# Revisión multi-vocal de arquitecturas de software para Blockchain

Sobral, Juan Martín; Solari, Martín; Matalonga, Santiago

*Published in:*
Proceedings of the XXXIX International Conference of the Chilean Computer Science Society

Accepted/In press: 18/10/2020

*Document Version*
Peer reviewed version

# Revisión multi-vocal de arquitecturas de software para Blockchain

Sobral, Juan Martín; Solari, Martín; Matalonga, Santiago

Accepted/In press: 18/10/2020

*Document Version*
Peer reviewed version

# Revisión multi-vocal de arquitecturas de software para Blockchain

Juan Manuel Sobral
*Universidad ORT Uruguay*
Montevideo, Uruguay
juanmsobral@gmail.com

Martin Solari
*Universidad ORT Uruguay*
Montevideo, Uruguay
martin.solari@ort.edu.uy

Santiago Matalonga
*University of the West of Scotland*
Glasgow, United Kingdom
santiago.matalonga@uws.ac.uk

***Resumen*—*Contexto*: La tecnología Blockchain ha propiciado muchos proyectos, que han visto en ella una alternativa para llevar a cabo el manejo de datos sin un ente central que los rija. *Objetivo*: El objetivo de este trabajo es identificar la mayoría de las redes de Blockchain disponibles. Identificando las características principales de las mismas: el tipo de algoritmo de consenso, la centralización, estructura del bloque y origen de la red, entre otros. *Método*: Realizamos una revisión multi-vocal para identificar las redes Blockchain disponibles y analizar sus características más relevantes desde el punto de vista de la arquitectura de software. *Resultado*: Obtuvimos una caracterización de 114 redes de Blockchain, ofreciendo una guía para el arquitecto de software, para que este pueda tomar decisiones estratégicas al momento de incorporar esta tecnología.**

***Index Terms*—Blockchain, Smart Contracts, Arquitectura de Software, Revisión Multi-Vocal**

## I. Introducción

Blockchain es una nueva forma de guardar información con el potencial para revolucionar la economía del mundo [25]. Es considerada una tecnología emergente para la descentralización y el intercambio de datos transaccionales en grandes redes de participantes desconocidos. Esta tecnología introduce cambios, donde los nuevos estados del sistema son alcanzados sin confiar en una autoridad central [26]. La estructura de los datos es organizada en bloques, los cuales tienen referencias al bloque anterior de la cadena. Mediante técnicas criptográficas, la información contenida en un bloque sólo se puede editar modificando todos los bloques posteriores [9].

Blockchain es una tecnología emergente, por lo que muchas veces su incorporación representa un desafío para los arquitectos de software. En este estudio desarrollamos una *revisión multi-vocal de la literatura* (o *multi-vocal literature review*), [12] para identificar y caracterizar las principales redes de Blockchain disponibles y sus aspectos claves. Se utilizó esta metodología porque se trata de un contexto donde existe información relevante cuyas fuentes no son académicas o no pasaron un proceso formal de revisión de pares.

Luego de identificar las redes de Blockchain disponibles, analizamos los algoritmos de consenso, si las redes aceptan o no *smart contracts*, junto con otras características como: dominio, centralización, estructura del "ledger" y configuración de los bloques. Siendo estos aspectos fundamentales que se pueden considerar para la adopción de la tecnología Blockchain en una arquitectura de software.

Al incorporar tecnología de Blockchain a un proyecto, se deben tomar en consideración una serie de decisiones de arquitectura que afectan como los atributos de calidad del sistema, tales como: privacidad, escalabilidad, seguridad, eficiencia y transparencia y confiabilidad [26]. Las características de la red afectan estos atributos.

El presente artículo se estructura de la siguiente manera: II. Definiciones y Trabajos Previos, III. Metodología, IV. Resultados, V. Discusión y VI. Conclusiones..

## II. Definiciones y trabajos previos

### II-A. Tipos de redes de Blockachain

Se define un **sistema centralizado**, como aquel en el que los procesos de cómputo son efectuados en una localización central, usando terminales conectados a una computadora central. La computadora en sí misma puede controlar todos los puertos periféricos directamente (si están físicamente conectados con la computadora central), o conectados a través de un servidor de terminal. También están los sistemas de información interconectados en el que ninguna entidad es la autoridad única, sino que hay un centro colectivo de diversos nodos. En informática y en la tecnología de la información, estos sistemas usualmente adoptan la forma de computadoras en red y son conocidos como **sistemas descencentralizados**. En estos, si bien la red no cae ante la caida de nodos, cuando uno de los nodos reguladores cae, se produce la desconexión de uno o varios nodos del conjunto de la red. Finalmente, los **sistemas distribuidos** se caracterizan como una colección de computadoras independientes que es presentada a sus usuarios como un sistema coherente único, [24]. Cada nodo es independiente y puede moverse libremente, por lo cual hay una ausencia de un centro individual o colectivo.

