaba cuestiones legales, ya que no existían o eran muy pocas las leyes o regulaciones, por ejemplo, para la Criptoeconomía (Se refiere a las combinaciones de criptografía , redes informáticas y teoría de juegos que proporcionaban sistemas seguros y descentralizados que utilizaban algún conjunto de incentivos económicos para garantizar su mantenimiento).

Otra consecuencia que se pudo observar es en el ámbito laboral. Se demandaban grandes cantidades de recursos especializados en tecnología, donde la demanda por parte de las empresas solía ser mucho mayor a la oferta, la demanda de desarrolladores de blockchain cubrían la mayor cuota de estas vacantes en países como Estados Unidos y se esperaba que esto se replique en el resto del mundo.

Por otro lado, también se esperaba una mayor utilización de los Smart Contrat. Los que existían no eran inteligentes ni se consideran contratos. Además, eran muy inflexibles y no se adaptaban a las circunstancias cambiantes ya que eran, básicamente, pedazos de código que permitían una acción específica dadas unas circunstancias. Con el desarrollo de la Inteligencia Artificial, sin embargo, sería posible que estos contratos sean más inteligentes.

La tecnología blockchain se encontraba todavía en una etapa incipiente, particularmente en el sector inmobiliario, por ese motivo, muchas de sus aplicaciones fueron determinadas a través de un proceso de experimentación continua. El tiempo, así se convertía en el factor primordial para llegar a comprender y cumplir con las expectativas plantadas por blockchain. Si esta tecnología llegaba a cumplir con las expectativas planteadas por las empresas, era posible que en un futuro no muy lejano este dejara de ser un concepto para convertirse no solo en un hecho, sino en el paradigma reinante. (Ayacán, 2020)

Marco Empírico

Para realizar el trabajo de campo, en la presente investigación exploratoria, se realizó una revisión sobre la evolución del mercado inmobiliario en la Ciudad de Buenos Aires desde el año 2001 al año 2021 para evaluar cómo fue evolucionando el precio del M2 a lo largo de los años. Para ello se tomaron como fuente los datos brindados por distintas entidades como Reporte inmobiliario, Maure Inmobiliaria y Zona Prop.

Este mercado sufrió altibajos a lo largo del tiempo y se pueden encontrar dos grandes causas que explican la situación a la que se llegó al año 2021: escases de crédito y el aumento de la oferta de viviendas.

Con respecto al primer punto, se revisó bibliografía y datos brindados por el Banco Central de la República Argentina que explicaron el escaso acceso que hubo a lo largo de los años, lo que provocó que cada vez menos gente pueda acceder a la vivienda propia.

Con respecto al aumento de la oferta de viviendas, se analizó el impacto que tuvo la Ley de Alquileres analizando los datos brindados por Zona Prop año por año donde se puede ver reflejado que producto de esta Ley, gran parte de la oferta de viviendas que se destinaban a alquiler, se volcaron al mercado de compra venta.

Cada uno de estos puntos fueron tratados con más detalle a continuación:

Capítulo 1 - Evolución del mercado inmobiliario desde el 2001 a la actualidad

En la Ciudad Autónoma de Buenos aires, el mercado inmobiliario se fue consolidando con su crecimiento como metrópoli y su rol de centro urbano líder del país en función de su localización, desarrollo económico y la movilización de importantes factores de producción que concentraron en ella una importante masa de población.

El corralito (este fue el nombre informal que recibieron las medidas económicas adoptadas en Argentina a finales de 2001 por el Ministro de Economía , Domingo Cavallo, con el fin de detener una corrida bancaria , y que eran plenamente vigente por un año. El corralito congeló casi por completo las cuentas bancarias y prohibió los retiros de cuentas denominadas en dólares estadounidenses) y el plan de pesificación de los depósitos en dólares fueron implementados a finales de 2001 para evitar una corrida bancaria que hubiese derivado en la quiebra de todo el sistema financiero generando una fuerte caída en los saldos monetarios reales, pero tuvo como contrapartida el derrumbe de los precios de los activos reales. Luego de los primeros años de la

crisis, más especialmente desde 2003, los precios de los inmuebles empezaron a recuperarse a pesar de la inexistencia de crédito hipotecario.

El aumento de los precios que se produjo en 2003 fue producto de que se fue liberando dinero de los ahorristas mediante amparos judiciales y la posibilidad que dio el gobierno de comprar dinero con depósitos bancarios y en dos años el mercado se recuperó.

El aumento sostenido de los precios de las viviendas se mantuvo contante hasta mediados del 2012 al 2013 donde se presentó una pequeña caída producto de la implementación del cepo cambiario, ya que, la imposibilidad de acceder a los dólares contrajo de forma abrupta las operaciones de compraventa.

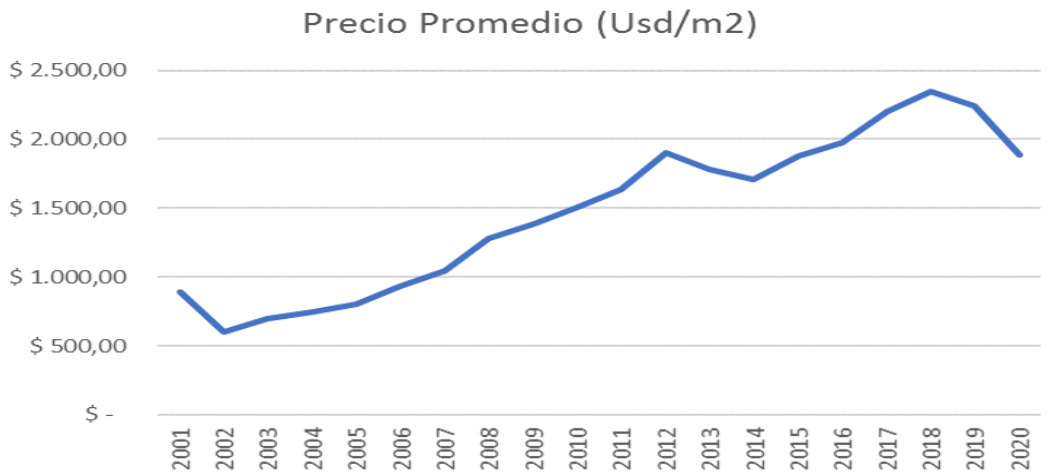
En 2014 hubo una mejora en esta situación. El cambio de gobierno atrajo consigo la normalización del mercado de cambios, lo que sumado al surgimiento de los créditos UVA (la unidad de valor adquisitivo era un instrumento financiero que se utilizó en Argentina y era una medida que equivalía a la milésima parte del costo promedio de construcción de un metro cuadrado de vivienda tipo. La misma era ajustada en función de la inflación y su ajuste era con el índice del coeficiente de estabilización de referencia CER) permitió que la actividad se reanime.

Esta situación se mantuvo hasta el 2018 donde se produjo una fuerte devaluación de la moneda, lo que disparó la cotización de los UVA afectando a quienes poseían créditos ajustados por esta medida y produciendo como contrapartida una caída de los precios de las propiedades.

Las sucesivas devaluaciones y la profundización de la crisis por la pandemia de 2020 hicieron que comenzaran a ser más evidentes los ajustes en los valores iniciales de publicación con caídas interanuales de dos dígitos (ver figura 8).

FIGURA 8

EVOLUCIÓN DEL PRECIO DEL METRO CUADRADO EN CABA



Nota: En los últimos años se observó una baja en el precio del metro cuadrado en Ciudad de Buenos Aires. Fuente: https://maureinmobiliaria.com/el-mercado-inmobiliario-en-los-medios/valor-m2-historico-caba/

Capítulo 2 - Escases de crédito

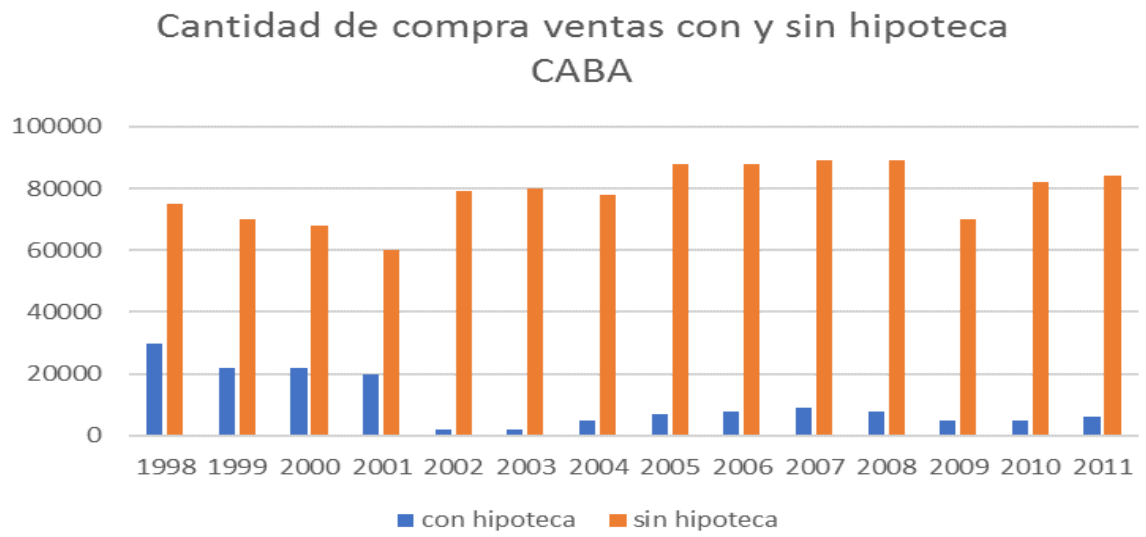
Una de las principales razones de los vaivenes que se dieron en el precio del M2 en CABA, fue la escasa oferta de créditos hipotecarios.

Adquirir una vivienda propia era una de las principales aspiraciones que tenía una familia, por esa razón, contar con un mercado crediticio hipotecario desarrollado y fuerte era una necesidad imperiosa. En los últimos años hubo intentos de cubrir esta deficiencia y aunque los resultados preliminares han sido positivos, los mismos se vieron empañados por la inestabilidad económica del país.

