Universidad ORT Uruguay
Facultad de Ingeniería

Cómo integrar Blockchain en una arquitectura de software: resultados de una Revisión Multivocal de la Literatura

Entregado como requisito para la obtención del título de Máster en Ingeniería

Juan Manuel Sobral – 161320

Tutores:
Martin Solari
Santiago Matalonga

2021

Declaración de Autoría

Yo, Juan Manuel Sobral, declaro que el trabajo que se presenta en esta obra es de mi propia mano. Puedo asegurar que:

- La obra fue producida en su totalidad mientras realizaba el Máster en Ingeniería por Investigación;
- Cuando he consultado el trabajo publicado por otros, lo he atribuido con claridad;
- Cuando he citado obras de otros, he indicado las fuentes. Con excepción de estas citas, la obra es enteramente mía;
- En la obra, he acusado recibo de las ayudas recibidas;
- Cuando la obra se basa en trabajo realizado conjuntamente con otros, he explicado claramente qué fue contribuido por otros, y qué fue contribuido por mi;
- Ninguna parte de este trabajo ha sido publicada previamente a su entrega, excepto donde se han realizado las aclaraciones correspondientes.

Juan Manuel Sobral
23/08/2021

Abstract

Blockchain es un registro distribuido e inmutable que facilita el proceso de almacenar transacciones y el seguimiento de activos en una red descentralizada. Es una tecnología con el potencial de revolucionar industrias, desde las finanzas hasta el IoT. Sin embargo, el panorama actual de las implementaciones de Blockchain disponibles es heterogéneo. Un arquitecto de software que busca incorporar esta tecnología a una arquitectura se enfrenta a un vasto número de redes con capacidades distintas. El objetivo de este trabajo es identificar las redes de Blockchain disponibles y sus principales características (algoritmo de consenso, descentralización, smart contracts, origen de la red), así como las posibles implicaciones de estas particularidades. Para cumplir el objetivo y analizar las principales características desde el punto de vista del arquitecto de software, se llevó a cabo una Revisión Multivocal de la Literatura. El resultado es la identificación y caracterización de 112 redes de Blockchain divididas en tres grandes familias: de uso general, de uso específico (financiero, videojuegos, identidad, pagos) y derivadas de criptomonedas. Se presenta una lista detallada de las redes disponibles. Este mapeo provee una guía a los arquitectos de software para que puedan tomar decisiones justificadas a la hora de incorporar la tecnología Blockchain.

Palabras Clave

Blockchain, Smart Contracts, Algoritmos de Consenso, Arquitectura de Software, Revisión Multivocal de la Literatura

Índice

1. Introducción

1.1. Presentación del tema

Blockchain es una tecnología emergente para la descentralización y el intercambio de datos transaccionales en grandes redes cuyos participantes son desconocidos. Blockchain permite nuevas formas de arquitectura de software descentralizada, donde los nuevos estados son alcanzados sin necesidad de confiar en una autoridad central [1]. El concepto de Blockchain en los últimos años ha tenido tanta relevancia en la discusión técnica como Machine Learning, Big Data o Inteligencia Artificial [2].

Blockchain provee un libro mayor o libro de contabilidad (ledger en inglés), que es inmutable y que facilita el proceso de registro de transacciones y seguimientos de activos en una red de negocios [3]. Un activo puede ser tangible (una casa, un automóvil, efectivo, tierra) o intangible (propiedad intelectual, patentes, derechos de autor).

El concepto detrás de Blockchain, y que es considerado una de las razones de su existencia, es la descentralización [4]. Lo cual contrasta con los sistemas centralizados, los modelos más comunes para aplicaciones de software [5, Ch. 1]. Los sistemas centralizados controlan directamente las operaciones de un individuo y el flujo de información desde un nodo central. Todos los individuos son directamente dependientes de ese nodo central de poder para enviar y recibir información. Facebook, Amazon, Google, y muchos otros servicios usan este modelo. Estos son útiles ya que nos proveen un servicio valioso, pero tienen también ciertas debilidades que se discutirán más adelante.

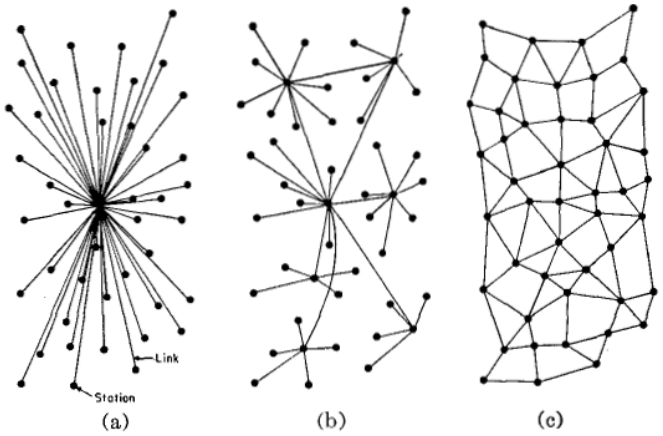

Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

Figura 1- Representación de sistemas distribuidos, descentralizados y distribuidos [5, Ch. 3]

Como muestra la Figura 1 [5, Ch. 3], la diferencia con los sistemas distribuidos, es que las relaciones están repartidas en varios nodos en vez de simplemente uno. Descentralizado significa que ningún nodo está dando las órdenes a otros nodos sobre qué es lo que hay que hacer. Un gran número de los servicios centralizados como Google, han adoptado una arquitectura descentralizada o distribuida en algunos aspectos, para mejorar la velocidad de

cómputo y la latencia de los datos. Siendo un ejemplo de que un sistema puede ser a la vez centralizado y distribuido.

Para ver un ejemplo de las áreas de aplicación de esta tecnología en casos reales, se puede presentar la industria de los títulos inmobiliarios. En la cual en algunos países donde la corrupción puede dominar, la integridad de un documento oficial puede ser cuestionable, por eso el uso de Blockchain puede potencialmente ayudar a proveer más transparencia mediante una verificación pública. Llevado a la práctica, la república de Georgia tiene un registro de los títulos de los terrenos en una red de Blockchain [6], conocido como Project Capsule.

Se estima que las ganancias globales de Blockchain van a tener un crecimiento masivo en los siguientes años [7], con un mercado que se espera que supere los 39 billones de dólares para 2025.

Para poder incluir Blockchain en una arquitectura de software, es necesario poder analizar que impacto tiene en los atributos de calidad. También elegir que datos a almacenar en la red o qué tipo de red es la que se adapta más a las necesidades. Así también como la elección de la implementación específica a utilizar de las redes de Blockchain disponibles.

1.2. Motivación

Como muchas tecnologías disruptivas que han aparecido en la última década, Blockchain ofrece nuevas posibilidades. Los problemas aparecen al momento de la integración y aplicación, y se relacionan con la temprana etapa en la que se encuentra [8]. Por lo cual creemos que es necesario investigarlo aplicando métodos rigurosos y generar evidencia para contribuir a su adopción en forma madura.

A la hora de incorporar esta tecnología en una arquitectura de software, deben tenerse en cuenta atributos de calidad propios de esta tecnología, tales como: privacidad, escalabilidad, seguridad, eficiencia, transparencia y confiabilidad [1]. Y por lo tanto, las características de cada red van a afectar estos atributos de calidad. No solo es importante conocer sobre estrategias generales de diseño arquitectónico, sino también contar con conocimientos generales de Blockchain, y conocimientos del dominio que se va a aplicar.

Al mismo tiempo que hay un gran número de proyectos y redes de Blockchain en la industria, no existe hasta el momento un catálogo disponible de todas las redes de Blockchain disponibles, el cual detalle las características y capacidad de cada una. Algunos listados parciales existen [9], pero generalmente están relacionados a un dominio en especial, como los relacionados a criptomonedas [10], o aplicados a la salud [11].

La publicidad explosiva (hype) que tuvo Blockchain, hizo que surgiera mucha literatura (formal o no) que no cumple con los estándares necesarios para ser considerada creíble. Una

investigación sobre Blockchain debe producir, consumir, y diseminar evidencia válida. En la sección 2.3, se puede ver que no hay tantas investigaciones basadas en ejercicios prácticos de aplicación, lo cual es unos de los pilares sobre la calidad en la investigación científica [12]. Muchas veces las afirmaciones en la práctica por los proveedores deben ser validadas por la investigación independiente, por eso también la tesis intenta apoyar esta información.

1.3. Objetivos de investigación

Para favorecer la adopción de Blockchain, esta tesis propone formalizar las definiciones de los conceptos relacionados, para poder profundizar y entender cómo forman parte de Blockchain.

Se realizó una Revisión Multivocal de la Literatura (MLR por sus siglas en inglés) [13] de las redes de Blockchain disponibles, analizando las características de cada una. Mientras que una Revisión Sistemática de Literatura (SLR) generalmente no describe el estado del arte en sentido práctico, ya que no considera literatura gris (no publicada), una MLR es una forma de revisión la cual incluye la literatura gris sumada a la literatura formal.

1.4. Justificación

La falta de volumen y calidad en la literatura formal se puede ver en algunas revisiones sistemáticas [14], donde solo pudieron filtrar 41 papers, de los cuales más del 80% estaban relacionados a Bitcoin.

Otros investigadores han seleccionado esta metodología (MLR) no solo para estudiar la tecnología de Blockchain [15] [16], sino también para otras tecnologías similares como Microservicios [17] y Function-as-a-Service [18]. Estas tecnologías emergentes comparten con el panorama actual de Blockchain que gran parte de la información y el conocimiento están impulsados por la industria, y la literatura académica formal no ha podido proporcionar conocimiento basado en evidencia de aplicación.

1.5. Contribuciones y resultados

A través de la aplicación de una MLR, se identificaron 112 redes de Blockchain. Para cada una de estas redes, se analizaron sus algoritmos de consenso, si aceptan o no smart contracts, junto con otras características como: dominio, descentralización, estructura del ledger y configuración de los bloques. Considerando estas características analizadas, los aspectos fundamentales que pueden ser considerados a la hora de adoptar Blockchain en una arquitectura de software. Sintetizamos esta investigación en un mapeo ortogonal de las redes encontradas. Este mapeo provee una guía al arquitecto de software para facilitar la elección sobre incorporar Blockchain.

Al tener un catálogo se pudo llegar a una investigación de los grupos más comunes de atributos, así como tener una categorización inicial de las redes. Del cruzamiento de la información con las preguntas de investigación se llegan a conclusiones como que las criptomonedas son el mayor dominio específico para las redes de Blockchain (29), de las cuales la mayoría son una mejora incremental o derivada de Bitcoin. Las criptomonedas además son el grupo con menor referencia en la literatura formal. De los que no son criptomonedas, 81 de 83 aceptan el desarrollo de smart contracts, y un tercio derivan de Ethereum.

Además, del cruzamiento de información se pudo concluir que los atributos de calidad más evaluados a la hora de elegir una red son la performance y la escalabilidad. Estos atributos están íntimamente relacionados al algoritmo de consenso, que a la vez es el tema más tratado en los artículos sobre arquitectura de Blockchain [16].

Un artículo con resultados preliminares fue presentado en las Jornadas Chilenas de Computación 2020[1] [19]. Un reporte completo de la MLR y discusión del impacto de Blockchain en la arquitectura de software fue enviado para su publicación en el journal arbitrado Future Generation Computer Systems[2] [20] (en proceso de revisión).

[1] https://jcc2020.cl/
[2] https://www.sciencedirect.com/journal/future-generation-computer-systems

2. Estado del arte

2.1. Criptomonedas

Las criptomonedas y las Blockchain emergieron y evolucionaron juntos. Sin embargo, una búsqueda de los resultados de Google de “Bitcoin” y “Blockchain”, arrojan resultados de las magnitudes de 11 a 1 favorables para Bitcoin [21]. Esto es debido a la exposición pública que tuvo. Blockchain puede existir sin las criptomonedas, pero las criptomonedas no pueden existir sin Blockchain, a pesar de haber algunas criptomonedas basadas en soluciones criptográficas avanzadas, que no necesitan Blockchain para su operación [22].

Dentro de este grupo, se encuentran algunos predecesores a Bitcoin, como es eCash, cuya idea de dinero electrónico anónimo aparece en un artículo en 1983 [23]. El software de eCash era instalado en la computadora local de la persona y almacenaba dinero en formato digital, criptográficamente firmado por el banco [24]. El usuario podía gastar ese dinero digital en cualquier tienda que aceptara eCash, sin la necesidad de abrir una cuenta o transmitir números de tarjeta de crédito.

E-Gold fue propuesto en 1996 (dos años antes del lanzamiento de Paypal) y fue el primer servicio de pagos sin tarjeta de crédito en ofrecer una API (application programming interface), permitiendo a otros servicios y e-commerce integrarse con ellos. E-Gold estaba respaldado por unidades reales de metales preciosos y fueron los primeros en introducir el concepto de micropayments.

Otro ejemplo previo es Hashcash, presentado en 1997 por Adam Back[3] y descrito formalmente en 2002 [25]. Hashcash introduce la idea de usar proof of work para verificar la validez de los fondos digitales, incluyendo el concepto de que el dinero existe solamente en el internet. Al usar proof of work, se empieza a considerar que las computadoras necesitan producir algún tipo de salida verificable y difícil de resolver computacionalmente, para que el dinero tenga valor.

La crisis financiera del 2007-2008, fue considerada por economistas como una de las más grandes luego de la Gran Depresión. La poca regulación financiera, la toma excesiva de riesgos por los bancos y el estallido de la burbuja inmobiliaria de Estados Unidos, llevaron a afectar las instituciones financieras de todo el mundo, desencadenando una crisis bancaria internacional. Esto es relevante para la discusión de Blockchain, ya que muchos de los conceptos y tecnologías por detrás de Bitcoin existían antes del 2008, pero la situación económica afectó de forma positiva para mezclar los conceptos del dinero virtual existentes para crear un sistema que permite transparencia y confianza digital [22].

[3] http://www.hashcash.org/papers/announce.txt

La aplicación del concepto “Chain of Blocks” fue presentada por la persona o grupo Satoshi Nakamoto, en el whitepaper “Bitcoin: A peer to peer digital cash system” [26]. Cuyo objetivo es explicar el algoritmo de consenso Proof of Work, mediante la representación de encadenamiento de un bloque con su anterior en una cadena. El concepto de cadena de bloques, aparece en la literatura en dos artículos. En 1991 [27] un estudio que presentaba el concepto de cadena de bloques unidos mediante un timestamp, para establecer la propiedad intelectual para documentos digitales. La otra aparición es en 1976, en una patente titulada “Message Verification and Transmission Error Detection by Block Chaining” [28]. Su idea básica era proporcionar un intercambio de mensajes seguros mediante funciones criptográficas, en las cuales cada bloque es generado por todos los anteriores bloques encriptados en el mensaje.

Otro hito dentro del mundo de las criptomonedas, fue el lanzamiento de Ethereum en Julio de 2015, siendo la primera red en proponer que una Blockchain se convierta de una ledger a una máquina de estados descentralizada. Esto es alcanzado mediante el concepto de los smart contracts. La red de Ethereum es una gran estructura de datos que contiene no solo todas las cuentas y saldos, sino también un estado de máquina, que puede cambiar de un bloque a otro de acuerdo con un conjunto predefinido de reglas, y que puede ejecutar códigos de máquina arbitrarios [29]. Al igual que varios de los conceptos de Blockchain, el concepto de smart contract no fue introducido por Ethereum, si no que fue introducido por Szabo en 1994 [30], antes de la aparición de las redes de Blockchain, y lo definió como un protocolo programable de transacciones que ejecuta los términos de un contrato.

2.2. Proveedores tecnológicos y ejemplos de aplicación

Con el crecimiento de la tecnología Blockchain, muchas de las grandes empresas quieren ofrecer herramientas para facilitar y favorecer su adopción. IBM cuenta con IBM Blockchain [31], un servicio de Blockchain as a service, que está basado en la implementación de Hyperledger Fabric [32], desarrollada por la Linux Foundation (explicada en la investigación). Esta herramienta es un servicio cloud público, que los clientes pueden usar para construir redes seguras de Blockchain [33]. Microsoft ofrece su kit de desarrollo Blockchain Workbench sobre Azure [34]. En resumen, es una colección de servicios de Azure designados para crear y desplegar aplicaciones de Blockchain.

Existen redes de Blockchain ya funcionando en producción para solucionar problemas en distintas áreas, por ejemplo en el de las aseguradoras y los seguros. Blockchain puede ayudar mediante intercambios de datos verificables, visibilidad para todas las partes y transacciones criptográficamente respaldadas, a aumentar la seguridad y la confianza de un sistema. Un ejemplo es Open Insurance Data Link (openIDL) [35], una red creada en IBM Blockchain con la American Association of Insurance Services (AAIS). El proyecto se encarga de automatizar los contratos de informe, programando los requisitos de cumplimiento de los contratos del seguro. Buscando el objetivo de mejorar la eficiencia y la precisión de

ejecución de los contratos, tanto para las aseguradoras como para los departamentos de seguros estatales.

En el área de la trazabilidad y los alimentos, IBM y Walmart establecieron un acuerdo para hacerle frente al problema de la contaminación de los alimentos [36]. Hicieron una prueba de concepto de un sistema de trazabilidad de la cadena de suministro para carne de cerdo en China, y mangos en las américas. La solución basada en Hyperledger permite reducir el tiempo para trazar el origen de un mango de 7 días a 2.2 segundos. Provee una completa trazabilidad de principio a fin [37], no solo promoviendo mayor transparencia, sino previniendo o respondiendo rápidamente a la contaminación de los alimentos, enfermedades, residuos de drogas o pesticidas, o intentos de bioterrorismo. Nestlé también incursionó en este terreno, aliándose con AWS para comenzar a hacerle el seguimiento de la ubicación de 15 materias primas, para permitirle a sus clientes que pueden hacer el seguimiento de sus productos en la Blockchain desde la granja hasta su consumo [38]–[40].

IBM también se alió con Maersk para aplicar otra red de Blockchain basada en Hyperledger a la cadena de suministro del transporte de contenedores [38]. Todos los documentos para el envío fueron digitalizados y los containers cuya ubicación es registrada durante todo su viaje. Uno de los objetivos es reducir los costos mediante la digitalización de la información, así como la transparencia e información en tiempo real de los bienes. Amazon tiene en cambio, un acuerdo con TEUwork para brindar eficiencia y transparencia en el sistema global de la cadena de suministro[38], [39].