Las redes de Blockchain pueden ser clasificadas según su accesibilidad [5]. Las **Blockchain públicas** son aquellas que están accesibles para que cualquier usuario pueda leer, enviar transacciones, y participar en el proceso de consenso. Estas son las redes consideradas como totalmente descentralizadas. Mientras que las **Blockchain de consorcios**, se refieren a redes donde el proceso de consenso es controlado por un número preseleccionado de nodos. El derecho a leer puede ser público o permisionado para participantes, y pueden agregarse reglas de acceso. Estas Blockchain son consideradas parcialmente descentralizados. Las **Blockchain privadas** son Blockchain

en donde los permisos de escrituras se centralizan en una organización. El acceso puede ser público o restrictivo. Una red Blockchain de este tipo puede considerase como un sistema centralizado con un grado de auditabilidad criptográfica.

Generalmente se asocia a las redes de Blockchain con las criptomonedas, pero con la segunda generación de las redes nace el concepto de **smart contracts** (contratos inteligentes). Estos son 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. Como residen dentro de la red de Blockchain, cada contrato tiene un identificador único para diferenciarlos, y permitir que los usuarios que pueden interactuar con ellos. [23]

Una de las características más relevantes de Blockchain es cómo una red de nodos desconocidos se pone de acuerdo para validar y registrar nuevos conjuntos de datos. Esta situación es otra aplicación del problema de Byzanteine Generals (BG), presente desde 1982 [15]. Como lograr el concenso en un sistema distribuido es un desafío del **algoritmo de consenso**.

El **algoritmo de consenso** es un acuerdo alcanzado por la mayoría de los nodos participantes de una red con respecto a el estatus de estos y su protocolo [18]. Se encargan de asegurar que las reglas del protocolo son respetadas y garantizando que todas las transacciones tienen lugar de una forma fiable; lo que implica, por ejemplo, que las criptomonedas sólo podrán ser gastadas una vez [18]. Es el algoritmo de consenso el encargado del rendimiento y seguridad en una red [10] [2].

### *II-B. Trabajos Previos*

Existen mapeos sistemáticos sobre Blockchain aplicado en diversos sectores, como la cadena de suministro, negocios, atención médica, IoT, privacidad y gestión de datos, donde se establecen temas claves, tendencias y áreas emergentes para la investigación. Pero ninguno de estos caracterizan cuáles son las redes redes que se están aplicando, sino que resumen el numero de artículos.

- Blockchain for the Internet of Things: a Systematic Literature Review [16]: A partir de 1.511 artículos, de los cuales se quedan con 35.
- A Systematic Review of the Use of Blockchain in Healthcare - MDPI [17]: A partir de 12.000 artículos, de los cuales se quedan con 71.
- Blockchain for Cities—A Systematic Literature Review [7]: A partir de 3827 artículos, de los cuales se quedan con 1591.
- Supply Chain Management based on Blockchain: A Systematic Mapping Study [27]: A partir de 227 artículos, de los cuales se quedan con 24.

Con esta motivación, otros autores han realizado mapeos sistemáticos mas generales con la finalidad de estudiar el estado actual de esta tecnología. En el trabajo realizado por Yli-Huumo y colegas [28] tuvo como objetivo comprender las tendencias de investigación actuales en el marco de la tecnología Blockchain, los desafíos y las direcciones futuras con respecto a dicha tecnología desde la perspectiva técnica. En su trabajo utilizaron 41 artículos primarios de bases de datos científicas. Los resultados obtenidos en esta investigación muestran que el foco en más del 80 % de los documentos está en el sistema Bitcoin y menos del 20 % se ocupa de otras aplicaciones de Blockchain que incluyen, por ejemplo, contratos inteligentes y licencias.

En el la revisión sistemática realizada por Konstantinidis y colegas [14], se realizó a cabo una encuesta con el objetivo de señalar las áreas en las que se están desarrollando aplicaciones y servicios de tecnología Blockchain tanto en el sector público como en el privado. Este artículo concluye en que si bien hay áreas de aplicación, es necesario mas avance en la investigación y literatura formal. De estos estudios secundarios se ha obtenido como conclusión que existe falta de investigación cualitativa y cuantitativa. Lo que implica que el alcance de utilizar la tecnología Blockchain aún no se ha evaluado sobre una base científica empírica. [19].

Es importante aclarar que no se encontraron trabajos con un resultado similar al alcance de este artículo.