La disponibilidad de crédito hipotecario (Ciudad, 2020) ha sido tradicionalmente muy baja en el país y en la medida que no aumentaba el plazo promedio de los depósitos y se desarrollaran instrumentos de ahorro a largo plazo, no era factible esperar un rol determinante de esta variable (ver figura 9).

FIGURA 9

ADQUISICIÓN DE INMUEBLES EN CABA CON Y SIN HIPOTECA



Nota: Las transacciones con préstamos hipotecarios disminuyeron a partir de 1998 cuando el Plan de Convertibilidad comenzó a debilitarse, luego aumentaron levemente por la recuperación post crisis y la caída producida con la debacle financiera que afecto al sector internacional en 2008, que fue acompañado por un contexto económico interno inflacionario. Fuente: https://www.reporteinmobiliario.com/nuke/article141-indices-inmobiliarios.html

A partir del Plan de Convertibilidad (donde la caja de conversión argentina fijó el peso argentino al dólar estadounidense entre 1991 y 2002 en un intento de eliminar la hiperinflación y estimular el crecimiento económico. Esta vinculación no existió, excepto en los primeros años del plan. Pero, le permitió al gobierno eximirse de utilizar a las reservas de divisas del país para el mantenimiento de la paridad, excepto cuando la recesión y los retiros bancarios masivos comenzaron en 2000) se produjo un aumento en el precio de los inmuebles y en la cantidad de transacciones motivado por la aparición del crédito y por la baja de la tasa de inflación, lo que permitió a su vez un entorno de mayor certeza en las variables macroeconómicas, fortaleciendo la inversión en bienes durables. La baja de la tasa de inflación hizo aumentar el poder adquisitivo del dinero y permitió un mayor horizonte de planeamiento, lo que tuvo un impacto directo en la demanda de bienes durables y en especial de los inmuebles. La combinación de una baja tasa de inflación y la consecuente monetización de la economía potenció el ahorro que se canalizó hacia el sector.

Con los sucesos del 2001 desapareció el crédito, pero excepto en el período más profundo de la crisis, los precios no bajaron. La pérdida de confianza en el sistema bancario y financiero redujo las

posibilidades de colocación de excedentes financieros, lo que puso freno a la venta de los inmuebles por la carencia de alternativas de inversión. De esta manera se podría inferir que en esta etapa de la economía argentina el rol de la propiedad como reserva de valor adquirió una relevancia mayor a la experimentada hasta ese momento. Adicionalmente a la disponibilidad de crédito, el contexto macroeconómico tuvo una importancia significativa para explicar la evolución del precio de los inmuebles. Más allá de un lógico rebote luego de los bajos niveles alcanzados en el año 2002, fue la mejora económica experimentada luego de un fuerte período de retracción, acompañada por el crecimiento del precio internacional de los commodities lo que promovió un aumento sostenido en los precios de estos bienes.

A partir del año 2016, para mejorar la oferta de créditos hipotecarios y fomentar el sector, existieron distintos planes fomentados desde el gobierno de turno:

- ✓ *2.1 - PRO.CRE.AR*

En 2012 se lanzó el Programa de Crédito Argentino del Bicentenario para la Vivienda Única Familiar (Wikipedia, Wikipedia, 2014), el cual estaba respaldado por el Fondo de Garantía de Sustentabilidad de la ANSES. El objetivo era atender las necesidades habitacionales de la población, otorgando créditos a aquellas personas que no tenían la posibilidad de acceder a un préstamo tradicional, con una tasa subsidiada por el estado.

Hasta fines de 2015, se otorgaron alrededor de 176.000 créditos que sumaron más de $44 mil millones de pesos, mientras que, en ese mismo periodo, los préstamos hipotecarios tradicionales brindados por todos los bancos alcanzaron los $19 mil millones.

- ✓ *2.2 - PRO.CRE.AR UVA*

En 2016 el sistema PRO.CRE.AR sufrió modificaciones ya que los prestamos se empezaron a brindar a través del sistema de Unidades de Valor Adquisitivo (UVA) otorgando un subsidio sobre el capital (ya no sobre la tasa de interés) por parte del estado y además se readaptó la manera en la que se seleccionaban los candidatos mediante un scoring de acuerdo con su nivel socioeconómico, limitando la entrada a aquellas familias que declaraban ingresos de entre dos y cuatro salarios mínimos.

Entre 2016 y 2018 se entregaron $23 mil millones en este tipo de créditos.

- ✓ *2.3 - Créditos Hipotecarios UVA*

En 2016 se lanzó también otro instrumento, los créditos hipotecarios ajustables por medio de la Unidad de Valor Adquisitivo (UVA) (Wikipedia, Wikipedia, 2017), cuyo valor era publicado diariamente por el Banco Central de la República Argentina (BCRA). Esta unidad representa el valor

promedio de la construcción de una milésima parte de un metro cuadrado modelo, la cual se ajustaba de forma mensual por medio del Coeficiente de Estabilización de Referencia (CER). De esta manera, el monto de cada cuota mensual se ajustaba por la inflación presente en ese momento del tiempo.

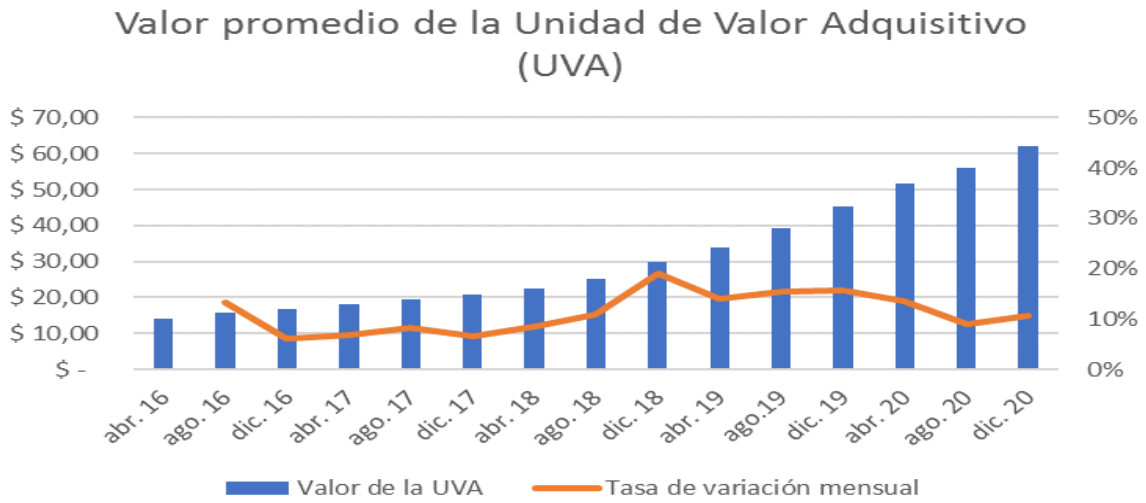
La diferencia fundamental entre los préstamos en UVAs y los convencionales residía en que la UVA era una medida ajustable de valor, por tanto, permitía que la tasa de interés nominal anual vinculada a la operación sea comparativamente más baja. De esta manera, se exigían menores ingresos para calificar a un préstamo por el mismo monto en relación con una operación convencional. Asimismo, bajo la modalidad en UVAs, el capital residual se iba actualizando por el nivel general de precios, de manera que la cuota del crédito en pesos crecía nominalmente a lo largo del tiempo, pero mantenía su valor real – en UVAs – constante. Este factor hizo posibles cuotas más accesibles al inicio.

Solo durante el 2017, según datos del Banco Central de la República Argentina, el monto de préstamos hipotecarios UVA otorgados alcanzo los $54 mil millones a nivel nacional. Sin embargo, la devaluación del peso a partir del segundo trimestre afecto notablemente el mercado inmobiliario, provocando que disminuya el otorgamiento de créditos (ver figura 10).

En economías con alta inflación, este tipo de préstamos presentaba un alto riesgo de descalce entre la actualización de los salarios y el nivel de aumento de los precios que repercutía en el valor de la UVA. Además, la posibilidad de una devaluación podía perjudicar el poder adquisitivo que brindaba el préstamo dado que, a lo largo del periodo entre la aprobación del crédito y la escrituración del inmueble, el valor de la propiedad podía aumentar en pesos (ver figura 11).

FIGURA 10

VALOR PROMEDIO DEL UVA

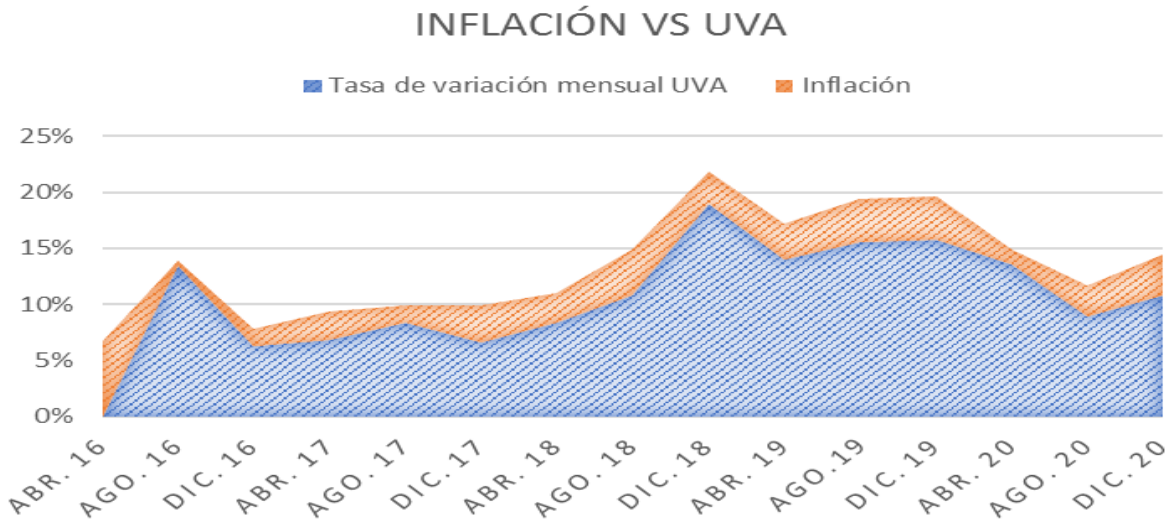


Nota: Durante el año 2016, cada unidad de valor adquisitivo (UVA) experimentó una variación total

del 442%. Esta variación en gran medida se debió a las devaluaciones de la moneda argentina en conjunto con el constante crecimiento de los precios. Fuente: http://www.bcra.gov.ar/publicacionesestadisticas/Principales_variables_datos.asp