Bitfury Group, proveedor de infraestructura y de soluciones relacionadas a Blockchain, en su alianza con la National Agency of Public Registry (NAPR) de la República de Georgia, diseñaron e implementaron un sistema de Blockchain integrado con el sistema de registros digitales de NAPR [41]. Esta Blockchain privada y con permisos implementada sobre Bitcoin, permite que el NAPR pueda verificar y firmar documentos que contienen la información esencial para los ciudadanos acerca de la posesión de una propiedad. Esta solución open source [42] protege la información de la manipulación interna y de los ciberataques externos, instaurando confianza en la integridad de los datos del sistema de registro digital de terrenos. El proyecto fue extendido para incluir la compra y venta de los terrenos, registro de nuevos terrenos, demolición de propiedades, hipotecas, alquileres, y servicios notariales.

Junto con los ejemplos de arriba, actualmente vemos cada vez más ejemplos de aplicaciones que usan Blockchain en producción. Ya pasaron de ser pruebas de concepto a aplicaciones siento utilizadas en producción, incluso algunas sin que nos demos cuenta de que esta tecnología se encuentra por detrás. Para nombrar algunos ejemplos:

- **BurstIQ**: Sus smart contracts ayudan a los pacientes y médicos a transferir de forma segura información médica confidencial. Los contratos inteligentes establecen los

parámetros de qué datos se pueden compartir e incluso muestran detalles de planes de salud personalizados para cada paciente.

- **Mediachain:** Utiliza smart contracts para que los músicos obtengan el dinero sin intermediarios. Al celebrar un contrato descentralizado y transparente, los artistas pueden acordar regalías más altas y recibir el pago completo y puntual. Spotify adquirió Mediachain en abril de 2017.

- **OPSkins:** Los jugadores que buscan comprar skins raras, accesorios e incluso emotes pueden usar Bitcoin como método de pago en el mercado en línea de OPSkins. Los vendedores reciben el bitcoin en su billetera virtual y optan por quedarse con la criptomoneda o cambiarla por efectivo. Este sistema procesa más de dos millones de transacciones virtuales a la semana.

Relacionado al crecimiento de Blockchain y su ecosistema, Linkedin muestra en su reporte anual de trabajos emergentes, como Blockchain tuvo un crecimiento de x33 [43]. Según la CNBC [44], los desarrolladores de Blockchain están dentro de los puestos más pagados en el desarrollo de software (de un 25% a un 35% más), a la par con los especialistas en inteligencia artificial.

2.3. Trabajos de investigación

El crecimiento presentado en la sección anterior, hace que sea necesario que surjan investigaciones bien fundadas sobre esta tecnología. En la Figura 2, podemos ver cómo la cantidad de artículos indexados en Google Scholar fue incrementando pero no a la par del crecimiento en la industria.

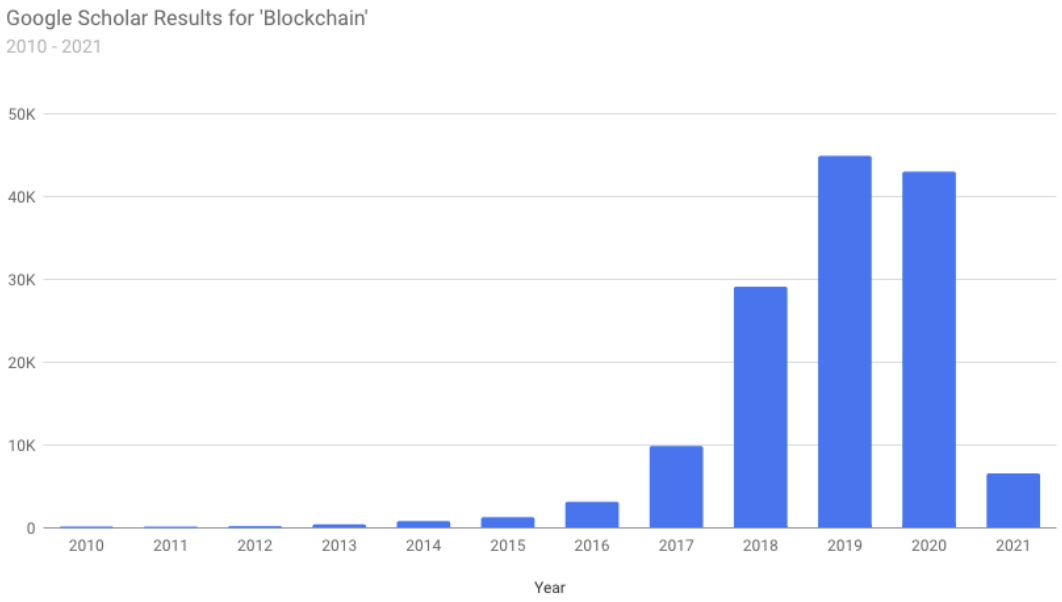

Figura 2 Resultados de Google Scholar a “Blockchain”

Podemos ver en la Tabla 1 tomada de [45] la cantidad de artículos de investigación disponibles hasta 2019 en las plataformas: ACM Digital Library, IEEEXplore, ISI Web of Knowledge, ScienceDirect y SpringerLink. La revisión sistemática de literatura muestra que el método de investigación más utilizado para estos artículos es la investigación conceptual, lo que demuestra que están más enfocados en explorar esta nueva área, que en la aplicación práctica de la misma. Es difícil realizar una investigación interdisciplinaria sobre la tecnología Blockchain, en especial sobre cómo integrarlo en una arquitectura de software, ya que necesita conocimientos de: Blockchain, arquitectura de software, y del dominio de aplicación. Por lo tanto, será importante que los investigadores con experiencia en TI, comprendan y profundicen en los conceptos de criptografía, protocolos, descentralización, para colaborar con otros investigadores de formación no técnica.

Step	Description	ACM Digital Library	IEEE-Xplore DL	ISI Web of Science	Science Direct	Springer Link	Total
1	# of results	178	346	338	61	280	1.203
	- Blockchain*	119	258	256	50	172	855
	- Smart Contract(s)	34	63	59	8	70	234
	- Ethereum*	25	25	23	3	38	114
2	# of distinct papers	125	265	274	52	191	753
3	# of articles published in journals	8	51	118	49	154	334
4	# of papers in high-impact journals	0	15	22	27	18	68
5	# of papers with relevant content	0	8	12	13	4	29

Tabla 1 - Resultados de búsqueda de artículos en 2019 [44]

2.3.1. Revisiones sistemáticas de Blockchain

Hemos identificado varias revisiones sistemáticas sobre cómo Blockchain ha sido aplicado a varios dominios, como en la cadena de suministro, finanzas, salud, IoT, privacidad y gestión de datos. Pero estos artículos no especifican las alternativas de redes de Blockchain, sino que se concentran en el número de artículos disponible en cada dominio, sin considerar las aplicaciones del mundo real. Algunos ejemplos:

- **Blockchain for the Internet of Things: a Systematic Literature Review** [46]. En donde de 1511 artículos, pasaron el filtro definido 35. Los autores encuentran que hay varios casos de uso para manejo de datos descentralizados para IoT. A pesar de la

integridad y la adaptabilidad, ellos creen que la escalabilidad de Bitcoin lo hace poco adaptable a IoT.

- **A Systematic Review of the Use of Blockchain in Healthcare** [11]. De 12000 artículos, pasaron el filtro definido 71. Las conclusiones del artículo indican que los estudios sobre Blockchain aplicados a la salud están creciendo. Actualmente, la investigación se centra en el intercambio de datos, los registros médicos y el control de acceso, pero rara vez en otros escenarios, como la gestión de la cadena de suministro o la gestión de recetas de medicamentos. Esto abre el lugar para que la investigación siga avanzando.

- **Blockchain for Cities — A Systematic Literature Review** [47]. De 3827 artículos, pasaron el filtro definido 1591. Los autores mantienen que en algunos sectores, como el medio ambiente o la gestión de residuos y agua en general reciben menos atención que otros sectores como energía, transporte, economía, salud, educación, gobierno. Independientemente del sector, todos ellos enfrentan los mismos desafíos: rendimiento, escalabilidad, estandarización e interoperabilidad, seguridad y privacidad de datos de activos, además de las cuestiones regulatorias. Encontraron que Ethereum e Hiperledger Fabric son las Blockchain más usadas en el área de Smart Cities.

- **Supply Chain Management based on Blockchain: A Systematic Mapping Study** [48]. De 227 artículos, pasaron el filtro definido 24. Los resultados demuestran que el 42,5% de los artículos se centran en la trazabilidad de la cadena de suministro, el 17% de los artículos abordan la información de SCM y el 17% de los estudios se realizaron sobre la financiación de la cadena de suministro impulsada por Blockchain. La gran parte de los estudios seleccionados (45.7%) se concentra en proponer soluciones a los desafíos actuales de la cadena de suministro mediante el diseño de nuevos marcos basados en Blockchain. Sin embargo, muchas de las soluciones basadas en marcos propuestas carecen de una evaluación real del desempeño en el contexto industrial.

Otros autores han llevado a cabo mapeos sistemáticos sin enfocarse en ningún dominio. En [14] se presenta un mapeo donde el objetivo es comprender las tendencias actuales de investigación de la tecnología Blockchain, junto con los desafíos y direcciones futuras de dicha tecnología. El objetivo de [49] es identificar las áreas en las que se están desarrollando aplicaciones de Blockchain, tanto en el sector público como el privado. Este artículo concluye que aunque hay áreas de aplicación, más progreso es necesario en investigación y literatura formal.

De todos estos estudios se puede concluir que hay una falta de investigación cualitativa y cuantitativa. Esto implica que el uso de Blockchain no fue todavía evaluado en una base

científica empírica. Esto también fue observado en el estudio [45], que concluye que las investigaciones sobre la tecnología en sí misma, así como sobre sus aplicaciones e implicaciones se encuentran en una etapa muy temprana.

A nuestro entender, solo [16] aplica una MLR para estudiar Blockchain. Los autores presentan una revisión de más de 10 motores de búsqueda[4] como literatura científica, además de utilizar los primeros 160 resultados de Google para la literatura gris. Dentro de este grupo consideran libros, revistas, reportes técnicos, whitepapers, reportes anuales de empresas, pero descartan bases de datos, audio, video y presentaciones. Luego de aplicar los criterios de exclusión, listan 75 artículos científicos y 32 artículos de literatura gris. Algunos resultados interesantes que concluyeron es que la mayoría de los resultados sobre la arquitectura Blockchain (44) están relacionados con algoritmos de consenso (24), el resto son visiones generales de la arquitectura (14) y alternativas de Blockchain (6). También presentan una evolución detallada de los algoritmos de consenso relacionados con los desafíos que enfrentó Blockchain, en orden cronológico. Tomados en conjunto, los resultados muestran que ha habido intentos desesperados de abordar Bitcoin. Un enfoque uniforme que aborde simultáneamente conjuntos específicos de problemas sigue sin existir. Si bien su objetivo es una caracterización inicial de la tecnología y una descripción detallada del estado del arte, nuestro trabajo difiere del de ellos, ya que nuestro objetivo es proporcionar evidencia para incorporar la tecnología en una arquitectura de software.

2.4. Catálogos

Uno de los objetivos de esta tesis es obtener un listado de las redes de Blockchain disponibles. Existen catálogos online que listan las alternativas (directa o indirectamente) pero sin incluir las características de cada una de las redes. Algunos se centran en criptomonedas y no cubren otros dominios de aplicación. Los catálogos más reconocidos, y que contienen decenas de redes son:

- **CoinMarketCap** [50]: Un servicio web que provee información en tiempo real sobre la industria de criptomonedas. Contiene detalles sobre los precios y los últimos movimientos para más de 4800 criptomonedas.

- **Golden** [51]: Una base de datos de conocimiento basado en la comunidad, que a través de inteligencia artificial y procesamiento de lenguaje natural obtienen información relacionada a tecnologías emergentes de noticias, sitios web y bases de datos públicas. Tienen una sección enfocada en Blockchain y criptomonedas, donde además de listar a las redes, contienen marco teórico de Blockchain y los algoritmos de consenso.

[4] ACM Digital Library, SCOPUS, IEEE Xplore Digital Library, Science Direct, SpringerLink and Wiley InterScience, EBSCO electronic library, JSTOR knowledge storage and, ProQuestABI/Inform

- **Crypto & Blockchain** [52]: El sitio de noticias Forbes tiene una sección específica de Blockchain y criptomonedas. Todos los años se presentan las 50 empresas con más de $1B de valuación o en ganancias, que están implementando Blockchain. Dentro de este listado se pueden reconocer las nuevas redes alternativas que van surgiendo, además de poder ver qué redes están siendo utilizadas por las grandes empresas.

Además, existen varios sitios web indexados en las primeras páginas de Google [53] [54] [55] que presentan alternativas de redes de Blockchain. Siendo ninguna tan extensa o de la calidad y el respaldo como las mencionadas arriba.

3. Marco conceptual

3.1. Arquitectura de software

Ya que Blockchain puede ser considerada una herramienta para que el arquitecto de software construya la mejor solución para satisfacer los requerimientos de un sistema, es importante profundizar sobre el concepto de arquitectura de software. Generalmente se define como los componentes y conectores que hacen la estructura general de un sistema [56]. Pero esto incluye más detalles como qué tipos de componentes son, dónde están alojados, son código desarrollado o herramientas de terceros, además de otros detalles. Según Bass et al. [56], se puede definir a la arquitectura de software de un programa o sistema de cómputo como la estructura de las estructuras del sistema, lo cual comprende los componentes, las propiedades vistas exteriormente de los mismos, y las relaciones que tienen entre ellos.

La arquitectura restringe la implementación de un sistema desde las decisiones iniciales de diseño. Además, permite alcanzar los atributos de calidad deseados en un sistema, logrando tener una representación abstracta y transferible de un sistema.

Es importante entender las principales propiedades funcionales y no funcionales de la tecnología Blockchain para tener un buen diseño de arquitectura, apoyando una eficiente inclusión de esta tecnología. En especial porque los sistemas basados en Blockchain son distintos de los sistemas tradicionales [57], en especial porque hay que considerar configuraciones y funcionalidades de una red para analizar su impacto en los atributos de calidad de todo el sistema. Por ejemplo, cómo definir el algoritmo de consenso que más aplique a las necesidades del sistema, o qué información va a ser guardada en la red.

Es importante aclarar que la arquitectura de un sistema, es una respuesta humana sobre cómo resolver los requerimientos, aplicando procesos y modelos para llegar a esta solución. Esto genera errores humanos ya que no existe una fórmula matemática fácilmente aplicable. Según Bass et al. en los sistemas complejos, los atributos de calidad (ver siguiente sección) nunca pueden ser alcanzados de forma aislada. El satisfacer alguno, va a tener un efecto que puede ser positivo o negativo, sobre otros [56]. Esta afirmación tiene sentido ya que un sistema es la suma de todas sus partes, y no puede considerarse un atributo específica aislado como referencia del todo.

3.2. Atributos de calidad

Los atributos de calidad en el software son un conjunto de características que demuestran la calidad de un sistema de software [58]. O pueden ser definidos como una propiedad medible o que puede ser probada [56], que puede ser indicada para ver qué tan bien satisface las necesidades del negocio. El modelo de calidad representa una base

fundamental a partir de la cual se establece un sistema para la evaluación de la calidad del producto. La calidad de un producto de software se puede interpretar como el grado en que dicho producto satisface los requisitos de sus usuarios aportando de esta manera un valor.

Según la norma ISO/IEC 25010:2011, un modelo de calidad de un producto está compuesto por ocho características de calidad [59]:

- **Adecuación funcional:** representa la capacidad del producto de software para proporcionar funciones que satisfacen las necesidades declaradas e implícitas, cuando el producto se usa en las condiciones especificadas.

- **Eficiencia de desempeño:** representa el desempeño relativo a la cantidad de recursos utilizados bajo determinadas condiciones.

- **Compatibilidad**: capacidad de dos o más sistemas o componentes de funcionar correctamente cuando comparten el mismo entorno, hardware o software.

- **Usabilidad**: grado en el que un producto o sistema puede ser utilizado por usuarios específicos para lograr objetivos específicos con efectividad, eficiencia y satisfacción en un contexto de uso específico.

- **Fiabilidad**: grado en el que un sistema, producto o componente realiza funciones específicas en condiciones específicas durante un período de tiempo específico.

- **Seguridad**: grado en el que un producto o sistema protege la información y los datos para que las personas u otros productos o sistemas tengan el grado de acceso a los datos apropiado para sus tipos y niveles de autorización.

- **Mantenibilidad**: representa la capacidad del producto software para ser modificado efectiva y eficientemente, debido a necesidades evolutivas, correctivas o perfectivas

- **Portabilidad**: grado de eficacia y eficiencia con el que un sistema, producto o componente se puede transferir de un hardware, software u otro entorno operativo o de uso a otro.

Las críticas al modelo ISO/IEC 25010:2011 sugieren que los estándares garantizan la uniformidad de las salidas de los sistemas, lo cual pueden llevar a la producción estandarizada de malos productos [60]. Además de que los atributos son de uso general de todos los sistemas, los mismos se basan en los descritos en la ISO/IEC 9126:1991, casi 20 años de la fecha de lanzamiento de Bitcoin (2009) y de que los sistemas distribuidos y Blockchain comenzaran a tener importancia. Creemos importante que para analizar un modelo de calidad de un sistema de Blockchain, investigar otras caracterizaciones de los atributos de calidad, pero aplicados a sistemas distribuidos.

Por ejemplo Forslund et al. establecen una caracterización y división de los atributos específicamente para sistemas distribuidos. Ellos sostienen que son: confiabilidad, disponibilidad, replicación, tolerancia a fallas, integridad transaccional, persistencia, seguridad, movilidad de objetos, heterogeneidad, escalabilidad y rendimiento [61].

A la vez encontramos una división de atributos propuesta por Pérez-Martínez et al. según la siguiente taxonomía [62]:

- **Intrínsecos**: Son los que se derivan directamente de la propia naturaleza del sistema, estos están relacionados directamente con la descentralización. Dentro de este grupo están: concurrencia, heterogeneidad, comunicación, transparencia y recursos compartidos.

- **Específicos**: Son requerimientos que demuestran un objetivo a cumplir, relacionados al uso que quiera dársele al sistema. Dentro de estos se encuentran: rendimiento, confiabilidad, escalabilidad, extensibilidad, performance, acceso y seguridad, y reconfiguración dinámica.

