



COMUNICACIONES

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES



Transformación digital blockchain: cómo adentrarse a la Web 3.0

Cesar Jaime Montiel Moctezuma
Miguel Gastón Cedillo Campos
Marisol Barrón Bastida
Bernardo Hernández Sánchez

Publicación Técnica No. 731
Querétaro, México
2023

ISSN 0188-7297

Esta investigación fue realizada en la Coordinación de Transporte Integrado y Logística del Instituto Mexicano del Transporte, por el Dr. Cesar Jaime Montiel Moctezuma, el Dr. Miguel Gastón Cedillo Campos, la Mtra. Marisol Barrón Bastida y el Mtro. Bernardo Hernández Sánchez.

Esta investigación es el producto final del proyecto de investigación interna TI 06/22 Estudio Exploratorio sobre la evolución de la Web 3.0 como transformación digital de las cadenas de suministro.

Así mismo, se agradece el apoyo brindado por el Laboratorio Nacional en Sistemas de Transporte y Logística (SiT-LOG Lab), cuyas capacidades tecnológicas facilitaron el buen desarrollo de este proyecto.

Tabla de Contenido

	Página
Índice de Figuras.....	v
Sinopsis.....	vii
Abstract.....	ix
Introducción.....	1
1. Antecedentes.....	3
2. Web 3.0.....	9
2.1 Tecnologías.....	10
2.1.1 Blockchain.....	10
2.1.2 Inteligencia Artificial.....	11
2.1.3 Web Semántica.....	12
2.2 Plataformas existentes.....	14
2.2.1 Redes Sociales.....	15
2.2.2 Servicios de Intercambio.....	15
2.2.3 Mensajería.....	16
2.2.4 Almacenamiento.....	16
2.2.5 Seguros e información bancaria.....	16
2.2.6 Streaming.....	17
2.2.7 Trabajo Remoto.....	17
2.2.8 Navegación.....	18
3. Implementación de la Web 3.0.....	19
3.1 Blockchain Stack 3.0.....	19
3.1.1 Capa de Aplicación.....	20
3.1.2 Capa de Servicios y Componentes Opcionales.....	21

3.1.3	Capa de Protocolo.....	22
3.1.4	Capa de Red	24
3.1.5	Capa de Infraestructura.....	25
3.2	Metodología de Implementación.....	26
	Conclusiones.....	33
	Bibliografía	35

Índice de Figuras

	Página
Figura 1.1 Usuarios de Internet en el Mundo 2022	5
Figura 1.2 Tasa de Penetración de Usuarios en Internet 2022	5
Figura 1.3 Conectividad gráfica de Internet 2022.....	6
Figura 2.1 Red de <i>Blockchain</i> 2022.....	11
Figura 2.2 Campos de Investigación IA.....	12
Figura 2.3 Capas de la Arquitectura de la Web Semántica	13
Figura 3.1 Capas de la Arquitectura de Blockchain Stack.....	19
Figura 3.2 Arquitectura general Web 2.0.....	26
Figura 3.3 Código de un Contrato Inteligente en Solidity	28
Figura 3.4 Blockchain de Ethereum	28
Figura 3.5 Blockchain de Ethereum.....	29
Figura 3.6 Consulta y Almacenamiento dentro de Ethereum	30
Figura 3.7 Escalado de Aplicaciones en Ethereum	31

Sinopsis

En los últimos años, debido al auge de la migración digital causada por el aislamiento de la pandemia por COVID-19, se incrementó notablemente la implementación de nuevas tendencias tecnológicas. La Web 3.0, la generación de Internet en la cual nos encontramos actualmente, está muy ligada a estas nuevas tecnologías tales como Inteligencia Artificial, *blockchain*, Web Semántica, y la Realidad Mixta; y se enfoca principalmente en la descentralización. El entender cómo funciona la Web 3.0 da la posibilidad al desarrollo de nuevas aplicaciones descentralizadas que puedan resolver problemas de logística y cadena de suministro, y que contemplen las ventajas que estas tecnologías nos ofrecen. Esta investigación se enfoca en un análisis exploratorio de Web 3.0 y la identificación de nuevos sistemas, aplicaciones y/o servicios que han sido implementados para mejorar la toma de decisiones del sector logístico.

Abstract

In recent years, due to the rise of digital migration caused by the isolation of the COVID-19 pandemic, the implementation of new technological trends has increased significantly. Web 3.0, the generation of the Internet in which we currently find ourselves, is closely linked to these new technologies such as Artificial Intelligence, blockchain, Semantic Web, and Mixed Reality; and focuses mainly on decentralization. Understanding how Web 3.0 works gives the possibility to the development of new decentralized applications that can solve logistics and supply chain problems, and that contemplate the advantages that these technologies offer us. This research focuses on an exploratory analysis of Web 3.0 and the identification of new systems, applications and/or services that have been implemented to improve decision making in the logistics sector.

Introducción

Los problemas atraídos por el COVID-19 y las medidas sanitarias adoptadas por los países para reducir la cantidad de contagios, impactó directamente en la economía y en la sociedad de todo el mundo. Las cadenas de suministro y la logística fueron de las primeras áreas afectadas por la pandemia debido a que se detuvo el comercio internacional de manera drástica. De acuerdo a la Organización Internacional del Trabajo, todos los niveles de las cadenas de suministro, desde las industrias para la extracción de materia prima hasta aquellas que se dedican al ensamblaje, distribución y venta, fueron afectadas por los efectos económicos y sociales que provocó el COVID-19, y a pesar que existe una buena resiliencia por parte de los involucrados debido a los avances en las tecnologías, aún no han sido implementadas en todos los sectores.

Dentro de la evolución de las tecnologías podemos identificar el auge que ha tenido el *blockchain*, la cual se vio beneficiada debido a la aceleración de la era digital provocada por esta emergencia sanitaria, y gracias a la idea base de descentralización de información que utiliza esta tecnología, se comenzó a considerar una nueva era en la evolución de la Web: la Web 3.0.

Esta era emergente hace referencia a la nueva generación de Internet, donde los dispositivos se encuentran conectados en una red descentralizada en lugar de depender de servidores basados en bases de datos, tal y como funciona una parte de la arquitectura de *blockchain*, de hecho, las plataformas que utilizan esta tecnología serán la base para la evolución de la Web 3.0. Pero eso no es todo, la Web 3.0 también se apoya de otras tecnologías como lo son la Web semántica, inteligencia artificial, realidad aumentada, realidad virtual; y tiene características mejoradas de las versiones anteriores de la Web como lo son: gráficos 3D, redes descentralizadas (sin la necesidad de una autoridad), conectividad mejorada a través de metadatos semánticos y ubicuidad en la conectividad. Todo ello ha impulsado la mejora y desarrollo de un Internet más inteligente, con un enfoque en contenido personalizado para cada usuario.

Es crucial para los administradores y tomadores de decisiones de las cadenas de suministro que se encuentren actualizados con respecto a las tecnologías que se desarrollan a nivel mundial para seguir siendo

competitivos y mantener las operaciones lo más eficientes y actualizadas posible. Esta es la razón, de que en muchas industrias han implementado relativamente nuevos resultados, pero muy eficientes, de esta nueva etapa del Internet a través del involucramiento de sus operaciones logísticas en plataformas de *blockchain* y NFT's, o la migración de sus sistemas a nueva infraestructura de comunicaciones enfocada en la Organización Autónoma Descentralizada.

De acuerdo a las estrategias prioritarias del Programa Sectorial de Comunicaciones y Transportes 2020-2024 , específicamente la estrategia 3.4.1 "Identificar, analizar y experimentar tecnologías y herramientas de telecomunicaciones, radiodifusión e información para fomentar el desarrollo tecnológico de México", este proyecto pretende realizar un análisis exploratorio de como el Internet ha evolucionado en estos últimos años en el sector transporte y logístico, como se ha involucrado para optimizar sus operaciones, identificar las características y ventajas que la Web 3.0 traerá en los próximos años, y cuáles serían las capacidades necesarias para el desarrollo e implementación de aplicaciones distribuidas.

1. Antecedentes

Para poder entender la Web 3.0, es necesario conocer que es la Web y cómo ha evolucionado a lo largo de los años desde su aparición.

Para empezar, es necesario conocer el Internet, el cual puede representarse como una inmensa red de computadoras alrededor del mundo conectadas entre sí. Su origen se remonta a 1969 cuando se estableció la primera conexión de computadoras, conocida como ARPANET (*Advanced Research Projects Agency Network*), creada por el Departamento de Defensa de los Estados Unidos con el objetivo de conectar algunas universidades de ese país (Hafner & Lyon, 1996).

Años después, nació uno de los servicios con mayor éxito en Internet, conocido como *World Wide Web* (WWW) o la Web, la cual se representaría como una enorme colección de páginas y un conjunto de protocolos, que permiten la consulta remota de archivos que se transmiten por Internet. Aunque en muchas ocasiones Internet y la Web son confundidos como el mismo término, no es así. Como una analogía podríamos describir que el Internet es una red carretera, y la Web serían los vehículos que atraviesan esta red. La Web se desarrolló como un proyecto en el año de 1989 por Tim Berners-Lee y Robert Cailliau mientras trabajaban en la Organización Europea para la Investigación Nuclear, también conocida como Consejo Europeo para la Investigación Nuclear (CERN- *Conseil Européen pour la Recherche Nucléaire*) (Berners-Lee & Cailliau, 1990).

Después de que el proyecto de WWW comenzará a implementarse a nivel mundial, se comenzó a considerar la primera versión de esta intercomunicación llamada la Web 1.0. La característica principal de esta plataforma era la comunicación unidireccional. En esta primera generación de la Web solo se consideraba las actividades de búsqueda y lectura de contenido, es decir, los usuarios de las paginas no tenían la posibilidad de agregar contenido, y estas tareas solo se delegaban a los expertos en sistemas. Principalmente se utilizaba para la presentación de sitios en los cuales las organizaciones mostraban información estática y limitada para los usuarios finales, con el objetivo de que estos se interesarán en los productos o servicios que ofrecían, y más tarde, se comunicarán con la organización (Berners-Lee, 1998). Los protocolos principales fueron el Protocolo de Transferencia de Hipertexto (*Hypertext*

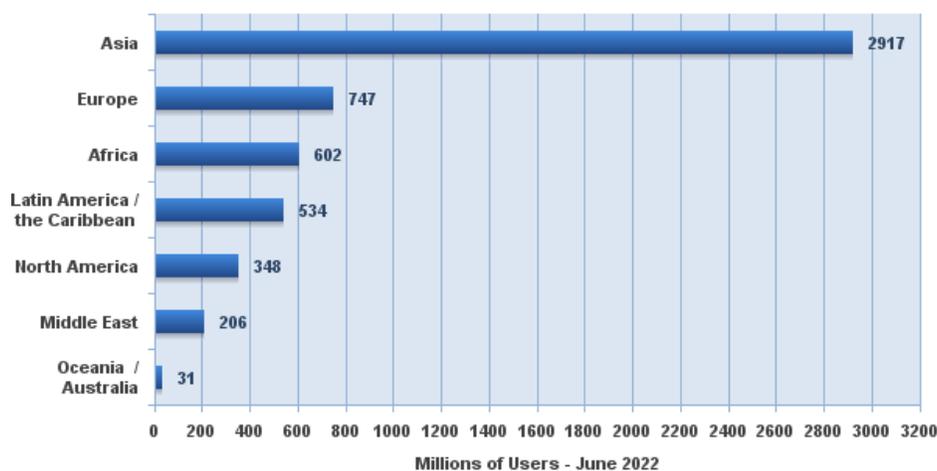
Transfer Protocol - HTTP), el Lenguaje de Marcado de Hipertexto (*HyperText Markup Language* - HTML) y el Identificador de Recursos Uniforme (*Uniform Resource Identifier* - URI).