FIGURA 11

INFLACIÓN VS VALOR UVA

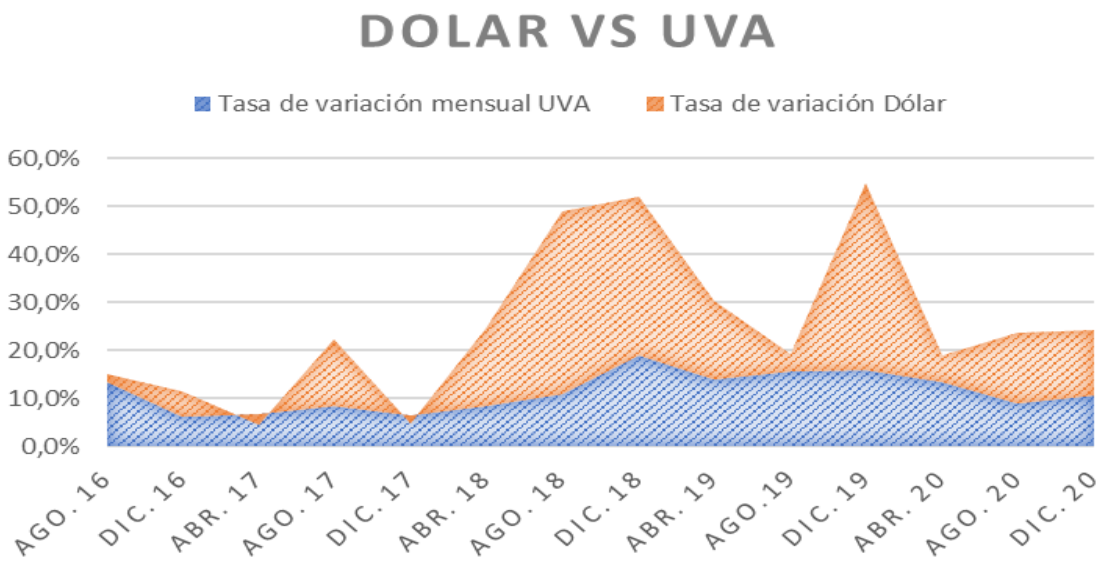


Ante un aumento en los niveles de inflación, se dió un aumento en el valor de las UVAs, lo que generó que la persona que tomó una hipoteca de este tipo deba en pesos cada vez más dinero. Fuente*:* http://www.bcra.gov.ar/publicacionesestadisticas/Principales_variables_datos.asp

Con respecto al precio del dólar, existía cierta correlación respecto el aumento del precio de la divisa y el incremento que experimenta el UVA (ver figura 12).

FIGURA 12

DÓLAR VS UVA



Nota: Si bien estos préstamos eran sensibles a los saltos del dólar por el traslado a precios, el capital en pesos medido en dólares se licuaba debido a que el salto del dólar no se veía reflejado inmediatamente en la UVA. Fuente: http://www.bcra.gov.ar/publicacionesestadisticas/Principales_variables_datos.asp

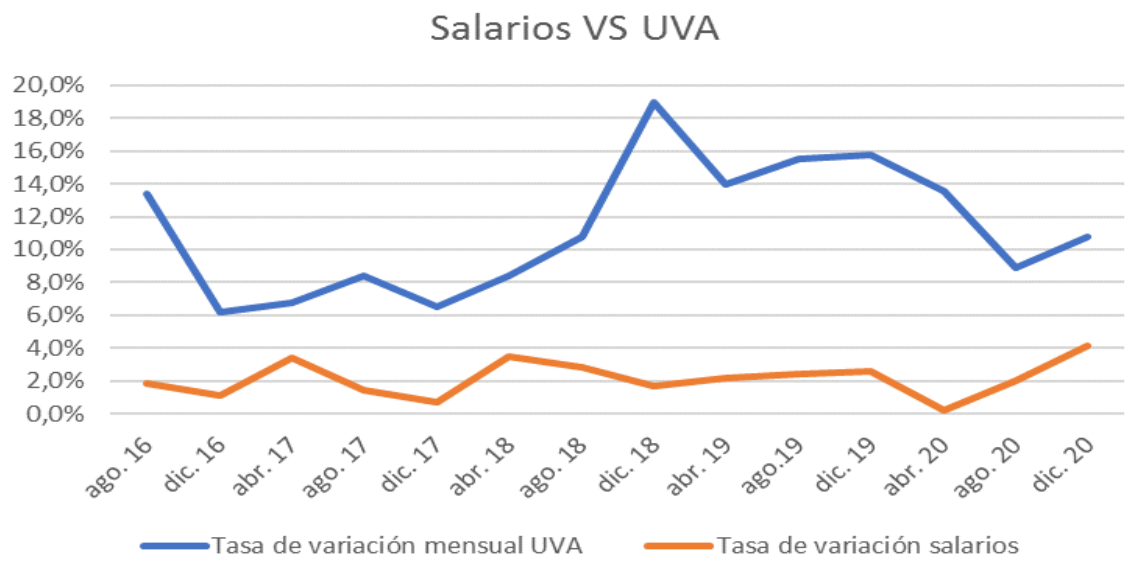
Con respecto al salario, el porcentaje en que varió quedó muy por debajo del porcentaje en que varió el precio de las UVAs (ver figura 13).

Para poder mitigar este desfasaje entre el aumento del valor de las UVAs y la evolución de los salarios, se estableció una cláusula para que, si la inflación superaba por más de un 10% la evolución de los salarios, los bancos deberían ofrecerles a sus deudores la posibilidad de extender en un 25% el plazo del préstamo originalmente otorgado.

Esta cláusula gatillo se activaba cuando la UVA era 10 puntos más alta que el Coeficiente de Variación de Salarios (CVS).

FIGURA 13

SALARIOS VS UVA



Nota: Siempre que hubo un salto devaluatorio afectó a la totalidad del sueldo ya que subieron las expensas, los servicios, los alimentos. Más allá de que la cuota de la UVA, en principio, parecía estar más o menos estable, el resto se descompaginaba. Si el salario seguía la inflación o se actualizaba como la cuota, no hubiera habido problemas para pagar, pero como esto no pasó el salario necesitaba mayor porcentaje de la totalidad para pagar la cuota. Fuente: http://www.bcra.gov.ar/publicacionesestadisticas/Principales_variables_datos.asp

Ante el disparo del precio de la cuota de los créditos del año 2020, el Banco Central de La República Argentina (BCRA) repartió la suba de las cuotas a lo largo de un año. Igualmente, de los 500.000 deudores de créditos UVA, entre personales, prendarios e hipotecarios, sólo 95.000 respiraron aliviados. Estas personas fueron los que sacaron préstamos ajustados por la inflación para comprar una vivienda única por hasta el equivalente a u$s 100.000.

Existieron otros 10.000 deudores hipotecarios que fueron beneficiados porque sobrepasaron el monto de 120.000 UVAs, unidad de medida que cotizaba a $ 49, por lo que equivale a casi $ 6.000.000. En tanto, los 400.000 deudores de personales y prendarios UVA no tuvieron ningún beneficio.

En un régimen de mayor flotación del tipo de cambio, los saltos en la cotización de la moneda extranjera fueron un dolor de cabeza para quienes firmaron la entrega de un crédito hipotecario, ya que entre el momento de la aprobación del crédito y el desembolso de los fondos en promedio pasaron entre 30 y 45 días. Por ejemplo, en diciembre de 2017 el tipo de cambio se movió más de

15%, al pasar de un valor en torno a los $ 17,6 a los $ 20,25 actuales. Esto implicó que un préstamo de $ 1 millón compra, en vez de adquirir aproximadamente u$s 57.000 al momento de la aprobación, puedo comprar menos de u$s 50.000 (es decir, una pérdida superior a los u$s 7000). La devaluación también repercutió sobre el precio de las propiedades, ya que estaban nominadas en dólares, por lo que había que pagar más pesos por las viviendas. El Índice de Salario Real en Términos del Valor del metro cuadrado de Vivienda (ISRV) elaborado por la Fundación UADE reflejó una disminución del poder de compra de los salarios del metro cuadrado de viviendas usadas de 5,2 % en agosto de 2017, respecto de un año atrás.

Otra situación que se tenía que evaluar en un contexto inflacionario era el crecimiento permanente de las cuotas, acorde al ritmo de aumento de los precios. Si bien de mediano plazo los salarios tendían a crecer a la par de la inflación, en el corto plazo podía producirse un desfasaje, por lo que la cuota a pagar se podía volver muy onerosa para las familias. Incluso, cuando los salarios se ajustaban anualmente según la inflación (por ejemplo, por la introducción de la “cláusula gatillo”), en general los incrementos salariales no se realizaban mensualmente, por lo que a lo largo de un año se podían producir desbalances entre las cuotas y los ingresos de las familias.