## III. Metodología de Investigación

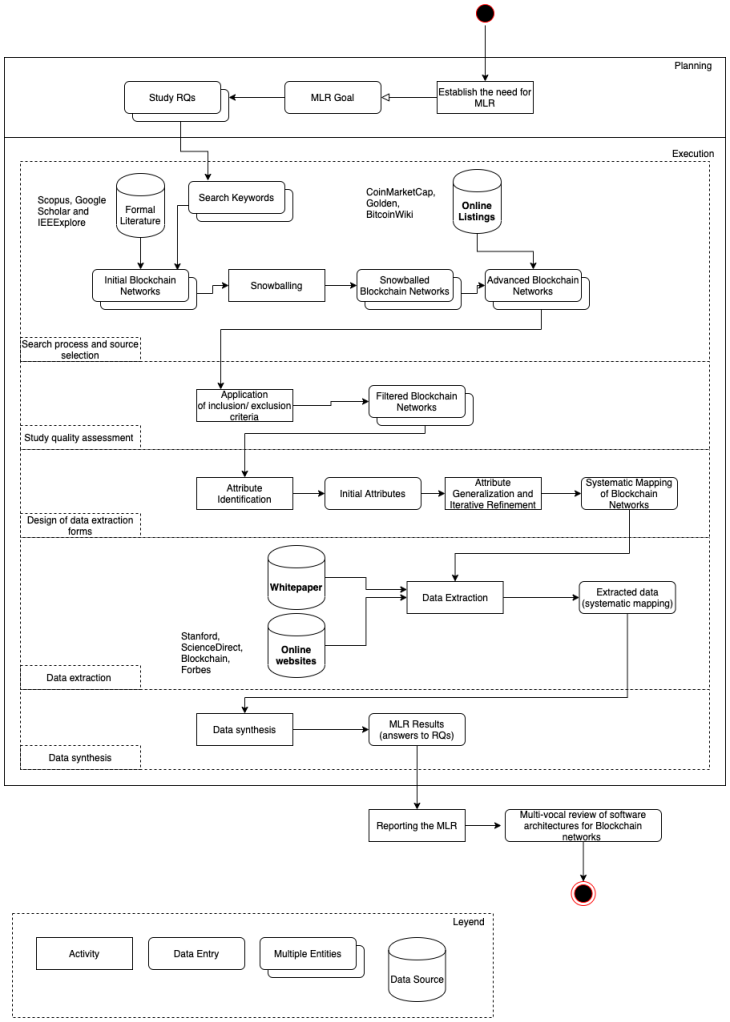


Figura 1. Diagrama de la metodología de investigación

### III-A. Introducción

La metodología de investigación seleccionada es una Multivocal Literature Review (MLR), la cual ha sido escogida en nuestro trabajo por ser la que une las características que se adaptan a nuestro tema de investigación. Una MLR permite incluir un abanico más amplio de información, principalmente en temas tecnológicos innovadores [12] . Con esta metodología se puede considerar como información válida literatura gris tal como blogs, videos, whitepapers. En particular para la área este trabajo, mucha información relevante se encuentra en blogs y whitepapers[1] de los creadores/programadores de las distintas redes. Además que existe un relativo bajo número de trabajos académicos que aporten evidencia al problema [6].

Respecto al procesos de la MLR, en este trabajo se aplicaron las guías de Garousi y colegas [12] para determinar la pertinencia de este método de investigación al área de trabajo:

- ¿Es el tema complejo y no solucionable únicamente considerando la literatura formal?
- ¿Existe una falta de volumen o calidad de evidencia, o una falta de consenso de medición de resultados en la literatura formal?
- ¿La información contextual es importante para el tema en estudio?
- ¿Es el objetivo validar o corroborar los resultados científicos con experiencias prácticas?
- ¿Es el objetivo desafiar los supuestos o falsear los resultados de la práctica utilizando la investigación académica?
- ¿Sería la síntesis de ideas y evidencias de la industria, útiles para el área académica o para ambas?
- ¿Existe un gran volumen de datos en el área práctica, que indiquen un alto interés de los profesionales en un tema?

La respuesta a todas estas preguntas es afirmativa, ya que la tecnología Blockchain es considerado un tema de investigación emergente, en la cual mucha de la información que existe en esta área no es académica. En la sección de anterior presentamos estudios secundarios que identifican redes de Blockchain en la magnitud de las decenas por área de aplicación. Es un área que podemos asegurar que evolucionó antes en la practica industrial que en el mundo académico. Por todo esto consideramos que es apropiado utilizar una MLR.

Para garantizar el rigor y la replicación del método descrito en este trabajo, se desarrolló un protocolo de investigación basado en las recomendaciones de [1].

### III-B. Objetivo

El objetivo de este MLR es identificar cuáles son las distintas redes de Blockchain y caracterizarlas. Reconociendo propiedades que puedan afectar los atributos de calidad relacionados con la misma, como: seguridad, transparencia, privacidad, escalabilidad, eficiencia. La importancia de cada uno de estos atributos, radica en que le aportan valor a cada proyecto, ya que son estos los que garantizan el buen rendimiento y funcionamiento de la red, así como la integridad de la información que dicha red maneja.

Establecer esta identificación servirá en un futuro de referencia para arquitectos de software y desarrolladores al poder decidir sobre la necesidad de aplicar Blockchain en sus proyectos y sobre cuál red es más aplicable.

### III-C. Preguntas de la investigación

Para facilitar la estructura y desarrollo del trabajo hemos formulado las preguntas específicas que deseamos responder en esta investigación, lo cual nos ha servido de referencia para llevar a a cabo una ruta coherente para el alcance de los objetivos trazados.

