https://doi.org/10.37815/rte.v33n2.828
Artículos originales

Análisis comparativo de Métodos de Consenso sobre plataformas Blockchain

Comparative analysis of Consensus Methods on Blockchain platforms

Ximena Campaña Iza[1] https://orcid.org/0000-0001-5929-2085, Xavier Zumba Sampedro[1] https://orcid.org/0000-0002-8292-5490, Mario Raúl Morales[3] http://orcid.org/0000-0002-7493-8072, Santiago Morales Cardoso[1] http://orcid.org/0000-0002-3833-9654

[1]*Facultad de Ingeniería y Ciencias Aplicadas, Universidad Central del Ecuador*, Quito, Ecuador
xmcampana@uce.edu.ec, wxzumba@uce.edu.ec, smorales@uce.edu.ec

[3]*Universidad de Alicante*, Alicante, España
mrmm17@alu.ua.es

Esta obra está bajo una licencia internacional Creative Commons Atribución-NoComercial 4.0.

Enviado: 2021/06/29
Aceptado: 2021/09/28
Publicado: 2021/11/30

Resumen

En la presente investigación se plantea realizar un análisis comparativo entre los diferentes métodos de consenso existentes, los cuales son los encargados de registrar, validar y realizar transacciones dentro de la tecnología Blockchain. Se identifica la presencia de propiedades consideradas como esenciales para su aplicabilidad y eficacia. Se considera características relevantes que permitan determinar cuál o cuáles de los diferentes métodos de consenso ayudan a mejorar problemas de escalabilidad o seguridad que tiene, hasta el momento, esta tecnología en cada plataforma. Se determina el valor de cada una de las características y posteriormente se asigna ponderaciones. Cada una de las características consideradas para la comparación no poseen la misma relevancia, por lo cual, se realiza una nueva ponderación que permite obtener resultados de acuerdo al valor e importancia de éstas en cada uno de los protocolos. Finalmente, se determina que los protocolos con mejores características son Tolerancia Delegada de Fallas Bizantinas, Prueba de Participación Delegada y Prueba de Trabajo; siendo Tolerancia Delegada de Fallas Bizantinas el mejor método por realizar 10.000 transacciones por segundo con baja latencia y un bajo consumo de recursos, entre las características más relevantes.

Palabras clave: criptomoneda, cadena de bloques, tecnología primaria, métodos de consenso, minería.

Sumario: Introducción, Materiales y Métodos, Resultados y Discusión y Conclusiones.

Como citar: Campaña, X., Zumba, X., Morales, M., & Morales, S. (2021). Análisis comparativo de Métodos de Consenso sobre plataformas Blockchain. *Revista Tecnológica - Espol, 33(2), 25-42.* http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/828

Abstract

A comparative analysis between different existing methods for registering, validating, and carrying out transactions within Blockchain technology was performed in this research. Properties considered essential because of their applicability and efficacy were identified. Relevant characteristics to determine which of the different consensus methods help improve scalability or security problems that this technology has, so far, in each platform, were considered. These characteristics do not have the same importance. Therefore, a new score that allows obtaining results according to the value and relevance of its protocols was introduced. The protocols with the best characteristics were: Delegated Tolerance of Byzantine Faults, Delegated Proof of Participation, and Proof of Work; being Delegated Tolerance of Byzantine Faults, the best method to, among the most relevant characteristics, carry out 10000 transactions per second with low latency and low resource consumption.

Keywords: criptocurrency, blockhchain, primary technology, consensus methods, mining.

Introducción

Blockchain (BC) o cadena de bloques es considerada una tecnología primaria (Conti, Kumar, Lal, & Ruj, 2018) y, definida como la aplicación principal de las criptomonedas que permite la inmutabilidad e integridad de los datos (Mora et al., 2021). Se conoce como un libro de contabilidad distribuido para registrar transacciones, mantenido por varios nodos sin autoridad central mediante un método criptográfico distribuido (Cachin & Vukolić, 2017).

BC tiene numerosos beneficios como descentralización, persistencia, anonimato y auditabilidad. Varios estudios se centran en el uso de la tecnología Blockchain en diversos aspectos de aplicación que va desde las criptomonedas, servicios financieros, gestión de riesgos, internet de las cosas (IoT) hasta servicios públicos y sociales. BC fundamenta la validez de las transacciones mediante mecanismos conocidos como Métodos de Consenso. La presente investigación tiene como objetivo comparar los Métodos de Consenso sobre Plataformas Blockchain a través de la identificación de sus principales características para garantizar el aprovechamiento óptimo de los mismos. Adicionalmente, la novedad que presenta este trabajo radica en la evaluación de Métodos de Consenso de acuerdo con la eficiencia que presentan y su aplicabilidad en distintos campos.