Ante la situación de inestabilidad que se vivía, difícilmente el mercado iba a ofrecer financiamiento para la adquisición de viviendas accesible, minimizando los riesgos para el tomador, ya que tenía la economía un problema de inflación aún irresuelto. (Medios Cifras, 2020)

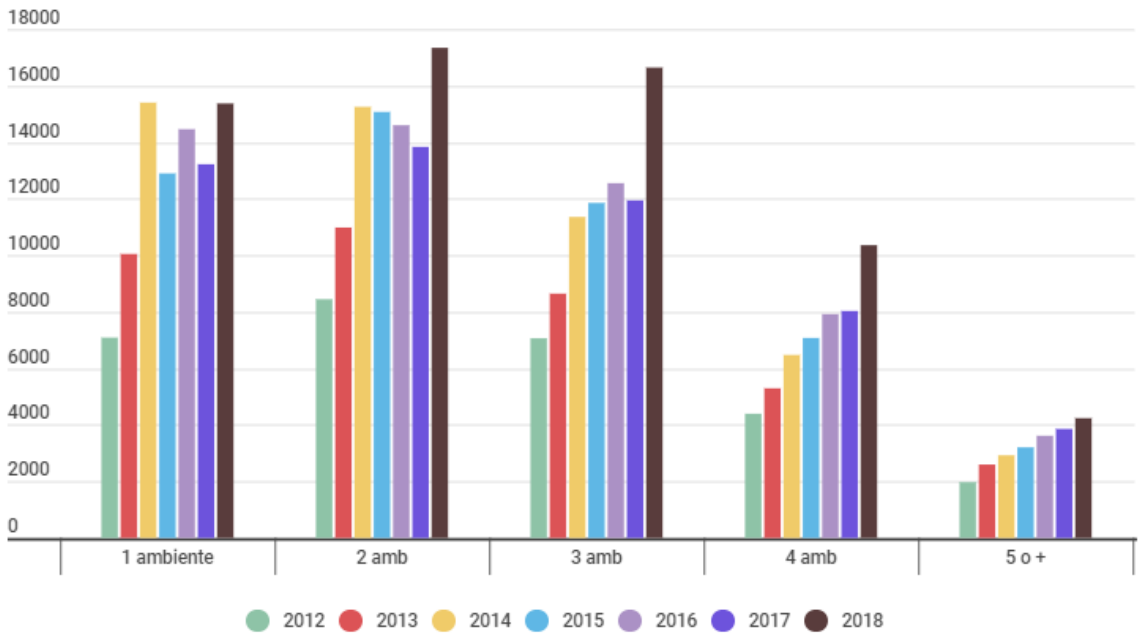
Capítulo 3 - La oferta de viviendas

Con los cambios introducidos en la Ley de Alquileres (el contrato de arrendamiento, contrato de alquiler o locación era un contrato por el cual existe una relación entre dos partes, mediante la cual se obligaban de manera reciproca y por un tiempo determinado la cesión de un bien o servicio quedando obligada la parte que aprovecha la posesión a pagar un precio determinado), al extender un año más los contratos dificultaba una posterior venta por los próximos tres años, y los decretos oficiales que impedían los aumentos y prohibían los desalojos, se advertía una nueva tendencia: cada vez eran más los que dejaban de alquilar sus propiedades para ponerlas a la venta porque ya no les resulta rentable. Si bien esta tendencia venía desde hace algunos años, con esta novedad, se profundizó.

Ante la falta de perspectiva de incremento en los valores de los alquileres en el corto y mediano plazo, muchos consideraron que no era una opción redituable mantener ese capital inmovilizado y optaron por hacerse de liquidez: un inmueble que valía u$s100.000 le generaba al propietario un ingreso de apenas $30.000 por mes y esta situación no ayudaba al que quería vivir de un alquiler (ver figura 14).

FIGURA 14

CANTIDAD DE AVISOS EN ZONAPROP PARA VENTA DE INMUEBLES POR AÑO EN CABA

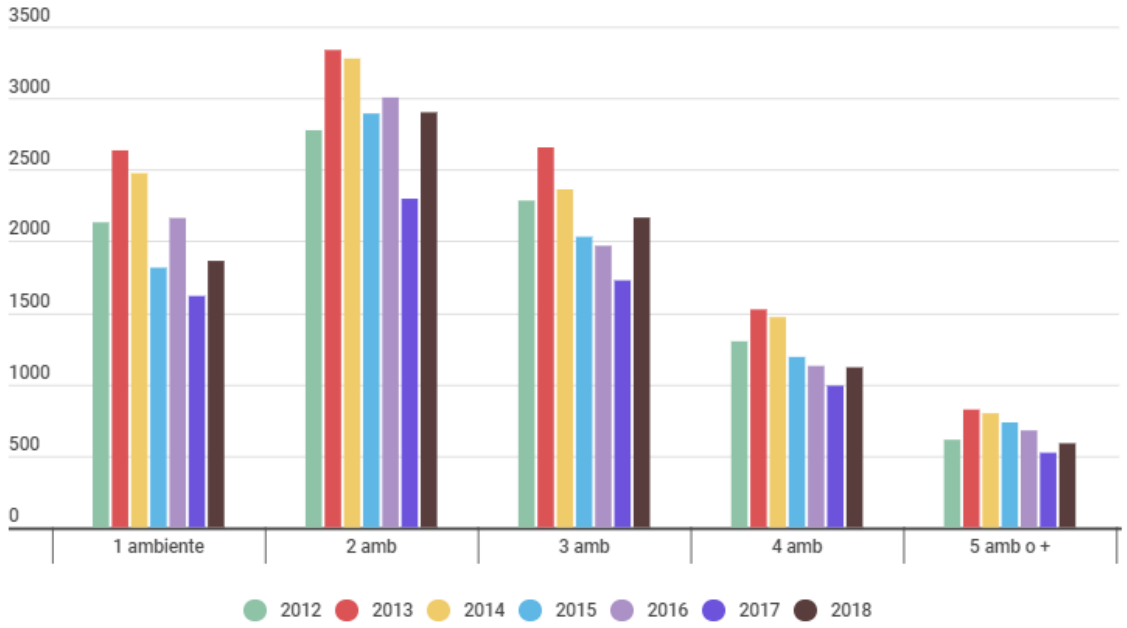


Nota: En el año 2018 fue récord la cantidad de avisos que fueron publicados para la vente en el portal ZonaProp en todas las categorías de departamentos por ambientes. Fuente: https://maureinmobiliaria.com/estadisticas-mercado-inmobiliario/

Una alternativa que se utilizó fue la de vender esos inmuebles y reinvertir en departamentos desde el pozo que era una oportunidad única de financiarse en pesos a largo plazo y no estar preocupado por la variable del dólar de todos los meses. El propietario compraba m2 a precios muy atractivos y se capitalizaba apostando a generar spreads (ver figura 15).

FIGURA 15

CANTIDAD DE AVISOS EN ZONAPROP PARA ALQUILER DE INMUEBLES EN CABA

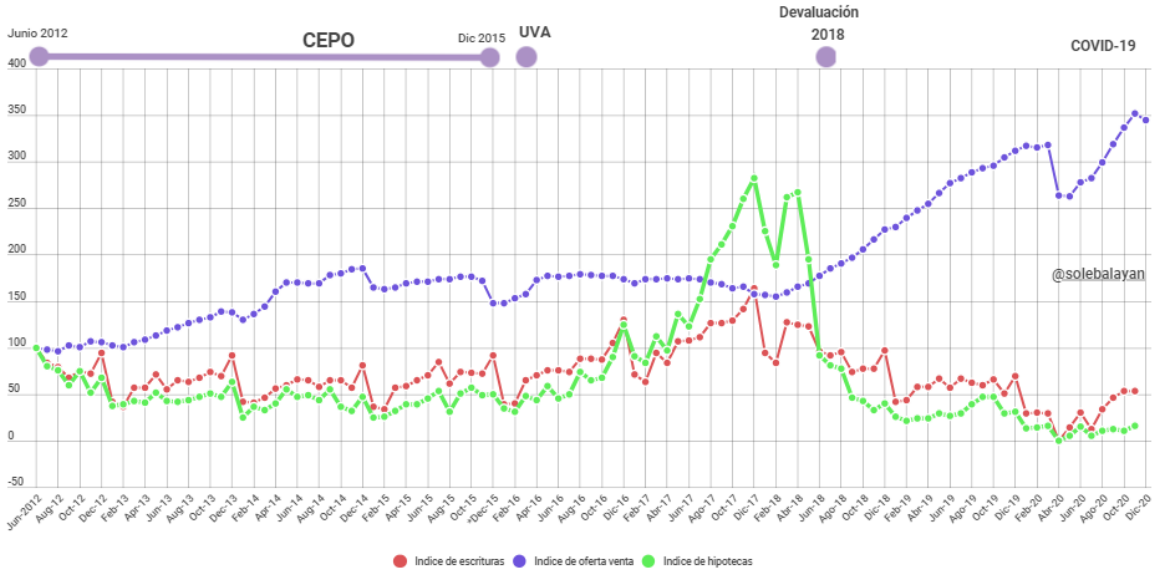


Nota: La oferta de departamentos para alquiler fue la más baja de los últimos años en todas las categorías de departamentos por ambientes. Fuente: https://maureinmobiliaria.com/estadisticas-mercado-inmobiliario/

Las obras a largo plazo eran las que se presentan más accesibles, con cuotas en pesos ajustadas por el índice de la Cámara Argentina de Construcción, incluso después de la posesión. Lo más conveniente era vender la unidad de pozo antes de escriturar para evitar todos los costos notariales y volver a reinvertir en ladrillos. La tasa de retorno que producía la compra y venta de unidades en construcción superaba ampliamente la de un alquiler y es por ellos que se convirtió en una de las opciones preferidas (Ver figura 16). (Iprofesional, 2020).

FIGURA 16

CANTIDAD DE AVISOS EN ZONAPROP PARA ALQUILER DE INMUEBLES EN CABA



Nota: La oferta de viviendas para compraventa estuvo en un máximo histórico desde 2012, sin que todavía se pudiera hablar de un techo para el mismo. En cuanto a las escrituras, las mismas se encontraban en descenso, registrándose los menores valores en junio y julio de 2020 desde 2012.