RQ1 ¿Cuáles son las redes de Blockchain disponibles?
RQ2 ¿Qué tipo de centralización tienen?
RQ3 ¿Cuál es su dominio de aplicación?
RQ4 ¿Cuál es su algoritmo de consenso?
RQ5 ¿La red permite smart contracts? En caso de ser afirmativo: ¿Cuáles son los lenguajes de programación que utilizan?
RQ6 ¿Cuál es la naturaleza de la red? ¿Nace como una tecnología independiente o a partir de otra red previamente existente?

Las preguntas planteadas ayudarán a tener una visión de cada Blockchain incluida. Presentar una respuesta precisa de cada una de las interrogantes ha permitido generar un contenido acerca de los aspectos técnicos fundamentales para la puesta en marcha del desarrollo de una red Blockachain.

Es de gran ayuda ya que proporcionaremos gran cantidad de información de forma condensada, ahorrándole tiempo a los arquitectos de software que se planteen la posibilidad de utilizar la tecnología Blockchain en alguno de sus proyectos.

### III-D. Estrategia de búsqueda

Para la búsqueda de información, el subconjunto de artículos académicos se tomaron de las siguientes fuentes: Scopus, Google Scholar e IEEExplore. Así como en la realización de snowballing usando Scopus sobre los artículos más referenciados.

Se realizó primero una búsqueda general intentando encontrar artículos en la intersección de las arquitecturas de software y Blockchain, sin éxito. Luego de varias pruebas sobre cadenas de búsqueda, se decidió utilizar una cadena más general, buscando en título y abstract:

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

Vale destacar que la unidad de estudio en esta MLR son las redes de Blockchain, y no los artículos. La cadena de búsqueda anterior resulta en la identificación de mas de 100.000 artículos en distintos buscadores. Se revisaron títulos y abstract de los primeros 500 de cada portal (ordenado por cantidad de

[1] El término *whitepaper* ser refiere a la documentación técnica provista por los creadores de las redes de Blokchain en donde documentan sus decisiones de diseño. Esta es una práctica que se ha vuelto usual en el área de desarrollo de redes de Blockchain

referencias), buscando las redes de Blockchain a las cuales los artículos hacían referencia. Fue muy importante para poder completar la identificación de las redes, recurrir a los siguientes sitios: [3], [13] o [8]. Además de analizar las opciones ofrecidas por los principales proveedores de computación en la nube: Amazon, IBM, Google, Oracle y Microsoft. Fueron utilizados portales externos de información para abordar sobre los detalles de cada una de las redes, como: [4] [21] [22] [8] o [11]. Además de utilizar los whitepapers oficiales de cada una de las redes.

Los criterios de inclusión descritos en el sección siguiente aplican a las redes de Blockchain, no a los artículos.

### *III-E. Criterio de inclusión de una Red Blockchain en el estudio*

Para elegir si una red era incluida o no en alcance del estudio, se tuvieron en cuenta las siguientes consideraciones:

- La red debe tener whitepaper publicado y accesible.
- Tener actividad en el último año, es decir proyectos activos. Lo cual puede verificarse con que aparezca en las noticias y/o tenga artículos de investigación recientes.
- Tener proyectos de aplicación práctica (disponibles en el mercado) y que no sea sólo una red teórica o resultado de una propuesta académica.

Algunas de las redes de Blockchain que fueron descartadas

- Decentraland: Es un producto representar un mundo virtual.
- Bitshares: No esta lanzada al publio todavía.
- UZHBC (University of ZuricH BlockChain): Es una red académica para menejar diplomas [**?**].

### *III-F. Procedimiento de extracción de datos*

Para extraer la información para responder las preguntas de investigación se desarrollo un formulario de extracción de datos con los siguientes atributos:

- Nombre. Identifica el nombre de la red Blockchain.
- Algoritmo(s) de consenso utilizado. Identifica el nombre de el/los algoritmos de consenso que la red puede aplicar.
- Dominio específico de la red (si es que lo tiene). Si la red es específica para un dominio de aplicación o su uso es general.
- Incluye smart contracts.
- Tipo de centralización. Totalmente descentralizada (sin permisos), con permisos para escribir pero no para leer, con permisos detallados en las transacciones.
- Método para escalar. Por ejemplo si usan Sharding o Raiden Network.
- Lenguaje de programación para smart contract. Nombre de el(los) lenguajes de programación que pueden usarse en esta red.
- Link al sitio web y fuente de información técnica (whitepaper).
- Si existe o no literatura formal que hable de la red. Buscando en Scopus la cadena: "Blockchain + Nombre de la Red".
- Si es una implementación especifica de una red ya existente (por ejemplo si son derivadas de Bitcoin o Ethereum) o si surgen independientemente.

La extracción de datos para completar esta tabla se realizó a partir del sitio web oficial de la red, el whitepaper, y eventualmente de publicaciones realizadas por los autores de cada red. El formulario de extracción de datos esta disponible online .