En los siguientes párrafos se revisan varios conceptos utilizados a lo largo del presente trabajo.

Criptomoneda

Conocidas como una clase de activos en crecimiento (Grobys et al., 2019) o monedas digitales que dependen de algoritmos criptográficos para proporcionar a los usuarios un medio de intercambio seguro, creación de dinero y transacciones. Definidas legalmente como "monedas digitales convertibles" o como un "equivalente digital de efectivo" (Papadopoulos, 2015).

Bitcoin es la criptomoneda más conocida que registra sus transacciones monetarias en tecnología BC (Swan, 2018); se trata de un sistema de pago electrónico criptográficamente seguro, basado en el esquema de clave pública (Conti et al., 2018). Es la primera aplicación desarrollada con tal tecnología y se piensa que fue creada en 2008 por Satoshi Nakamoto (Islam et al., 2019). La escalabilidad es una de sus desventajas, lo que ocasiona que se torne lenta (Mora et al., 2019); no obstante, usa un mecanismo conocido como *Lightning Network* que proporciona pagos ágiles fuera de la cadena (Zhang & Lee, 2019).

Actualmente es la criptodivisa más exitosa y ha impulsado la creación de nuevas monedas digitales que mantienen el concepto de descentralización (Conti, Kumar, Lal, & Ruj, 2018) tal como Ethereum, Ripple, Litecoin, Dash, NEM, Stellar y NEO (Ruozhou et al., 2019).

Cadena de bloques

BC permite la inmutabilidad e integridad de los datos en los que se mantiene un registro de las transacciones (Viriyasitavat & Hoonsopon, 2018). Es una base de datos distribuida o libro de contabilidad distribuido controlado por múltiples entidades (Cachin & Vukolić, 2017) y es resistente a la manipulación (Salimitari & Chatterjee, 2019), lo cual brinda resistencia a la censura, es decir, ninguna autoridad central puede impedir que una de las partes realice negocios en la red (Swan, 2018) y, todas las personas pueden compartir y acceder (Salimitari & Chatterjee, 2019). Las transacciones son registradas cronológicamente en el libro mayor (Swan, 2018); mientras más larga sea la cadena, más complicado será falsificarla (Tahar et al., 2018).

Se resume a BC como un sistema que ofrece servicios confiables a un conjunto de nodos o mineros que no confían plenamente entre sí o, como un protocolo distribuido seguro (Cachin & Vukolić, 2017) basado en un método de consenso para ponerse de acuerdo sobre los nuevos datos (Salimitari & Chatterjee, 2019) como la transferencia segura de instancias únicas de valor mediante internet para mantener la integridad y autenticidad de documentos (Swan, 2018).

Una característica principal de BC es la intervención de mineros o nodos que validan y agrupan transacciones en bloques y posteriormente los agregan a la cadena (Islam et al., 2019). En la actualidad BC tiene mayor apertura (Morales et al., 2020) y conduce a una gran cantidad de nuevos métodos de consenso (Viriyasitavat & Hoonsopon, 2018). Existen tres tipos de BC: i) públicos, que son descentralizados, ii) privados, el acceso depende de un tercero, iii) consorcio, son cadenas híbridas entre las dos anteriores (Salimitari & Chatterjee, 2019).

Mineros

Son personas o grandes empresas que poseen poder de cómputo limitado (Islam et al., 2019), no necesitan de una autenticación previa para unirse a la red (Conti et al., 2018) y son los encargados de efectuar métodos de consenso en un sistema BC (Viriyasitavat & Hoonsopon, 2018). Cada uno de los mineros almacena una copia local de BC y reciben recompensas para garantizar que la cadena se mantenga con honestidad (Conti et al., 2018). El proceso de registrar un nuevo bloque a la cadena se denomina minería (Fairley, 2017). Un bloque obtiene más credibilidad cuando se construyen sobre él más bloques (Salimitari & Chatterjee, 2019).

Los nodos o mineros pueden comportarse de manera maliciosa originando el Problema del General Bizantino (Swan, 2018) y pueden afectar la comunicación en la red (Cachin & Vukolić, 2017). Estos nodos maliciosos reciben el nombre de fallas bizantinas (Gramoli, 2017). Para evitar este comportamiento y garantizar un servicio continuo, los mineros ejecutan un protocolo o método de consenso tolerante a fallas (Cachin & Vukolić, 2017).