Fuente: https://maureinmobiliaria.com/estadisticas-mercado-inmobiliario/

Conclusión

A lo largo de la tesis, se abordaron las características más sobresalientes de esta tecnología: la cadena de bloques se basaba en un protocolo común que verificaba y confirmaba las transacciones realizadas y aseguraba la irreversibilidad de estas. Era el consenso el que proporcionaba a todos los usuarios una copia inalterable y actualizada de las operaciones realizadas en la blockchain. No existía un usuario que tuviera más poder que otro en la red y todos los nodos eran iguales entre sí. Por otro lado, la tecnología blockchain mediante una innovadora forma resolvía un importante problema informático que había sido una barrera para tener un sistema monetario digital funcional durante años: el problema del doble gasto ya que el dinero solo debía gastarse una vez. Blockchain abordó este problema requiriendo que los mineros resolvieron un problema matemático complejo para verificar la transacción. La complejidad del cálculo se ajustaba de modo que, en promedio, se necesitaban 10 minutos para resolver un problema utilizando los poderes de procesamiento de los mineros. Porque solo bloques con respuestas correctas al problema matemático se podían agregar a la cadena, solo uno entre los pagos múltiples era aceptado y registrado en la blockchain, por lo que era casi imposible para las partes gastar fondos doblemente.

Aunque el sistema era muy robusto, fueron varios los problemas con los que se debía enfrentar todavía este sistema para sobrevivir, tal como se detalló a lo largo del trabajo, pero si hay algo que demostró durante estos escasos años de vida, es que se estaba ante la presencia de una tecnología muy adaptativa, que cada vez era más aceptada en el mundo y que los distintos países poco a poco empezaban a impulsar como alternativa al dinero tal cual hoy lo conocemos. No obstante, esto, el alto consumo de energía que se requería para que una cadena de bloques se pudiera desarrollar no es menor. Sobre todo, en un mundo donde en el último tiempo surgieron líderes, como Greta Thunberg, que proclamaban e invitaban a apoyar las causas por el cuidado del medioambiente.

En cuanto al mercado inmobiliario es de destacar que, como se abordó en los capítulos anteriores, el tema de la escases de crédito ha sido una constante en el país. Poder adquirir una vivienda propia era una de las principales aspiraciones que tiene una familia, por esa razón, poder contar con un mercado crediticio hipotecario desarrollado y fuerte era una necesidad imperiosa. En los últimos años hubo intentos impulsados por los diferentes gobiernos de turno de cubrir esta deficiencia por medio del lanzamiento de planes crediticios. Y aunque los resultados preliminares fueron positivos, los mismos se han visto empañados por la inestabilidad económica del país.

El mercado inmobiliario de compraventa de inmuebles en la Ciudad de Buenos Aires se encontraba en un momento crítico. La cantidad de escrituras que se realizaron en el año 2020 fue de las más bajas de la historia y esto sucedió por varias razones:

- ✓ Escaso acceso al crédito para quienes deseaban comprar una vivienda.

- ✓ Era un mercado dolarizado, por lo que un contexto de sucesivas devaluaciones lo afectaron.
- ✓ Altos costos para realizar la transacción.
- ✓ Contexto desfavorable para alquilar un inmueble.

Argentina no era un país que a lo largo de su historia se haya caracterizado por la estabilidad o por la posibilidad de adquirir un inmueble mediante una hipoteca, pero en los últimos 20 años, la situación se agravó.

Aun ante la intención de llevar adelantes algunos tipos de financiación por parte del gobierno (como lo que ocurrió durante el 2016 con los créditos hipotecarios UVA) en la medida que no aumentara el plazo promedio de los depósitos y se desarrollaran instrumentos de ahorro a largo plazo, no era factible esperar un rol determinante para esta variable.

Por otro lado, los habitantes de la Ciudad de Buenos Aires estaban pasando por una situación económica poco favorable, con devaluaciones de la moneda constantes que hicieron que desde 2001, donde el valor de cada dólar era de $3,00, la moneda se deprecie y llegara a un dólar de $86,84 en enero de 2021, a lo que además se le debía sumar un 35% de impuesto a las ganancias y un 30% de impuesto país encareciendo aún más el precio de la divisa que se hacía cada vez más inalcanzable para la gran mayoría de los Argentinos.

El punto anterior fue justamente uno de los motivos que explicaron la inflación que sufrió Argentina y que hicieron que sea muy riesgoso la toma de crédito atado a UVAs, por ejemplo. Por otro lado, esta variable también impactaba directamente en el salario, provocando un derrumbe de estos en términos reales.

A este escenario, se le agregó que, para adquirir un departamento, las comisiones se calculaban como un porcentaje sobre el precio de venta de la unidad (tanto para la inmobiliaria, como para los entes recaudadores y escribanos) y los mismos oscilaban entre un 7,5% y un 8,6% para la parte compradora. La justificación para ceder ante semejantes porcentajes era que, de esta manera, se disminuía el riesgo de sufrir un fraude, pero, aun así, se registraron innumerables cantidades de transacciones fraudulentas, con lo cual, la justificación de se debía pagar esos porcentajes para garantizar una transacción sin problemas, era una falacia.

También se trataba de un mercado altamente dolarizado, donde era casi imposible que una transacción de este tipo se realizara en esta moneda dado los altibajos que sufre el peso como resguardo de valor. Como ya se mencionó, la búsqueda de la casa propia era algo que la mayoría de las personas anhela a lo largo de su vida, por lo cual, al vender una propiedad, nadie quería que ese valor se pierda. En este punto la blockchain y más puntualmente la moneda en la cual se realizarían las transacciones, por ejemplo, Bitcoin, cobraba particular interés ya que el diseño descentralizado de la misma, y de otras monedas digitales, protegía contra la inflación. Las monedas

tradicionales dependían de un banco central para regular el suministro de dinero, introduciendo dinero nuevo en circulación según sea necesario. Bitcoin, por el contrario, usaba la criptografía para garantizar un suministro de dinero relativamente fijo, que se permitía crecer a intervalos regulares.

Aun ante este contexto desfavorable para la venta de inmuebles, en los últimos meses, se han registrado un aumento de la cantidad de viviendas que se ofertaban para la venta y una razón importante fue el actual contexto de pandemia sumado a las nuevas condiciones de la ley de alquileres.

La resolución por parte del gobierno de prohibir los desalojos y las subas en los precios de los alquileres desaliente a los poseedores de viviendas que buscaban tener alguna rédito (aunque muy bajo en relación al capital invertido) mediante un alquiler a deshacerse de la unidad ya que preferían recuperar ese capital e invertirlo en algún nuevo desarrollo inmobiliario ya que les era mucho más redituable y reducía el riesgo de que el inquilino deje de pagarle el alquiler y no pudiera desalojarlo por ese incumplimiento.

La intromisión del estado en el sector privado, llevado adelante por el actual gobierno Alberto Fernández, ha sido casi una constante ya que en el último tiempo hemos vivido situaciones de intentos de expropiación de algunas empresas, regulación en el precio del dólar y la aplicación de impuestos excesivos sobre algunos productos como la soja.

Ante esta situación, blockchain surgió como una alternativa viable ya que era una base de datos distribuida entre distintos participantes, que se encontraba protegida criptográficamente, organizada en bloques de transacciones relacionados uno con el otro matemáticamente, posibilitando que partes que no confiaban plenamente unas en las otras, lleguen a un acuerdo sobre la realización de una transacción. El consenso era la clave en todo este proceso. Por otro lado, ante un estado que no le temía a la intromisión dentro del ámbito privado, quizás fue esta una oportunidad para que esta propuesta prospere ya que se estaba eliminando uno de los problemas actuales para la compraventa de viviendas: los altos costos destinados a los intermediarios ya que no iba a ser necesario que un tercero certifique la propiedad de una vivienda ni que la transferencia de dominio se realizó.

Fue la red la que de manera eficiente certificó que el movimiento (tanto la transferencia de propiedad y como contrapartida la entrega de dinero) se realizó, por lo cual, ya no era necesario contar con una inmobiliaria que realizara las certificaciones de dominio y de inhibición, como tampoco un escribano que certificara la transacción, reduciendo los altos costos que se pagaban para poder llevar adelante la transacción, los tiempos y por sobre todo, se tenía la garantía de que la operación era lícita para ambas partes.

Por otro lado, teniendo definidos cuáles eran los parámetros valorados por el consumidor para la elección de su vivienda, una blockchain bien configurada podía brindarle un mejor asesoramiento a

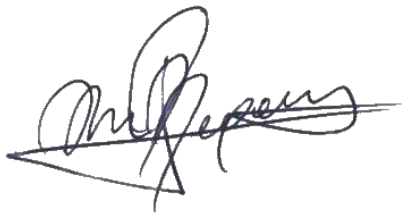
quien estaba buscando una propiedad, como también, una mayor certeza sobre quien era la persona con la que estaba negociando el vendedor reduciendo el riesgo de sufrir algún tipo de delito por parte de quien visitaba la propiedad.

Otra de las características favorables de las blockchains era que se podían utilizar criptomonedas como medio de pago para realizar las transacciones. Esta singularidad, brindaba la oportunidad de poder realizar el intercambio de inmuebles en otra moneda que no era el dólar y que no se encontraba atada a las decisiones de política monetaria que maneja el Estado.

El Bitcoin, por ejemplo, como se mencionó anteriormente podía haber sido una alternativa para realizar una transacción y además permitía, si se daban las condiciones, que se fomente la conformación de un fondo en dicha moneda que hubiera podido brindar opciones de financiación.

Con todo lo detallado anteriormente, se pudo inferir que la blockchain tenía mucho potencial para desarrollarse en una economía con tanta inestabilidad como la de Argentina, puntualmente el de la Ciudad de Buenos Aires, ofreciendo alternativas para la reducción de costos y fomentaba la disponibilidad de créditos lo que la hacía muy atractiva para desarrollar.

No iba a ser fácil el camino, porque se tocaban intereses de muchos sectores, como el de las inmobiliarias, escribanías y bancos, pero si se tenían en cuenta la imposibilidad de acceder a una vivienda propia, dado el momento de crisis del sector inmobiliario por el que pasaba la Ciudad de Buenos Aires, sin dudas era necesario plantear alternativas de este tipo.