### *III-G. Procedimiento de Síntesis*

En esta revisión, el formulario de extracción provee una forma sintetizada de representar los datos extraídos. Por lo tanto no hicimos un proceso de Síntesis.

## IV. Resultados

La búsqueda fue realizada por el primer autor del artículo en los meses de Enero y Febrero del 2020. Las fuentes consideradas fueron discutidas y revisadas entre todos los autores del artículo.

En las siguientes secciones se presentan las respuestas a las preguntas de investigación.

### *IV-A. [RQ1] ¿Cuáles son las redes de Blockchain disponibles?*

Se identificaron 114 redes de Blockchain distintas que cumplen con los criterios de inclusión. Las podemos ver en las tablas de arriba, separadas por su dominio de aplicación: de uso general (Cuadro I), cryptomonedas (Cuadro II) y de uso específico (Cuadro III).

En las tablas tuvimos la siguiente consideración:

- Si bien hay mas algoritmos de consenso, decidimos agruparlos en grupos: Proof Of Stake$^{POS}$, Proof Of Work$^{POW}$, relacionados a Bizantine Fault Tolerance$^{BFT}$, Federated Consensus$^{FC}$, Delegated Proof Of Stage$^{DPOS}$, Proof Of Authority$^{POA}$, Proof Of Elapsed Time$^{POET}$ y Otros (sin identificar en la lista)

### *IV-B. [RQ2] ¿Qué tipo de centralización tienen?*

En cuanto a este aspecto nuestro hallazgo reflejó que el 75 de las 114 redes estudiadas son totalmente descentralizada, (sin permiso), 22 poseen permisos detallados en las transacciones, mientras que 17 tienen permiso para escribir, pero no para leer.

### *IV-C. [RQ3] ¿Cuál es su dominio?*

En esta tabla (Cuadro IV) mostramos la clasificación de acuerdo a la principal área o dominio de aplicación.

### *IV-D. [RQ4] ¿Cuál es su algoritmo de consenso?*

En esta tabla (Cuadro V) se hace una clasificación de acuerdo al tipo de consenso empleado por las redes, donde se observa que se separan las redes en 7 grandes grupos.

[1]Disponible en: https://tinyurl.com/uo9po2c

[2]En esta tabla hemos considerado bajo el nombre de "Relacionados con BFT" a los siguientes algoritmos de consenso: 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.

Cuadro I
REDES DE BLOCKCHAIN - GENERAL

| Nombre de red | Algoritmo de concenso | Soportan smart contracts? | Derivan de otra red |
|---|---|---|---|
| 0chain | POW | SI | |
| Aelf | DPOS | Si | |
| Aion | Otros | Si | Ethereum |
| ArcBlock | Otros | Si | |
| Ardor | POS | Si | NXT |
| Blockstack | POS | Si | |
| Byteball Bytes | POS | Si | |
| Chain Core | FC | Si | |
| Chain | FC | SI | Ethereum |
| ConsenSys | POS | Si | Ethereum |
| Cypherium | POW | Si | |
| Decent | POW | Si | |
| Dfinity | POS | Si | |
| Dragonchain | POS | Si | |
| Elements | Otros | Si | |
| EOS.IO | POS | Si | |
| Ethereum | POS | Si | |
| Ethereum Classic | POW | Si | Ethereum |
| Everledger | Otros | Si | Bitcoin Cash |
| Factom | Otros | Si | |
| Hedera Hashgraph | Otros | Si | |
| Hydrachain | BFT | Si | Ethereum |
| HyperLedger Fabric | Otros | Si | |
| HyperLedger Iroha | Otros | Si | |
| ICON | Otros | Si | |
| Kadena | BFT | Si | |
| Komobo | Otros | Si | |
| Lisk | dPOS | Si | |
| Mijin | Otros | Si | NEM |
| Monax | POW | No | Ethereum |
| Multichain | BFT | Si | Bitcoin |
| Multiven | POS | Si | Ethereum |
| Neblio | POS | Si | Ethereum |
| NEO | BFT | Si | |
| Netki | POS | Si | |
| NKN | Otros | Si | |
| Ontology | Otros | Si | |
| Qtum | POS | Si | Ethereum |
| Quorum | Otros | Si | Ethereum |
| R3 Corda | Otros | Si | |
| Smilo | BFT | Si | |
| Tezos | POS | Si | |
| Tron | DPOS | Si | |
| Ubiq | dPOS | Si | Ehereum |
| Unita | POS | Si | Qtum |
| Urbit | FC | Si | Ethereum |
| Vechain | Otros | Si | |
| Veriblock | Otros | Si | |
| Waves | POS | Si | Ethereum |
| Zilliqa | BFT | Si | Ethereum |

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

A través de la revisión de las 114 redes Blockchain se determinó que el 84 % de las redes analizadas si aceptan o utilizan smart contracts, mientras que el resto que representa el 16 % no.

Esta tabla (Cuadro VI) muestra la clasificación de acuerdo a los lenguajes de programación empleados para el desarrollo de los smart contracts de la red. Hay que tener en cuenta que varias redes ofrecen varios lenguajes.