Posteriormente, con la evolución de las actividades y el contenido digital, se desarrolló una segunda fase en la Web, llamada Web 2.0. Esta generación se enfocaba en la interactividad y los usuarios que utilizaban la Web, es decir, las nuevas plataformas tenían un enfoque social y colaborativo, en las cuales, los usuarios tenían la oportunidad de crear contenidos que compartían con otros usuarios (O'Reilly, 2005). Las aplicaciones desarrolladas eran interfaces interactivas, en las cuales los usuarios podían escribir datos además de leerlos (Aghaei, 2012). En la Web 2.0 se puede identificar claramente a través de las aplicaciones de redes sociales como Facebook, Instagram, YouTube o Twitter; simplemente todo comenzó a estar en línea y la Web comenzaba a centrarse en las personas o comunidades con ideologías similares (Pérez Salazar, 2011). Aquí se pueden identificar las mejoras a través del uso de tecnologías, como por ejemplo Ajax, para hacer dinámicas las páginas que se mostraban. En este punto, se comienza a identificar la diferencia entre aplicaciones web y páginas web. Entre algunos de los servicios que aparecieron en esta generación se pueden identificar los blogs (Mallory, 2006), wikis (Microsoft, 2018), *mashups*¹ (Guo et al., 2010), RSS (*Really Simple Syndication*)² (Instituto Nacional de Estadística y Geografía [INEGI], 2022), redes sociales, entre otros. La Web 2.0 también incluyó un cambio importante en el uso de Internet, debido a que comenzó la sobrecarga de información por el incremento radical de usuarios de millones a miles de millones de usuarios a la vez.

Internet ha crecido de manera exponencial, las tecnologías siguen impactando de forma acelerada las operaciones en muchos ámbitos, y continúan sustituyendo y optimizando sistemas que con el paso del tiempo se vuelven obsoletos. En el último mes se estimaba aproximadamente 5,385 millones de usuarios conectados en Internet, distribuidos por regiones del mundo tal como se muestra en la Figura 1.1

¹ Son páginas o aplicaciones web que combinan información y servicios de múltiples fuentes en la Web a través del uso de las API's de otras aplicaciones web.

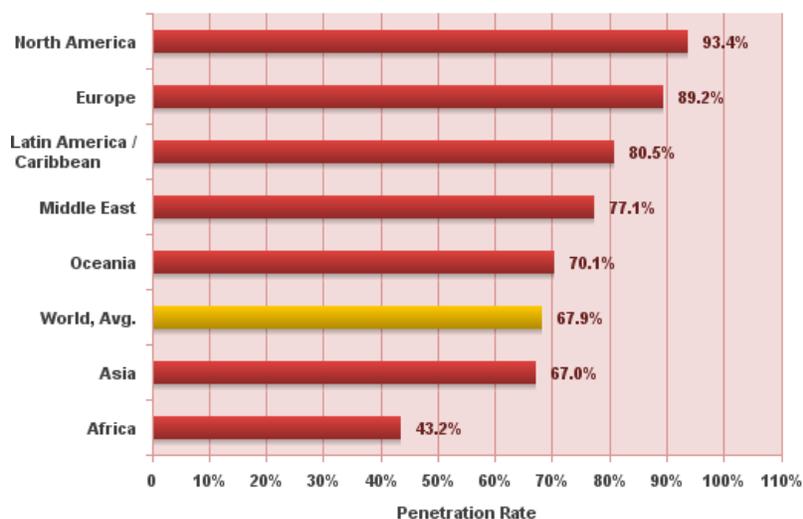
² Es un formato XML para distribuir contenido en la web, utilizado principalmente para la difusión e información a usuarios que están suscritos a la fuente de contenidos.



Fuente: Obtenido de Internet World Stats ©2022 (Miniwatts Marketing Group, 2022)

Figura 1.1 Usuarios de Internet en el Mundo 2022

Por otro lado, no tienen la misma tasa de penetración en todas las áreas a nivel mundial, donde se puede identificar una mayor cantidad de usuarios por población en el área de Norteamérica, tal como se observa en la Figura 1.2



Fuente: Obtenido de Internet World Stats ©2022 (Miniwatts Marketing Group, 2022)

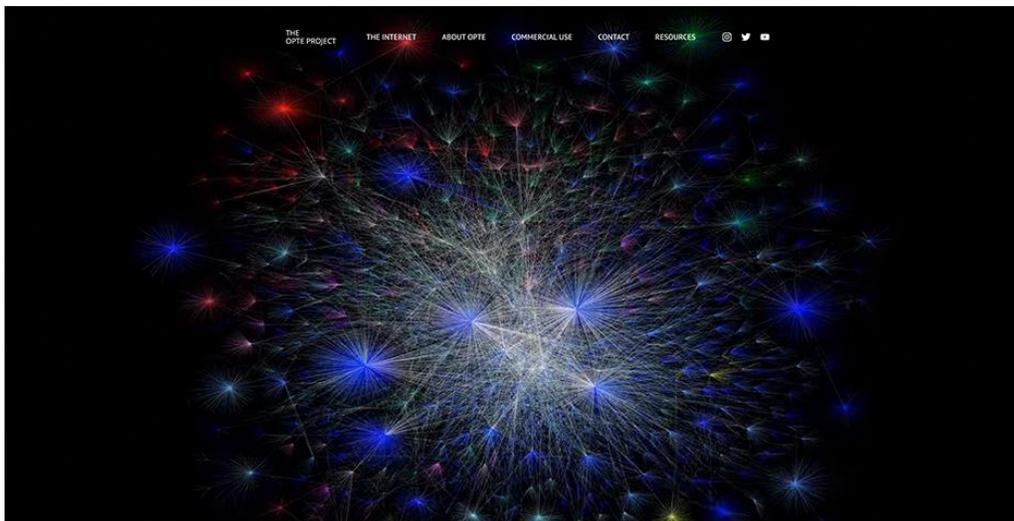
Figura 1.2 Tasa de Penetración de Usuarios en Internet 2022

Para visualizar el crecimiento de Internet desde un enfoque informático, se puede identificar a través del Registro de Internet Regional (Regional Internet Registry - RIR), donde se almacena la información de las IP's de cada una de las regiones en el mundo. Actualmente se cuenta solo con 5 RIR's a nivel mundial:

- Servidores de África (AFRINIC – African Network Information Center) (Regional Internet Registry for Africa, 2022),

- Servidores que contemplan Antártica, Canadá y Estados Unidos (ARIN – American Registry for Internet Numbers) (American Registry for Internet Numbers, 2022),
- Servidores Oceanía, del Sur y Este de Asia Asia (APNIC - Pacific Network Information Centre) (Pacific Network Information Centre, 2022) (APNIC, 2022),
- Servidores que registran la información de Latinoamérica y países del Caribe (LACNIC - Latin America and Caribbean Network Coordination Centre) (Registro de Direcciones IP en Latinoamerica, 2022),
- Servidores con información de Europa, Rusia, del Centro y Oeste de Asia (RIPE NCC - Réseaux IP Européens Network Coordination Centre) (Network Coordination Centre, 2022).

En la Figura 1.3 se puede observar la evolución de la conectividad de Internet en el mundo, cada color representa un RIR diferente, ARIN – Azul, RIPE – Verde, APNIC – Rojo, LANIC – Morado, AFRINIC – Amarillo, además, se incluye un color café que representa las redes del Departamento de Defensa de EUA. Cada nodo dentro de la Red representa una IP a nivel mundial, y las líneas que conectan dichos nodos representan la latencia³ existente.



Fuente: Obtenido de The OPTE Project ©2022 (Barrett Lyon, 2022)

Figura 1.3 Conectividad gráfica de Internet 2022

³ La latencia hace referencia a la descripción del tiempo total que tarda un paquete de datos (información) en viajar de un nodo origen a un nodo destino.

La Web 1.0 fue el primer escenario y el servicio más importante que definiría la evolución de la conectividad en Internet; la Web 2.0 aprovecha la inteligencia colectiva de los usuarios que interactúan en esta red; y actualmente, la Web 3.0 representa a la Web Semántica, la cual será explicada en el siguiente capítulo.

Hay que recordar que la Web no solo es un conjunto de páginas estáticas o dinámicas que describen algo en el mundo, sino que, la Web es el comportamiento del mundo, personas interactuando con computadoras para generar información, la cual es capturada y procesada por sistemas para mejorar su comunicación. Por lo tanto, las versiones de Web 1.0, 2.0 y 3.0, son ideas abstractas que tratan de agrupar características de estos comportamientos a través de diferentes tecnologías y protocolos, y que describen estos fenómenos de comunicación y colaboración entre computadoras y personas.

2. Web 3.0

La generación de Internet en la cual nos encontramos actualmente es llamada Web 3.0. Aunque, aún continua en desarrollo y no está establecida completamente en todo el mundo incluyendo las definiciones, ya existe una idea que soporta la definición más actual: la descentralización (Zur et al., 2021).

Tim Bernes-Lee, considerado como uno de los padres del internet, en la apertura de la 18va Conferencia Mundial de la WWW (SIGWEB & ACM, 2009) en el 2009, comentó la apuesta que tiene en la mejora de Internet a través de redes sociales abiertas que mejoren las posibilidades de interactuar a los usuarios, enfocándose en lo relativo al tratamiento de los datos que albergan y no en el funcionamiento de dichos servicios. En esta conferencia también se comentaba ya de la evolución del Internet con la tercera generación, y en ese momento se mantenía como una idea de que la Web 3.0 sería la Web 2.0 pero sin barreras. La idea original de Tim Bernes-Lee para la Web 3.0 fue la definición de una Web Semántica, definiendo la base de cómo datos en Internet pueden ser leídos e interpretados por máquinas, es decir, incluir datos con un formato fácilmente procesado por las computadoras sin intervención humana, mientras que se asegura que no se pierda el significado semántico de la información (Marchiori, 2004). Para identificar de mejor manera las diferencias entre las generaciones de la Web se puede observar la siguiente tabla.

Tabla 2.1 Comparación entre generaciones de la Web

Operación	Web 1.0	Web 2.0	Web 3.0
Origen (Tiempo)	1990-2000	2000-2010	2010-Actual
Intercambio de Información	Unidireccional	Bidireccional	Bidireccional
Interacciones	Solo lectura	Lectura y escritura	Lectura, escritura y ejecución
Sitios Web	Estáticos	Dinámicos	Semánticos
Estructura de la Red	Centralizada	Centralizada	Descentralizada
Capacidad de Usuarios	Millones	Miles de millones	Billones
Contenido	Administrador por expertos	Gestionado por cualquier usuario	Transmisiones personalizadas
Motores de Búsqueda	Nombres de dominio	Optimización para motores de búsqueda (SEO)	Motores de búsqueda basados en IA
Ejemplos	Envío de imágenes por email	Administración de imágenes en redes sociales	Gestión de imágenes como criptoactivos

Fuente: Elaboración propia con base en (Anwar, 2018; Chong, 2019; Pinto, 2019; Rodriguez, 2018)

Actualmente, aún no se define formalmente lo que es Web 3.0, pero con el auge de nuevas tecnologías, como inteligencia artificial, *blockchain*, web semántica, y la realidad mixta, se ha comenzado a establecer una idea.