Mariana Riquelme

DNI 30.556.321

Bibliografía

Allidina, S. (27 de Junio de 2016). *https://www.raconteur.net*. Obtenido de https://www.raconteur.net/the-future-of-blockchain-in-8-charts/

Argentina, B. D. (20 de octubre de 2020). *Banco De La Nación Argentina*. Obtenido de Banco De La Nación Argentina: http://www.bcra.gob.ar/PublicacionesEstadisticas/Principales_variables.asp.

Ayacán, N. (14 de Febrero de 2020). *https://blog.ida.cl*. Obtenido de https://blog.ida.cl/experiencia-de-usuario/el-futuro-de-blockchain/

BCRA. (s.f.). Obtenido de http://www.bcra.gov.ar/publicacionesestadisticas/Principales_variables_datos.asp

BCRA. (2021). Obtenido de http://www.bcra.gov.ar/publicacionesestadisticas/Principales_variables_datos.asp

Bitcoin.com. (2018). Obtenido de https://www.bitcoin.com.mx/el-volumen-de-transacciones-de-bitcoin-se-acerca-de-nuevo-a-su-cumbre/

Buterin, V. (6 de mayo de 2014). *Ethereum fundation blog*. Obtenido de http://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Ciudad, G. D. (01 de octubre de 2020). *Gobierno De La Ciudad*. Obtenido de Gobierno De La Ciudad: https://www.buenosaires.gob.ar/noticias/informe-de-accesibilidad-la-vivienda-traves-del-credito-hipotecario-en-la-ciudad.

Corebi. (Agosto de 2019). *www.corebi.com.ar*. Obtenido de https://corebi.com.ar/blog/que-es-el-blockchain-y-porque-interesa-tanto-en-el-rubro-financiero/?lang=en

Deloitte. (8 de Octubre de 2017). *https://www2.deloitte.com*. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-dcfs-blockchain-in-cre-the-future-is-here.pdf

Ente Nacional de Comunicaciones. (2019). Obtenido de https://www.enacom.gob.ar/

INDEC. (15 de enero de 2020). *INDEC*. Obtenido de INDEC: https://www.indec.gob.ar/uploads/informesdeprensa/salarios_01_21DE49B4DF29.pdf.

Inmobiliario, R. (13 de julio de 2009). *Reporte Inmobiliario*. Obtenido de Reporte Inmobiliario: https://www.reporteinmobiliario.com/nuke/article1436-que-valora-el-comprador-de-una-vivienda-hoy.html

Iprofesional. (20 de diciembre de 2020). *https://www.iprofesional.com*. Obtenido de https://www.iprofesional.com/negocios/330198-mercado-inmobiliario-mas-inmuebles-en-venta-y-menos-alquileres

J. Leon Zhao, S. F. (2016). *Overview of business innovations and.*

Libre, M. (septiembre de 2018). *Mercado Libre*. Obtenido de Mercado Libre: https://ideas.mercadolibre.com/ar/inmuebles/gastos-de-escrituracion-cuales-son/

Martín, D. (31 de Octubre de 2019). *https://www.libertaddigital.com/*. Obtenido de https://www.libertaddigital.com/ciencia-tecnologia/internet/2019-10-31/blockchain-tecnologia-futuro-1276647203/

Maure Inmobiliaria. (2020). Obtenido de https://maureinmobiliaria.com/el-mercado-inmobiliario-en-los-medios/valor-m2-historico-caba/

Maure Inmobiliaria. (2021). Obtenido de https://maureinmobiliaria.com/estadisticas-mercado-inmobiliario/

Maximiliano Gómez Aguirre, Camara Argentina de la Construcción. (21 de diciembre de 2020). *http://biblioteca.camarco.org.ar*. Obtenido de http://biblioteca.camarco.org.ar/libro-16/

Medios Cifras. (20 de febrero de 2020). *https://www.cifrasonline.com.ar*. Obtenido de https://www.cifrasonline.com.ar/credito-hipotecario-uva-como-impacta-el-dolar-y-la-proyeccion-de-paritarias/

MiEthereum. (08 de Mayo de 2018). *https://www.miethereum.com*. Obtenido de https://www.miethereum.com/smart-contracts/dapps/#toc17

miethereum.com. (2020). Obtenido de https://www.miethereum.com/blockchain/

Nakamoto, S. (2009). *Bitcoin.org*. Obtenido de https://bitcoin.org/bitcoin.pdf

Oroyfinanzas. (15 de octubre de 2015). *Oro y finanzas - diferencias entre cadenas de blockchain públicas y privadas*. Obtenido de https://www.oroyfinanzas.com/2015/10/diferencias-cadenas-bloques-blockchain-publicas-privadas/

Ortín, A. (07 de Noviembre de 2019). *www.lavanguardia.com*. Obtenido de https://www.lavanguardia.com/economia/20191023/471161613685/blockchain-el-camino-de-la-interconexion-de-futuro.html#:~:text=La%20previsi%C3%B3n%20que%20hace%20la,tan%20solo%20cinco%20a%C3%B1os%20despu%C3%A9s.

Pérez, J. L. (2016). La economía de Blockchain: Los modelos de negocios de la nueva web. En J. L. Pérez, *La economía de Blockchain: Los modelos de negocios de la nueva web*.

Preukschat, A. (2017). Blockchain, la revolución industrial de internet. En A. Preukschat, *Blockchain, la revolución industrial de internet.* Barcelona: Grupo Planeta.

Reporte Inmobiliario. (2021). Obtenido de https://www.reporteinmobiliario.com/nuke/article141-indices-inmobiliarios.html

Tapscott, D. T. (2016). Blockchain Revolution. En D. T. Tapscott, *Blockchain Revolution.* Nueva York: Penguin Random House.

Vanci, M. (31 de diciembre de 2020). *Criptonoticias*. Obtenido de https://www.criptonoticias.com/tecnologia/tamano-blockchain-bitcoin-aumento-25-en-2020/

We are social. (2019). *https://wearesocial.com*. Obtenido de https://wearesocial.com/global-digital-report-2019

Wikipedia. (06 de septiembre de 2014). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/PRO.CRE.AR

Wikipedia. (07 de junio de 2017). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Unidad_Valor_Adquisitivo.

Wikipedia. (21 de 12 de 2020). *https://en.wikipedia.org*. Obtenido de https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

Wikipedia. (5 de Diciembre de 2020). *https://es.wikipedia.org*. Obtenido de https://es.wikipedia.org/wiki/Brecha_digital

Wikipedia. (29 de Noviembre de 2020). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/Historia_de_bitcoin

Zorrilla, J. P. (23 de mayo de 2019). *El analista económico y financiera*. Obtenido de https://elanalistaeconomicofinanciero.blogspot.com/2019/05/grafico-de-financiacion-de-capital.html

Anexos

Anexo 1 - Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario

Por Satoshi Nakamoto

Abstracto

Una versión puramente electrónica de efectivo permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera. Firmas digitales proveen parte de la solución, pero los beneficios principales se pierden si existe un tercero confiable para prevenir el doble-gasto. Proponemos una solución al problema del doble gasto utilizando una red usuario-a-usuario. La red coloca estampas de tiempo a las transacciones al crear un hash de estas en una cadena continua de pruebas de trabajo basadas en hashes, formando un registro que no puede ser cambiado sin volver a recrear la prueba de trabajo. La cadena más larga no solo sirve como la prueba de la secuencia de los eventos testificados, sino como prueba de que vino del gremio de poder de procesamiento de CPU más grande. Siempre que la mayoría del poder de procesamiento de CPU esté bajo el control de los nodos que no cooperan para atacar la red, estos generarán la cadena más larga y le llevarán la ventaja a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes son enviados sobre la base de mejor esfuerzo, y los nodos pueden irse y volver a unirse a la red como les parezca, aceptando la cadena de prueba de trabajo de lo que sucedió durante su ausencia.

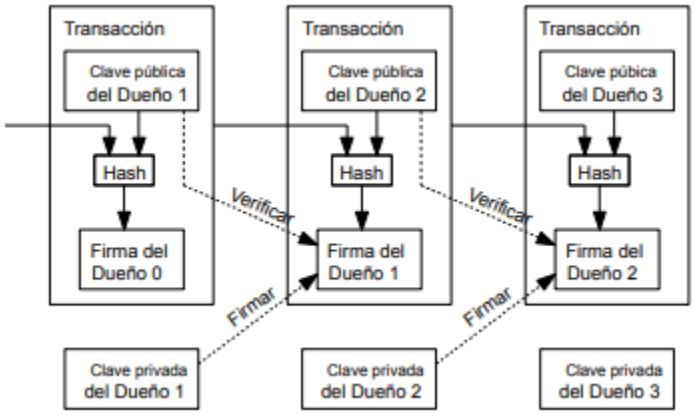
Introducción

El comercio en el Internet ha venido a depender exclusivamente de instituciones financieras las cuales sirven como terceros confiables para el procesamiento de pagos electrónicos. Mientras que el sistema funciona lo suficientemente bien para la mayoría de las transacciones, aún sufre de las debilidades inherentes del modelo basado en confianza. Transacciones completamente no reversibles no son realmente posibles, dado que las instituciones financieras no pueden evitar mediar disputas. El costo de la mediación incrementa costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de pequeñas transacciones casuales, y hay un costo más amplio en la pérdida de la habilidad de hacer pagos no-reversibles por servicios no-reversibles. Con la posibilidad de revertir, la necesidad de confianza se expande. Los comerciantes deben tener cuidado de sus clientes, molestándolos, pidiendo más información de la que se necesitaría de otro modo. Un cierto porcentaje de fraude es aceptable como inevitable. Estos costos e incertidumbres de pagos pueden ser evitadas en persona utilizando dinero físico, pero no existe un mecanismo para hacer pagos por un canal de comunicación sin un tercero confiable. Lo que se

necesita es un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas en realizar transacciones directamente sin la necesidad de un tercero confiable. Las transacciones que son computacionalmente poco factibles de revertir protegerían a los vendedores de fraude, y mecanismos de depósitos de fideicomisos de rutina podrían ser fácilmente implementados para proteger a los compradores. En este trabajo, proponemos una solución al problema del doble-gasto utilizando un servidor de marcas de tiempo usuario-a-usuario distribuido para generar una prueba computacional del orden cronológico de las transacciones. El sistema es seguro mientras que nodos honestos controlen colectivamente más poder de procesamiento (CPU) que cualquier grupo de nodos atacantes en cooperación.