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

La siguiente tabla (Cuadro VII) muestra el recuento de la naturaleza de las redes. Es decir, si son una implementación específica de otra red o si son una implementación independiente.

## V. DISCUSIÓN

Al realizar la revisión multi-vocal de redes Blockchain pudimos obtener una visión amplia sobre los atributos que caracterizan cada red. Cruzando los datos, podemos observar lo siguiente:

- El algoritmo de consenso Proof Of Stake es el mayoritariamente utilizado, pero puede estar relacionado a que fue el primero utilizado en las redes de Blockchain, con la aparición de Bitcoin.
- Dentro de la categoría específica mas grande (cryptomonedas) la mayoría son mejoras incrementales o derivadas de Bitcoin (18 de 31). Y que el algoritmo de consenso mayoritario es Proof Of Work (15). La mayoría de estas redes no les interesa servir smart contracts (18 vs 13)

Cuadro II
REDES DE BLOCKCHAIN - CRYPTOMONEDAS

| Nombre de red | Algoritmo de concenso | Soportan smart contracts? | Derivan de otra red |
|---|---|---|---|
| Alphapoint | Otros | Si | Ethereum |
| AnonCoin | POW | No | Bitcoin |
| Augur | POS | Si | Ethereum |
| AuroraCoin | POW | No | Bitcoin |
| Bancor | POW | Si | EOS |
| Bitwala | POS | Si | Bitcoin |
| BlackCoin | POW | No | Bitcoin |
| Bytecoin | POW | No | Bitcoin |
| Cardano | POS | Si | Ethereum |
| CloackCoin | Otros | No | Bitcoin |
| Cryptobullions | Otros | No | Bitcoin |
| CureCoin | POS | No | Bitcoin |
| Dash | POW | No | Bitcoin |
| Decred | Otros | No | Bitcoin |
| Devcoin | POW | No | Bitcoin |
| DigitalCoin | POW | No | Bitcoin |
| Dogecoin | POW | No | Bitcoin |
| Elastos | POS | Si | |
| ForkDelta | POW | Si | Ethereum |
| IDEX | POW | Si | Ethereum |
| Litecoin | POW | No | Bitcoin |
| MaxCoin | POW | No | Bitcoin |
| Monero | POW | No | Bitcoin |
| Nextledger | Otros | Si | |
| Nxt | POS | Si | |
| Ox | POA | Si | Ethereum |
| Ripple | Otros | No | |
| Stellar | Otros | Si | |
| Tether | POS | Si | Ethereum |
| Zcash | POW | No | Bitcoin |
| Zetacoin | POW | No | Bitcoin |

- El resto de las redes que no son para uso de Cryptomonedas (83), derivan aproximadamente 1/3 de Ethereum. Aunque suponemos que muchas pueden haber tomado como base esta última, ya que es de código abierto. En estas la mayoría utilizan Proof Of Stake (29)
- La mayoría de las redes que no tienen literatura formal, son las relacionadas a las Cryptomonedas
- Las redes permisionadas (39) parecen surgir independientemente (26), y la mayoría aceptan smart contracts (37).
- La amplia mayoría de las redes que no son aplicación a cryptomonedas (81 vs 2), aceptan el desarrollo de smart contracts en la red.

En base a estos resultados preliminares consideramos que el atributo que se evalúa con mayor cautela al implementar la tecnología Blockchain es la selección del algoritmo de consenso que se va a utilizar, dado que este atributo pone en juego varios aspectos técnicos de la red, como por ejemplo, si la red es pública o privada, o las necesidades de escalabilidad. Este aspecto está estrechamente ligado al tema de la seguridad de una red que es sin dudas un factor fundamental que debe ser considerado al implementar cualquier tecnología [29].

En cuanto a las decisiones de arquitectura de software una de las preocupaciones más recurrentes en los arquitectos es la escalabilidad, entendida en este contexto como la capacidad de una aplicación para mantener el crecimiento de la red sin perder sus características básicas que la hacen funcionar [20]. Si se elije un algoritmo de consenso que tenga mayor seguridad y dificultad de resolución del bloque, se pierde la escalabilidad ya que va a requerir mayor poder de computo, por lo tanto menor eficiencia energética.

Además se estudia la flexibilidad de una red en distintos aspectos, en ocasiones puede utilizarse este término al indicar el tipo de Blockchain (pública o privada), por ser una tecnología versátil que ofrece una variedad de opciones que se adecúan a los requerimientos que se tienen para llevar a cabo el desarrollo de una red, es decir debe hacerse una selección tomando en cuenta el fin último que se desea alcanzar con la red Blockchain que se desarrollará, [26].

Creemos que Solidity es el lenguaje de programación mas adecuado para desarrollar smart contracts. Por su definición, es un lenguaje de alto nivel orientado a objetos para crear smart contracts. Solidity es staticamente tipado, ademas de chequear y verificar en tiempo de compilación restricciones de los smart contracts, evitando errores antes del runtime. En resumen, su simplicidad, el ser especifico para desarrollar smart contracts, y ser el lenguaje detrás de uno de los precursores de las Blockchain 2.0 (Ethereum). Creemos que lo hace ser el favorito.