2.1 Tecnologías

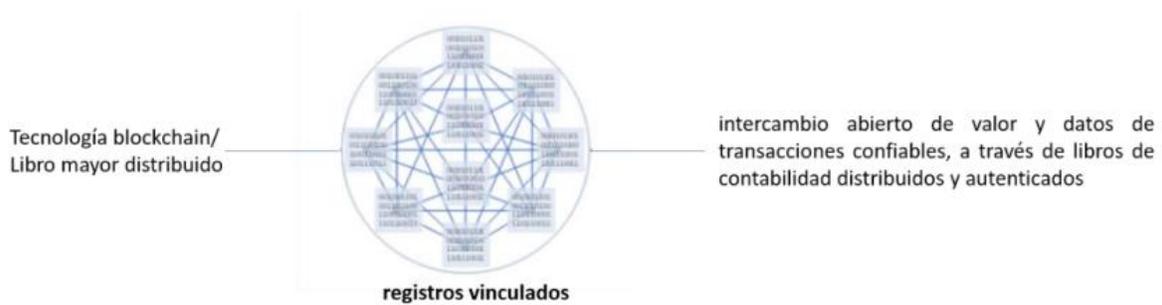
Blockchain se identifica como la tecnología principal y sirve como base para la fundación de la Web 3.0, pero también se pueden identificar algunas otras tecnologías que aportan a la estructura final y a las características de esta generación, las cuales serán explicadas brevemente a continuación, debido a que son áreas muy amplias en la investigación.

2.1.1 Blockchain

Es una estructura de datos cuya información se agrupa en bloques a los cuales se les agregan metadatos de un bloque anterior registrado dentro de la cadena, con el objetivo de darle seguimiento de manera temporal a cada registro a través de cálculos criptográficos (Barrón et al., 2022). En general se caracteriza por 4 atributos principales: transparencia, trazabilidad, confianza y gobernanza distribuida.

De esta tecnología se pueden identificar algunas características como:

- **Incorruptibilidad.** Debido a que la *blockchain* se basa en transacciones que deben verificarse por cada nodo dentro de la cadena, la validez de cualquier nueva transacción es transparente para todo el conjunto de bloques.
- **Descentralización.** Evita la centralización de las decisiones tomadas por un grupo selecto, es decir, la administración y autorización de los activos dentro de la red se realiza por cada uno de los nodos que desea realizar alguna transacción y se valida/verifica por el conjunto restante.
- **Seguridad.** La sincronización de los nodos dentro de la red para cualquier bloque que sea integrado o modificado, asegura la validación en todo el sistema, y esto se realiza a través de criptografía asimétrica y funciones hash que se encargan de generar huellas digitales para cada bloque.
- **Información distribuida.** Se puede considerar como una base de datos distribuida que registra la información de la red en cada uno de los nodos pertenecientes a la cadena, y dichas operaciones son realizadas por cada nodo, es decir, se distribuyen las tareas en el poder de computo de todas las computadoras conectadas.



Fuente: Obtenido de Publicación Técnica 646 IMT (Barrón et al., 2022)

Figura 2.1 Red de Blockchain 2022

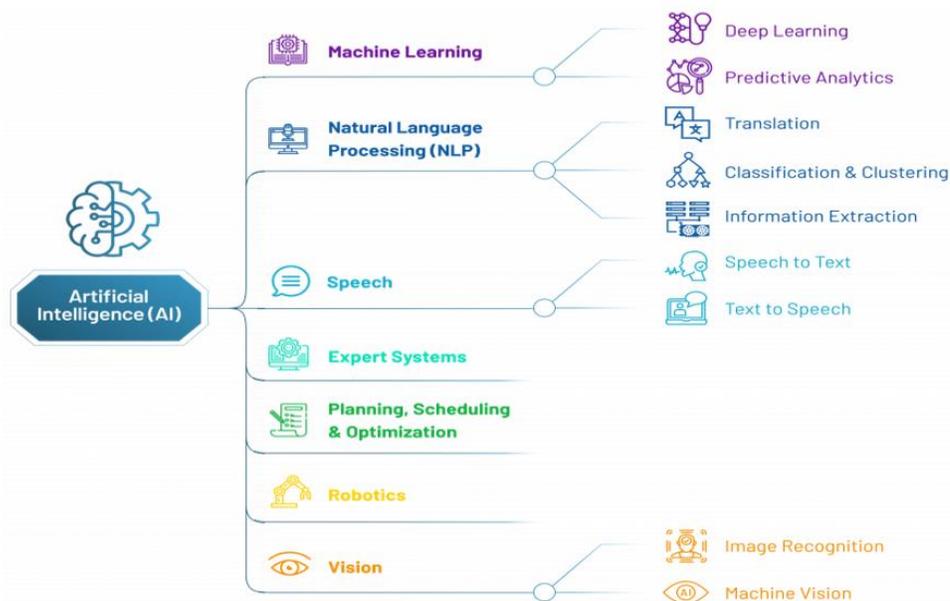
2.1.2 Inteligencia Artificial

La Inteligencia Artificial (IA) es la ciencia y la ingeniería de las máquinas que actúan de manera inteligente, cuando son las máquinas capaces de tomar decisiones apropiadas en circunstancias inciertas y mejorar su comportamiento a partir de sus experiencias (Sossa Azuela & Reyes Cortes, 2021). El término de inteligencia artificial fue formalmente acuñado en 1956 durante la Conferencia de Dartmouth, donde se desarrolló un estudio para proceder sobre la base de la conjetura de que cada aspecto del aprendizaje o cualquier otra característica de la inteligencia puede ser descrito con tanta precisión que puede fabricarse una máquina para simularlo (McCarthy et al., 1955). La IA cuenta con dos características principales:

- son sistemas capaces de aprender por sí mismos,
- son sistemas capaces de aprender a través de iteraciones pasadas, mejorando sus capacidades y conocimiento.

Por otro lado, dentro de la IA se encuentran varias líneas de investigación que se pueden observar en la Figura 2.2.

En la implementación de la IA en diferentes áreas de investigación y desarrollo se han identificado algunos objetivos principales (Association for Computing Machinery, 2007), tales como: razonamiento y resolución de problemas, representación del conocimiento, planificación y planeación, aprendizaje automático, procesamiento del lenguaje natural, y la percepción.



Fuente: Obtenido de Curso Distribución Urbana de Mercancías 4S (Secretaría de Desarrollo Agrario Territorial y Urbano [SEDATU] et al., 2020)

Figura 2.2 Campos de Investigación IA

2.1.3 Web Semántica

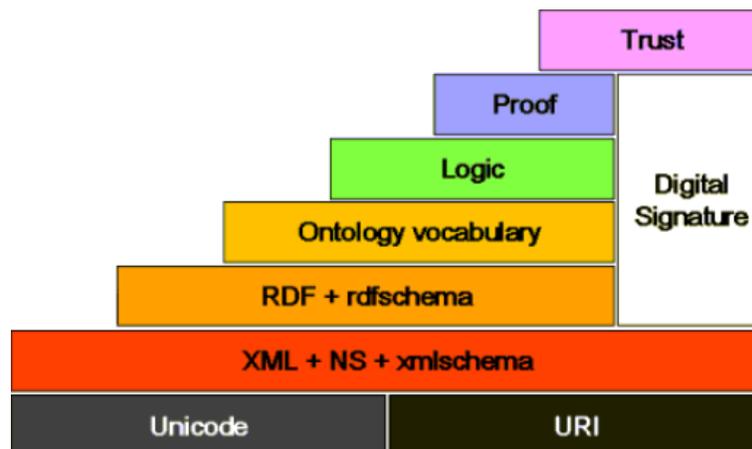
Se basa en la idea de añadir metadatos semánticos y ontológicos a la web, con los cuales se describa el contenido, significado y la relación de la información dentro de las aplicaciones web para que puedan ser evaluadas y procesadas automáticamente por las máquinas. Con esto, se pretende optimizar la interoperabilidad entre los diferentes sistemas informáticos a través del uso de agentes inteligentes. Esta idea quería ser implementada por Tim Berners-Lee desde su propuesta de la WWW, pero por lo escaso de la tecnología de ese entonces, no pudo ser implementada desde su creación; sin embargo, posteriormente en el año 2005, presentó un artículo en la revista *Scientific American* donde establece los primeros postulados para el uso de este término (Berners-Lee et al., 2001).

La web semántica tiene dos bases fundamentales: la descripción del significado o definición de los conceptos, y la manipulación automática de estas descripciones a través de motores de inferencia y lógica (World Wide Web Consortium [W3C], 2022). Para definir adecuadamente la descripción del significado se necesitan tres términos importantes:

- **La semántica.** La interpretación por parte de las máquinas del significado interpretable, es decir, términos lingüísticos que pueden ser comprendidos y procesados por las máquinas.

- **Los metadatos.** Son datos que describen otros datos, es decir, datos que describen los recursos que pueden ser accedidos en la web.
- **Las ontologías.** Una ontología es una jerarquía de conceptos con atributos y relaciones, definiendo una terminología consensuada para identificar redes semánticas de unidades con información interrelacionada y con reglas específicas, con cuatro características principales:
 - Explícito. Debe definir los conceptos, propiedades, relaciones, funciones, axiomas y restricciones que la componen.
 - Formal. Legible e interpretable por las máquinas.
 - Conceptual. Es un modelo abstracto y una vista simplificada de las entidades que representa.

Compartida. Existe un consenso previo sobre la información que se muestra, definida por expertos.



Fuente: Obtenido de (World Wide Web Consortium [W3C], 2022)

Figura 2.3 Capas de la Arquitectura de la Web Semántica

- **Unicode/URI.** Son la base para la representación e identificación de recursos en Internet.
- **XML/NS/xmlSchema.** Son los estándares relacionados para la estructuración y la comunicación de los datos en la web.
- **Resource Description Framework (RDF).** Es la primera capa de la web semántica como tal, y se describe como un *framework* para la representación de metadatos, usando las URI's para identificar a los recursos de la web y un modelo gráfico que representa las relaciones entre estos recursos; además se incluyen descripciones sintácticas para las búsquedas en entre relaciones.

- **Ontologías.** Es un lenguaje utilizado para proporcionar restricciones más complejas sobre los recursos en la web y sus propiedades.
- **Lógica / Pruebas.** Es un sistema de razonamiento automático en la parte superior de la estructura de las ontologías, utilizado para realizar inferencias. Un agente inteligente se encarga de deducir si un recurso particular satisface una petición o no.
- **Verdad.** La capa final de la web semántica, encargada de validar la confiabilidad de los problemas en la web semántica, es decir, verificar y brindar garantía de la calidad y la confiabilidad de la información que se proporciona en la web.