Método de consenso

BC se actualiza cuando hay un acuerdo utilizando un método de consenso (Swan, 2018). Los métodos o protocolos de consenso son la columna vertebral o núcleo de cualquier aplicación BC (Viriyasitavat & Hoonsopon, 2018). Un sistema basado en BC es tan seguro y robusto como su método de consenso y, la elección de un método está basada en los requisitos que un sistema necesita para ser implementado (Salimitari & Chatterjee, 2019).

Los protocolos de consenso aseguran que el libro mayor sea compartido e inalterable durante toda su vida (Nawari & Ravindran, 2019), evita eliminar registros o agregar información que no haya sido validada, garantizando de esta forma su integridad; verifica la continuidad del servicio siendo tolerante a fallas para asegurar que los mineros estén de acuerdo con el orden que se agregan las entradas en la BC (Conti et al., 2018), siendo el orden único los mineros incorporan bloques a la cadena actualizando de esta manera el libro mayor distribuido (Cachin & Vukolić, 2017).

El consenso se determina como un acuerdo general entre todos los nodos del estado actual del libro mayor (Swan, 2018) y la efectividad de un protocolo de consenso depende también del rendimiento y estabilidad de la red, comúnmente necesitan de altos cálculos computacionales y capacidades de comunicación (Salimitari & Chatterjee, 2019).

Según (Viriyasitavat & Hoonsopon, 2018) existen propiedades claves para definir la aplicabilidad y eficacia de los protocolos de consenso:

- Seguridad: garantiza que no suceda algo anormal. Un algoritmo de consenso es seguro si por lo menos un minero honesto produce una salida válida, luego los demás mineros reciben la misma salida.
- Validez: un algoritmo de consenso confirma la validez si todos los mineros honestos que intervienen en un acuerdo generan un valor y todas las peticiones válidas se procesarán eventualmente.
- Tolerancia a fallas: un método de consenso ofrece tolerancia a fallas si es resistente a errores que producen algunos nodos que intervienen en un consenso en un momento dado.

En los siguientes párrafos se describen los principales métodos de consenso analizados.

Prueba de trabajo

Proof of Work (PoW) está basado en un complejo y criptográfico rompecabezas matemático (Conti et al., 2018), difícil de calcular pero fácil de verificar por un patrón de poder (Nawari & Ravindran, 2019); es descentralizado por lo cual los participantes no necesitan autenticación para unirse a la red (Conti et al., 2018). Asegura la continuidad de la red y tolerancia a fallas (Viriyasitavat & Hoonsopon, 2018), brindando así transparencia, robustez, incorruptibilidad de la red (Nawari & Ravindran, 2019) y un alto nivel de seguridad (Young, 2019) a los usuarios contra ataques Sybil que podrían dañar el funcionamiento del método de consenso y conducir a un posible ataque de doble gasto (Conti et al., 2018).

La mayor desventaja de PoW es el consumo de energía al realizar los cálculos hash para la verificación en el proceso de minería, la que a su vez depende de la potencia de los recursos informáticos de un minero. Es susceptible a sufrir ataques del 51%, una situación en la que un adversario aparta a los mineros honestos del proceso minero, lo cual debilita el protocolo de consenso (Conti et al., 2018). Es el algoritmo más conocido utilizado por Bitcoin que posee 1 MB de tamaño de bloque, tiempo promedio para resolver cada bloque de 10 minutos (Salimitari & Chatterjee, 2019), es computacionalmente costoso y permite realizar 7 transacciones por segundo (TPS) (Frumkin, 2019). También es usado por las monedas virtuales Ethereum y Litecoin (Fairley, 2017). Existen métodos de consenso basados en PoW que son mencionados a continuación (Salimitari & Chatterjee, 2019):

- ***Prueba de capacidad***

Proof of Capacity (PoC) es similar a PoW, fue presentado como un protocolo básico de la criptomoneda Burst. En lugar de depender de la potencia informática de los mineros, se basa en su capacidad de disco duro, lo cual lo convierte en un método de consenso más eficiente energéticamente. La función hash que utiliza este método de consenso es Shabal, donde, los hash son complejos y lentos de calcular y, además están precompuestos y almacenados en la unidad de disco duro (Porta, 2019).

- ***Prueba de tiempo transcurrido***

Proof of Elapsed Time (PoET), es propuesto por Intel y funciona de forma parecida a PoW pero con un consumo de energía menor. Los mineros deben resolver un hash, pero a diferencia de una competencia entre mineros por resolver el siguiente bloque, el minero ganador o líder es elegido de manera aleatoria en función de un tiempo de espera obligatorio y cuyo temporizador expira primero (Cachin & Vukolić, 2017). Posee una baja latencia y un alto rendimiento. Su desventaja es la dependencia de Intel (Salimitari & Chatterjee, 2019).