- **Mecánicos**: Relacionados a los mecanismos de soporte a los requerimientos de los grupos anteriores. Como pueden ser: replicación, movilidad o migración de objetos, asignación o equilibrio de carga, persistencia, estructura del software, mantenimiento de la coherencia, integridad transaccional y tolerancia a fallos.

Esta división fue la que más se acerca a nuestro trabajo, porque por un lado establece una clara distinción entre lo que es un atributo de calidad, y los mecanismos para lograrlos. Y por el otro lado, diferencia aquellos atributos que están presentes en todos los sistemas distribuidos (intrínsecos), y aquellos que dependen de la aplicación en particular (específicos). En una primera etapa de la tesis, los atributos dentro de cada taxonomía y otros van a ser explicados y analizados desde el punto de vista de por qué son importantes para las distintas redes de Blockchain.

3.3. Sistemas distribuidos

Vamos primero a definir los conceptos de Descentralizado y Centralizado, ya que son palabras que están pobremente definidas, y que pueden afectar distintos ejes [4]. Cuando se habla de sistemas distribuidos en software, hay realmente tres ejes separados sobre los que se puede estar refiriendo. Mientras que en algunos casos es difícil separar estos ejes, son generalmente independientes uno del otro. Estos son:

- **Descentralización de arquitectura:** Se refiere a cuántas computadoras físicas conforman el sistema. Lo cual nos lleva a preguntarnos cuántas de esas computadoras pueden fallar a la misma vez para dejar el sistema inhabilitado.

- **Descentralización política:** ¿Cuántos individuos o organizaciones controlan las computadoras con las cuales el sistema está sostenido?

- **Descentralización lógica:** ¿Las interfaces del sistema y las estructuras de datos que el sistema presenta y mantiene, se ven como un objeto con una estructura concreta, o algo totalmente sin forma ni estructura? Una posible medida de esto puede ser analizada de la siguiente manera: si se separa el sistema en dos partes, quedando de un lado los proveedores del servicio y por el otro los usuarios, ¿van a poder los dos seguir operando como elementos independientes?

En la Figura 3 tomada de [4] podemos ver los tres niveles de descentralización representados.

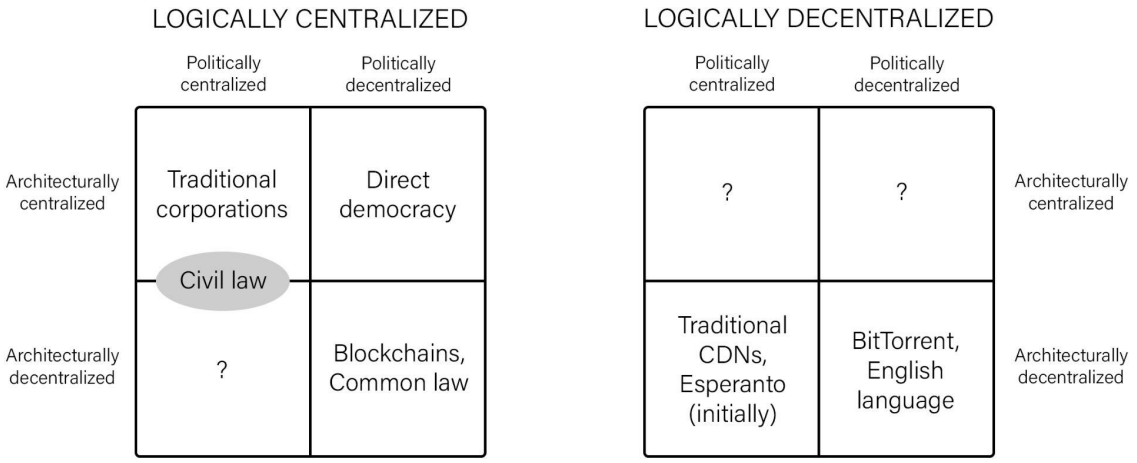

Figura 3 - Ejemplos sobre los distintos tipos de descentralización [4].

Se pueden establecer algunas analogías entre los tipos de descentralización y otros sistemas humanos:

- Las empresas tradicionales son políticamente centralizadas (en un CEO), - arquitecturalmente centralizadas (en una oficina central) y lógicamente centralizadas (no se puede partir a la mitad)

- El derecho civil, se sostiene en un grupo centralizado encargado de crear las leyes, mientras que el derecho consuetudinario se basa en precedentes creados por un historial de jueces individuales. El derecho civil tiene cierta descentralización arquitectónica, ya que hay un número elevado de tribunales y con gran discreción para tomar sus decisiones, pero los de derecho común tienen aún más . Ambos están lógicamente centralizados, ya que hay una única ley.

- Los lenguajes son lógicamente descentralizados, ya que el inglés hablado entre dos personas en un lugar, no es necesariamente el mismo que el hablado en otra región

o país. No hay una infraestructura central requerida para que un lenguaje exista, y las reglas gramaticales no son controladas por una sola persona.

- BitTorrent es lógicamente centralizado al igual que inglés. Las redes de entrega de entrega de contenidos (content delivery network) [20] son similares, pero controladas por una sola compañía (ej: Cloudinary [21])

- Las redes de Blockchain son políticamente descentralizadas (nadie las controla) y arquitectónicamente descentralizadas (no hay un punto de falla infraestructural), pero son lógicamente centralizadas (ya que hay un estado acordado, y el sistema se comporta como una sola computadora)

Algunos autores presentan cuáles son algunas de las ventajas de la descentralización [4] [5]:

Beneficios de punto de vista técnico:

- **Tolerancia a los fallos:** Los sistemas descentralizados tienen menos posibilidad de falla, ya que dependen de varios componentes separados que es poco probable que todos tengan un problema a la misma vez.

- **Resistencia a los ataques:** Tienen un costo más elevado para ser atacados, ya que no hay un único punto que puede ser atacado, destruido o manipulado. Sino que habría que realizar un ataque a gran escala de todo el sistema.

- **Uniformidad del sistema:** Al tener sistemas centralizados, se hace más difícil la intercomunicación de distintos sistemas ya que tienden a ser distintos. Teniendo un único sistema descentralizado, todas las partes siguen las mismas reglas y tienen las mismas interfaces.

Beneficios de punto de vista político:

- **Resistencia a la colisión:** Es más difícil para los participantes de un sistema descentralizado para actuar en su beneficio, ya que cualquier gobierno o empresa puede favorecerse a sí misma a expensas de los ciudadanos, empleados, clientes o del público en general.

- **No lugar a discrepancias:** Sin la descentralización, cada uno sigue su propia historia con discrepancias que ocasiona disputas, lo que puede llegar a tener necesidad de un intermediario. Sin embargo, en un sistema descentralizado, donde ningún dato puede ser alterado, y cuando se tiene que tener un consenso para cualquier cambio. Los participantes pueden ahorrar tiempo y costos, disminuyendo el riesgo. [22]

- **Confianza en una autoridad central:** Los usuarios pueden dejar de brindarle a las compañías y a los gobiernos su información y el dinero. En un sistema

descentralizado, los participantes no tienen que confiar en nadie más que en el sistema.

- **Desprivatización de los datos:** Relacionado con el punto anterior, los datos dejan de pertenecer a un ente privado. De esta forma se hace casi imposible que una compañía de redes sociales, venda la información recolectada a empresas del mundo.

- **Menos censura:** Lamentablemente se está volviendo común que los gobiernos corten el acceso a las redes sociales, de manera de poder controlar la imagen de la realidad. Es más difícil de censurar un sistema descentralizado peer-to-peer, ya que habría que controlar el tráfico entre todos los participantes de la red.

- **Contribución descentralizada:** Hay una idea de que la gente que contribuye a los sistemas descentralizados reciben una participación o recompensa económica dentro de la red, lo cual se vuelve más valioso cuando el sistema crece. De esta forma en contraste a los sistemas centralizados, en los cuales el dueño de la información es el único que recibe valor a medida que el sistema crece.

Estas ventajas no significan que Blockchain sea una tecnología capaz de solucionar todos los problemas del área en que sea aplicada, pero lo que sí demuestra en teoría es el potencial que tiene. Por lo cual tiene sentido investigar esta área y poder profundizar en sus aplicaciones.

3.4. Blockchain

Blockchain fue inventado por Satoshi Nakamoto (puede ser una persona desconocida o un grupo de personas) en 2008 para servir al libro mayor de transacciones (public ledger) de la moneda digital (criptomoneda) Bitcoin [63]. Con esta tecnología se solucionaba el problema del doble gasto de una moneda, sin la necesidad de una autoridad confiable o servidor central que lo controle. Una criptomoneda es un activo digital definido por un protocolo de Blockchain e intercambiado a través de ese sistema.

Blockchain puede ser definido como una secuencia de bloques (blocks), las cuales tienen toda la información sobre la lista de transacciones realizadas [64]. La Figura 4 muestra un ejemplo de Blockchain, en donde un hash de información sobre el bloque anterior está contenido en el siguiente bloque, habiendo un único padre. El primer bloque de una Blockchain es llamado bloque génesis, y es el único que no va a tener un padre.

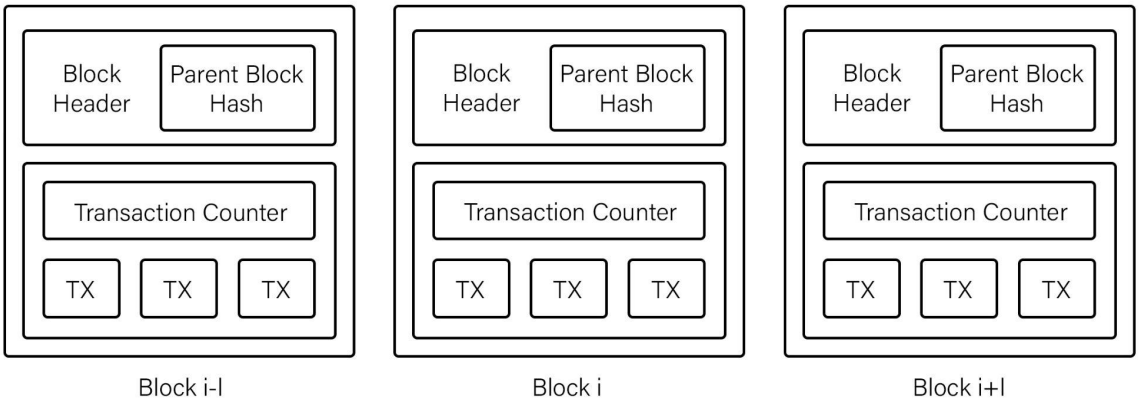

Figura 4: Un ejemplo de una cadena de Blockchain. Fuente: Elaboración propia.

Cuando hablamos de hash de información en Blockchain, nos referimos a información que ha sido transformada mediante una función de hash criptográfica. Idealmente, una función de hash debe ser simple de computar, y debería asegurar que si es aplicada a dos entradas de datos, devuelve valores distintos. Al haber un tope a lo largo de la salida y hay un número infinito de entradas, esto es claramente imposible. Entonces lo que se busca generalmente es una función de hash que distribuya los resultados de forma equitativa [65].

En el caso de una función de hash criptográfica, la salida tiene un largo establecido y tiene que cumplir [66]:

- **Determinista**: No importa cuántas veces se aplique la función a un input, siempre tiene que devolver el mismo resultado.
- **Velocidad de Cómputo**: La función tiene que ser capaz de retornar la salida rápidamente.
- **Pre-Image Resistance**: Se refiere a que dado el resultado de la función de hash, no es factible determinar la entrada. Si la entrada de datos es grande, la única forma de obtener el resultado es mediante fuerza bruta. Lo que significa probar con entradas de datos random hasta que el hash sea el que estamos buscando.
- **Resistencia a las Colisiones**: Que sea difícil encontrar dos entradas que produzcan un mismo resultado.
- **Pseudo-Randomness**: Que no se pueda distinguir entre el retorno de la función y un resultado random.

La etimología de la palabra Blockchain, nos lleva a definirlo como una lista concatenada de datos y punteros de hash que apuntan a los bloques anteriores, por lo tanto creando una cadena. Estos punteros están formados por las direcciones únicas del bloque, más toda la

información contenida. Esto hace que cualquier cambio pequeño en los datos, resulte en un hash totalmente distinto, lo que hace una red de Blockchain totalmente confiable en sus datos.

Blockchain utiliza mecanismos de criptografía asimétrica (o también llamada public key cryptography) para validar la autenticidad de las transacciones y poder confiar que las personas dicen quien realmente dicen ser. Utiliza una firma digital (digital signature) basada en esta criptografía, para dar confianza acerca de los datos en una red de participantes desconocidos [67]. Esta firma es un formato aceptado llamado Public Key Infrastructure (PKI), en la que cada usuario tiene una clave privada y una pública. La privada se usa para firmar los documentos, y la pública para desencriptar.

La Figura 5 [66] muestra un ejemplo de cómo se aplican generalmente las firmas digitales en una Blockchain. Un usuario (Signer) quiere firmar una transacción, primero usa un algoritmo de hashing a los datos que quiere enviar, luego estos datos son encriptados utilizando su clave privada. Este documento firmado digitalmente viaja por la red hasta otro usuario (Verifier), el cual se desencripta usando la clave pública (ya que se encuentra disponible para toda la red). Si el hash resultado de Desencriptar el documento con la clave pública, se corresponde con el hash del documento, la firma es válida y el que recibe el documento puede estar seguro de la validez de los datos [68].

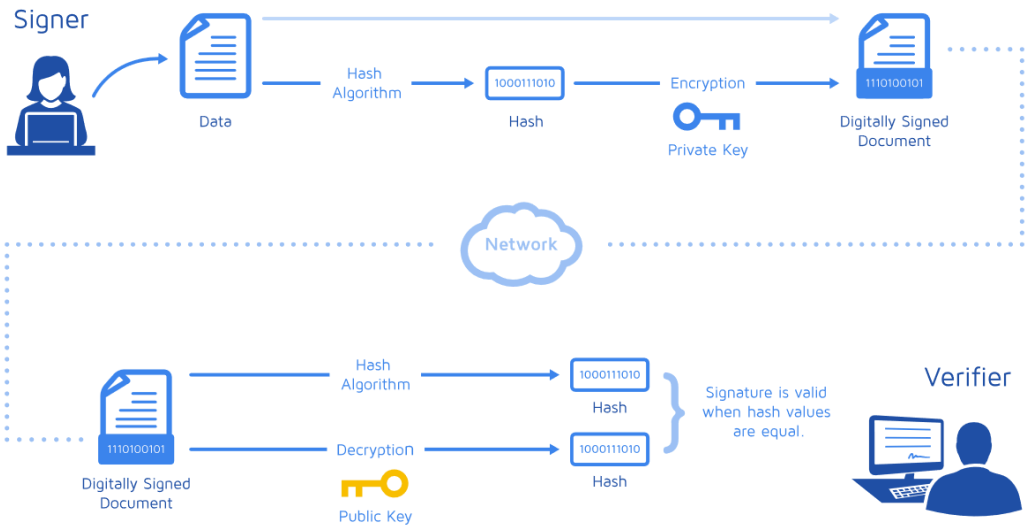

Figura 5: Firmas digitales en Blockchain [66]

Un bloque consiste de un cabezal y de un cuerpo, entre otras cosas contiene registro de todas las transacciones recientes (o todas) y una referencia al bloque que vino inmediatamente anterior a él. Además de esto contiene la respuesta a un puzzle matemático de difícil resolución, cuya respuesta es única para cada bloque. Los nuevos bloques no pueden ser ingresados en la red sin la respuesta correcta. Este es el llamado proceso de "mining", que esencialmente es el proceso de competir para ser el siguiente en encontrar la

respuesta que soluciona el próximo bloque. La respuesta es extremadamente difícil de resolver, pero una vez que uno lo encuentra, es fácil para el resto de la red confirmarlo como la solución.

El cuerpo de un bloque contiene información de las transacciones. Estas son transformadas meidante una función de hash en el merkle tree root hash (explicado abajo). Las transacciones no son transformadas mediante una función de hash directamente porque crear un hash de un bloque con una transacción, le toma el mismo esfuerzo de calcular el hash de un bloque con 10.000 transacciones. El máximo número de transacciones que un bloque puede tener depende del tamaño del bloque y de las transacciones.

A modo de ejemplo un cabezal puede contener :

- **Block version**: indica las reglas que el Bloque tiene que seguir.
- **Merkle tree root hash:** el hash de todos los hashes de todas las transacciones del bloque
- **Timestamp**: Tiempo actual como segundos en tiempo universal. Desde el 1 de enero de 1970.
- **Parent block hash:** un hash de 256-bit que apunta al bloque anterior

Lansiti et al. [69], reconocen 5 principios por debajo de esta tecnología:

- **Base de datos distribuida:** Cada parte dentro de la red tiene acceso a la base de datos completa y a toda su historia. Ninguna agencia central controla la información ni el flujo de la misma. Cada parte puede verificar los registros de las transacciones de otra persona directamente sin un intermediario. El public ledger de una Blockchain, puede ser visto entonces como una base de datos criptográficamente segura y distribuida. [70]
- **Transmisión peer-to-peer:** La comunicación ocurre directamente mediante pares en vez de pasar por un nodo central. Cada nodo almacena y reenvía información a todos los nodos. [71]
- **Transparencia con pseudo-anonimidad:** Cada transacción y su valor asociado son visibles para cualquiera con acceso al sistema. Cada nodo o usuario en una red de Blockchain, tiene una dirección alfanumérica de 30 caracteres o más que lo identifica. Los usuarios pueden mantenerse anónimos o probar su identidad frente a otros. Las transacciones ocurren mediante dos direcciones cualesquiera.
- **Irreversibilidad de los registros:** Una vez que una transacción es ingresada en l a base de datos y las cuentas son actualizadas, los registros no pueden ser alterados,

porque están vinculadas con cada registro de transacción que vinieron antes que ellos (por eso el termino chain: cadena)

- **Lógica computacional:** La naturaleza digital de los registros en la red, significa que las transacciones en Blockchain pueden ser programadas. Es decir que los usuarios pueden codificar algoritmos y reglas que automáticamente disparan transacciones. Los llamados smart contracts en la red Ethereum [72] son un ejemplo.

3.4.1. Tipos de Blockchain

Hay generalmente tres categorías en las que se pueden dividir los sistemas basados en Blockchain [73].