2.2 Plataformas existentes

En los últimos años, debido al auge de la migración digital causada por el aislamiento de la pandemia por COVID-19, se incrementó notablemente la implementación de nuevas tendencias como las criptomonedas⁴, los NFT's⁵ y el metaverso⁶. Sin embargo, aunque este último año ha bajado el impacto por problemas industriales, tal como el desabasto de componentes electrónicos, se ha abierto una nueva puerta para el desarrollo de aplicaciones distribuidas, que ganarán importancia rápidamente en los próximos años.

Se pueden identificar una gran cantidad de nuevas plataformas que ya tienen implementada las tecnologías principales de la Web 3.0, las cuales se pueden clasificar en varias categorías:

- Redes Sociales
- Servicios de intercambio
- Mensajería
- Almacenamiento
- Seguros e información bancaria
- *Streaming*
- Trabajo Remoto

⁴ Una criptomoneda es un activo digital que emplea un cifrado criptográfico para garantizar su titularidad y asegurar la integridad de las transacciones, y controlar la creación de unidades adicionales.

⁵ Token No Fungible (Non Fungible Token NFT) - es un activo digital encriptado. Se trata de un tipo especial de token criptográfico que representa algo único.

⁶ Es un mundo virtual al que nos conectaremos utilizando una serie de dispositivos que nos harán pensar que realmente estamos dentro de él, interactuando con todos sus elementos.

- Navegación

2.2.1 Redes Sociales

Las redes sociales actualmente son uno de los servicios más utilizados a nivel mundial. Sin embargo, las aplicaciones actuales tienen la limitante de que las empresas son las que tienen toda la autoridad sobre los datos que se comparten y almacenan en la plataforma. En el caso de las redes sociales dentro de la Web 3.0 desaparecerá esta limitante, debido a que a través la base tecnológica de *blockchain*, no habrá ningún intermediario y cada usuario será dueño de la información que genera, por otro lado, también desaparecerán las restricciones geográficas que existen actualmente, tal como es el caso de China, que desarrolló su propia red social y limita a que solo usuarios residentes de este país puedan acceder a esta plataforma. Entre algunas de las plataformas más reconocidas en este ámbito se pueden encontrar:

- **Steemit.** Se describe como una plataforma de recompensa descentralizada que ayuda a los contribuyentes a monetizar su contenido. Es una alternativa a Reddit (Steemit, 2022).
- **Sapien.** Es una plataforma de noticias sociales democratizadas basada en la cadena de bloques de Ethereum⁷. Es una alternativa a Facebook (Sapien Inc., 2022).
- **Indorse.** Es una red social descentralizada basada en recompensas donde puede compartir sus datos y ganar con ellos. Es una alternativa a LinkedIn (Indorse Pte. Ltd, 2022).

2.2.2 Servicios de Intercambio

Con la llegada de las criptomonedas, los servicios de intercambio ganaron gran importancia, y muchas empresas y servicios de intercambio entre criptos y monedas han comenzado a migrar a esta tecnología. Actualmente, los servicios de intercambio descentralizados han ganado popularidad lentamente, debido a las preocupaciones de hackeo o transparencia en las operaciones realizadas por sus usuarios, por algunas situaciones que ya han pasado tal como el caso de Mt. Gox, que fue hackeado y se perdieron un aproximado de 850,000 bitcoins en el 2014 (bit2me Academy, 2022). Algunas plataformas de intercambio son:

⁷ Ethereum es la tecnología de gestión comunitaria que impulsa la criptomoneda ether (ETH) y miles de aplicaciones descentralizadas

- **IDEX.** Es un servicio de intercambio descentralizado para el comercio de tokens ERC-20, que está incluida dentro de la cadena de bloques de Ethereum (Aurora Labs S.A., 2022).
- **EOSFinex.** Es el servicio de intercambio del software EOS.IO, desarrollado por BitFinex (iFinex Inc., 2021).

2.2.3 Mensajería

Los mensajes se han vuelto una parte importante para la comunicación en diferentes aspectos de la vida, aunque la generación actual de mensajería no tiene tantos aspectos negativos, el problema principal de las plataformas es la centralización de la información en empresas que dirigen el camino de la comunicación. La plataforma más reconocida en mensajería que utiliza Web 3.0 es **Secretum**, la cual está construida en la cadena de bloques de Solana, aunque su enfoque principal es como aplicación de mensajería segura, también permite a los usuarios intercambiar criptoactivos fácilmente (Secretum.io, 2022). Sin embargo, no es la única compañía que ha estado explorando estas nuevas tecnologías, también Meta ha comenzado a experimentar con los NFT's para ser incorporados en sus plataformas de Facebook e Instragram. Tal vez a futuro, también desarrollen su propia plataforma de mensajería en Web 3.0 (Andersen, 2022).

2.2.4 Almacenamiento

Existe un gran número de servicios que nos ofrecen almacenamiento en la nube, tal como Google Drive o Dropbox, pero la información queda centralizada en los servidores de las empresas que nos ofrecen estos servicios, y son propensos a tener problemas de seguridad. La idea básica del almacenamiento descentralizado consiste en compartir archivos y datos a través de una conexión punto a punto. La seguridad se encuentra en el cifrado que el remitente pone en sus archivos y luego los envía al receptor, el cual puede romper los archivos en pedazos y enviarlos a otros receptores sin conocer su contenido. El alojamiento se refiere a que cada nodo mantendrá un fragmento del archivo con un formato cifrado y estos pueden ser recuperados a través de la clave privada que tendrá el usuario original. Algunos ejemplos de plataformas que ofrecen este servicio son **Storj** (Storj Labs Inc, 2022), **Sia** (Sia Foundation, 2022) y **Filecoin** (Protocol Labs, 2022).

2.2.5 Seguros e información bancaria

Tanto el sector bancario y el de los seguros pueden ver una revolución con la tecnología de *blockchain* debido a que los sistemas centralizados actuales son susceptibles a corrupción. A través de los contratos

inteligentes se pueden automatizar la mayoría de las tareas sin que un humano intervenga. Sin embargo, aún no existen aplicaciones distribuidas completamente enfocadas a estos servicios, pero hay algunas compañías que comienzan a involucrarse y que poco a poco realizan estas operaciones:

- **Casha.** Es la plataforma más cercana a realizar operaciones bancarias como cualquier banco, ofrece préstamos bancarios criptográficos instantáneos y también la capacidad de realizar diferentes operaciones con las criptomonedas (Cashaa, 2022).
- **Hyperledger Fabric.** Es un proyecto desarrollado por IBM que apunta a crear una plataforma de financiamiento comercial, facilitando los pagos internacionales (IBM, 2022).

2.2.6 Streaming

En los últimos años, las plataformas de streaming han ganado una gran relevancia a nivel mundial, debido al aislamiento por pandemia que provocó la digitalización de la vida cotidiana. Plataformas como YouTube, Twitch, Netflix, Spotify, entre otras, ya son aplicaciones escuchadas y vistas casi por cualquier persona. Sin embargo, al ser aplicaciones centralizadas aún continúa el uso de información con fines publicitarios, lo que rompe la privacidad de los usuarios, y ya que algunas de estas son gratuitas, al final muchos usuarios terminan siendo el producto. Algunas de las plataformas que se identifican en la Web 3.0 son:

- **LivePeer.** Es una red de transcodificación de video descentralizada basada en la cadena de bloques de Ethereum (Livepeer, 2022).
- **LBRY.** Es una biblioteca digital descentralizada que alberga diferentes formas de contenido (LBRY Inc., 2022).

2.2.7 Trabajo Remoto

Al comenzar la pandemia, los trabajos remotos se volvieron la principal fuente de trabajo a nivel mundial, y hasta el momento, aún continúa esta misma dinámica y está incrementando poco a poco. Algunas páginas nuevas enfocadas en trabajo remoto e independiente, permite a las personas trabajar desde casa con proyectos que coinciden con las habilidades de los profesionales independientes (*freelancers*). El problema más común con estas plataformas es, el incorporarse como nuevos integrantes de la comunidad, debido a que, por la misma razón de ser nuevos, los primeros contratos son mal pagados. Además, al ser plataformas centralizadas, existe una tarifa asociada la cual corresponde a un honorario sustraído del salario de los profesionales que trabajan en estas aplicaciones. Es por esto, que plataformas de trabajo remoto

descentralizado desaparecían estos problemas incluyendo cualquier brecha laboral. Algunos ejemplos son:

- **Ethlance.** Plataforma desarrollada en la cadena de bloques Ethereum donde cualquiera puede contratar y trabajar a cambio de la criptomoneda Ether. La ventaja principal es que no existen tarifas de servicio, ni restricciones en membresías (Ethlance.com, 2017).
- **Atlas.Work.** Es una plataforma que utiliza contratos inteligentes y aprendizaje automático para potencial el ecosistema independiente de la comunicación entre empleados y empleadores. Existe una tarifa de dos dólares por tarea (Atlas.Work, 2022).
- **CryptoTask.** Otro proyecto que no tiene cargos ni censura para los usuarios, además de utilizar un algoritmo avanzado para coincidir a los *freelancers* con los contratos (CryptoTask, 2022).

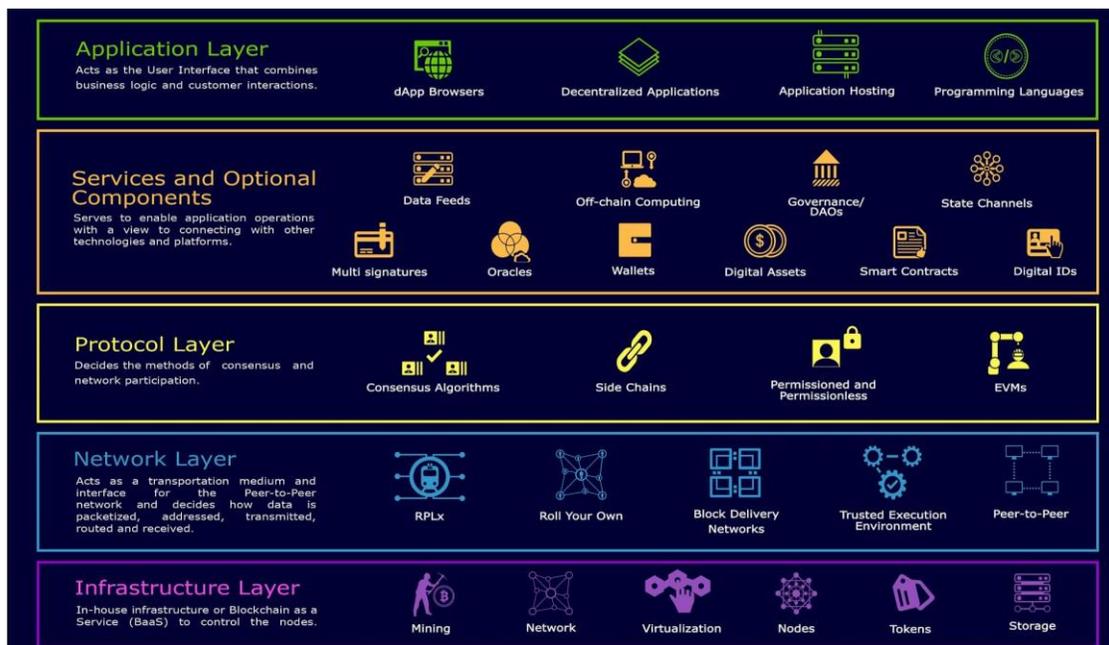
2.2.8 Navegación

Los principales navegadores que existen actualmente en el mercado son Google Chrome, Edge, Firefox y Safari, los cuales captan la mayor parte del mercado. Sin embargo, es necesario comenzar a trabajar con navegadores que utilicen redes *blockchain* para mejorar características de seguridad y compatibilidad con la descentralización. Por otro lado, la seguridad, es un punto importante a considerar en los navegadores, para evitar cualquier tipo de intrusión al estar en la web, debido a que, al entrar a sitios infectados con algún virus, es muy probable que la computadora también quede infectada, sin contar, que los navegadores también almacenan la ubicación, información de hardware y software, y la conectividad correspondiente. Algunos ejemplos de estas plataformas que son capaces de conectarse a redes de *blockchain* e interactuar con sus servicios son Brave (Brave Software, 2022), Breaker Browser (Blue Link Labs, 2022), Trust DApp (Trust Wallet, 2022).