Nos parece interesante explorar si de verdad hay diferencias significativas entre las redes que son derivadas de Bitcoin o de Ethereum. En especial las que tienen el mismo algoritmo de concenso, ya que puede ser que sean distintas implementaciones para satisfacer los mismos atributos de calidad.

## VI. CONCLUSIONES

Este trabajo presentó una revisión multi-vocal de la literatura orientada a identificar las redes de Blockchain activas y

Cuadro III
REDES DE BLOCKCHAIN - DOMINIO ESPECÍFICO

| Nombre de red | Algoritmo de concenso | Soportan smart contracts? | Derivan de otra red | 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 | | Distributed Ledgers |
| NEM | Otros | Si | | Distributed Ledgers |
| Openchain | Otros | Si | | Distributed Ledgers |
| Tierion | Otros | Si | Bitcoin | Document Verification |
| EnergyWeb | Otros | Si | | Energy |
| Filecoin | Otros | Si | Ethereum | File managment |
| Bankchain | Otros | Si | | Finance |
| KYC-CHAIN | POS | Si | | Finance |
| OmiseGO | POS | Si | Ethereum | Finance |
| Straitis | POS | Si | Ethereum | Finance |
| Symbiont Assembly | BFT | Si | | Finance |
| Wanchain | POS | Si | Ethereum | Finance |
| Hydro | POS | Si | Ethereum | Identity |
| Shocard | Otros | Si | Bitcoin | Identity |
| Wibson | POS | Si | | Identity |
| OpenIDL | Otros | Si | | Insurance |
| IOTA | Otros | Si | | IoT |
| Platin | Otros | Si | | Location |
| Bitwala | POS | Si | Bitcoin | Loyalty programs |
| Mediachain | FC | SI | | Music |
| Apirone | POW | No | Bitcoin | Payments |
| Earthport | Otros | Si | | Payments |
| KodakCoin | POA | Si | | Photographs |
| Enigma | POS | Si | | Security |
| Steem | POS | Si | Tron | Social media |
| Aventus | POS | Si | Bitcoin | Ticket managment |
| Filament | FC | Si | Bitcoin | Vehicle data |
| DMarket | POS | Si | Bitcoin | Videogames |
| Horizon | Otros | Si | | Videogames |

Cuadro IV
CLASIFICACIÓN DE LAS REDES POR DOMINIO

| Dominio | Nro. de redes |
|---|---|
| Generales | 50 |
| Criptomonedas | 31 |
| Financiero | 6 |
| Ledgers distribuidos | 4 |
| Identidad | 3 |
| Pagos | 2 |
| Videojuegos | 2 |
| Otros | 16 |

Cuadro V
CLASIFICACIÓN DE LAS REDES POR ALGORITMO DE CONSENSO UTILIZADO

| Tipos de consenso | Nro. de redes |
|---|---|
| Proof Of Stake | 36 |
| Proof Of Work | 21 |
| Relacionados con BFT[2] | 7 |
| Federated Consensus | 5 |
| Delegated Proof Of Stake | 4 |
| Proof Of Authority | 3 |
| Otros (30 distintos) | 38 |

Cuadro VI
LENGUAJES DE PROGRAMACIÓN DE LOS SMART CONTRACTS

| Lenguaje de Programación | Nro. de redes |
|---|---|
| C/C++ | 36 |
| Solidity | 31 |
| Java | 22 |
| JavaScript | 15 |
| Go | 12 |
| Python | 9 |
| NodeJs | 2 |

Cuadro VII
NATURALEZA DE LA RED

| Naturaleza | |
|---|---|
| Independiente | 54 |
| Derivada de Ethereum | 27 |
| Derivada de Bitcoin | 27 |
| Otras | 6 |

extraer información sobre aspectos técnicos de las mismas.

A través de esta revisión se logró identificar más de 114 redes de Blockchain que tienen proyectos activos. Además, este artículo propone la agrupación de estas redes en en familias. Consideramos que estas características pueden estar relacionadas a decisiones que deben tomar los arquitectos de software para diseñar redes de Blockchain, o interconectar sus sistemas a las redes existentes.

Nuestros resultados destacan al algoritmo de concenso como un punto central de la arquitectura de la red de Blockchain. El mismo impacta en algunos atributos de calidad que son de interés para los arquitectos de software (por ejemplo escalabilidad y performance). Como trabajo futuro nos proponemos profundizar el impacto de estos algoritmos en los atributos de calidad.

Blockchain ofrece un sistema Turing-completo, con características diferentes a las que estamos acostumbrados: número de nodos, algoritmos de consenso, tamaño y datos del bloque, contratos inteligentes. Es responsabilidad del arquitecto del software decidir qué red utilizar.