Transacciones

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

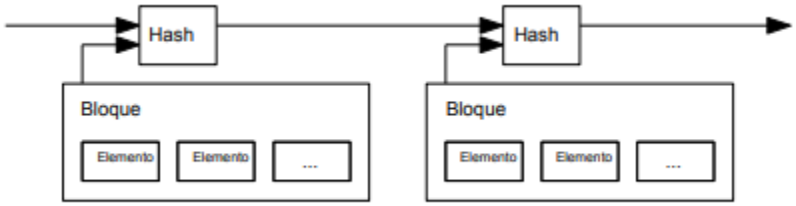


El problema claro es que el beneficiario no puede verificar si uno de los dueños no se hizo un doble-gasto de la moneda. Una solución común es introducir una autoridad central confiable, o casa de moneda, que revisa cada si cada transacción tiene doble-gasto. Después de cada transacción, la moneda debe ser regresada a la casa de moneda para generar una nueva moneda, y solo las monedas generadas directamente de la casa de moneda son las que se confían de no tener doble-gasto. El problema con esta solución es que el destino del sistema monetario entero depende de la compañía que gestiona la casa de moneda, con cada transacción teniendo que pasar por ellos, tal como un banco. Necesitamos una forma para que el beneficiario pueda saber que los dueños previos no firmaron ningunas transacciones más tempranas. Para nuestros propósitos, la transacción más temprana es la que cuenta, así que no nos importan otros intentos de doble-gasto más tarde. La única forma de confirmar la ausencia de una transacción es estando al tanto de todas las

transacciones. En el modelo de la casa de moneda, la casa de moneda estaba al tanto de todas las transacciones y esta decidiría cuales llegaban primero. Para lograr esto sin un tercero confiable, las transacciones deben ser anunciadas públicamente [1], y necesitamos un sistema de participantes que estén de acuerdo con una historia única del orden en que estas fueron recibidas. El beneficiario necesita prueba de que, a la hora de cada transacción, la mayoría de los nodos estuvieron de acuerdo que esta fue la primera que se recibió.

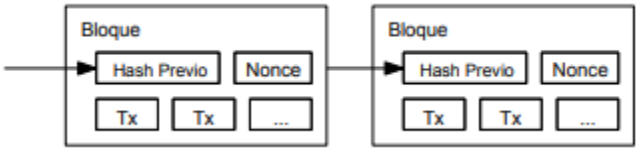
Servidor de marcas de tiempo

La solución que proponemos comienza con un servidor de marcas de tiempo. Un servidor de marcas de tiempo funciona al tomar un hash de un bloque de elementos a ser fechados y publicando ampliamente el hash, tal como en un periódico, o una publicación Usenet [2-5]. La marca de tiempo prueba que la data debe haber existido en el tiempo, obviamente, para meterse dentro del hash. Cada marca de tiempo incluye la marca de tiempo previa en su hash, formando una cadena, con cada marca de tiempo adicional reforzando las anteriores a esa.



Prueba de trabajo

Para implementar un servidor de marcas de tiempo en una base usuario-a-usuario, necesitaremos utilizar un sistema de prueba-de-trabajo similar al Hashcash de Adam Back [6], en vez de un periódico o una publicación en Usenet. La prueba-de-trabajo envuelve la exploración de un valor que, al calcular un hash, tal como SHA-256, el hash empiece con un número de bits en cero. El trabajo promedio requerido es exponencial en el número de bits puestos en cero requeridos y puede ser verificado ejecutando un solo hash. Para nuestra red de marcas de tiempo, implementamos la prueba-de-trabajo incrementando un nonce en el bloque hasta que un valor es encontrado que del número requerido de bits en cero para el hash del bloque. Una vez que el esfuerzo de CPU se ha gastado para satisfacer la prueba de trabajo, el bloque no puede ser cambiado sin rehacer todo el trabajo. A medida que más bloques son encadenados después de este, el trabajo para cambiar el bloque incluiría rehacer todos los bloques después de este.



La prueba-de-trabajo también resuelve el problema de determinar la representación en cuanto a decisión por mayoría. Si la mayoría fuese basada en un voto por dirección IP, podría ser subvertida por alguien capaz de asignar muchos IPs. Prueba-de-trabajo es esencialmente un CPU un voto. La decisión de la mayoría es representada por la cadena más larga, la cual tiene la prueba-de-trabajo de mayor esfuerzo invertido en ella. Si la mayoría del poder de CPU es controlada por nodos honestos, la cadena honesta crecerá más rápido y pasará cualquier cadena que esté compitiendo. Para modificar un bloque en el pasado, un atacante tendría que rehacer la prueba-de-trabajo del bloque y de todos los bloques después y luego alcanzar y pasar el trabajo de los nodos honestos. Luego demostraremos que la probabilidad de un atacante más lento de alcanzar disminuye exponencialmente a medida que bloques subsecuentes son añadidos. Para compensar por el incremento de velocidad de hardware y en el interés variante de corre nodos en el tiempo, la dificultad de la prueba-de-trabajo es determinada por una media móvil dirigida a un número promedio de bloques por hora. Si estos se generan muy rápido, la dificultad incrementa.

La Red

Los pasos para gestionar la red son como sigue:

1) Transacciones nuevas son emitidas a todos los nodos.
2) Cada nodo recolecta nuevas transacciones en un bloque.
3) Cada nodo trabaja en encontrar una prueba-de-trabajo difícil para su bloque.
4) Cuando un nodo encuentra una prueba-de-trabajo, emite el bloque a todos los nodos.
5) Los nodos aceptan el bloque si todas las transacciones en el bloque son válidas y no se han gastado ya.
6) Los nodos expresan su aceptación del bloque al trabajar en crear el próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash previo.

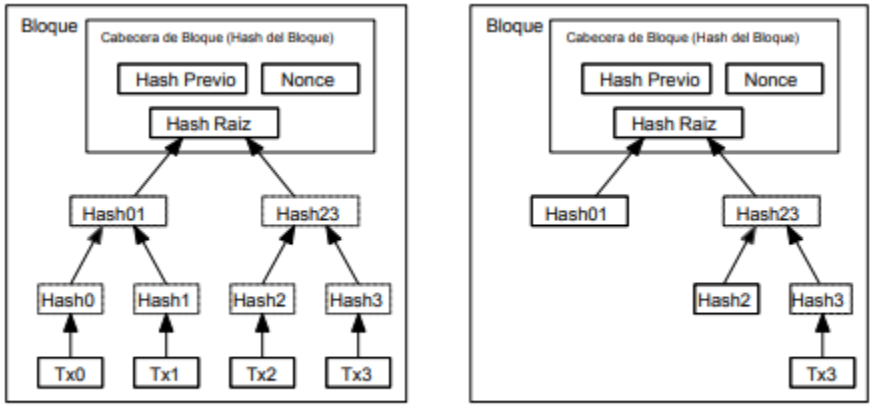
Los nodos siempre consideran la cadena más larga como la correcta y empiezan a trabajar en extenderla. Si dos nodos emiten versiones diferentes del próximo bloque simultáneamente, algunos nodos puede que reciban uno o el otro primero. En ese caso, trabajan en el primero que reciban, pero guardan la otra rama en caso de que esta se vuelva más larga. El empate se rompe cuando la próxima prueba-de-trabajo es encontrada y una rama se vuelve más larga; los nodos que estaban trabajando en la otra rama luego se cambian a la más larga. 3 Bloque Hash Previo Nonce Tx ...

Bloque Hash Previo Nonce Tx ... Las emisiones de nuevas transacciones no necesariamente necesitan llegar a todos los nodos. Tanto estas lleguen a muchos nodos, entrarán a un bloque antes de que pase mucho tiempo. Las emisiones de bloques también son tolerantes a mensajes perdidos. Si un nodo no recibe un bloque, lo va a pedir cuando reciba el próximo bloque y se dé cuenta que se perdió uno.
Incentivo

Por convención, la primera transacción en el bloque es una transacción especial que comienza una moneda nueva cuyo dueño es el creador del bloque. Esto agrega un incentivo para que los nodos apoyen a la red, y provee una forma inicial de distribuir monedas en circulación, dado que no hay una autoridad para crearlas. Esta adición estable de una cantidad constante de monedas nuevas es análoga a mineros de oro gastando recursos para agregar oro a la circulación. En nuestro caso, es el tiempo del CPU y la electricidad que se gasta. El incentivo también puede ser fundado con costos de transacción. Si el valor de salida de una transacción es menor que la entrada, la diferencia es una tarifa de transacción que se le añade al valor de incentivo del bloque que contiene la transacción. Una vez que un número predeterminado de monedas han entrado en circulación, el incentivo puede transicionar enteramente a tarifas de transacción y ser completamente libre de inflación. El incentivo puede ayudar a animar a los nodos a mantenerse honestos. Si un atacante egoísta es capaz de reunir más potencia de CPU que todos los nodos honestos, este tendría que elegir entre utilizarla para defraudar a la gente robando sus pagos de vuelta, o en utilizarla para generar monedas nuevas. Debería encontrar más rentable jugar por las reglas, tales reglas lo favorecen a él con más monedas que a todos los demás combinados, que socavar el sistema y la validez de su propia riqueza.

Reclamando Espacio en Disco

Una vez que la última transacción en una moneda es enterrada bajo suficientes bloques, las transacciones gastadas antes de estas pueden ser descartadas para ahorrar espacio en disco. Para facilitar esto sin romper el hash del bloque, las transacciones se les comprueba en un árbol Merkle [7] [2] [5], con la única raíz incluida en el hash el bloque. Los bloques viejos pueden ser compactados al sacar ramas del árbol. Los hashes interiores no necesitan ser guardados.