3. Implementación de la Web 3.0

3.1 Blockchain Stack 3.0

Para poder implementar aplicaciones distribuidas de la Web 3.0, es necesario conocer la arquitectura que describe la comunicación entre las diferentes capas. Para eso es necesario conocer la infraestructura de Blockchain Stack 3.0, diferente en la descentralización de las operaciones que se realizan en la red, pero puede ser explicada en capas para entenderse mejor, tal como se muestra en la Figura 3.1. Sin embargo, aunque a futuro se trabaja en la descentralización de internet, los sistemas centralizados no serán reemplazados tan fácilmente, debido a las ventajas que estos atraen, y que pueden trabajar en colaboración con esta tecnología (Alabdulwahhab, 2018).



Fuente: Obtenido de (Anwar, 2018)

Figura 3.1 Capas de la Arquitectura de Blockchain Stack

La arquitectura se divide principalmente en 5 capas muy parecidas al modelo OSI⁸, aunque trabajan de manera muy diferente:

- Capa de Aplicación,
- Capa de Servicios y Componentes Opcionales,
- Capa de Protocolos,
- Capa de Red,
- Capa de Infraestructura.

3.1.1 Capa de Aplicación

Actúa como la interfaz de usuario que combina la lógica de negocios y las interacciones entre los clientes. Esta capa está encargada de gestionar las aplicaciones distribuidas a través de un navegador dApps, el alojamiento de estas y las interfaces de usuario. El navegador dApps es un navegador que permite explorar las nuevas aplicaciones descentralizadas desarrolladas, algunos ofrecen aplicaciones completas y otros pueden ser complementos que se agregan a los exploradores comunes como Mozilla o Chrome, que permiten tanto interactuar con aplicaciones de web 3.0 como las aplicaciones de las versiones anteriores. Entre algunas de las aplicaciones que se encuentran en esta capa podemos identificar las redes sociales, servicios de intercambio, mensajería, almacenamiento, entre otras; además, el complemento de los navegadores más reconocido llamado MetaMask.

Todas las aplicaciones distribuidas son alojadas en una red descentralizada a través de una aplicación que funciona como Software as a Service (SaaS). Este software permite acceder e integrar cualquiera de las apps alojadas de una manera sencilla, además, de que el mantenimiento para este SaaS es muy bajo.

Por otro lado, las mismas aplicaciones distribuidas finales también pertenecen a esta capa; para considerarse una aplicación sólida es necesario que cuenten con un conjunto de características tales como información externa, computación, monetización, almacenamiento de archivos y sistemas de pago.

⁸ El modelo de interconexión de sistemas abiertos, conocido como “modelo OSI”, es un modelo de referencia para los protocolos de la red, creado en el año 1980 por la Organización Internacional de Normalización.

3.1.2 Capa de Servicios y Componentes Opcionales

Sirve para habilitar las operaciones de la aplicación y permite la conectividad con otras tecnologías y plataformas. Se enfoca principalmente en la tecnología que se emplea, cubre las herramientas para la creación y ejecución de las aplicaciones distribuidas. Algunos de los elementos o características más importantes de esta capa son:

- **Fuente de los datos.** son un mecanismo utilizado para la recepción y actualización de información de fuentes confiables, también son conocidos como alimentadores web o *web feed*, y se encargan que los nodos conectados a una cadena puedan actualizar su información de manera descentralizada.
- **Computación *off-chain*.** Es el proceso de computo fuera de la aplicación stack blockchain, debido a que es menos costoso y ahorra tiempo el ejecutar de manera separada algunas operaciones que dentro de una cadena. A través de la computación fuera de la cadena proporciona una capa adicional de privacidad y garantizará la credibilidad de los valores, además no puede ser revertida. Los sistemas de memoria virtual son un ejemplo de cómo trabaja este elemento.
- **Gobernanza.** Funciona a través de DAO's (Organización Autónoma Descentralizada) que se ocupan de los contratos inteligentes dentro de las aplicaciones distribuidas. Los DAO definen un conjunto de normas que regirán el funcionamiento de la cadena, funcionan de manera autónoma, pero se coordinan a través de un protocolo de consenso distribuido.
- **Canales estatales.** Hace referencia a una vía bidireccional entre dos pares de nodos que desean comunicarse entre sí a través de medios de transacción definidos. Todos los usuarios del canal deben firmar sus transacciones con su clave privada para asegurarse de que estén completamente autorizados y provengan del usuario real. Estos canales también son privados y están disponibles por un tiempo limitado para los participantes dentro de la cadena.
- **Firma múltiple.** Esta firma habilita la seguridad en la transacción al proporcionar un signo único, forzando a que el usuario firme una transacción con otro conjunto de nodos dentro de la web antes de que el paquete sea transmitido, la cantidad de firmas es definido por el usuario y entre más firmas tenga más seguro es.
- **Oráculos.** Es una fuente de datos utilizada en la red *blockchain* para admitir contratos inteligentes. Actúa como un agente que descubre información sobre la situación del mundo real y lleva esta información a los contratos inteligentes. Para desbloquear condiciones en los contratos inteligentes se necesita un valor, este

valor es proporcionado por el oráculo, y estos valores pueden ser evaluaciones de mercado o pagos.

- **Cartera.** Son las billeteras que guardan las criptomonedas, en otras palabras, son programas que almacenan claves públicas y privadas de un usuario e interactúan con las redes *blockchain*, a través de estas se puede monitorear los activos digitales.
- **Recursos Digitales.** Pueden ser representados por las criptomonedas o los NFT's actualmente, sin embargo, también pueden ser imágenes, multimedia y contratos textuales.
- **Contratos Inteligentes.** Son acuerdos entre las partes interesadas, definen las reglas de antes y después de la ejecución de los acuerdos de manera automatizada, y todas las operaciones involucradas se encuentran dentro de un proceso extremadamente transparente.
- **Identidad Digital.** Es la identificación digital que define o autoriza permisos a los usuarios. Se pueden tener múltiples identidades digitales en varias plataformas, sin embargo, la identidad garantiza la seguridad y privacidad por completo. Los atributos que deben tener las identidades digitales son: nombre, usuario, contraseña, fecha de nacimiento, actividad en línea, número de seguridad social, historial de transacciones, registros médicos. Estas Identidades se usan para vincular los activos digitales.
- **Almacén de archivos distribuidos.** Es una ubicación dentro del servidor donde se guardan los datos y para acceder a ellos es necesario una autenticación adecuada para otorgar el nivel de control correspondiente.

3.1.3 Capa de Protocolo

Dentro de esta capa se enmarcan los algoritmos dentro de las cadenas de bloques, los requisitos de participación y los requerimientos virtuales.

- **Algoritmos de consenso.** Son procesos de toma de decisiones grupales, donde cada individuo construye y apoya la decisión que funcione mejor para el grupo. Es una forma de resolución donde los miembros apoyan la decisión mayoritaria. Los modelos de consenso utilizados dentro de *blockchain* son métodos utilizados para crear igualdad y equidad en la cadena. Tienen algunos objetivos particulares tales como: a) llegar a un acuerdo, b) colaboración entre integrantes, c) cooperación, d) igualdad de derechos, e) participación, y f) actividad. Algunos de los algoritmos más utilizados en *blockchain* son:
 - Proof-of-Work (POW) optimizada por ASIC – Bitcoin y Bitcoin Cash
 - POW resistente a ASIC – Ethereum 1.0, Zcash, Monero, otros
 - POW y POS con respaldo – Thunder

- Proof of Elapsed Time (POET) y Proof of Space and Time (POST) – Chia
 - POST con datos útiles – Filecoin
 - POW trenzado – Kadena
 - Casper TFG proof of stake (POS) – Ethereum 2.0
 - POS / POW híbrido – Decred
 - Acuerdo bizantino con elección de líder (BA*) – Algorand
 - Honeybadger POS – Polkadot
 - Delegated proof of stake (DPOS) – EOS
 - Variante DPOS – Tezos
 - Variante DPOS – Tendermint
 - Proof of history (POH) – Solana
 - Protocolo de consenso Stellar
 - Protocolo de consenso Ripple
 - Consenso de blockchain centrado en el líder
- **Cadenas Laterales.** Las *sidechain* son un tipo de mecanismo emergente que permite que los tokens u otros activos pasen de la *blockchain* madre a una *blockchain* separada y luego regresa a su origen. Estas permiten desarrollar aplicaciones descentralizadas dentro de la cadena lateral sin influir en la cadena principal de ninguna manera. Sin embargo, todos en la red podrán utilizar la efectividad de las aplicaciones.
 - **Requisitos de participación.** Hace referencia a los diferentes tipos de redes *blockchain*, de las cuales se pueden identificar tres tipos de infraestructura: la cadena de bloques pública o sin permiso en la que cualquier usuario puede unirse sin necesidad de cumplir ninguna condición; Las redes privadas o autorizadas donde se necesita cumplir términos para unirse como miembros y utilizar los protocolos y beneficios de la red; las *blockchain* de consorcio donde varias organizaciones comparten responsabilidades de mantener activa la cadena, las organizaciones determinan quien puede enviar transacciones o acceder a los datos.
 - **Máquina Virtual.** El enfoque principal es mantener la seguridad y ejecutar el código fuente no confiable desde las computadoras en la red, es decir, evitar la amenaza de ataques de denegación de servicio. Este tipo de ataques evitan que los recursos de la red estén disponibles para el usuario. Algunos de los ejemplos de máquinas virtuales en la *blockchain* son:
 - **Ethereum 1.0, WANchain, Hashgraph, Ethermint** – Ethereum Virtual Machine (EVM) (Ethereum Foundation, 2022),
 - **Solana, Cardano** – Exposición directa a LLVM,
 - **Ethereum 2.0, EOS, Dfinity, Polkadot** – Máquina virtual de ensamblado web (Web Assembly Virtual Machine WASM) (Ethereum Foundation, 2022),

- **Kadena, Corda, Tezos**– Tienen sus propias máquinas virtuales (Kadena LLC, 2022; R3, 2022; Tezos, 2022).