## Referencias


[1] Adams, R.J., Smart, P., Huff, A.S.: Shades of grey: Guidelines for working with the grey literature in systematic reviews for management and organizational studies. International Journal of Management Reviews **19**(4), 432–454 (2017). https://doi.org/10.1111/ijmr.12102, https://onlinelibrary.wiley.com/doi/abs/10.1111/ijmr.12102

[2] Baliga, A.: Understanding blockchain consensus models (2017), https://www.persistent.com/wp-content/uploads/2018/02/wp-understanding-blockchain-consensus-models.pdf

[3] BitcoinWiki project: Blockchain projects list (2019), https://en.bitcoinwiki.org/wiki/Blockchain_Projects_List

[4] Blockchain Luxemburg SA: Conectamos las criptomonedas con el mundo (2019), https://www.blockchain.com/

[5] Buternin, V.: On public and private blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (2015)

[6] Butijn, B.J., Tamburri, D.A., Heuvel, W.J.V.D.: Blockchains: a systematic multivocal literature review (2019)

[7] C. Shen 1, F.P.M.: Blockchain for cities—a systematic literature review. Columbia University (2018), http://www.cs.columbia.edu/~charles/paper/BlockchainForCities.pdf

[8] Coin Market Cap: List of blockchain companies (2019), https://coinmarketcap.com/

[9] Crosby, M., Nachiappan, P.P., Sanjeev Verma, V.K.: Blockchain technology: Beyond bitcoin. In: Applied Innovation Review. Issue No. 2. Pantas and Ting Sutardja Center for Entrepeneurship and Technology. Berkeley Engineering. UC Berkeley (2016)

[10] Ferdous, M.S., Chowdhury, M.J.M., Hoque, M.A., Colman, A.: Blockchain consensus algorithms: A survey (2020)

[11] Forbes: Blockchain 50 - forbes (2020), https://www.forbes.com/sites/michaeldelcastillo/2020/02/19/blockchain-50/#51a06ceb7553

[12] Garousi, V., Felderer, M., Mäntylä, M.V.: Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and Software Technology **106**, 101 – 121 (2019). https://doi.org/https://doi.org/10.1016/j.infsof.2018.09.006, http://www.sciencedirect.com/science/article/pii/S0950584918301939

[13] Golden Recursion Inc.: List of blockchain companies (2019), https://golden.com/list-of-blockchain-companies

[14] Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., Decker, S.: Blockchain for business applications: A systematic literature review. In: Abramowicz, W., Paschke, A. (eds.) Business Information Systems. pp. 384–399. Springer International Publishing, Cham (2018)

[15] L. Lamport, R.S., Pease, M.: The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS) (1982)

[16] M. Conoscenti, A. Vetro, J.D.M.: Blockchain for the internet of things: a systematic literature review (2016), https://nexa.polito.it/nexacenterfiles/BlockchainfortheInternetofThings:aSystematicLiteratureReview.pdf

[17] M Hölbl, M. Kompara, A.K.L.N.: A systematic review of the use of blockchainin healthcare (2018), https://www.researchgate.net/publication/328208535_A_Systematic_Review_of_the_Use_of_Blockchain_in_Healthcare

[18] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C.: A review on consensus algorithm of blockchain. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). pp. 2567–2572 (Oct 2017). https://doi.org/10.1109/SMC.2017.8123011

[19] Schedlbauer, M., Wagner, K.: Blockchain beyond digital currencies - a structured literature review on blockchain applications. SSRN (2018). https://doi.org/http://dx.doi.org/10.2139/ssrn.3298435

[20] Scherer, M.: Performance and Scalability of Blockchain Networks and Smart Contracts. Master's thesis, Umeå University, Department of Computing Science (2017)

[21] Science Direct: Explore scientific, technical, and medical research on sciencedirect (2019), https://www.sciencedirect.com/

[22] Standford University: Standford center for blockchain (2019), https://cbr.stanford.edu/

[23] Szabo, N.: Smart contracts: Building blocks for digital markets (1994), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[24] Tanenbaum, A., Van Steen, M.: Distributed Systems. Principles and Paradigms. Pearson Prentice Hall, USA, 2nd edn. (2006)

[25] Tapscott, D.: How blockchains could change the world (2016), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-blockchains-could-change-the-world#

[26] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of blockchain-based systems for architecture design. In: 2017 IEEE International Conference on Software Architecture (ICSA). pp. 243–252 (April 2017). https://doi.org/10.1109/ICSA.2017.33

[27] Y. Tribis, A. El Bouchti, H.B.: Supply chain management based on blockchain: A systematic mapping study. Research Gate (2018), https://www.researchgate.net/publication/327650323_Supply_Chain_Management_based_on_Blockchain_A_Systematic_Mapping_Study

[28] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where is current research on blockchain technology?—a systematic review. PLOS ONE **11**(10), 1–27 (10 2016). https://doi.org/10.1371/journal.pone.0163477, https://doi.org/10.1371/journal.pone.0163477

[29] Zhang, R., Xue, R., Liu, L.: Security and privacy on blockchain. CoRR **abs/1903.07602** (2019), http://arxiv.org/abs/1903.07602