- **Blockchain pública:** Las cuales cualquiera en el mundo puede leer, enviar transacciones que si son válidas pueden ser incluidas en la red, y también pueden participar en el proceso de consenso. Este proceso es el que determina qué bloques son agregados a la cadena. En vez de confiar en la autoridad central, Blockchain está respaldada por crypto economía, lo que combina incentivos económicos y verificación criptográfica usando mecanismos como proof of work o proof of stake, los cuales van a ser explicados luego. Estas Blockchain son generalmente consideradas como totalmente descentralizadas.

- **Blockchain de consorcio:** Se refieren a redes donde el proceso de consenso es controlado por un número preseleccionado de nodos. Tomando como ejemplo, nos podemos imaginar un consorcio de 10 empresas financieras, las cuales controlan cada una un nodo, y tienen que firmar todos un nuevo bloque para ser considerado válido. El derecho a leer puede ser público o restricto para participantes, y pueden agregarse reglas de acceso. Estos Blockchain son considerados parcialmente descentralizados.

- **Blockchain privada:** Las cuales son Blockchain en donde los permisos de escrituras se centralizan en una organización. El acceso puede ser público o restrictivo. Se acerca más a un sistema tradicional centralizado con un grado de auditabilidad criptográfica.

En la Tabla 2, se resumen las características para cada uno de estos tipos de Blockchain [24].

	Blockchain públicas	Blockchain de consorcio	Blockchain privada
Determinación del consenso	Todos los nodos	Nodos seleccionados	Una organización
Permisos lectura	Público	Público o restringido	Público o restringido

Inmutabilidad	Casi imposible	Puede ocurrir	Puede ocurrir
Eficiencia	Baja	Alta	Alta
Centralizado	No	Parcial	Si
Proceso de Consenso	Sin permisos	Con permisos	Con permisos

Tabla 2 - Tabla comparativa de los distintos tipos de Blockchain

3.4.2. Taxonomías de las redes de Blockchain

Para viabilizar un análisis en profundidad, se han propuesto varias taxonomías para redes de Blockchain. Estas taxonomías permiten clasificar la gran diversidad de redes existentes y analizar su impacto en la arquitectura del sistema. Una taxonomía captura las características arquitectónicas y el impacto de las decisiones principales de diseño. Ayuda a tener en cuenta decisiones de diseño de la arquitectura, como por ejemplo la performance de un sistema de Blockchain [1].

Existen atributos que tienen que considerar todas las taxonomías a la hora de analizar una red de Blockchain. Por ejemplo la información que está contenida en una transacción confirmada, se vuelve eventualmente inmutable en la práctica. La inmutabilidad del historial de una cadena de transacciones firmada criptográficamente provee el no repudio de los datos guardados. Las herramientas de criptografía también apoyan la integridad de los datos.

El acceso público de la información provee transparencia y la igualdad de derechos permite que cada participante tenga la misma habilidad de acceder y manipular la red de Blockchain. Siempre dentro de una red, hay un mecanismo de consenso distribuido que gobierna la forma en que se agregan nuevas transacciones. Consiste en las reglas para validar y emitir los bloques, resolver conflictos y el algoritmo de incentivos. El mecanismo asegura que todas las transacciones son válidas, y que cada una es agregada una única vez.

Todas las propiedades anteriores se ven contrastadas por las dificultades técnicas que tiene una red de Blockchain. La privacidad se ve directamente impactada porque la información en la red está disponible para todos los participantes. O también es importante hablar de escalabilidad, ya que las blockchain públicas hasta el momento solo pueden manejar un promedio de 3-20 transacciones por segundo [74], mientras que un servicio de pagos popular como Visa, puede manejar un promedio de 24000 transacciones por segundo. Y la escalabilidad no solo se refiere al número de transacciones, sino que también al tamaño de los datos almacenados en un bloque y la latencia de la transmisión de datos.

Esto nos lleva a pensar que una taxonomía en donde se puedan ver las distintas configuraciones y variables de una red de Blockchain, puede ayudar a analizar los distintos

atributos de calidad y tomar las decisiones de manera más inteligente. Algunas de las categorizaciones que se pueden hacer, dependen de decisiones como:

- **Decisiones de arquitectura acerca de la descentralización:** Se analiza la descentralización según dos puntos de vista: permisos y verificación. Por ejemplo, si en vez de acceso público a la información, una red de Blockchain tiene permisos para que una o más autoridades decidan la participación. O cuáles son los mecanismos de verificación que tienen las fuentes de información del exterior de la red.

- **Decisiones de arquitectura acerca al cómputo y almacenamiento:** Mientras que las Blockchain favorecen directamente algunos atributos, es importante analizar el poder computacional y el espacio disponible de almacenamiento de información, ya que estos recursos permanecen limitados. A mayor espacio y cómputo, las redes de Blockchain cuestan dinero y deberían poder analizarse desde distintos puntos de vista que los sistemas de software convencionales. Por esto es bueno separar a las redes teniendo en cuenta: el almacenamiento de información y la ubicación del cómputo.

- **Decisiones de arquitectura acerca la configuración de la red de Blockchain:** Es importante decidir cuál es el tipo de red de Blockchain, cómo se va a guardar la información o cuáles son los algoritmos que participan en el sistema.

3.5. Interoperabilidad con Blockchain

Blockchain y los smart contracts proveen capacidades para solucionar problemas en múltiples dominios. Sin embargo, hay poca información disponible acerca de estilos arquitectónicos y patrones a aplicar para solucionar los problemas de los distintos dominios. Como puede ser en la salud, como almacenar y entregar la información de forma segura a una variedad de organizaciones [75].

Esto también lleva a un problema más general, la interoperabilidad de Blockchain. Un problema que emerge como uno de los problemas cruciales frente a la adopción de Blockchain [76]. Mientras Blockchain fue concebido como una tecnología descentralizada, las redes individuales de Blockchain no son intrínsecamente abiertas y no pueden comunicarse correctamente entre sí. Además, existen múltiples alternativas de Blockchain, las cuales tienen distintas características: el tipo de transacciones, algoritmos de hash, algoritmos de consenso.

El término de interoperabilidad de Blockchain no solo significa la posibilidad que distintas redes puedan comunicarse con las otras. Arriba de esto está la habilidad de ver, compartir y acceder a la información de distintas redes de Blockchain sin la necesidad de un intermediario.

Para atacar este problema, se propuso el Blockchain Interoperability Framework para evaluar la interoperabilidad de una red de Blockchain, permitiendo clasificar y sistemáticamente comparar soluciones existentes [76]. Asi también como el World propone su propio framework para esto [77].

Una MLR acerca de las distintas soluciones para la interoperabilidad de Blockchain clasifica los resultados en tres grupos [76]:

- **Conectores públicos:** esta primera categoría surge bajo la necesidad de proveer interoperabilidad entre criptomonedas. Identifican y definen diferentes estrategias de interoperabilidad para Blockchain públicas de criptomonedas, basadas en:
    - **Sidechains**: este mecanismo permite que los tokens y otros activos digitales se utilicen de forma segura en otra cadena de bloques y luego se devuelvan a la cadena de bloques original cuando sea necesario
    - **Notary schemes:** son terceras partes que ayudan a los participantes de una red de Blockchain, a validar/ver un evento/estado ocurrido en otra red y viceversa
    - **Hash time hashlocks:** pagos condicionales, en los que básicamente el receptor o el beneficiario deben acusar recibo del pago antes de un tiempo predeterminado o una fecha límite preestablecida
- **Blockchain de Blockchains:** son marcos que proporcionan capas de datos, red, consenso, incentivos y contratos reutilizables, para la creación de cadenas de bloques específicas de la aplicación (cadenas de bloques personalizadas) que interoperan entre sí.
- **Conectores híbridos:** cuando no son de ninguna de los grupos anteriores. Enfocado a las redes de Blockchain públicas y privadas, intentan ofrecer una capa de abstracción sobre Blockchain [78], capaz de exponer un conjunto de operaciones uniformes que permiten que una aplicación interactúe con Blockchains sin la necesidad de utilizar diferentes API.

3.6. Smart contracts

El concepto de smart contract fue introducido por Szabo en 1994 [30], antes de la aparición de las redes de Blockchain, y lo definió como un protocolo programable de transacciones, que ejecuta los términos de un contrato. Un contrato es un conjunto de acuerdos definidos por gente con experiencia, y es la forma tradicional de formalizar una relación, es un componente básico dentro de la economía de mercado actual (una garantía, una vinculación entre dos partes, una delineación de los derechos de propiedad). Lo que se proponía entonces era trasladar cláusulas contractuales en código, y embeberlas en un hardware o software que se encargará de ejecutarlas. Minimizando la necesidad de un intermediario entre las partes, y la posibilidad de accidentes o excepciones.

Visto dentro de una red de Blockchain, los smart contracts son scripts (segmentos de código procesable) que están almacenados en la propia red. Como residen en la cadena, tienen una dirección única. Un contrato se registra relacionado a una transacción, de forma que quede ejecutándose independientemente y automáticamente en cada nodo de la red. Se va a ejecutar siguiendo los datos que estaban especificados en el contrato.

Dicho de una forma más técnica, un Smart Contract es un segmento de código ejecutable que corre sobre la red de Blockchain para autónomamente facilitar, ejecutar y hacer cumplir un conjunto de reglas predefinidas en un acuerdo, sin la necesidad de una tercera parte. Cómo residen en la cadena, cada contrato tiene un identificador único para diferenciarlos de los usuarios que pueden interactuar con ellos [72]. Por ejemplo, en un caso de pérdida frente a un desastre natural, un contrato inteligente puede ser ejecutado para que la gente pueda reclamar su dinero. Los detalles como la compensación o las razones por las que se tiene que pagar, se pueden guardar en el contrato.

Un smart contract no puede ser cambiado una vez que está desplegado en la red de blockchain, por lo cual ya vemos que la seguridad es un elemento muy importante a la hora de desarrollar estas aplicaciones. Por eso es que se han hecho estudios para que los desarrolladores conozcan la taxonomía de las vulnerabilidades [79] que van desde cómo manejar las excepciones no controladas, hasta cómo responder ante ataques de DoS (Denial of Service).

El aspecto de costos de ejecución de estos contratos también ha sido investigado [80]. Por ejemplo en Ethereum, el llamado gas (representado en Ether, su moneda criptográfica como Bitcoin) es la tarifa para compensar el cómputo de las distintas operaciones de la red para ejecutar los contratos. Si el mismo no está optimizado, puede llegar a costar más gas del necesario, y los creadores van a tener que pagar más por su ejecución.

Los contratos en la red Ethereum están implementados en “Ethereum virtual machine code”, un lenguaje de bajo nivel, aunque son desarrollados en un lenguaje de alto nivel parecido a Javascript: Solidity.

Como Ethereum es un tipo de blockchain pública, lleva a que cada byte de código de cada contrato en la cadena, está disponible públicamente y cualquier nodo de la red puede analizar su código. Por lo tanto, su comportamiento se dice que es predecible [72]. Estos contratos tienen la funcionalidad de mantener un estado, cambiar activos digitales, recibir entradas, guardar y obtener información de servicios externos, y expresar lógica de negocio. Una vez liberados en la red, la función del smart contract es ejecutada por mensajes o transacciones enviadas a su identificador único [81]. Los contratos tienen que ser determinísticos (el mismo input tiene que producir siempre el mismo output). Si fueran no deterministas, tienen el potencial de romper la red, ya que si cada nodo ejecuta un contrato no determinístico, les va siempre a proveer distintos resultados, previniendo el consenso [30].

Algunos problemas que han surgido en contratos de Ethereum [82], algunos tan básicos como excepciones no controladas, que ocurren en un contrato cuando una excepción es lanzada (ej: no hay suficientes recursos para ejecutarse). Por lo cual el contrato termina, revierte su estado y devuelve falso. De 19.366 contratos en Ethereum, 27.9% tenía excepciones mal controladas. La inmutabilidad de bugs en contratos, también ha sido muy analizada ya que una vez que se despliegan los contratos en la red, no pueden ser alterados.

El concepto de Blockchain 2.0 [83], es relevante desde el punto de vista computacional teórico y práctico. Implica contar con una forma de “máquina de Turing completa” (un sistema es llamado así cuando puede completar cualquier paso lógico de un sistema computacional al igual que una máquina universal de Turing) dentro de un sistema de Blockchain.

3.7. Algoritmos de consenso

Los algoritmos de consenso son los mecanismos mediante los cuales los nodos en una red de Blockchain se ponen de acuerdo para validar y registrar nuevos datos. Nuestra investigación sostiene que estos algoritmos son uno de los atributos más importantes para distinguir a las redes de Blockchain. Estos algoritmos teóricamente fueron desarrollados como una solución al problema de los generales bizantinos [84].

El algoritmo de consenso describe cómo la mayoría de los nodos participantes en una red llegan a acuerdos con respecto a su estado según un protocolo [85]. Los nodos son los responsables de asegurar que las reglas del protocolo son respetadas asegurando que todas las transacciones pueden realizarse con seguridad. Por ejemplo en las criptomonedas, una de las responsabilidad del algoritmo de consenso es asegurar que una criptomoneda solo

puede ser gastada una vez [85]. El algoritmo de consenso influencia directamente en la performance y la seguridad de una red de Blockchain [86], [87].

Es útil contar con información acerca de qué algoritmo de consenso es el mayormente utilizado por las redes según nuestro estudio, ya que provee información al arquitecto de software acerca de cuál algoritmo es más apropiado para las necesidades de su sistema. Considerando eficiencia, seguridad, performance, y otros atributos de calidad.

La siguiente lista describe los principales algoritmos de consenso encontrados en la literatura y en las implementaciones de Blockchain. Los presentamos ordenados por el número de redes que los utilizan, de acuerdo a los resultados presentados en la sección: [RQ4] ¿Cuál es su algoritmo de consenso?

Proof of Stake (POS) aquellos con un mayor porcentaje de tokens emitidos tienen más posibilidad de ser elegidos para agregar un bloque nuevo a la cadena. En Blockchains basados en POS, generalmente no se generan nuevos tokens, entonces las recompensas están generadas exclusivamente de comisiones. En este sentido, su mayor ventaja: menor costo de mantener una red, lo cual lleva a menores comisiones. Sobre las desventajas, si un nuevo participante entra a la red, comprando la mayoría de sus tokens, puede comenzar a aceptar transacciones incorrectas[88]. Pero comprar la mayoría de los tokens, dependiendo de la red, puede superar los miles de millones de dólares.

Poof of Work (POW) es un proceso desarrollado con el objetivo de eliminar los ataques de SPAM mediante el cómputo de un problema moderadamente difícil antes de permitir que otra acción sea tomada. Este concepto nace en [89]. POW consiste en agregar determinados bytes de información al bloque para que el hash comience con un número predeterminado de ceros. Encontrar la combinación específica al problema es un problema que solo puede ser solucionado mediante la prueba con fuerza bruta. No solo no hay una fórmula para solucionar el proceso, si no que su dificultad crece exponencialmente con el número de bloques de la cadena. El proceso de encontrar una solución es llamado mining o minería en el lenguaje de las criptomonedas. POW es la alternativa principal a POS. Con POW los mineros solo pueden crear un número de bloques proporcional a su poder de cómputo. Con POS, los bloques son creados en proporción al número relativo de monedas que cada participante tiene.

Byzantine Fault Tolerance (BFT) está basada en el clásico problema de los generales bizantinos [84], que representa porque cualquier red o sistema distribuido es vulnerable mediante la ejemplificación del problema. El método utilizado en BFT representa la habilidad de un sistema distribuido de correctamente llegar al consenso a pesar de que hay nodos maliciosos que quieren enviar información incorrecta. El objetivo es proteger a la red contra fallas catastróficas, disminuyendo la influencia de los nodos malignos. Esta habilidad es importante para los sistemas distribuidos para prevenir y distribuir errores o información

incorrecta. Los sistemas que no toleran las fallas bizantinas son aquellas que no tienen suficiente consenso sobre el estado del nodo [85].

Federated Consensus (FC) es una forma de llegar a consenso bizantino, en la cual los nodos pueden compartir otro nodo y llevar al consenso sin haber conocido directamente todos los otros nodos.

Delegated Proof of Stake (DPOS) fue diseñado para ofrecer democracia a POW, usando votación y un proceso de elección para determinar los delegados o representantes para proteger a la red de las acciones maliciosas de los participantes más poderosos. Es importante aclarar, que este consenso tiene un aire a comportamiento o estructura centralizada.

Proof of Authority (POA) es una modificación del POS en el cual, en vez de tener en cuenta el valor monetario, la identidad del validador es tomada en consideración. Identidad significa la correspondencia entre la identificación personal real de un validador en la plataforma con la documentación emitida oficialmente para la misma persona, es decir, la certeza de que un validador es exactamente a quien esa persona representa. Estos validadores no son anónimos para la red y son la garantía de la transparencia de las transacciones en la red. Al igual que DPOS, se siente como una estructura centralizada [90].

En **Proof of Elapsed Time** (POET), las redes Blockchain autorizadas son aquellas que requieren que cualquier participante potencial se identifique antes de poder unirse. Basado en el principio de un sistema de lotería justo donde cada nodo tiene la misma probabilidad de ser un ganador, el mecanismo POET se basa en distribuir las oportunidades de ganar de manera justa entre el mayor número de participantes de la red. El temporizador varía para cada nodo, asignando a cada participante en la red una cantidad aleatoria de tiempo de espera, y el primer participante que termine de esperar puede enviar el siguiente bloque a Blockchain [91].

4. Metodología de investigación

La metodología elegida para este trabajo es una Revisión Multivocal de Software (MLR), basada en las guías de Gaurosi et al. en el artículo [13]. Esta metodología permite abarcar un abanico mayor de información, en especial para temas de innovación tecnológica. Esto le va a proponer a los arquitectos de software mayor cantidad de fuentes de información para tomar una decisión justificada sobre si incluir o no Blockchain en un proyecto.

Una revisión sistemática de literatura tradicional, solo tiene en cuenta la literatura académica. Con una MLR, literatura gris como blogs, videos, artículos o whitepapers[5] pueden ser considerados como fuentes válidas de información. Considerando también que hay relativamente un bajo número de papers académicos (únicamente 75 artículos de calidad) que proveen evidencia acerca de la arquitectura de las distintas redes de Blockchain, y menos sobre su adopción [16].