3.1.4 Capa de Red

Actúa como un medio de transporte de interfaz para la red Peer-to-Peer⁹ y decide cómo se empaquetan, direccionan, transmiten, enrutan y reciben los datos. En la capa de red se tienen definidos los protocolos de comunicación que se utilizan dentro de la *blockchain*. De los elementos principales más conocidos son RLPx, *Roll Your Own*, *Trusted Execution Environment*, *Block Delivery Network*.

- **RLPx.** Es un conjunto de protocolos y redes creados para la comunicación peer-to-peer, enfocado principalmente en el desarrollo de redes descentralizadas. Es el principal elemento utilizado por Ethereum. La función principal es enmarcar los límites de los diferentes protocolos de comunicación y controlar el flujo general de datos en la red, además, de encargarse de la seguridad y autenticación de los nodos en la red.
- **Roll Your Own.** Es un proceso utilizado solo cuando los protocolos estándar no van con la infraestructura original, es decir, permite a los usuarios crear un protocolo personalizado que se ajuste a las necesidades, debido a que, no todos los nodos se pueden adaptar de manera eficiente a los protocolos estándar de Blockchain, entonces tiene como objetivo garantizar la comunicación de nuevos protocolos y mantener el crecimiento potencial de la arquitectura web adaptándose a nuevas funciones.
- **Trusted Execution Environment (TEE).** Es uno de los componentes más importantes de la red debido a que se encarga de resolver el problema de escalabilidad en las cadenas. En realidad, es un área aislada o un servidor alejado de la red o sistema principal que permite a los datos almacenarse y garantizar la seguridad de esa información.
- **Block Delivery Network.** Es un sistema de red distribuida que entrega contenido web a cualquier usuario que lo solicita. El sistema se encarga de entregar los contenidos en función de la ubicación, servidor y el origen de la página web. Las funciones principales de este componente son:

⁹ Una red peer-to-peer es una red de ordenadores en la que todos los aspectos funcionan sin clientes ni servidores fijos, es decir, funcionan como una serie de nodos que se comportan iguales entre sí.

- La Seguridad en el acceso periférico. Accede directamente y protege la interfaz de usuario y ofrece soporte adicional para otras herramientas como cámaras o huellas digitales.
- Seguridad en la comunicación. Se encarga del procesamiento de las operaciones criptográficas y las claves de cifrado.
- Identidad del dispositivo y procedimiento de autenticación. Cada dispositivo tiene una identificación única, la cual sirve para reconocer y avisar de inicios de sesión no autorizados en dispositivos no reconocidos.

3.1.5 Capa de Infraestructura

Dentro de esta capa se define de manera general la infraestructura interna de la *blockchain* como servicio (BaaS) para controlar los nodos. Dentro de esta capa se pueden identificar los siguientes elementos:

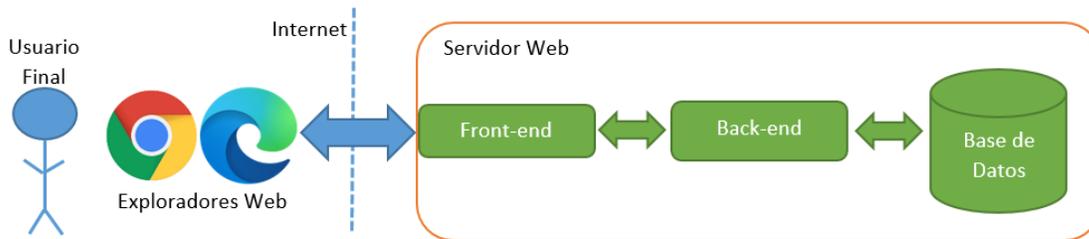
- **Minería.** El proceso con el cual se crean nuevas criptomonedas, el cual se realiza mediante computadoras que resuelven problemas matemáticos complejos, y para lo cual es necesario una gran cantidad de poder computacional y de energía.
- **Red.** Se hace referencia a la red física en la cual se encuentra trabajando la red de *blockchain*, es decir, redes descentralizadas sin autoridades centrales, además, se caracteriza porque puede ser escalable sin ninguna dificultad.
- **Virtualización.** Es la columna vertebral de la arquitectura web 3.0 en niveles, y hace referencia a imitar características de hardware a través del uso de solamente software para crear un sistema informático virtual. A través de esta tecnología se busca reducir el costo de implementación, recursos y costos operativos.
- **Computación distribuida.** El concepto se encuentra en que varias computadoras trabajan en un solo problema para resolverlo, con el objetivo de facilitar y ahorrar tiempo.
- **Nodos.** Cualquier dispositivo accesible dentro de la red descentralizada. Son los puntos centrales donde el tráfico de internet se dirige, y con la cual, la red puede dar un seguimiento a la transacción para actualizarla o tomar una decisión.
- **Tokens.** Es un activo que pueden ser utilizados para obtener las características que se ofrecen en una red de *blockchain*.
- **Almacenamiento.** Se hace referencia al almacenamiento físico utilizado por los nodos dentro de la red, pero con un enfoque descentralizado.

3.2 Metodología de Implementación

La arquitectura de las aplicaciones desarrolladas en la Web 3.0 es completamente diferente a las arquitecturas convencionales de versiones anteriores (Kasireddy, 2021). Por ejemplo, para el caso de la Web 2.0 se pueden encontrar una gran cantidad de arquitecturas diferentes, desde aplicaciones monolíticas hasta microservicios, pero de manera general, se toman en cuenta tres componentes principales:

- **Almacenamiento de información.** Lo que contempla guardar información esencial para las distintas aplicaciones.
- **Back-end.** El código ejecutado que contiene la lógica de negocio, es decir, la parte del sistema que se encarga de codificar las reglas de negocio del mundo real que determinan como la información debe ser creada, almacenada y actualizada.
- **Front-end.** Es la capa que representa la presentación de la lógica de negocio al usuario final, es mejor conocida como interfaz gráfica, y debe tener la característica de ser entendible y fácil de usar por los usuarios.

Estas tres capas principales son una visualización generalizada de la mayoría de las arquitecturas actuales y buscan la separación de las partes involucradas en las aplicaciones web que en la mayoría de los casos se encuentran alojados en servidores centralizados.



Fuente: Elaboración propia a partir de la Arquitectura de la Web 3.0 y (Kasireddy, 2021; Wackerow, 2022)

Figura 3.2 Arquitectura general Web 2.0

Como se ha mencionado anteriormente, en el caso de la Web 3.0 se eliminan los intermediarios, es decir, no existen servidores web centralizados que alojen la lógica de negocio ni existen bases de datos centralizadas para la información que se genera.

En lugar de esto, las aplicaciones descentralizadas se podrían considerar como una base de datos pública que es actualizada y compartida por un conjunto de computadoras en la red. Para realizar cualquier cambio

dentro de esta base de datos es necesario realizar una transacción, que se interpreta como un conjunto de instrucciones firmadas criptográficamente por una cuenta. Estas transacciones son agregadas a un bloque, perteneciente a un conjunto de bloques que se encuentran encadenados, es decir, tienen una referencia criptográfica con su antecesor lo que provoca que, para realizar cualquier cambio en un bloque determinado, es necesario realizar cambios en todos los bloques subsecuentes con el consentimiento de toda la red. Un ejemplo de esto se puede observar en el desarrollo de aplicaciones para Ethereum (Wackerow, 2022).

Ethereum es una plataforma de código abierto, que sirve para ejecutar contratos inteligentes, donde hay una sola computadora llamada Ethereum Virtual Machine (EVM) cuyo estado está identificado con todos los nodos dentro de la red Ethereum. Cada nodo guarda una copia del estado de esta EVM, además, cualquier nodo puede transmitir una solicitud para que esta computadora realice cálculos o funciones. Cada vez que se transmite una solicitud a esta computadora, otros participantes verifican, validan y ejecutan esa operación. La ejecución provoca un cambio en la EVM que se propaga por toda la red. El registro de todas las transacciones y el estado actual de la EVM son almacenados y aceptados por todos los nodos a través de mecanismos criptográficos que aseguran que las transacciones son válidas y no puedan ser manipuladas más adelante. También garantizan que todas las transacciones se firmen y ejecuten con los permisos apropiados definidos por cada cuenta.

Dentro de Ethereum se puede identificar la criptomoneda Ether (ETH), su propósito principal es definir un mercado computacional que proporciona incentivos económicos para que los participantes dentro de la red proporcionen recursos computacionales para verificar y ejecutar las solicitudes de las transacciones. Cualquier nodo que solicite una transacción también debe “pagar” con esta criptomoneda, y será la recompensa por los nodos que hagan el trabajo de verificar la transacción, ejecutar, comprometer la cadena de bloques y transmitirla en la red. La cantidad de ETH a pagar corresponde al tiempo requerido para realizar las operaciones computacionales.

Los contratos inteligentes son los encargados de definir la lógica detrás del cambio de los estados que pasan en la cadena de bloques, estos contratos pueden ser desarrollados en diferentes lenguajes de alto nivel tales como Solidity y Vyper. En la Figura 3.3 se muestra un ejemplo del desarrollo de un contrato sencillo en Solidity que permite a cualquiera guardar un solo número, el cual puede ser accedido por cualquier persona conectada en la cadena.

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.16 <0.9.0;

contract SimpleStorage {
    uint storedData;

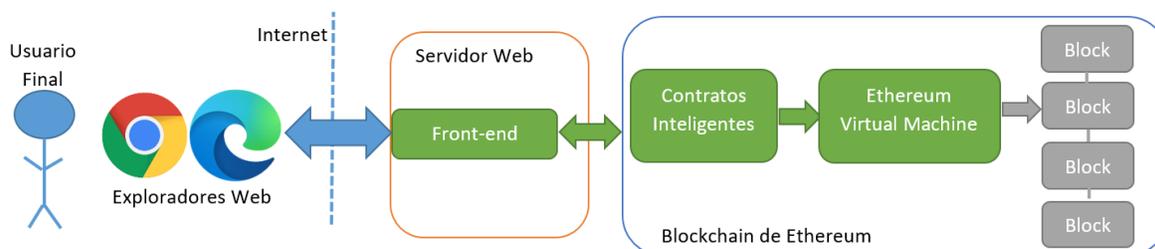
    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Fuente: Obtenido de (Wackerow, 2022)

Figura 3.3 Código de un Contrato Inteligente en Solidity

Posteriormente, este contrato es ejecutado en la EVM, sin embargo, debido a que la EVM no entiende lenguajes de alto nivel, este código debe ser compilado y convertido a bytecode¹⁰, para que pueda ser ejecutado.