Prueba de participación

*Proof of Stake (*PoS), es el segundo método de consenso más frecuente en BC. A diferencia de PoW no genera una competencia entre nodos, la lotería selecciona un nodo para que sea el encargado de resolver el siguiente bloque (Salimitari & Chatterjee, 2019). Este nodo es conocido como falsificador y es elegido de manera determinista, conforme a su participación en la red (Debus, 2017) o conforme a su riqueza en términos de esa criptomoneda (Swan, 2018). El nodo seleccionado usa una firma digital para demostrar su propiedad sobre la participación en lugar de resolver un problema de hash complejo, de esta forma no necesita altos recursos computacionales (Debus, 2017) y lo convierte en un método de consenso seguro (Young, 2019).

Es un protocolo de consenso de ahorro de energía al aprovechar un incentivo monetario; sin embargo, al requerir mayor cantidad de participación de nodos, ocasiona que la cadena de bloques esté centralizada (Salimitari & Chatterjee, 2019) y no necesariamente lo convierte en más eficiente que PoW (Swan, 2018). Además, se origina un problema conocido como "nada en juego" que consiste en que un nodo seleccionado no tiene nada que perder si se comporta de manera maliciosa, de forma que podría crear dos conjuntos de bloques nuevos para obtener más recompensas por las tarifas de transacción (Salimitari & Chatterjee, 2019).

En este protocolo de consenso no existe minería (Fairley, 2017) y, por lo tanto, no hay recompensa minera. Los mineros son recompensados únicamente con una tarifa de transacción (Salimitari & Chatterjee, 2019). Criptomonedas como Peercoin, Shadowcash, Nxt, Blackcoin, Cardano, entre otros, usan PoS como método de consenso (Fairley, 2017). Peercoin puede realizar 8 TPS con una latencia de 8,5 minutos; al igual que Bitcoin, posee un tamaño de bloque de 1 MB (peercoinDocs, s.f.). Cardano puede realizar hasta 250 TPS con un retardo de 10 minutos (Frumkin, 2019). Este método también presenta variaciones que se analizan seguidamente:

- ***Prueba de participación delegada***

Delegated Proof of Stake o DPoS, es un método de consenso democrático representativo, es decir, todas las partes interesadas votan para elegir algunos nodos como testigos y delegados. Los nodos testigos son los responsables de crear nuevos bloques y son recompensados, mientras que los nodos delegados son los encargados de mantener la red y sugerir cambios tales como el tamaño de los bloques, tarifas de transacciones o monto de

recompensa (Salimitari & Chatterjee, 2019); si los testigos no pueden generar bloques en sus turnos, serán despedidos y reemplazados (Zhang & Lee, 2019).

DPoS mejora el rendimiento y latencia en comparación a PoS, convirtiéndolo en un protocolo de consenso de bajo costo (Zhang & Lee, 2019) y con un nivel de seguridad bajo (Young, 2019). Cuenta con mecanismos incorporados para detectar y descartar a un delegado o testigo malicioso (Larimer, 2014). Bitshares y EOS son criptomonedas que utilizan este método de consenso (Zhang & Lee, 2019). EOS puede realizar 5.000 TPS y posee una latencia de 1.5 segundos (Frumkin, 2019).

- ***Prueba de participación alquilada***

Leased Proof of Stake o LPoS, pretende solucionar el problema de centralidad de PoS. Permite que los nodos con bajos saldos participen en la verificación de bloques al agregar una opción de arrendamiento permitiendo a los poseedores de riqueza con saldos más altos alquilar sus fondos a nodos con saldos bajos por un período de tiempo específico (Salimitari & Chatterjee, 2019); mientras mayor sea la cantidad arrendada a un nodo, las posibilidades de que ese nodo sea elegido para crear el siguiente bloque son mayores (CoinsTelegram, 2018). Una vez que los nodos resuelven un bloque, dividirán proporcionalmente la recompensa con los poseedores de riqueza (WavesDocs, s.f.).

- ***Prueba de importancia***

Proof of Importance (PoI) se encuentra en criptomonedas como NEM (Option Finance, s.f.). Además de considerar los saldos de los nodos para resolver el siguiente bloque, toma en cuenta más factores como la reputación de un nodo que es determinado por una función definida por el sistema particular y el número de transacciones ocurridas hacia o desde ese nodo (Salimitari & Chatterjee, 2019). De esta forma todos los nodos tienen la oportunidad de ser recompensados en función de su lealtad y esfuerzo (Option Finance, s.f.). En consecuencia, este protocolo de consenso considera la actividad productiva de la red de los nodos, que es más eficiente que solo el equilibrio de los nodos (Nem, s.f.).