En la Tabla 3 se presenta una discusión sobre la conveniencia de utilizar una MLR como nuestro método de investigación para nuestra revisión sistemática. La misma fue basada en las Preguntas para decidir si incluir la literatura gris en las revisiones de ingeniería de software, propuestas por Garousi et al. [13]

Pregunta	Respuesta	Justificación
¿Es el tema complejo y no solucionable sólo considerando literatura formal?	Si	Considerar solo las redes Blockchain que han sido estudiadas y consideradas por la literatura blanca proporciona una imagen parcial del estado actual y el estado del arte de la tecnología Blockchain y su arquitectura.
¿Existe una falta de volumen o calidad de la evidencia, o una falta de consenso sobre la medición de los resultados en la literatura formal?	Si	No pudimos encontrar ninguna lista de redes de Blockchain en la literatura formal.
¿Es la información contextual importante para el tema en estudio?	Si	Sí, y se ha convertido en una costumbre para los desarrolladores de redes Blockchain proporcionar documentos técnicos (no artículos académicos) donde se documentan las decisiones de diseño de redes.
¿El objetivo es validar o corroborar los resultados científicos con experiencias prácticas?	Si	Nuestra suposición es que la literatura gris complementará la evidencia científica disponible.
¿Es el objetivo desafiar las	No	Estamos mostrando el lado práctico pero sin

[5] Se refiere a los documentos técnicos provistos por los creadores de la red, los cuales explican las decisiones de diseño tomadas. Una práctica común con las nuevas redes.

suposiciones o falsificar los resultados de la práctica utilizando la investigación académica? O viceversa?		intentar desafiar supuestos o falsificar resultados.
¿Sería posible una síntesis de los conocimientos y la evidencia de la comunidad industrial y académica? ¿Útil para una o incluso para ambas comunidades?	Si	Afirmamos que ambas partes interesadas se benefician, junto con el arquitecto de software que busca integrar las soluciones Blockchain a las arquitecturas de software existentes.
¿Existe un gran volumen de fuentes de profesionales que indiquen un gran interés de los profesionales en un tema?	Si	Hay un interés industrial en Blockchain donde los jugadores más grandes son parte de él. Nuestro descubrimiento inicial demuestra que hay más de 110 redes Blockchain activas y diferentes.

Tabla 3 - Preguntas para decidir si incluir la literatura gris en las revisiones de ingeniería de software

Para resumir la Tabla 3, la tecnología Blockchain es un tema emergente de investigación, en el cual mucha de la información que existe en esta área no ha pasado por un proceso formal de revisión de a pares. Por lo tanto, para generar una mirada completa de las redes de Blockchain disponibles, consideramos necesario incluir fuentes de literatura gris. Un hecho importante, es que Blockchain evolucionó primero en el área industrial que en el mundo académico [92]. Lo cual apoya a que sea apropiado utilizar una MLR.

Para garantizar el rigor y la replicabilidad del método descrito en este trabajo, una vez establecido el objetivo, se desarrolló un protocolo basado en las recomendaciones de Adams et al. [93]. Este capítulo resume los puntos principales del protocolo.

4.1. Objetivo

El objetivo de esta MLR es identificar cuáles son las diferentes redes de Blockchain activas y caracterizarlas. Reconociendo propiedades que pueden afectar los atributos de calidad, como pueden ser: seguridad, transparencia, privacidad, escalabilidad, eficiencia. Estos atributos son importantes, ya que son los que agregan valor en el contexto de cada proyecto ya que garantizan la operación de la red y la integridad de la información que la red maneja.

Establecer esta identificación y caracterización, va a servir como referencia para que arquitectos de software puedan decidir justificadamente sobre la necesidad de aplicar Blockchain a sus proyectos, y ayudarlos a elegir cuál es la red que más aplica a su proyecto.

4.2. Preguntas de investigación

Para facilitar la estructura y el desarrollo de la MLR, en la Tabla 4 formulamos preguntas específicas que esperamos responder con esta investigación.

Pregunta	Justificación
[RQ1] ¿Cuáles son las redes de Blockchain disponibles?	Estamos planeando tener una lista exhaustiva de las redes Blockchain activas existentes y sus principales características.
[RQ2] ¿De quién es la propiedad de los datos?	Es importante diferenciar las redes en función de la propiedad de la red. Quién puede decidir quién puede unirse a la red y puede anular los comandos (o lanzarlos al público).
[RQ3] ¿Qué tipo de control de acceso tienen?	El arquitecto puede necesitar una red de Blockchain sin permisos donde no se imponen restricciones a ningún individuo para realizar transacciones y participar en el consenso o en el mío. O una red de Blockchain basada en permisos es una red donde una entidad central ha impuesto una condición para participar en la operación con Blockchain
[RQ4] ¿Las redes apuntan a un dominio de aplicación específico?	Algunas redes existentes apuntan a aplicaciones de dominio específicas, por lo que los arquitectos pueden filtrar y utilizar una que ya tenga usos prácticos en el dominio.
[RQ5] ¿Cuál es su algoritmo de consenso?	Los algoritmos de consenso son los mecanismos mediante los cuales se logra confiabilidad en la red Blockchain y establecen confianza entre pares desconocidos en un entorno informático distribuido. Este atributo afecta directamente los atributos de calidad [94].
[RQ6] ¿La red permite smart contracts? En caso de ser afirmativo: ¿Cuáles son los lenguajes de programación que utilizan?	Los smart contracts brindan funcionalidad adicional a Blockchain. El idioma puede proporcionar una curva de aprendizaje adicional para lograr la funcionalidad.
[RQ7] ¿Cuál es la naturaleza de la red? ¿Nace como una tecnología independiente o a partir de otra red previamente existente?	La naturaleza de Blockchain podría guiarnos para agrupar a las redes en familias, encontrando varias implementaciones que solucionen un mismo problema

Tabla 4 - Preguntas de investigación

4.3. Protocolo

Dada la importancia de establecer un protocolo de revisión para que futuros investigadores puedan iterar y profundizar sobre nuestros hallazgos, en la Figura 6 se puede ver todo el proceso definido.

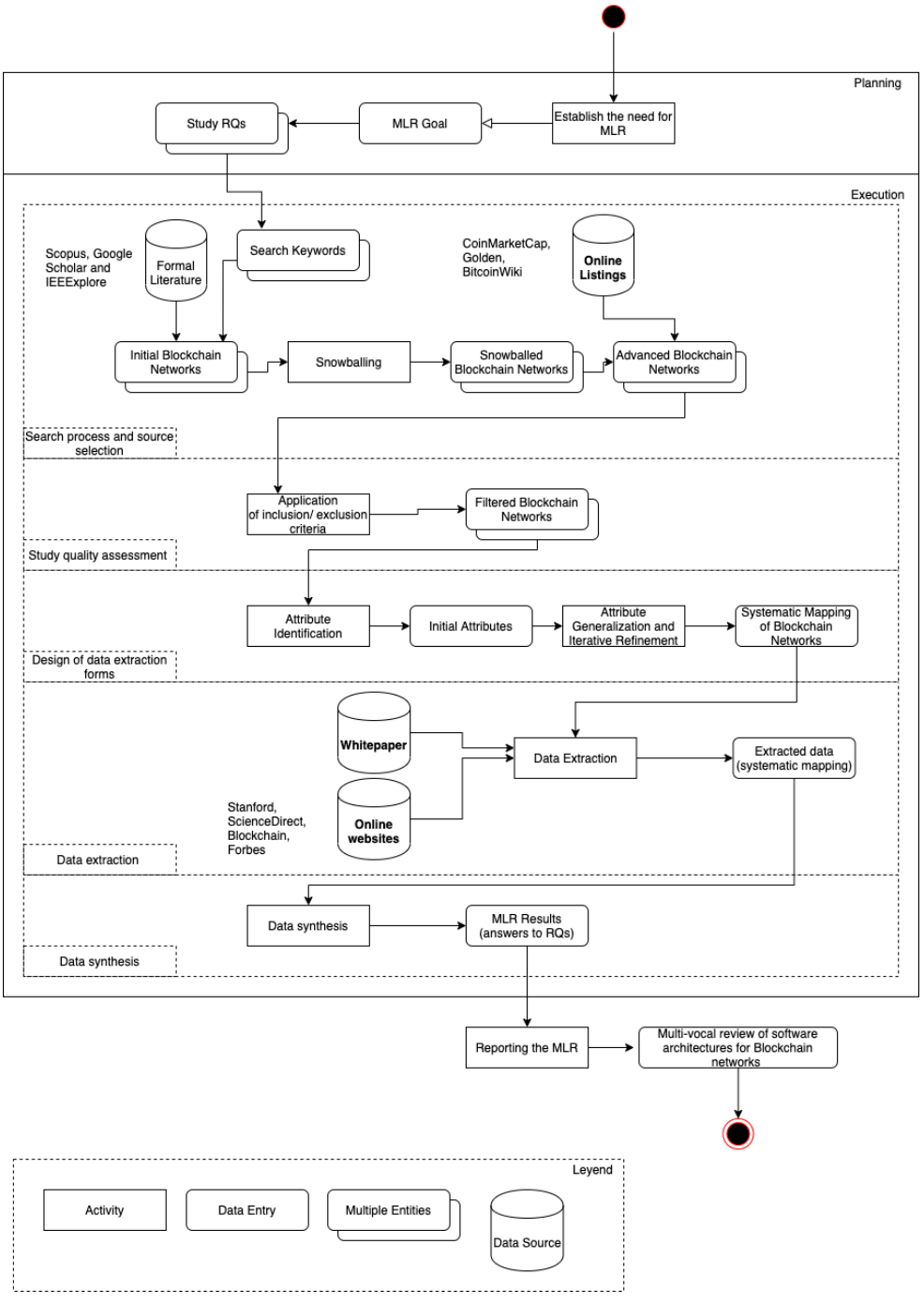

Figura 6 - Protocolo de Investigación

Luego de establecer la necesidad de realizar una MLR, definir los objetivos y listar las preguntas de investigación. Comenzamos realizando la selección de fuentes. La literatura blanca puede ser incorporada mediante bases de datos bibliográficas de amplia cobertura, como por ejemplo: Scopus y Google Scholar, o por bases de datos de texto completo como IEEE Xplore, ACM Digital Library, ScienceDirect. La estrategia de búsqueda para la literatura gris es diferente ya que las bases de datos anteriormente nombradas no incluyen literatura gris. Y esta puede proveer datos que no se encuentran en la literatura publicada.

Considerando la Guía 7 de Gaurosi et al. de su artículo: “General web search engines, specialized databases and websites, backlinks, and contacting individuals directly are ways to search for grey literature”. La Tabla 5 presenta todas las fuentes de información que consideramos necesarias para esta MLR.

Fuente	Cómo encontrarla	Información que provee
Papers revisados por pares	Búsqueda automática (Scopus, Google Scholar, IEEExplore)	Listados de Blockchain y detalles de implementación
Revistas comerciales / Blogs	Ejemplos: Standford University Magazine, Blockchain.com, Forbes	Listados de Blockchain
Listados online / Catálogos	Ejemplos: CoinMarketCap, Golden, BitcoinWiki	Listados de Blockchain
Proveedor de cloud computing	Amazon, IBM, Google, Oracle y Microsoft	Listados de Blockchain
Whitepaper de la Blockchain	Buscador de Google	Detalles de implementación de las Blockchain
Sitio oficial de la Blockchain	Buscador de Google	Detalles de implementación de las Blockchain

Tabla 5 - Fuentes de Datos

Para buscar la información en la literatura académica, un conjunto de artículos fueron seleccionados y revisados por pares. También se realizó snowballing de los artículos más referenciados.

Una búsqueda general fue inicialmente realizada para buscar artículos en la intersección entre software y arquitecturas de Blockchain sin resultados relevantes. Luego de varias iteraciones sobre las cadenas de búsqueda, se decidió utilizar una búsqueda con una cadena más general, buscando en el título y abstract:

'BLOCKCHAIN' OR 'BLOCKCHAIN SYSTEMS' OR 'BLOCKCHAIN SYSTEMS' OR 'BLOCKCHAIN PLATFORMS' OR 'BLOCKCHAIN NETWORKS' OR 'BLOCKCHAIN ARCHITECTURE' OR 'BLOCKCHAIN SOFTWARE ARCHITECTURE' '

Es importante señalar que la unidad de análisis de esta MLR son las redes en Blockchain en sí mismas y no la fuente bibliográfica (artículo de investigación, whitepaper, o sitio web) que discute la red. La cadena de búsqueda anterior resulta en la identificación de más de 100.000 artículos en los diferentes motores de búsqueda. El criterio para detener la búsqueda fue por esfuerzo[6], por lo cual los primeros 500 títulos y abstracts de cada portal

[6] Es importante aclarar que la búsqueda por esfuerzo es válida en una MLR, mientras que en una SLR no lo es.

fueron revisados (ordenados por número de referencia), buscando por las redes de Blockchain que fueran referenciadas. Para poder completar la identificación de las redes, fue importante contar con el resto de los listados detallados en la Tabla 5.

Para elegir si una red de Blockchain (no artículo o fuente) era incluida o no en el estudio, se tomaron los siguientes criterios de Inclusión:

- La red tiene que tener un whitepaper publicado y accesible.
- La red tiene que tener actividad en el último año, es decir, que tiene proyectos activos que pueden ser verificados revisando las noticias o artículos recientes.
- Tienen que tener proyectos de aplicación práctica disponibles en el mercado, y no son solo una red teórica o el resultado de una propuesta académica
- No son una implementación específica de una red, con el propósito de ser un producto.

Se diseñó un formulario de extracción iterativamente para soportar la síntesis y el análisis necesario para responder las preguntas de investigación.

Para extraer sistemáticamente los aspectos técnicos de cada Blockchain (en especial de los cuales no estaban listados en su sitio), se buscó e investigó el whitepaper de cada una de las redes a ser incluidas. Otros portales[7] también fueron consultados para obtener más detalles que no estuvieran presentes en el whitepaper.

Los formularios de extracción de datos fueron desarrollados en una hoja de cálculo (disponible en Google Docs: https://tinyurl.com/uo9po2c). En la Tabla 6 se pueden ver los atributos definidos en el formulario.

Atributo	Aclaración
Nombre	Identificar el nombre de la red
Link al Website	Dirección del sitio web comercial de la red
Fuente de información técnica	Whitepaper
Tipo de descentralización	Pública o Privada
Control de acceso	Totalmente descentralizada (sin permisos), con permisos para escribir pero no para leer, o con permisos detallados sobre transacciones
Dominio específico (si lo tiene)	Si la red es específica para un dominio de aplicación o si es de uso general
Algoritmo de consenso	Identificar cual es el nombre del algoritmo de consenso

[7] www.blockchain.com, www.sciencedirect.com, cbr.stanford.edu, coinmarketcap.com. www.forbes.com

	de la red
Smart contracts	Si permiten el uso de smart contracts en la red o no.
Lenguaje de programación del smart contract	Nombre del lenguaje o lenguajes de programación que pueden ser utilizados en los smart contracts
Método para escalar	Si usan Sharding o Raiden Network
Implementación específica de una red existente	Si son derivadas de Bitcoin, Ethereum u otra red, o si nacen independientemente.
Literatura formal	Si existe o no literatura formal que hable de la red. Buscando en los motores de búsqueda: “Blockchain + Nombre de la red”

Tabla 6 - Fuentes de Datos

Se realizó un refinamiento iterativo de la búsqueda a lo largo de la investigación. El primer cambio realizado fue agregar si las redes eran una implementación específica de una red existente, junto con si existía literatura formal o no. El segundo separó la descentralización del control de acceso.

4.4. Ejecución

En Tabla 7 presentamos el cronograma de la ejecución de la investigación.

La búsqueda inicial fue realizada por el autor de esta tesis durante febrero y junio del 2020. Los tutores revisaron el protocolo y los datos recopilados, para lo cual se cambió:

- Se definieron mejores criterios de inclusión para poder filtrar de mejor manera las redes de Blockchain
- El formulario de extracción fue modificado para capturar si eran una implementación específica de una red existente, y si existía o no literatura formal.
- Se mejoró el protocolo luego de revisar los pasos de Gaurosi et al, realizando ajustes de acuerdo a las lecciones aprendidas en la primera iteración.

Luego de trabajados estos comentarios, se publicó una primera iteración en español del artículo [19] describiendo 112 redes de las cuales fueron descartadas 20.

Luego de este hito, se tradujo el artículo publicado al inglés entre noviembre 2020 y febrero 2021, recopilando varios detalles del protocolo que no habían sido registrados. También se aprovechó para separar el concepto entre descentralización de acceso a control. En marzo se realizó una nueva búsqueda, de la cuales una nueva red fue agregada, y una eliminada (por haber cesado su funcionamiento).

Los resultados finales están disponibles online en https://tinyurl.com/uo9po2c.

Fecha	Etapa
Febrero 2020 - Junio 2020	Búsqueda inicial
Junio 2020 - Julio 2020	Revisión protocolo y datos recopilados
Agosto 2020 - Octubre 2020	Iteración sobre comentarios.
Noviembre 2020	Publicación en IEEE - Jornadas Chilenas de Computación [19]
Noviembre 2020 - Febrero 2021	Traducción de artículo
Febrero 2021	Búsqueda de nuevas redes
Marzo 2021 - Actual	Revisión con papers arbitrados

Tabla 7 - Fuentes de Datos

4.4.1. Aplicación del criterio de inclusión/exclusión

Un proceso preliminar de extracción de datos era necesario para determinar si una red de Blockchain era incluida o no en el estudio. El proceso de extracción siguió, por necesidad, un proceso incremental. Cuando una red era identificada, se buscaron las fuentes para completar la información requerida por el formulario de extracción de datos, al estilo de proceso teórico de parada por saturación. La mayoría de las veces, el whitepaper de la red proporcionó información suficiente para decidir sobre la inclusión.