Fuente: Elaboración propia a partir de la Arquitectura de la Web 3.0 y (Kasireddy, 2021; Wackerow, 2022)

Figura 3.4 Blockchain de Ethereum

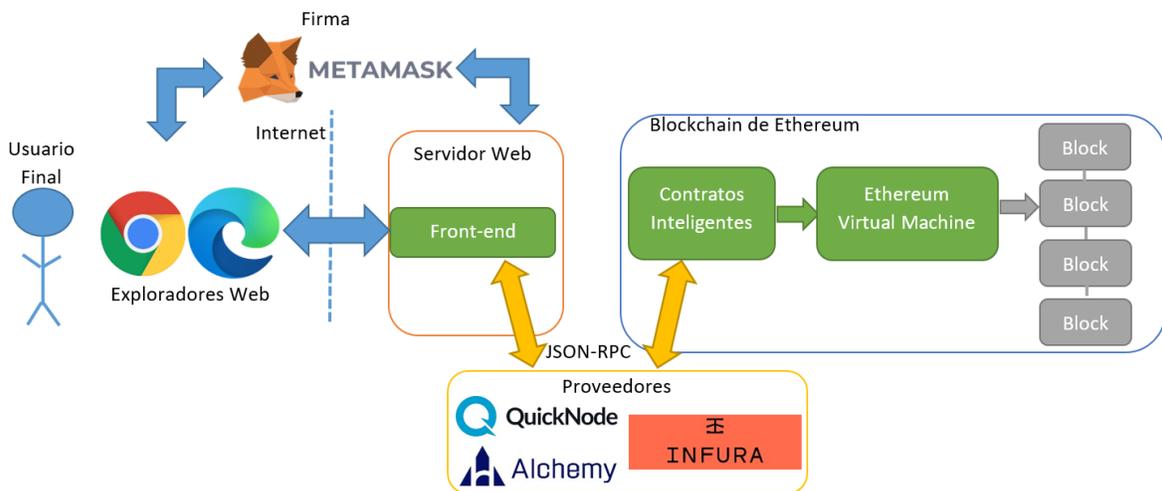
Para el caso del Front-end también existen cambios, ya que debe comunicarse con la lógica de la aplicación definida por los contratos inteligentes a través de “proveedores”. Para esto existen dos maneras: configurar un nodo propio que ejecuta el software de la cadena de bloques de Ethereum o usar nodos ofrecidos como servicios por terceros.

Estos proveedores también son conocidos como clientes Ethereum los cuales implementan la especificación JSON-RCP para garantizar un

¹⁰ También conocido como lenguaje ensamblador, donde se especifican instrucciones básicas de bajo nivel que se convierten directamente a código binario, que son operaciones que realiza directamente la CPU del ordenador.

conjunto de métodos estandarizados para la comunicación entre el Front-end y los contratos inteligentes. Estos métodos son independientes de la capa de transporte, por lo que pueden utilizarse a través de peticiones HTTP o en entornos de paso de mensajes. El formato de la información transferida es JSON.

Una vez conectada a la cadena a través de estos proveedores, se puede leer el estado guardado dentro de la cadena, pero para escribir un nuevo estado es necesario firmar la transacción a través de una llave privada, con el objetivo de que, al estar conectados a la cadena con cuentas no autorizadas, los cambios en el estado solicitados por las transacciones serán rechazadas por los demás nodos. La tarea de firmar las transacciones es realizada por Metamask, la cual se define como una herramienta que facilita que las aplicaciones manejen la gestión de llaves y la firma de transacciones, este se puede encontrar como una extensión para los navegadores web convencionales.



Fuente: Elaboración propia a partir de la Arquitectura de la Web 3.0 y (Kasireddy, 2021; Wackerow, 2022)

Figura 3.5 Blockchain de Ethereum

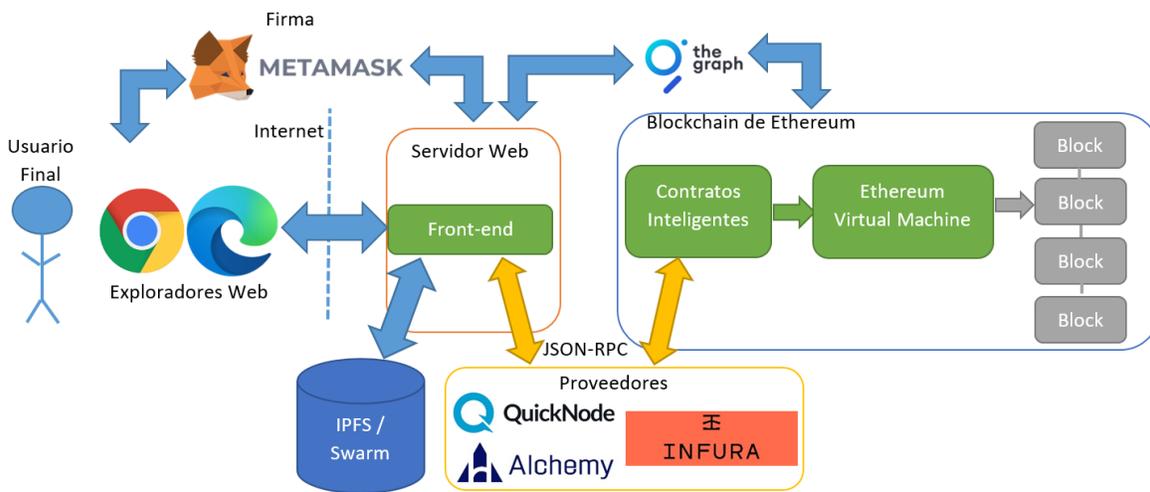
Sin embargo, para realizar la inserción de nuevos datos a la cadena suele ser muy costoso, debido a que se necesitan realizar las operaciones en toda la cadena de bloques cada que se agrega un estado nuevo. Para solucionar este problema se utilizan las off-chain descentralizadas, tales como IPFS o Swarm.

IPFS es un sistema de archivos distribuido para almacenar y acceder a datos, para agilizar la recuperación de la información cuando se necesite sin la necesidad de una base de datos centralizada. También tiene una capa de incentivos conocida como Filecoin, la cual es una criptomoneda pública de código abierto y un sistema de pago digital. Por otro lado, Swarm también es un sistema de archivos distribuido, pero la gran

diferencia recae en que utiliza su propio sistema de incentivos a través de contratos inteligentes.

Para poder acceder a la información de los contratos inteligentes, existen dos formas principales para realizar esta tarea, la primera es a través de los eventos que generan dichos contratos, lo cual se puede efectuar con el uso de la biblioteca de javascript Web3.js. Esta biblioteca permite escuchar eventos específicos de los contratos y ejecutar acciones específicas basadas en estos eventos.

Sin embargo, el gestionar las respuestas de las llamadas para manejar varias lógicas de interfaz de usuario es algo complejo, debido a esto, se identifica la segunda estrategia a través de The Graph. The Graph es una off-chain para la consulta de datos dentro de Ethereum, permite la indexación de los contratos inteligentes, que eventos y llamadas deben ser escuchadas, y como transformar los eventos entrantes en entidades que el Front-end puede consumir. Una ventaja de esta herramienta es que es muy parecida si se compara con el consumo de API's REST.



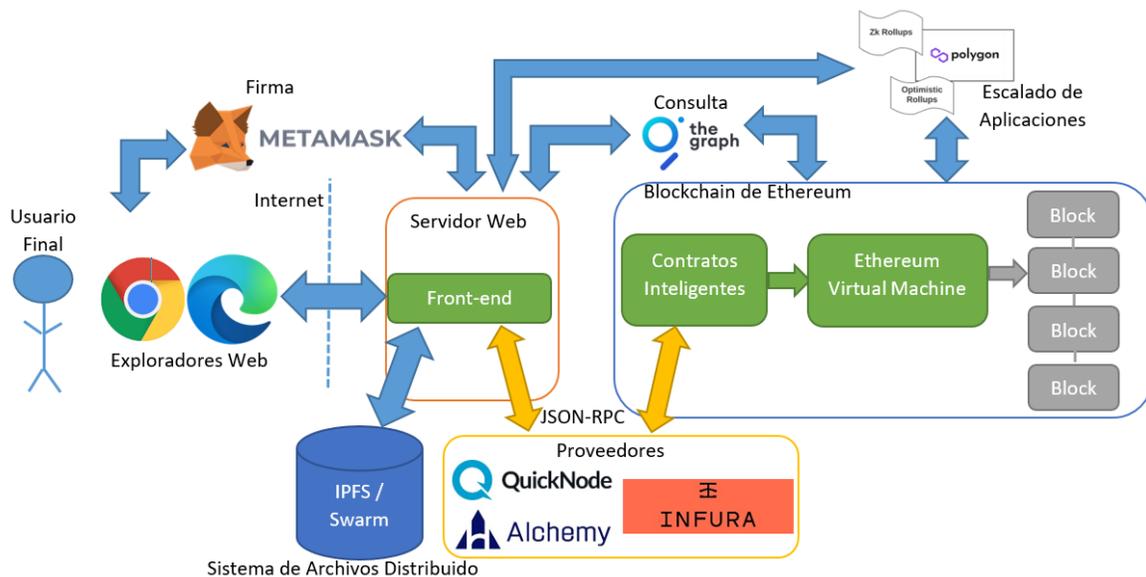
Fuente: Elaboración propia a partir de la Arquitectura de la Web 3.0 y (Kasireddy, 2021; Wackerow, 2022)

Figura 3.6 Consulta y Almacenamiento dentro de Ethereum

Tal como se mencionó anteriormente, para realizar las operaciones dentro de las cadenas de bloques, debe de haber incentivos para el uso de los recursos de los nodos anónimos, estas cuotas requeridas por transacción son medidas a través de un término llamado “gas”, el cual hace referencia al costo en ETH que se debe cubrir por el uso de los recursos. Para Ethereum son denotados en “gwei” equivalentes a 10^{-9} ETH. Para cuando se deseen realizar operaciones dentro de la cadena, se pueden pagar más gwei para solicitar más recursos computacionales y obtener resultados en

menor tiempo. Por otro lado, si el tiempo no es una variable tan importante, se puede pagar menos por resolver alguna transacción con el costo de un tiempo mayor de ejecución.

Al contemplar aplicaciones distribuidas, el problema surge en el escalado de la misma, esto provoca mayores costos de gas y una mayor cantidad de bloques para que se utilice de manera correcta la aplicación. No obstante, existen algunas herramientas para escalar las DApp's desarrolladas. La más popular en Ethereum es Polygon, que funciona como una side-chain que ejecuta transacciones de manera paralela en lugar de la cadena principal, la cual, cada cierto periodo reenvía la información y el estado de sus bloques a la cadena principal para mantenerla actualizada. Otras herramientas que se pueden identificar son Optimistic Rollups y zkRollups.



Fuente: Elaboración propia a partir de la Arquitectura de la Web 3.0 y (Kasireddy, 2021; Wackerow, 2022)

Figura 3.7 Escalado de Aplicaciones en Ethereum

Finalmente, para el desarrollo de las aplicaciones distribuidas, no es necesario empezar de cero, ya existen un conjunto de frameworks que dan soporte y agilizan la implementación de estas aplicaciones, algunos de estos son: Truffle, Hardhat, Ape, Brownie, Embark, Web3j, Alchemy, entre otros. Cada uno de estos dan una pauta a seguir para el desarrollo de los contratos y algunos ofrecen plataformas o ambientes de desarrollo para la construcción y testeado de nuevas aplicaciones distribuidas.

Conclusiones

Actualmente, la implementación de nuevas tecnologías para la solución de problemas en logística ha sido la clave competitiva más importante para las organizaciones. Sin embargo, el desarrollo de nuevos sistemas computacionales que implementen los avances tecnológicos más novedosos no ha sido una tarea fácil. El auge de nuevas tecnologías como inteligencia artificial, *blockchain*, realidad mixta y la Web semántica, han dado la pauta para el desarrollo de estos sistemas en la nueva generación de la Web.