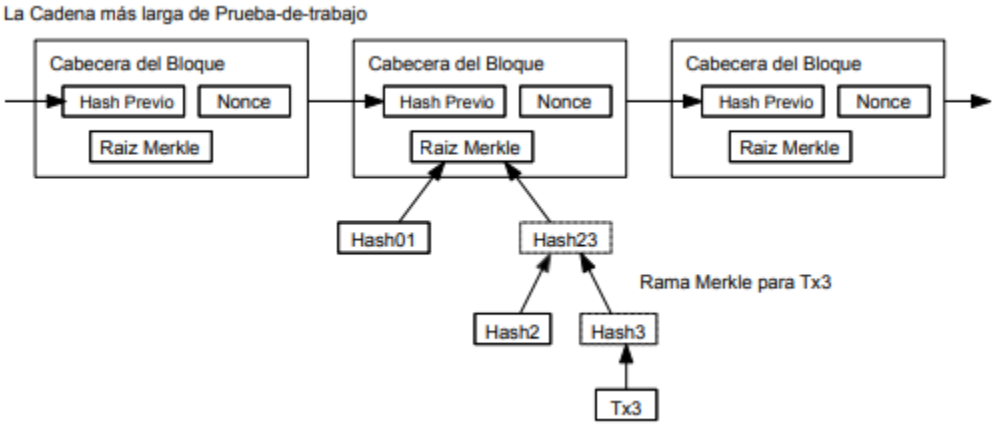
Transacciones *Hasheadas* en un árbol Merkle

Después de podar Tx0-2 del Bloque

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

Verificación de Pagos

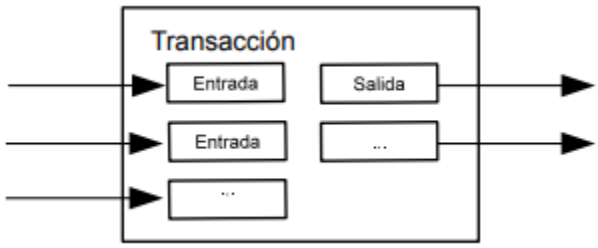
Simplificada Es posible verificar pagos sin correr un nodo de red completo. Un usuario solo necesita mantener una copia de las cabeceras de los bloques de la cadena más larga de prueba-de-trabajo, la cual puede obtener haciendo una búsqueda en los nodos de red hasta que esté convencido que tenga la cadena más larga, y obtenga la rama Merkle que enlaza la transacción al bloque en que ha sido fechado. No puede verificar la transacción por sí mismo, pero al enlazarla a un lugar en la cadena, ahora puede ver que un nodo de la red la ha aceptado y los bloques añadidos después confirman aún más que la red lo ha aceptado.



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

Combinando y Dividiendo Valor

Aunque sería posible manipular monedas individualmente, sería difícil de manejar el hacer una transacción por cada centavo en una transferencia. Para permitir que el valor se divida y se combine, las transacciones contienen múltiples entradas y salidas. Normalmente habrá o una sola entrada de una transacción previa más grande o múltiples entradas combinando cantidades más pequeñas, y al menos dos salidas: una para el pago, y una para devolver el cambio, si es que hay algún cambio, de vuelta al emisor.

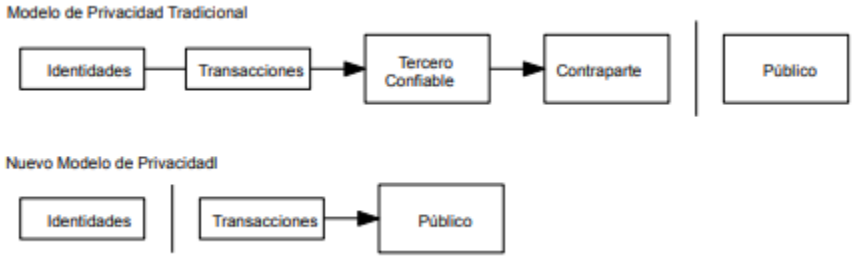


Debe ser notado que donde una transacción depende de varias transacciones, y esas transacciones dependen en muchas más, no hay ningún problema. Nunca existe la necesidad de extraer una copia completa de la transacción por si sola de la historia de transacciones.

Privacidad

El modelo bancario tradicional logra un nivel de privacidad al limitar el acceso a la información de las partes envueltas y del tercero confiado. La necesidad de anunciar todas las transacciones públicamente se opone a este método, pero la privacidad aún puede ser mantenida al romper el flujo de la información en otro lugar: al mantener las claves públicas anónimas. El público puede ver que alguien está enviando una cantidad a otra persona, pero sin información que relacione la transacción a ninguna persona. Esto es similar al nivel de información mostrado por las bolsas de valores, donde

el tiempo y el tamaño de las transacciones individuales, la “cinta”, es público, pero sin decir quiénes son las partes.



Como un cortafuegos adicional, un par nuevo de claves debe ser utilizado para cada transacción de modo que puedan ser asociadas a un dueño en común. Algún tipo de asociación es inevitable con transacciones de múltiples entradas, las cuales pueden revelar que sus entradas fueron apropiadas por el mismo dueño. El riesgo está en que, si el dueño de una clave es revelado, el enlazado podría revelar otras transacciones que pertenecieron al mismo dueño.

Cálculos

Consideramos el escenario en el que un atacante intenta generar una cadena alterna más rápido que la cadena honesta. Aún si esto es logrado, esto no abre el sistema a cambios arbitrarios, tal como crear valor del aire o tomar dinero que nunca le perteneció al atacante. Los nodos no aceptarían una transacción inválida como pago, y los nodos honestos nunca aceptará un bloque que las contenga. Un atacante puede únicamente intentar cambiar solo una de sus propias transacciones para retomar dinero que ha gastado recientemente. La carrera entre una cadena honesta y la cadena de un atacante puede ser caracterizada como una Caminata Aleatoria Binomial. El evento de éxito es la cadena honesta siendo extendida por un bloque, incrementar esta ventaja por +1, y el evento de fracaso es la cadena del atacante siendo extendida por un bloque reduciendo la distancia por -1. La probabilidad de que un atacante pueda alcanzar desde un déficit dado es análoga al problema de la Ruina del Apostador. Supóngase que un apostador con crédito ilimitado empieza en un déficit y juega potencialmente un número infinito de intentos para intentar llegar a un punto de equilibrio. Podemos calcular la probabilidad de que llegase al punto de equilibrio, o que un atacante llegue a alcanzar a la cadena honesta, como sigue [8]:

p = probabilidad de que un nodo honesto encuentre el próximo bloque
q = probabilidad de que el atacante encuentre el próximo bloque
q_z = probabilidad de que el atacante llegue a alcanzar desde z bloques atrás

$$q_z=\begin{cases}1 & if\ p\leq q\\ (q/p)^z & if\ p>q\end{cases}$$

Dada nuestra hipótesis de que p > q, la probabilidad cae exponencialmente mientras que el número de bloques el cual el atacante debe alcanzar incrementa. Con las probabilidades en contra, si no hace una estocada afortunada desde el principio, sus chances se vuelven extremadamente pequeños a medida que se queda más atrás. Ahora consideramos cuánto necesita esperar el recipiente de una nueva transacción antes de tener la certeza suficiente de que el emisor no puede cambiar la transacción. Asumimos que el emisor es un atacante el cual quiere hacerle creer al recipiente que le pagó durante un rato, luego cambiar la transacción para pagarse de vuelta a sí mismo una vez que ha pasado un tiempo. El receptor será alertado cuando esto suceda, pero el emisor espera que sea demasiado tarde. El receptor genera un nuevo par de claves y entrega la clave pública al emisor poco después de hacer la firma. Esto previene que el emisor prepare una cadena de bloques antes de tiempo al trabajar continuamente hasta que tenga la suerte de adelantarse lo suficiente, y luego ejecutar la transacción en ese momento. Una vez que la transacción es enviada, el emisor deshonesto empieza a trabajar en secreto en una cadena paralela que contiene una versión alterna de su transacción. El recipiente espera a que la transacción sea añadida al bloque y z bloques han sido enlazados después de la transacción. El no necesita saber la cantidad exacta de progreso que al atacante ha logrado, pero asumiendo que los bloques honestos se tardaron el promedio esperado por bloque, el progreso potencial del atacante será una distribución de Poisson con un valor esperado:

$$\lambda=z\frac{q}{p}$$

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

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{cases}(q/p)^{(z-k)} & if\ k\leq z\\ 1 & if\ k>z\end{cases}$$

Reorganizamos para evitar la suma de la cola infinita de la distribución:

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

Convertimos a código en C:

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

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

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Resolvemos para P menor que 0.1%:

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

Conclusión

Hemos propuesto un sistema para transacciones electrónicas sin depender en confianza. Comenzamos con el marco habitual de monedas hechas de firmas digitales, el cual provee un control fuerte de propiedad, pero es incompleto sino existe una forma de prevenir doble-gasto. Para

solucionar esto, hemos propuesto una red usuario-a-usuario que utiliza prueba-de-trabajo para registrar una historia pública de transacciones la cual rápidamente se convierte impráctica computacionalmente para que un atacante pueda cambiar si nodos honestos controlan la mayoría del poder de CPU. La red es robusta en su simplicidad no estructurada. Los nodos pueden trabajar todos al mismo tiempo con poca coordinación. No necesitan ser identificados, dado que los mensajes no son enrutados a ningún lugar en particular y solo necesitan ser entregados bajo la base de un mejor esfuerzo. Los nodos pueden irse y volver a la red a voluntad, aceptando la cadena de prueba-de-trabajo como prueba de lo que sucedió mientras estuvieron ausentes. Votan con su poder de CPU, expresando su aceptación de los bloques válidos al trabajar extendiéndose y rechazando bloques inválidos al refutar trabajar en ellos. Cualquier reglas necesarias e incentivos se pueden hacer cumplir con este mecanismo de consenso.

Referencias

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.