A continuación presentamos algunos ejemplos de redes de Blockchain que no cumplieron nuestro criterio de inclusión/exclusión:

- **Bitshares**: No estaba liberada al público al momento del estudio, por lo cual no hay productos activos utilizandolo (Criterio 2)
- **UZHBC** (University of Zurich Blockchain): Es una propuesta de red teórica basada en Blockchain para manejar diplomas[95] (Criterio 3)
- **Decentraland**: Es un producto descentralizado para manejar avatares. Fue descartado porque es una implementación específica de Ethereum (Criterio 4)

En contraste, vemos Ocean como un ejemplo de una red de Blockchain que cumple con el criterio de inclusión/exclusión:

- La red tiene que tener un whitepaper publicado y accesible

- “Ocean Protocol: A Decentralized Substrate for AI Data & Service” [8]

- La red tiene que tener actividad en el último año, es decir, que tiene proyectos activos que pueden ser verificados revisando las noticias o artículos recientes.
    - La red está activa y con publicaciones en las noticias [95], [96]
- Tienen que tener proyectos de aplicación práctica disponibles en el mercado, y no son solo una red teórica o el resultado de una propuesta académica
    - Hay una implementación específica para Daimler AG. (Mercedes Benz) [95], [96]
- No son una implementación específica de una red, con el propósito de ser un producto.
    - No es un producto derivado de otra red de Blockchain

4.4.2. Formulario de extracción de datos

En la Tabla 8 se presenta un ejemplo de un formulario de extracción completo.

Atributo	Respuesta
Nombre	Nextledger
Link al Website	https://www.samsungsds.com/global/en/solutions/off/nexledger/Nexledger.html
Fuente de información técnica	https://github.com/nexledger/accelerator/blob/master/docs/Whitepaper-Acceleratoring Throughput in Permissioned Blockchain Networks.pdf
Tipo de descentralización	Privada
Control de acceso	Con permisos para escribir pero no para leer
Dominio específico (si lo tiene)	General
Algoritmo de consenso	Nexledger Consensus Algorithm
Smart contracts	Si
Lenguaje de programación del smart contract	C++
Método para escalar	Raiden Network

[8] https://oceanprotocol.com/

Implementación específica de una red existente	Independiente
Literatura formal	Si

Tabla 8 - Fuentes de Datos

5. Resultados

5.1. [RQ1] ¿Cuáles son las redes de Blockchain disponibles?

Identificamos 112 redes de Blockchain distintas que cumplen con el criterio de inclusión definido para esta MLR. Agrupamos estas redes en 3 categorías distintas considerando su dominio de aplicación:

- **Uso general**: La Tabla 9 presenta las 51 redes de este grupo, subdivididas por algoritmo de consenso.
- **Criptomonedas**: La Tabla 10 presenta las 29 redes de este grupo, subdivididas por la naturaleza de la red.
- **De dominio específico**: La Tabla 11 presenta las 32 redes de este grupo, subdivididas por su dominio de aplicación.

Nombre de la red	Algoritmo de consenso	Smart contracts	Derivadas de
Hydrachain	BFT	Si	Ethereum
Kadena		Si	-
Multichain		Si	Bitcoin
NEO		Si	-
Smilo		Si	-
Ziliqa		Si	Ethereum
Aelf	dPOS	Si	-
Lisk		Si	-
Tron		Si	-
Ubiq		Si	Ethereum
Chain Core	FC	Si	-
Chain		Si	Ethereum
Urbit		Si	Ethereum
Ardor	POS	Si	NXT
Blockstack		Si	-
Byteball Bytes		Si	-
ConsenSys		Si	Ethereum
Dfinity		Si	-
Dragonchain		Si	-
EOS.IO		Si	-
Ethereum		Si	-
Multiven		Si	Ethereum
Neblio		Si	Ethereum
Netki		Si	-

Qtum		Si	Ethereum
Tezos		Si	-
Unita		Si	Qtum
Waves		Si	Ethereum
0chain	POW	Si	-
Cypherium		Si	-
Decent		Si	-
Ethereum Classic		Si	Ethereum
Monax		No	Ethereum
Aion	Otro	Si	Ethereum
ArcBlock		Si	-
Elements		Si	-
Everledger		Si	Bitcoin Cash
Factom		Si	-
Hedera Hashgraph		Si	-
HyperLedger Fabric		Si	-
HyperLedger Iroha		Si	-
ICON		Si	-
Komobo		Si	-
Mijin		Si	NEM
NKN		Si	-
Ontology		Si	-
Quorum		Si	Ethereum
R3 corda		Si	-
Vechain		Si	-
Veriblock		Si	-

Tabla 9 - Blockchains de uso general

Nombre de la red	Algoritmo de consenso	Smart contracts	Derivadas de
AnonCoin	POW	No	Bitcoin
AuroraCoin	POW	No	
Bitwala	POS	Si	
BlackCoin	POW	No	
Bytecoin	POW	No	
CloackCoin	Otro	No	
Cryptobullions	Otro	No	
CureCoin	POS	No	
Dash	POW	No	
Decred	Otro	No	
Devcoin	POW	No	
DigitalCoin	POW	No	
Litecoin	POW	No	
MaxCoin	POW	No	
Monero	POW	No	
Zcash	POW	No	
Zetacoin	POW	No	

Bancor	POW	Si	EOS
Alphapoin	Others	Si	Ethereum
Augur	POS	Si	
Cardano	POS	Si	
ForkDelta	POW	Si	
IDEX	POW	Si	
Ox	POA	Si	
Tether	POS	Si	
Elastos	POS	Si	
Nextledger	Otro	Si	
Nxt	POS	Si	
Ripple	Otro	No	
Stellar	Otro	Si	

Tabla 10 - Blockchains de dominio criptomonedas

Nombre de la red	Algoritmo de consenso	Smart contracts	Derivadas de	Dominio
Ocean	POS	Si	Ethereum	Artificial Intelligence
Storj	POS	Si	Bitcoin	Cloud Storage
SONM	POS	Si	-	Computing Platform
Hyperledger Quilt	POET	Si	-	Distributed Ledgers
Hyperledger Sawtooth	POET	Si	-	
NEM	Otro	Si	-	
Openchain	Otro	Si	-	
Tierion	Otro	Si	Bitcoin	Document Verification
EnergyWeb	Otro	Si	-	Energy
Filecoin	Otro	Si	Ethereum	File Management
KYC-CHAIN	POS	Si	-	Finance
OmiseGO	POS	Si	Ethereum	
Straitis	POS	Si	Ethereum	
Symbiont Assembly	BFT	Si	-	
Wanchain	POS	Si	Ethereum	
Hydro	POS	Si	Ethereum	Identity
Shocard	Otro	Si	Bitcoin	
Wibson	POS	Si	-	
OpenIDL	Otro	Si	-	Insurance
IOTA	Otro	Si	-	IoT
Platin	Otro	Si	-	Location
Bitwala	POS	Si	Bitcoin	Loyalty Programs
Mediachain	FC	Si	-	Music
Apirone	POW	No	Bitcoin	Payments
Earthport	Otro	Si	-	
KodakCoin	POA	Si	-	Photographs
Enigma	POS	Si	-	Security

Steem	POS	Si	Tron	Social Media
Aventus	POS	Si	Bitcoin	Ticket Management
Filament	FC	Si	Bitcoin	Vehicle Data
DMarket	POS	Si	Bitcoin	Videogames
Horizon	Otro	Si	-	

Tabla 11 - Blockchains de dominio específico

En todas las tablas de arriba, las redes identificadas están ordenadas alfabéticamente en su subdivisión. También establecimos el siguiente criterio para agrupar los algoritmos de consenso en 8 grupos:

- Proof of Stake (POS) (36)
- Proof of Work (POW) (20)
- Relacionados a Bizantine Fault Tolerance (BFT) (7): Loop Fault Tolerance (LFT), Practical Byzantine Fault Tolerance, Delegated Byzantine Fault Tolerance (DBFT), Smilo BFT +, Practical Byzantine Fault Tolerance (PBFT), Byzantine Fault Tolerant Tendermint, Byzantine Fault-Tolerance.
- Federated consensus (FC) (5)
- Delegated proof of Stake (dPOS) (4)
- Proof of Authority (POA) (3)
- Proof of Elapsed Time (POET) (2)
- Others (35)

5.2. [RQ2] ¿De quién es la propiedad de los datos?

Encontramos que 74 de las 112 redes estudiadas eran redes públicas de Blockchain. Donde cualquier usuario puede leer, enviar transacciones y participar del algoritmo de consenso. Ejemplos en este grupo pueden ser Bitcoin y Ethereum. Las restantes 38 son redes privadas, donde hay una entidad central controlando quién puede unirse a la red y quien puede ejecutar comandos. Ejemplo de este grupo pueden ser Ripple y HyperLedger Iroha.

5.3. [RQ3] ¿Qué tipo de control de acceso tienen?

Encontramos que 74 de las 112 redes estudiadas son totalmente descentralizadas, sin restricciones impuestas en ningún individuo para transaccionar del algoritmo de consenso. En la Tabla 12 mostramos que las redes públicas son las mismas a aquellas que proveen un acceso descentralizado.

Del resto, 21 de las redes tienen permisos detallados sobre las transacciones, mientras que 17 tienen permisos para agregar datos en la Blockchain, pero no ofrecen restricciones para leer registros.

	Públicas	**Privadas**
Descentralizadas	74	-
Con permisos detallados	-	21
Permisos para escribir, pero no para leer	-	17

Tabla 12 - Fuentes de Datos

5.4. [RQ4] ¿Las redes apuntan a un dominio de aplicación específico?

La Tabla 13 presenta la clasificación mediante el dominio de aplicación específico de la red. Podemos ver cómo 51 de las redes no tienen un dominio específico (45%). La familia más grande de dominios específicos son las criptomonedas (29) (~26%). Los otros dominios con más de una red son: financial (5), distributed ledgers (4), identity (3), payments (2) y videojuegos (2). La categoría "Otros" incluye 16 dominios distintos que no tienen más de 1 elemento. Estas son: Artificial intelligence, cloud storage, computing platform, document verification, energy, file management, insurance, IoT, location, loyalty programs, music, photographs, security, social media, ticket management, vehicle data.

Dominio	Número de Redes
General	51
Criptomonedas	29
Financial	5
Distributed Ledgers	4
Identity	3
Payments	2
Videogames	2
Others (16 diferentes)	16

Tabla 13 - Clasificación por dominio de aplicación

5.5. [RQ4] ¿Cuál es su algoritmo de consenso?

El criterio para la agrupación por algoritmo de consenso fue explicado en la respuesta a la RQ1, cuando la estructura de las tablas fue comentada. La Tabla 14 presenta el agrupamiento de las redes identificadas por el tipo de algoritmo de consenso. Se reconocieron 8 grupos.

Tipo de Algoritmo de Consenso	Número de Redes
Proof of Stake	36
Proof of Work	20
Relacionados a BFT	7
Federated Consensus	5
Delegated Proof of Stake	4
Proof of Authority	3
Proof of Elapsed Time	2
Others (30 diferentes)	37

Tabla 14 - Clasificación por algoritmo de consenso

5.6. [RQ5] ¿La red permite smart contracts? En caso de ser afirmativo: ¿Cuáles son los lenguajes de programación que utilizan?

Del análisis de las 112 redes de Blockchain, se determinó que 93 (83%) de las redes analizadas aceptan el uso de smart contracts, mientras que las 19 restantes (17%) no lo permiten. La Tabla 15 muestra la clasificación de acuerdo al principal lenguaje de programación usado en los smart contracts. El lenguaje más utilizado es C/C++ (35), seguido por Solidify (31) y Java (22). Hay 6 redes (Komodo, Multichain, NEM, Openchain, Tierion, Horizon) que son “Developer Friendly” y sus smart contracts pueden ser escritos en cualquier lenguaje. Hay 21 redes que aceptan más de un lenguaje de programación.

Lenguaje de Programación	Número de Redes
C/C++	35
Solidity	31
Java	22
Javascript	14

Go	11
PYthon	9
NodeJS	2

Tabla 15 - Lenguaje de programación primario de los smart contracts

5.7. [RQ6] ¿Cuál es la naturaleza de la red? ¿Nace como una tecnología independiente o a partir de otra red previamente existente?

Agrupamos a las redes identificadas según su origen o naturaleza. La Tabla 16 muestra el número de redes de cada uno de los grupos. Encontramos que Ethereum (27) y Bitcoin (26) son las dos redes que han resultado en un gran número de redes derivadas. Las otras 6 redes que inspiraron nuevos desarrollos son: NEM, Cash, NXT, Tron, Qtumand EOS). Finalmente, 53 de las redes no parecen evolucionar o derivar de ninguna red padre, y proveen nuevas implementaciones a los conceptos de Blockchain.

Origen	Número de Redes
Independiente	53
Ethereum	27
Bitcoin	26
Otros	6

Tabla 16 - Lenguaje de programación primario de los smart contracts

6. Discusión

6.1. Observaciones extraídas del cruzamiento de la información

Luego de conducir una MLR de las redes de Blockchain, podemos obtener una amplia visión de los atributos que caracterizan cada red. Cruzando los datos, podemos realizar algunas observaciones:

- El algoritmo Proof of Stake (36) es el más comúnmente utilizado, esto puede estar relacionado a que es el utilizado por Ethereum. 27 de las redes usan Proof of Stake y derivan de Ethereum.

- Dentro de la categoría específica más grande (criptomonedas), la mayoría son una mejora incremental o derivan de Bitcoin (17 de 30). Dentro de estas redes, la mayoría implementa el algoritmo de consenso Proof of Work (11), el introducido por Bitcoin.

- Las criptomonedas generalmente no proveen soporte para smart contracts (17 vs 13). De las derivadas de Bitcoin, sólo Bitwala los soporta.

- Al mirar las redes fuera de las criptomonedas (83), aproximadamente un tercio derivan de Ethereum. Asumimos que es por la naturaleza open source de Ethereum. Dentro de este grupo, la mayoría utilizan Proof of Stake (29).

- 81 de las 83 redes que no son criptomonedas aceptan el desarrollo de smart contracts en su red.

- La mayoría de las redes que no tienen referencias en la literatura blanca, son las relacionadas con criptomonedas. Lo cual nos da la idea de la inmadurez del área en la literatura formal. Esto también nos confirma la decisión de utilizar una MLR como método de investigación.

- Las redes basadas en permisos (39) parecen nacer independientemente (26), y la mayoría acepta smart contracts.

6.2. Programabilidad de las Blockchain y smart contracts

La importancia de los smart contracts como uno de los responsables de la revolución de la Blockchain 2.0 ha sido discutida en la literatura [83] y en la industria [97]. El término sirve para distinguir Bitcoin como un activo, frente a una “infraestructura programable confiable y distribuida” [98]. Blockchain 2.0 permite la descentralización de los mercados, contemplando la transferencia de otros activos además de las criptomonedas. Deja abierto

el camino a Blockchain 3.0, descrito como la aplicación de la tecnología a otras áreas además de divisas y finanzas, como pueden ser gobierno, salud, ciencia, cultura y arte [99].

Blockchain 3.0 busca un modelo más evolucionado que solo smart contracts, busca la aplicación y el establecimiento de unidades organizacionales descentralizadas autónomas, que confían en sus propias leyes para operar con un nivel más alto de autonomía [100]. Su acercamiento no es el de guardar pequeñas transacciones en la red principal de Blockchain, reduciendo la carga de trabajo en la red principal de Blockchain, lo cual lleva a que se corran pequeñas transacciones en las sub redes. Esto es llamado acercamiento "off-chain". Funciona creando pequeñas comunidades donde las transacciones se ejecutan sin que cada una de las transacciones estén registradas en la cadena principal [101]. Redes apoyando a la Blockchain 3.0 son: ICON, IOTA y Cardano [102].

La mayoría de los lenguajes de programación para smart contracts son Turing Complete [57]. Lo que significa que pueden resolver cualquier problema computacional si se le proporciona suficiente tiempo y espacio. Como resultado, las redes de Blockchain pueden ser una plataforma computacional, en vez de simplemente una base de datos distribuidos (con la que generalmente se la compara).

Creemos que Solidity es el lenguaje de programación más popular para desarrollar smart contracts. Por definición, es un lenguaje de alto nivel, basado en contratos, orientado a objetos. Los contratos en Solidity son similares a las clases en los lenguajes orientados a objetos. Cada contrato contiene declaraciones de variables de estado, funciones, modificadores de funciones, eventos, enumerados e interfaces. Solidity está tipado, además de revisar y verificar en tiempo de compilación restricciónes sobre los smart contracts, evitando errores antes de tiempo de ejecución. En pocas palabras, creemos que las razones detrás del éxito de Solidity son su simplicidad, ser específico para desarrollar smart contracts, y ser el lenguaje detrás de uno de los precursores de la Blockchain 2.0 (Ethereum).

Sin embargo, los resultados muestran que 21 de las 83 redes de Blockchain que aceptan smart contracts aceptan más de un lenguaje de programación, lo cual disminuye la curva para que los desarrolladores puedan comenzar a trabajar con ellas.

6.3. Respecto a los atributos de calidad y las redes Blockchain

Basado en nuestros resultados preliminares, consideramos que la performance y la escalabilidad son los atributos que son más detalladamente evaluados cuando se implementa una red de Blockchain. El atributo que tiene más directo impacto sobre estos atributos es el algoritmo de consenso. La importancia del consenso del algoritmo se ve reflejado en los resultados de la MLR [16], donde 24 de los resultados relacionados a arquitectura de Blockchain (44), están relacionados al algoritmo de consenso, ya que afecta distintos aspectos técnicos de la red. Por ejemplo, considerando la escalabilidad la habilidad

de que una aplicación mantenga el rendimiento de una red sin perder sus características que la hacen funcionar [103]. Si el algoritmo de consenso de la red elegida tiene mayor seguridad y dificultad para resolver un nuevo bloque, la escalabilidad se va a perder ya que se va a requerir de mayor poder de cómputo, requiriendo también mayor eficiencia energética.

En [57], los investigadores concluyen una manera clara de representar las relaciones entre el consenso de algoritmo y los atributos de calidad. En la Tabla 17, usamos la misma representación que [57], pero poblado con la evidencia que encontramos. La misma muestra las familias de algoritmos de consenso que reconocemos como las más utilizadas. Esta fue una tarea complicada, ya que estamos haciendo análisis cualitativo, en vez de cuantitativo. Intentando comparar entre los distintos algoritmos los atributos de calidad que estamos analizando, por lo cual cada celda requiere su tiempo de investigación. Investigamos cada uno de los algoritmos por separado, luego lo comparamos con los otros y los ordenamos. Cada celda demuestra el nivel de resultado (uno: menos favorable, dos: neutral, tres: más favorable).