A través del uso de las aplicaciones descentralizadas, se considera garantizada la fiabilidad y propiedad de la información, desapareciendo empresas intermediarias que limitaban en muchas ocasiones la gestión de los datos. También sobresaldrán las personalizaciones de las interacciones con productos y servicios, con la ayuda de la inteligencia artificial, se mejorará el análisis de los clientes y se podrán ofrecer estos servicios y productos de acuerdo a las preferencias de cada persona. Por otro lado, la descentralización de la información mejorará la seguridad ante robos de activos, incluyendo que las operaciones serán más transparentes para todos los involucrados en el uso de la *blockchain*.

Por otro lado, ni las operaciones logísticas, ni la cadena de suministro están exentas de estas novedades, debido a que la Web 3.0 ha acelerado la transformación digital de las tareas empresariales y da la capacidad de ofrecer nuevas experiencias, reduciendo cada vez más la línea que separa el contenido digital del físico. La gestión de nuevos activos digitales, tales como las criptomonedas o los NFT's se están convirtiendo en una opción viable para transacciones de bienes físicos.

Debido a la gran importancia a nivel mundial que ha tomado la Web 3.0, grandes compañías como NVIDIA, Coinbase, Paypal, IBM, Microsoft, Google, entre otras, han apostado por el mundo de la *blockchain*, y se han adentrado en el desarrollo de aplicaciones distribuidas, y la generación y uso de criptoactivos.

Finalmente, con esta investigación se identificaron algunas estrategias para el desarrollo de aplicaciones distribuidas, sin embargo, no se pudo realizar alguna de estas debido a la falta de activos digitales para la experimentación. Como trabajo futuro, se contempla conseguir recursos

para el desarrollo de una aplicación prototipo que considere alguna operación logística y ofrecerla para optimizar las decisiones dentro de esta.

Bibliografía

- Aghaei, S. (2012). Evolution of the World Wide Web : From Web 1.0 to Web 4.0. *International Journal of Web & Semantic Technology*, 3, 1–10. <https://doi.org/10.5121/ijwest.2012.3101>
- Alabdulwahhab, F. A. (2018). Web 3.0: The Decentralized Web Blockchain networks and Protocol Innovation. *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*, 1–4. <https://doi.org/10.1109/CAIS.2018.8441990>
- American Registry for Internet Numbers. (2022). *ARIN*. <https://www.arin.net/>
- Andersen, D. (2022). *NFTs to appear on Facebook, cross-post with Instagram as Meta Web3 expansion continues*. <https://cointelegraph.com/news/nfts-to-appear-on-facebook-cross-post-with-instagram-as-meta-web3-expansion-continues>
- Anwar, H. (2018). *Web 3.0 Blockchain Technology Stack: The Comprehensive Guide*. 101 Blockchains. <https://101blockchains.com/web-3-0-blockchain-technology-stack/>
- Association for Computing Machinery. (2007). *The ACM Computing Classification System*. <https://web.archive.org/web/20071012025921/http://www.acm.org/class/1998/1.2.html>
- Atlas.Work. (2022). *Atlas.Work*. <https://www.atlas.work/>
- Aurora Labs S.A. (2022). *IDEX*. <https://idex.io/>
- Barrett Lyon. (2022). *THE INTERNET — Opte*. <https://www.opte.org/the-internet>
- Barrón, M., de la Torre, E., & Hernández Sánchez, B. (2022). *Estudio exploratorio sobre la tecnología blockchain aplicada en cadenas de suministro [Publicación técnica No. 646]*. Mexico: Instituto Mexicano del Transporte [Archivo PDF]. <https://imt.mx/resumen-publicaciones.html?IdPublicacion=1095&IdTipo=Publicación técnica No.664&LbPalabra=0>

Berners-Lee, T. (1998, May 7). *The World Wide Web: A very short personal history*. <https://www.w3.org/People/Berners-Lee/ShortHistory.html>

Berners-Lee, T., & Cailliau, R. (1990, December 12). *World Wide Web: Proposal for a HyperText Project*. <https://www.w3.org/Proposal.html>

Berners-Lee, T., Hendler, J., & Lassila, O. (2001). The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities. *Scientific American*, 284(5), 1–5.

bit2me Academy. (2022). *¿Qué es Mt Gox?* <https://academy.bit2me.com/que-es-mt-gox/>

Blue Link Labs. (2022). *Beaker*. <https://beakerbrowser.com/>

Brave Software, I. (2022). *Brave*. <https://brave.com/es/>

Cashaa. (2022). *Cashaa*. <https://cashaa.com/>

Chong, K. (2019). *What is Web 3?* Decrypt. <https://decrypt.co/resources/what-is-web-3>

CryptoTask. (2022). *CryptoTask*. <https://www.cryptotask.org/en>

Ethereum Foundation. (2022). *Ethereum*. <https://ethereum.org/es/>

Ethlance.com. (2017). *The future of work is now hire or work for Ether cryptocurrency*. <https://ethlance.com/>

Guo, J., Chaisatien, P., Han, H., Noro, T., & Tokuda, T. (2010). Partial Information Extraction Approach to Lightweight Integration on the Web. In *Current Trends in Web Engineering* (pp. 372–383). https://doi.org/10.1007/978-3-642-16985-4_33

Hafner, K., & Lyon, M. (1996). *Where Wizards Stay up Late: The Origins of the Internet* (1st ed.). Simon & Schuster, Inc.

IBM. (2022). *¿Qué es Hyperledger Fabric?* <https://www.ibm.com/mx-es/topics/hyperledger>

iFinex Inc. (2021). *EOSFinex*. <https://www.bitfinex.com/posts/616>

Indorse Pte. Ltd. (2022). *Indorse*. <https://indorse.io/>

Instituto Nacional de Estadística y Geografía [INEGI]. (2022). *Servicio RSS*. <https://www.inegi.org.mx/servicios/rss/>

- Kadena LLC. (2022). *Build the future on Kadena*. <https://kadena.io/>
- Kasireddy, P. (2021). *The Architecture of a Web 3.0 application*. <https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application>
- LBRY Inc. (2022). *LBRY does to publishing, what Bitcoin did to money*. <https://lbry.com/>
- Livepeer, I. (2022). *La infraestructura global de video abierto*. <https://livepeer.org/es>
- Mallory, J. (2006, August 24). *Emerging Alternatives: A Brief History of Weblogs*. <https://web.archive.org/web/20060824162316/http://www.cjr.org/issues/2003/5/blog-jensen.asp?printerfriendly=yes>
- Marchiori, M. (2004). Towards a people's Web: Metalog. *Proceedings - IEEE/WIC/ACM International Conference on Web Intelligence, WI 2004*, 320–326. <https://doi.org/10.1109/WI.2004.10077>
- McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1955, August 31). *A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE*. <https://web.archive.org/web/20080930164306/http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html>
- Microsoft. (2018, October 4). *Crear y editar un wiki*. [https://support.microsoft.com/es-es/office/crear-y-editar-un-wiki-dc64f9c2-d1a2-44b5-ac59-b9d535551a32#:~:text=Un wiki es un sitio,información en un wiki empresarial](https://support.microsoft.com/es-es/office/crear-y-editar-un-wiki-dc64f9c2-d1a2-44b5-ac59-b9d535551a32#:~:text=Un%20wiki%20es%20un%20sitio,informaci%C3%B3n%20en%20un%20wiki%20empresarial)
- Miniwatts Marketing Group. (2022). *World Internet Users Statistics and 2022 World Population Stats*. <https://www.internetworldstats.com/stats.htm>
- Network Coordination Centre. (2022). *RIPE NCC*. <https://www.ripe.net/>
- O'Reilly, T. (2005, September 30). *What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software*. <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>
- Pacific Network Information Centre. (2022). *APNIC*. <https://www.apnic.net/>
- Pérez Salazar, G. (2011). La Web 2.0 y la sociedad de la información. *Revista Mexicana de Ciencias Políticas y Sociales*, 56, 57–68.

Pinto, A. (2019). *Exploring blockchain as the foundation for next gen apps on Web 3.0*. IBM. <https://www.ibm.com/blogs/blockchain/2019/03/exploring-blockchain-as-the-foundation-for-next-gen-apps-on-web-3-0/>

Protocol Labs. (2022). *Filecoin*. <https://filecoin.io/>

R3. (2022). *The future of digital finance is built on trust*. <https://corda.net/>

Regional Internet Registry for Africa. (2022). *AFRINIC the Region Internet Registry (RIR) for Africa*. <https://www.afrinic.net/>

Registro de Direcciones IP en Latinoamerica. (2022). *LACNIC*. <https://www.lacnic.net/>

Rodriguez, N. (2018). *La Web 3.0 Estará Impulsada Por La Tecnología Blockchain Stack*. 101 Blockchains. <https://101blockchains.com/es/web-3-0-tecnologia-blockchain-stack/#13>

Sapien Inc. (2022). *Sapien*. <https://www.sapien.network/>

Secretaría de Desarrollo Agrario Territorial y Urbano [SEDATU], Secretaría de Comunicaciones y Transportes [SCT], & Instituto Mexicano del Transporte [IMT]. (2020, September 8). *Curso virtual Distribución Urbana de Mercancías 4S: capacitación para personas tomadoras de decisiones en territorio urbano*. <https://www.gob.mx/sedatu/documentos/curso-virtual-distribucion-urbana-de-mercancias-4s-capacitacion-para-personas-tomadoras-de-decisiones-en-territorio-urbano>

Secretum.io. (2022). *Revolutionary Secure Messaging & Trading Dapp*. <https://secretum.io/>

Sia Foundation. (2022). *Sia*. <https://sia.tech/>

SIGWEB, & ACM. (2009). *WWW '09: Proceedings of the 18th International Conference on World Wide Web*. <https://dl.acm.org/doi/proceedings/10.1145/1526709>

Sossa Azuela, J. H., & Reyes Cortes, F. (2021). *Inteligencia Artificial aplicada a Robótica y Automatización* (Primera). Marcombo. <https://www.marcombo.com/inteligencia-artificial-aplicada-a-robotica-y-automatizacion-9788426733160/>

Steemit, I. (2022). *Steemit*. <https://steemit.com/>

Storj Labs Inc. (2022). *Storj*. <https://www.storj.io/>

Tezos. (2022). *A blockchain designed to evolve*. <https://tezos.com/>

Trust Wallet. (2022). *Navegador Trust DApp*. <https://trustwallet.com/es/dapp/>

Wackerow, P. (2022). *Ethereum Development Documentation*. Ethereum Foundation. <https://ethereum.org/en/developers/docs/>

World Wide Web Consortium [W3C]. (2022). *The Semantic Web Made Easy*. <https://www.w3.org/RDF/Metalog/docs/sw-easy>

Zur, C., Lacity, M., & Professor, W. (2021). *The Emergence of Web 3.0: Tokenization and the Internet of Value*. 0–19.



COMUNICACIONES

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES



Km 12+000 Carretera Estatal 431 "El Colorado-Galindo"
San Fandila, Pedro Escobedo
C.P. 76703
Querétaro, México
Tel: +52 442 216 97 77 ext. 2610

publicaciones@imt.mx

<http://www.imt.mx/>