Algoritmo de consenso	Costo/Eficiencia	Performance	Seguridad	Escalabilidad	Green Computing [104]
Proof of Stake	XX	XX	XXX	XX	XX
Proof of Work	X	X	XXX	X	X
Related to BFT	XXX	XXX	XX	X	XX
Federated Consensus	XXX	XXX	XXX	X	XX
Delegated Proof of Stake	XX	XXX	X	XXX	XXX
Proof of Authority	XXX	XXX	XXX	XXX	XXX
Proof of Elapsed Time	XXX	XXX	XXX	XXX	XXX

Tabla 17 - Algoritmos de consenso frente atributos de calidad

Algunos comentarios acerca de la Tabla 17:

- **Proof of Work** utiliza un puzzle criptográfico que es fácil de verificar, pero muy difícil de resolver en un tiempo aleatorio. Por lo cual utilizan grandes cantidades de poder

de cómputo, y por lo tanto de energía. Haciendo que la seguridad sea alta, pero el resto de los atributos no lo sean.

- **Proof of Stake** selecciona al próximo nodo para resolver el puzzle criptográfico basado en el control de los tokens relacionados a la red, generalmente junto a un factor aleatorio. Comparado con Proof of Work, este es más eficiente, con mejor rendimiento y escalable, ya que utiliza menos poder computacional y tiene menos latencia.
- **Related to BFT**, estos algoritmos apuntan a tener consenso sin que todos los participantes estén de acuerdo. El objetivo es brindar respuesta correcta ante fallas del sistema, aplicando una decisión colectiva cuyo objetivo es reducir la influencia de los nodos con errores. Las implementaciones son complejas y pueden llevar a problemas de seguridad. La correcta operación de estos sistemas requiere de una distribución mayor. Por lo cual cuanto más nodos tiene, más seguro es, pero eso lleva a impactos negativos en la escalabilidad de la red.
- **Delegated Proof of Stake** está basado en un sistema de votos, donde los participantes eligen a los validadores que van a proteger la Blockchain. Los miembros con mayores tokens de la red, tienen mayor porcentaje de votos. Los problemas que acarrea este algoritmo, están desde el punto de vista de la seguridad. Cuando un nodo o grupo de nodos contiene el 51% de los tokens, puede manipular a la red. Desde la escalabilidad y la eficiencia tienen mejores rendimientos.
- **Federated Consensus** es una forma de llegar a consenso bizantino, en la cual los nodos pueden compartir otro nodo y llevar al consenso sin haber conocido directamente todos los otros nodos. Es una alternativa a BFT, pero con el mismo problema del 51%
- **Proof of Authority** y **Proof of Elapsed Time** al ser algoritmos de consenso aplicado a Blockchains con permisos para los nodos que escriben en la red, el costo/eficiencia, la performance y la escalabilidad son mayores. Pero no son la realidad de las redes descentralizadas sin permisos que existen en Blockchain

Considerando que hay que minimizar el riesgo de elegir una red de Blockchain incompatible con los requerimientos, antes de invertir en el desarrollo de un producto o prototipo. Es importante estudiar el costo y performance de la red. El arquitecto de software puede llegar a necesitar estimar detalles no tan comunes sobre la latencia de la red basada en el tamaño del bloque, de la red, o de la transacción. Creemos que las pruebas de performance basadas en estos parámetros deben ser realizadas para superar fallas por picos de carga.

El poder computacional y la capacidad de almacenamiento de datos es limitada en Blockchain. Además de que las redes públicas de Blockchain cuestan indirectamente dinero, con un modelo de costos diferente al del software convencional. Estas decisiones sobre cuáles elementos tienen que ir en la nube (y cuáles afuera), afectan directamente la eficiencia, performance y flexibilidad. También si datos extra tienen que ir en la transacción o en un smart contract (on-chain), o en un sistema de terceros (off-chain). O decisiones

sobre si la lógica computacional tiene que ir en un smart contract (on-chain) o en otro software de terceros (off-chain). Algunas de estas decisiones ya fueron analizadas por la literatura [1].

Green computing es una aplicación de la ciencia ambiental que busca soluciones económicamente posibles para conservar la naturaleza y sus recursos. Los objetivos son usar el poder y la energía eficientemente, eligiendo hardware y software que sea favorable para el medio ambiente, además de reciclar materiales para aumentar el ciclo de vida de los productos [105]. Cuando se habla de Blockchain, se generaliza que consumen mucha energía, lo cual genera dudas acerca del futuro de la tecnología [106]. Sin embargo Blockchain está lejos de ser homogéneo, y estudios sugieren que el algoritmo de consenso, junto con la forma en que hacen hashing de la información, determina la eficiencia energética de la red [107]. Aunque otros factores como la propiedad de los datos (en general las redes con permisos son más eficientes que las que no tienen, ya que menos nodos tienen que estar activos y verificar las transacciones), el control de acceso, mining rewards y fees [108]. Ya existen estudios sobre el consumo energético de los diferentes algoritmos de consenso [109].

Consideramos interesante explorar si de verdad hay diferencias significativas entre las redes que son derivadas de Bitcoin y Ethereum. Especialmente las que tienen el mismo algoritmo de consenso, ya que pueden ser diferentes implementaciones para satisfacer los mismos atributos de calidad.

6.4. Madurez de los whitepapers

Es generalmente considerado que un whitepaper tiene que ser un reporte autoritativo o guía que informe a los lectores concisamente acerca de un problema complejo y presente la filosofía al respecto. Está destinado a ayudar a los lectores a comprender un problema, resolver un problema o tomar una decisión [110]. Luego de revisar más de 150 de estos whitepapers, concluimos algunas características que pueden ser utilizadas para juzgar la madurez de una red de Blockchain.

Un whitepaper de buena calidad necesita transmitir el propósito de una red sin intentar vender una idea o dimensionar el mercado. Los whitepapers de calidad necesitan describir las matemáticas y la criptografía adecuadamente y técnicamente. Ejemplos que consideramos de whitepapers buenos y profesionales son: Ethereum, Bitcoin, Stellar, Cardano. En contraste, los whitepapers de baja calidad consideramos que son como una presentación de PowerPoint, sin describir las matemáticas o la teoría por detrás de la red, carecen de referencias y principalmente intentan vender una idea. Por ejemplo, consideramos en este grupo, los whitepapers de NEO o Aventus.

Es importante aclarar que no descartamos ninguna red de Blockchain por tener un whitepaper de buena/mala calidad. Pero la calidad del mismo afecta en la capacidad y límite (y en la calidad) del proceso de extracción de datos. Ejemplos de whitepapers con pobre, y casi nula, información técnica pueden ser Dogecoin y Requests. Desde el punto de vista de la arquitectura, pensamos que no se pueden considerar como alternativas válidas de Blockchain, ya que no hay un fundamento técnico detrás de la red. Simplemente al considerarlos, no se sabe qué es lo que se está incluyendo en la arquitectura.

Independientemente de las decisiones de arquitectura, los whitepapers no apuntan a los arquitectos de software como los principales interesados. Son escritos para la comunidad de Blockchain, lo cual lo hacen difícil para los arquitectos de software para explotar la información de los mismos, para poder integrar una red de Blockchain a una arquitectura.

6.5. Reflexiones del método de investigación

Reflejado en nuestros resultados, encontramos que la MLR es un método de investigación pertinente para estudios secundarios de este estilo sobre tecnologías emergentes, donde la literatura blanca no está suficientemente desarrollada. Sin embargo, algo para señalar, es que la literatura gris no contiene exhaustivamente toda la información, y hay información incorrecta. Esto puede llevar a que los lectores dibujen conclusiones equivocadas. En Blockchain, evidencia de esto puede verse ya que 3/4 de las ICO (Initial Coin Offerings) de una nueva criptomonedas eran estafas [111].

Una MLR protocolizada basada en las guías de Garousi et al. [13] nos ayudó a identificar y excluir las redes de Blockchain de distintas fuentes. También nos permitió establecer la necesidad de utilizar literatura gris, el puente que divide la investigación de la práctica, compensando la falta de diversidad de los estudios de Blockchain en la literatura blanca.

Una de las lecciones aprendidas de la aplicación de una MLR, es el valor de los ciclos iterativos para el desarrollo del protocolo. En la investigación iteramos varias veces sobre los pasos del protocolo, definiendo y refinando el criterio de inclusión/exclusión, junto con el formulario de extracción de los datos. Todo esto a medida que fuimos descubriendo nueva evidencia e información en el proceso de identificar y caracterizar las redes de Blockchain. O al definir las fuentes de datos que encontramos en el proceso.

Cuando en una típica MLR, la unidad de análisis es la fuente (el artículo revisado por pares o la literatura gris), en nuestro estudio tomamos la decisión de utilizar la red de Blockchain como unidad de análisis. Esto se convirtió en el ancla para el formulario de extracción de datos, y la mayoría de las fuentes conducen a poblar los elementos de interés. Afirmamos que esta decisión fue la adecuada para nuestro objetivo de investigación, y especialmente para nuestros principales interesados. Un arquitecto de software puede navegar en nuestra

tabla de extracción de datos, encontrar su red postulada y revisar los elementos arquitectónicos en esa fila de datos.

6.6. Amenazas a la validez

La evaluación de las amenazas a la validez es fundamental para asegurar la calidad de los estudios empíricos en ingeniería de software [112]. Estas amenazas afectan todas las decisiones del método de investigación y pueden afectar sus resultados. Discutimos las posibles amenazas de validez en el contexto de los cuatro tipos adoptados de Wohlin et al. [113].

Validez interna es la propiedad de los estudios científicos que refleja hasta qué punto se justifica una conclusión causal basada en un estudio y los datos extraídos [113]. En el enfoque MLR para la selección de fuentes, los motores de búsqueda, los términos de búsqueda y los criterios de inclusión/exclusión se definieron cuidadosamente para garantizar que esta revisión sea repetible. Aún así, puede considerarse como una limitación del proceso. Para mitigar el riesgo de que falten fuentes relevantes, analizamos resultados relevantes en las primeras 100 páginas de resultados en la búsqueda en Google de "Blockchain Listings".

Otra amenaza para la validez interna es que los whitepapers fueron caracterizados y analizados por el autor de la tesis. Si alguna duda surgió sobre un whitepaper en especial, los otros investigadores fueron incluidos en la discusión. Con el objetivo de minimizar la inexperiencia en aplicar el nuevo criterio de inclusión/exclusión definido, se aplicó una votación después de la inclusión inicial de la fuente, y solo se seleccionaron para la revisión las redes de Blockchain que pasaron esta votación.

La **validez del constructo** se preocupa de la aplicabilidad de las RQs y del esquema de caracterización utilizado para la extracción de datos. Nuestras preguntas de investigación y nuestro formulario de extracción de datos para responderlas, fueron seleccionados e iterados múltiples veces por todos los investigadores. Otro riesgo viene de la falta de evidencia empírica para el análisis de las redes de blockchain, es imposible revisar el código fuente de cada una de las redes para chequear qué algoritmo de consenso utilizan. Utilizamos el whitepaper, la fuente de detalles técnicos más confiable, como proxy entre la arquitectura de software y la red de Blockchain.

La **validez de la conclusión** de un estudio se ocupa de si se llega a las conclusiones correctas mediante un tratamiento riguroso y repetible. Se pudieron analizar todas las fuentes de datos para las redes Blockchain, y los datos se revisaron, extrajeron y sintetizaron. El estudio fue protocolizado asegurando la replicabilidad de los resultados.

Validez externa se refiere a la medida en que los resultados de este estudio pueden generalizarse. Probablemente dejamos algo de Blockchain a un lado porque es imposible

descartar todo Internet en un área emergente. Intentamos obtener todos los listados o blogs de Blockchain más completos donde se pudieran identificar las redes.

7. Conclusiones y trabajo a Futuro

7.1. Lecciones aprendidas y resultados

Esta tesis presenta con fundamento teórico una MLR enfocada a identificar las redes de Blockchain activas, analizando sus algoritmos de consenso, si aceptan o no smart contracts, junto con otras características como: dominio, descentralización, estructura del ledger y configuración de los bloques. Encontramos que la metodología utilizada para la revisión es adecuada para tecnologías emergentes, además de ser amplia en lo que abarca y flexible para adecuarse al objetivo de la investigación. Gran parte de la información de este dominio no es académica y no está estructurada. No hay un lugar donde se pueda ir a consultar sobre todas las redes de Blockchain activas y disponibles. Además, Blockchain está siendo impulsada por la industria, y la investigación académica todavía necesita ponerse a punto con el conocimiento disponible en la industria. Con este trabajo intentamos acortar la distancia entre estos dos mundos mediante la sistematización de la información disponible desde distintas fuentes.

La fuente de información primaria establecida para las redes de Blockchain son los whitepapers. Estos no necesariamente apuntan a los arquitectos de software como los principales interesados, sino que apuntan a la comunidad más de Blockchain (técnica o de negocios). Esto hace difícil para arquitectos explorar la información de los mismos y sacar información acerca de cuál red aplicar en una arquitectura. Esto se ve dificultado por la calidad de alguno de estos, que no cuentan con detalle y estructura de un artículo formal.

Mediante la MLR, fue posible identificar 112 redes de Blockchain que tienen proyectos activos, además de realizar una caracterización de las mismas. Esta tesis permite además agrupar las redes identificadas en familias similares: de uso general, criptomonedas, y de dominio específico. Consideramos que estas categorías están relacionadas con las decisiones que un arquitecto de software debe realizar para hacer uso de una red de Blockchain, o interconectarse con un sistema existente. Sostenemos que pueden servir como guía para tomar mejores decisiones a la hora de incorporar Blockchain en una arquitectura de software.

Una de las lecciones aprendidas de la aplicación de MLR, es el valor de los ciclos iterativos para el desarrollo del protocolo. Mediante la iteración se obtiene un protocolo más adaptado a las necesidades del dominio, imposible de llegar sin tener resultados intermedios.

La investigación nos ayudó a entender cómo fue la evolución de Blockchain, y hacia dónde es su futuro. En la siguiente sección presentamos un resumen, junto con lo que creemos es el terreno fértil para la investigación. Luego presentamos nuestros aportes, junto con las líneas futuras de nuestra investigación.

7.2. Tendencias sobre Blockchain

Blockchain sale a la luz junto a Bitcoin como un ledger distribuido de transacciones, en los cuales cada bloque de información es seguro y unido a los siguientes mediante funciones de hash, resultando en una cadena de bloques descentralizada, inmutable y transparente. Con Ethereum, la aparición de los smart contracts, lleva a la creación de Blockchain 2.0, generando una "infraestructura programable confiable y distribuida" [98]. Dejando abierto el camino a la Blockchain 3.0, buscando una mayor aplicación y el establecimiento de unidades organizacionales descentralizadas autónomas mediante las aplicaciones descentralizadas (dApps). El paso final de esta evolución, la Blockchain 4.0, apunta a ofrecer la tecnología como una plataforma más rápida y reutilizable para crear y correr aplicaciones, haciendo todavía más fácil su adopción.

La evolución viene de la mano de nuevos algoritmos de consenso, mejoras en la escalabilidad, interoperabilidad y velocidad, eficiencia en los costos y en el consumo de energía. Es un terreno totalmente fértil para trabajos académicos que propongan ideas innovadoras desde nuevos algoritmos de consenso, formas de hashing, métodos de verificación, o cualquier concepto que proponga alternativas a las ya establecidas. Pudiendo atacar los problemas ya conocidos de escalabilidad, seguridad, green computing.

7.3. Contribuciones de la investigación

La primera contribución de esta tesis es el catálogo con atributos detallados de 112 redes de Blockchain activas. No hemos encontrado un catálogo similar publicado. No solo se tiene una visión de los atributos de cada red, si no que se pudo extraer datos interesantes del cruzamiento de la información, llegándose a una categorización en tres familias.

Independientemente del catálogo y resultados, se llegó a una aplicación estructurada del método MLR, que permite replicarlo para seguir expandiendo la lista de redes de Blockchain. Se considera también una innovación la unidad de análisis resultado de la MLR, siento las redes de Blockchain en vez de las fuentes de datos.

Las contribuciones de esta tesis fueron divulgadas en un artículo con resultados preliminares presentado en las Jornadas Chilenas de Computación 2020[9] [19]. Un reporte completo de la MLR y discusión del impacto de Blockchain en la arquitectura de software fue enviado para su publicación en el journal arbitrado Future Generation Computer Systems[10] [20] (en proceso de revisión).

[9] https://jcc2020.cl/
[10] https://www.sciencedirect.com/journal/future-generation-computer-systems

7.4. Líneas futuras de investigación

Nuestra futura línea de investigación va a estar enfocada en actualizar el catálogo de Blockchains con las nuevas redes que van emergiendo, además de expandir la caracterización de cada una. Queremos analizar cuál va a ser el impacto de las distintas familias de redes sobre los atributos de calidad.

Creemos que el algoritmo de consenso va a tener un alto impacto sobre los atributos de calidad de performance, seguridad y escalabilidad. Por ese motivo, en una futura línea de investigación se debe abordar en forma específica cada uno de los atributos de las redes, para analizar cómo afectan los atributos de calidad, influenciando la decisión de los arquitectos de incluirla en un sistema.

8. Referencias

[1] X. Xu, I. Weber, M. Staples, and P. Rimba, “A Taxonomy of Blockchain-Based Systems for Architecture Design,” *ICSA’17: IEEE International Conference on Software Architecture*, Apr. 2017, Accessed: Feb. 16, 2021. [Online]. Available: https://www.researchgate.net/publication/314213262_A_Taxonomy_of_Blockchain-Based_Systems_for_Architecture_Design

[2] Google, “Google Trends: Blockchain, Big Data, Machine Learning, Artificial Intelligence.” https://trends.google.com/trends/explore?date=all&q=blockchain,big%20data,machine%20learning,Inteligencia%20artificial (accessed Feb. 16, 2021).

[3] T. Laurence, *Blockchain For Dummies*. USA: John Wiley & Sons, 2017.

[4] V. Buterin, “The Meaning of Decentralization.” https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (accessed Feb. 16, 2021).

[5] S. Raval, *Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology*. USA: “O’Reilly Media, Inc.,” 2016.

[6] S. Underwood, “Blockchain beyond Bitcoin,” *Commun. ACM*, vol. 59, no. 11, pp. 15–17, Oct. 2016.

[7] S. Liu, “Global market for blockchain technology 2018-2025.” https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/ (accessed Mar. 25, 2021).

[8] D. Pollock, “Blockchain Or Bust: Businesses Need To Seek A Middle Ground,” *Forbes*, Jan. 18, 2019. https://www.forbes.com/sites/darrynpollock/2019/01/18/blockchain-or-bust-businesses-need-to-seek-a-middle-ground/ (accessed Feb. 16, 2021).

[9] H. Puri, “A complete list of Blockchain platforms — 2020,” *WikiDLT*, Jan. 21, 2020. https://medium.com/wikidlt/a-complete-list-of-blockchain-platforms-2020-49cf01ee6688 (accessed Feb. 17, 2021).

[10] CoinMarketCap, “Cryptocurrency prices, charts and market capitalizations.” https://coinmarketcap.com/ (accessed Feb. 17, 2021).

[11] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, “A Systematic Review of the Use of Blockchain in Healthcare,” *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018.

[12] A. R. Claes Wohlin, “Challenges and recommendations to publishing and using credible evidence in software engineering,” *Information and Software Technology*, vol. 134, p. 106555, Jun. 2021.

[13] V. Garousi, M. Felderer, and M. V. Mäntylä, “Guidelines for including grey literature and conducting multivocal literature reviews in software engineering,” *Information and Software Technology*, vol. 106, pp. 101–121, Feb. 2019.

[14] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where Is Current Research on Blockchain Technology?-A Systematic Review,” *PLoS One*, vol. 11, no. 10, p. e0163477, Oct. 2016.

[15] N. Dashkevich, S. Counsell, and G. Destefanis, “Blockchain Application for Central Banks: A Systematic Mapping Study,” *IEEE Access*, vol. 8. pp. 139918–139952, 2020.

[16] B.-J. Butijn, D. A. Tamburri, and W.-J. van den Heuvel, “Blockchains: A Systematic Multivocal Literature Review,” *ACM Comput. Surv.*, vol. 53, no. 3, pp. 1–37, Jun. 2020.

[17] J. Soldani, D. A. Tamburri, and W.-J. Van Den Heuvel, “The pains and gains of microservices: A Systematic grey literature review,” *J. Syst. Softw.*, vol. 146, pp. 215–232, Dec. 2018.

[18] J. Scheuner and P. Leitner, “Function-as-a-Service performance evaluation: A multivocal literature review,” *J. Syst. Softw.*, vol. 170, p. 110708, Dec. 2020.

[19] J. M. Sobral, M. Solari, and S. Matalonga, “Preliminary Results of a Multi-Vocal Literature Review of Blockchain Networks,” in *2020 39th International Conference of the Chilean Computer Science Society (SCCC)*, Nov. 2020, pp. 1–8.

[20] Juan Manuel Sobral, Martin Solari, Santiago Matalonga, “Multivocal Literature Review of

SoftwareArchitectures for Blockchain Networks."
[21] Google, "Google Trends." https://trends.google.com/trends/explore?date=today%205-y&q=bitcoin,Blockchain (accessed Jul. 25, 2021).
[22] L. Lantz and D. Cawrey, *Mastering Blockchain*. USA: O'Reilly Media, Incorporated, 2020.
[23] D. Chaum, "Blind Signatures for Untraceable Payments," in *Advances in Cryptology*, 1983, pp. 199–203.
[24] B. Schoenmakers, "Security Aspects of the Ecash™ Payment System," *State of the Art in Applied Cryptography*. pp. 338–352, 1998.
[25] A. Back and Others, "Hashcash-a denial of service counter-measure," 2002, [Online]. Available: ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf
[26] S. Nakamoto, "Bitcoin: a peer-to-peer digital cash system, 24 May 2009."
[27] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptology*, vol. 3, no. 2, pp. 99–111, Jan. 1991.
[28] W. F. Ehrsam, C. H. W. Meyer, J. L. Smith, and W. L. Tuchman, "Message verification and transmission error detection by block chaining," 4074066, Feb. 14, 1978 Accessed: Jul. 26, 2021. [Online]. Available: https://patentimages.storage.googleapis.com/73/3b/88/5942eef743a6a7/US4074066.pdf
[29] Ethereum, "Ethereum Virtual Machine (EVM)." https://ethereum.org/en/developers/docs/evm/ (accessed Jul. 24, 2021).
[30] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[31] IBM, "IBM Blockchain - Enterprise Blockchain Solutions & Services." https://www.ibm.com/blockchain (accessed Feb. 17, 2021).
[32] Hyperledger, "Hyperledger fabric – hyperledger," Apr. 11, 2017. https://www.hyperledger.org/projects/fabric (accessed Feb. 17, 2021).
[33] R. Miller, "IBM unveils Blockchain as a Service based on open source Hyperledger Fabric technology," *TechCrunch*, Mar. 20, 2017. Accessed: Feb. 17, 2021. [Online]. Available: http://techcrunch.com/2017/03/19/ibm-unveils-blockchain-as-a-service-based-on-open-source-hyperledger-fabric-technology/
[34] Microsoft, "Blockchain." https://azure.microsoft.com/en-us/solutions/blockchain/ (accessed Feb. 17, 2021).
[35] American Association of Insurance Services, "- openIDL - AAIS Online." https://aaisonline.com/openidl (accessed Feb. 17, 2021).
[36] R. Kamath, "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM," *The JBBA*, vol. 1, no. 1, p. 3712, Jun. 2018.
[37] ITU, "'Food Trust' partnership uses blockchain to increase food safety." https://www.itu.int:443/en/myitu/News/2020/04/09/13/48/Food-Trust-partnership-uses-blockchain-to-increase-food-safety (accessed May 09, 2021).
[38] T. Groenfeldt, "IBM And Maersk Apply Blockchain To Container Shipping," *Forbes*, Mar. 05, 2017. https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/ (accessed May 09, 2021).
[39] Amazon, "Amazon Managed Blockchain - Amazon Web Services." https://aws.amazon.com/managed-blockchain/customers/ (accessed May 09, 2021).
[40] IBM, "IBM Food Trust - Blockchain for the world's food supply." https://www.ibm.com/blockchain/solutions/food-trust (accessed May 09, 2021).
[41] National Agency of Public Registry-Georgia, "Bitfury, Republic of Georgia Push Ahead With Blockchain Land-Titling Project." https://napr.gov.ge/p/1513 (accessed Jul. 24, 2021).
[42] *Exonum*. Github. Accessed: Jul. 24, 2021. [Online]. Available: https://github.com/exonum
[43] E. G. Team, "LinkedIn 2018 Emerging Jobs Report," *introduction by Guy Berger, LinkedIn Economic Graph, LinkedIn Corp. , Microsoft*, vol. 13, 2018.

[44] S. Rodriguez, “Salaries for blockchain engineers are skyrocketing, now on par with AI experts,” *CNBC*, Oct. 21, 2018. https://www.cnbc.com/2018/10/21/how-much-do-blockchain-engineers-make.html (accessed Feb. 17, 2021).
[45] M. Schedlbauer and K. Wagner, “Blockchain beyond Digital Currencies - A Structured Literature Review on Blockchain Applications,” *SSRN Electronic Journal*.
[46] M. Conoscenti, A. Vetrò, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov. 2016, pp. 1–6.
[47] C. Shen and F. Pena-Mora, “Blockchain for Cities—A Systematic Literature Review,” *IEEE Access*, vol. 6, pp. 76787–76819, 2018.
[48] Y. Tribis, A. El Bouchti, and H. Bouayad, “Supply Chain Management based on Blockchain: A Systematic Mapping Study,” *MATEC Web of Conferences*, vol. 200, p. 00020, 2018.
[49] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, “Blockchain for Business Applications: A Systematic Literature Review,” in *Business Information Systems*, 2018, pp. 384–399.
[50] CoinMarketCap, “Cryptocurrency prices, charts and market capitalizations.” https://coinmarketcap.com/ (accessed Apr. 24, 2021).
[51] Golden, “Building the world’s knowledge engine.” https://golden.com/ (accessed Apr. 24, 2021).
[52] “Crypto & Blockchain,” *Forbes Magazine*, Forbes. Accessed: Apr. 24, 2021. [Online]. Available: https://www.forbes.com/crypto-blockchain/
[53] TechnoDuet, “A comprehensive list of blockchain platforms,” Jan. 14, 2021. https://www.technoduet.com/a-comprehensive-list-of-blockchain-platforms/ (accessed Apr. 24, 2021).
[54] Wikipedia contributors, “List of cryptocurrencies,” *Wikipedia, The Free Encyclopedia*, Mar. 08, 2021. https://en.wikipedia.org/w/index.php?title=List_of_cryptocurrencies&oldid=1011056953 (accessed Apr. 24, 2021).
[55] Gartner, Inc, “Blockchain Platforms Reviews 2021.” https://www.gartner.com/reviews/market/blockchain-platforms (accessed Apr. 24, 2021).
[56] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice*. Addison-Wesley Professional, 2003.
[57] X. Xu, I. Weber, and M. Staples, *Architecture for Blockchain Applications*, 1st ed. Cham, Switzerland: Springer Nature, 2019.
[58] K. Musa and J. Alkhateeb, “Quality model based on cots quality attributes,” *Int. j. softw. eng. appl.*, vol. 4, no. 1, pp. 1–8, Jan. 2013.
[59] International Organization for Standardization, *Systems and Software Engineering: Systems and Software Quality Requirements and Evaluation (SQuaRE) : System and Software Quality Models*. ISO, 2011.
[60] P. Kunz, “Software product quality evaluation using ISO/IEC 25000,” Sep. 2014.
[61] D. Lea, D. Forslund, T. Barry, D. Vines, R. Raj, and A. Tiwary, “Building distributed systems (panel),” in *Proceedings of the 13th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications*, Vancouver, British Columbia, Canada, Oct. 1998, pp. 412–416.
[62] J. E. Pérez-Martínez and A. Sierra-Alonso, “A taxonomy of the quality attributes for distributed applications,” *Computer* , vol. 1, p. 1, 2002.
[63] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Manubot*, Nov. 2008.
[64] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in *2017 IEEE International Congress on Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.
[65] Weiss and W. M. Allen, *Data Structures and Algorithm Analysis in C++*. Pearson Education, 2007.
[66] M. I. T. OpenCourseWare, “21. Cryptography: Hash Functions,” Mar. 04, 2016.

https://www.youtube.com/watch?v=KqqOXndnvic (accessed Apr. 24, 2021).
[67] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: a survey,” *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, Jan. 2018.
[68] M. Selvamanikkam, “Digital Signature Generation,” *Medium*, Feb. 01, 2018. https://medium.com/@meruja/digital-signature-generation-75cc63b7e1b4 (accessed Apr. 24, 2021).
[69] M. I. A. K. Lakhani, “The Truth About Blockchain,” *Harvard Business Review*, Jan. 01, 2017. Accessed: Apr. 24, 2021. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain
[70] MIT Technology Review Editors, *Technology review*. Accessed: Apr. 24, 2021. [Online]. Available: https://www.technologyreview.com/2018/04/23/143486/a-glossary-of-blockchain-jargon/
[71] A. Hu, “WTF is peer-to-peer? - Blockchain Beat - Medium,” *Blockchain Beat*, Sep. 06, 2017. https://medium.com/@alberthu/wtf-is-peer-to-peer-4b865d29e44e (accessed Apr. 24, 2021).
[72] V. Buterin and Others, “A next-generation smart contract and decentralized application platform,” *white paper*, vol. 3, no. 37, 2014, [Online]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf
[73] Ethereum Foundation, “On Public and Private Blockchains.” https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed Apr. 24, 2021).
[74] Ethereum Foundation, “Privacy on the Blockchain.” https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/ (accessed Apr. 24, 2021).
[75] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, “Applying Software Patterns to Address Interoperability in Blockchain-based Healthcare Apps,” *arXiv [cs.CY]*, Jun. 05, 2017. [Online]. Available: http://arxiv.org/abs/1706.03700
[76] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, “A Survey on Blockchain Interoperability: Past, Present, and Future Trends,” *arXiv [cs.DC]*, May 28, 2020. [Online]. Available: http://arxiv.org/abs/2005.14282
[77] “Blockchain Interoperability.” https://documents.worldbank.org/en/publication/documents-reports/documentdetail/373781615365676101/blockchain-interoperability (accessed Jun. 23, 2021).
[78] S. Nazarov, P. Shukla, A. Erwin, and A. Rajput, “Bridging the Governance Gap: Interoperability for blockchain and legacy systems,” 2020.
[79] A. Dika, “Ethereum smart contracts: Security vulnerabilities and security tools.” https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2479191/18400_FULLTEXT.pdf (accessed Apr. 24, 2021).
[80] T. Chen, X. Li, X. Luo, and X. Zhang, “Under-optimized smart contracts devour your money,” in *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, Feb. 2017, pp. 442–446.
[81] E. Hildenbrandt *et al.*, “KEVM: A complete semantics of the Ethereum Virtual Machine,” Aug. 2017.
[82] A. Mense and M. Flatscher, “Security Vulnerabilities in Ethereum Smart Contracts,” in *Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services*, Yogyakarta, Indonesia, Nov. 2018, pp. 375–380.
[83] M. Swan, *Blockchain: Blueprint for a New Economy*. “O’Reilly Media, Inc.,” 2015.
[84] L. Lamport, R. Shostak, and M. Pease, “The Byzantine generals problem,” in *Concurrency: the Works of Leslie Lamport*, New York, NY, USA: Association for Computing Machinery, 2019, pp. 203–226.
[85] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct. 2017, pp. 2567–2572.
[86] A. Baliga, “Understanding blockchain consensus models,” *Persistent*, vol. 4, pp. 1–14, 2017.

[87] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, “Blockchain Consensus Algorithms: A Survey,” *arXiv [cs.DC]*, Jan. 20, 2020. [Online]. Available: http://arxiv.org/abs/2001.07091
[88] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, “Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities,” *IEEE Access*, vol. 7, pp. 85727–85745, 2019.
[89] CRYPTO., *Advances in Cryptology--CRYPTO ’92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992 : Proceedings*. London, 1993.
[90] POA Network, “Proof of Authority: consensus model with Identity at Stake,” *POA Network*, Nov. 11, 2017. https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256 (accessed May 02, 2021).
[91] Consensus, “Proof of elapsed time (PoET).” https://tokens-economy.gitbook.io/consensus/chain-based-trusted-computing-algorithms/poet (accessed May 02, 2021).
[92] V. Garousi, M. Felderer, M. V. Mäntylä, and A. Rainer, “Benefitting from the Grey Literature in Software Engineering Research,” in *Contemporary Empirical Methods in Software Engineering*, M. Felderer and G. H. Travassos, Eds. Cham: Springer International Publishing, 2020, pp. 385–413.
[93] R. J. Adams, P. Smart, and A. S. Huff, “Shades of grey: Guidelines for working with the grey literature in systematic reviews for management and organizational studies: Shades of grey,” *Int. J. Manag. Rev.*, vol. 19, no. 4, pp. 432–454, Oct. 2017.
[94] N. Chaudhry and M. M. Yousaf, “Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities,” in *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, Dec. 2018, pp. 54–63.
[95] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, “The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling,” in *Business Information Systems Workshops*, Jul. 2018, pp. 185–196.
[96] E. Brown, “Ocean Protocol delivers blockchain-based decentralized data orchestration for Daimler AG,” *ZDNet*, Jul. 28, 2020. https://www.zdnet.com/article/ocean-protocol-delivers-blockchain-based-decentralized-data-orchestration-for-daimler-ag/ (accessed Apr. 04, 2021).
[97] D. T. A. T. Kirkland, “How blockchains could change the world,” May 06, 2016. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-blockchains-could-change-the-world (accessed May 02, 2021).
[98] T. Swanson, “Blockchain 2.0 – let a thousand chains blossom.” https://letstalkbitcoin.com/blockchain-2-0-let-a-thousand-chains-blossom (accessed May 02, 2021).
[99] J. Ackermann and M. Meier, “Blockchain 3.0: The next generation of blockchain systems,” 2018.
[100] A. Pieroni, N. Scarpato, L. Di Nunzio, F. Fallucchi, and M. Raso, “Smarter city: smart energy grid based on blockchain technology,” *Int. J. Adv. Sci. Eng. Inf. Technol*, vol. 8, no. 1, pp. 298–306, 2018.
[101] R. Srivastava *et al.*, “Blockchain : A Revolutionary Technology,” *International Journal of Trend in Scientific Research and Development*, vol. -2, no. -3. pp. 2368–2373, 2018.
[102] J. Ackermann and M. B. Meier, “3.0—The next generation of blockchain systems,” in *Proceedings of the Advanced Seminar Blockchain Technologies, Munich, Germany*, 2018, pp. 1–7.
[103] M. Scherer, “Performance and Scalability of Blockchain Networks and Smart Contracts,” 2017. Accessed: May 02, 2021. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1111497
[104] M. Comans, O. de Haas, R. Jongerius, D. Oudejans, and E. de Smidt, “Stop Boiling the Oceans:

A Review on Energy Efficient Proof of Work Alternatives," 2019, [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid:f1378204-cfcb-4ab6-84cc-b7249c0c3868
[105] J. Singh, "Green Computing," *J. Technol. Manag. Grow. Econ.*, vol. 7, no. 2, pp. 7–26, Oct. 2016.
[106] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The Energy Consumption of Blockchain Technology: Beyond Myth," *Business & Information Systems Engineering*, vol. 62, no. 6, pp. 599–608, Dec. 2020.
[107] J. Li, N. Li, J. Peng, H. Cui, and Z. Wu, "Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies," *Energy*, vol. 168, pp. 160–168, Feb. 2019.
[108] N. Sapkota and K. Grobys, "Blockchain Consensus Protocols, Energy Consumption and Cryptocurrency Prices," *SSRN Electronic Journal*.
[109] R. Cole and L. Cheng, "Modeling the Energy Consumption of Blockchain Consensus Algorithms," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1691–1696.
[110] L. Shipley, "The Whitepaper Revolution ~ the good, the bad and the sickening." https://hackernoon.com/the-whitepaper-revolution-the-good-the-bad-and-the-sickening-438b51333fa (accessed May 02, 2021).
[111] C. Kim, "Report: More than three-quarters of ICOs were scams," *CoinDesk*, Jul. 12, 2018. https://www.coindesk.com/report-more-than-three-quarters-of-icos-in-2017-were-scams (accessed May 02, 2021).
[112] X. Zhou, Y. Jin, H. Zhang, S. Li, and X. Huang, "A Map of Threats to Validity of Systematic Literature Reviews in Software Engineering," *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*. 2016.
[113] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering*. Springer Science & Business Media, 2012.