- ***Prueba de actividad***

Proof of Activity (PoA), es un método de consenso híbrido basado en PoW y PoS, además es robusto contra ataques DDoS (Salimitari & Chatterjee, 2019). Los mineros intentan solucionar una función hash en una carrera para encontrar el siguiente bloque como se realiza en PoW; sin embargo, el bloque resuelto únicamente contendrá un encabezado y la dirección del minero sin ninguna transacción. Posteriormente, usando PoS, se agregan las transacciones al bloque y conforme con el encabezado del bloque resuelto, se selecciona un grupo de nodos validadores o mineros para firmar el nuevo bloque con el fin de llegar a un acuerdo (Zheng et al., 2018).

PoA aumenta la defensa contra los ataques del 51% debido a que el atacante requerirá tener el 51% o más del poder minero total de la red y el 51% o más de las monedas insertadas en la red para concluir con éxito el ataque (Seth, 2018).

- ***Prueba de quemadura***

Proof of Burn (PoB) es un método basado en la quema de monedas o envío de monedas a una dirección irrecuperable (Salimitari & Chatterjee, 2019). Al quemar monedas los usuarios pueden mostrar su interés en la red obteniendo, de esta forma, el poder de minar y verificar las transacciones (Prasanna, 2019); los mineros tienen prioridad para resolver el siguiente bloque acorde con la cantidad de monedas que han quemado (Debus, 2017). Slimcoin es una criptomoneda que usa este método (Salimitari & Chatterjee, 2019).

Métodos de acuerdo bizantino

A continuación, se presentan algunos métodos basados en el problema de los generales bizantinos:

- ***Tolerancia práctica de fallas bizantinas***

Practical Byzantine Fault Tolerance (PBFT) es un método en el que todos los nodos o mineros son confiables y conocidos (Fairley, 2017) y deben intervenir en el proceso de votación para agregar el siguiente bloque; el consenso se logra cuando más de dos tercios de los nodos están de acuerdo con ese bloque (Salimitari & Chatterjee, 2019). Para cada bloque de transacciones, el algoritmo selecciona al azar un conjunto pequeño de usuarios únicos de manera segura y justa; además oculta la identidad de estos usuarios hasta confirmar el bloqueo para protegerlos de los atacantes (Swan, 2018).

PBFT es capaz de tolerar el comportamiento malicioso de hasta un tercio de todos los nodos para permitir la continuidad de las operaciones del sistema (Fairley, 2017). En comparación con PoW, este método alcanza el acuerdo de manera más rápida y económica, no necesita tener activos similares a PoS para participar en el proceso de consenso (Salimitari & Chatterjee, 2019).

Este método es apropiado para ser usado en BC privadas como Hyperledger. Debido a su escalabilidad limitada y su tolerancia relativamente baja frente a actividades maliciosas no lo hacen adecuado para BC públicas (Debus, 2017). PBFT posee un alto rendimiento, baja latencia, bajo uso de recursos computacionales y brinda seguridad (Salimitari & Chatterjee, 2019); sin embargo, puede ser vulnerable frente ataques Sybil cuando la red no posee muchos nodos (Blagojevic, 2019). Zilliqa es una criptomoneda que utiliza este protocolo y realiza 2.828 TPS (Frumkin, 2019).

- ***Tolerancia delegada de fallas bizantinas***

Delegated Byzantine Fault Tolerance (dBFT) se diferencia de PBFT al no necesitar la participación de todos los nodos para agregar un nuevo bloque. En este método, algunos nodos son seleccionados como delegados de otros nodos (Salimitari & Chatterjee, 2019), cualquier nodo puede ser delegado siempre y cuando posea equipos de computación adecuados, una identidad validada y 1.000 GAS que es la recompensa que reciben por su participación en la red (Comben, 2019).

Conforme a determinadas reglas es similar al protocolo PBFT, por ejemplo, ambas admiten únicamente un tercio de nodos maliciosos. Además, dBFT puede eliminar nodos maliciosos o poco confiables de la cadena (Salimitari & Chatterjee, 2019). Una de sus características es la finalidad absoluta, es decir, al final de la última confirmación un bloque no puede ser bifurcado y, por lo tanto, una transacción no puede ser revertida. Para que un bloque sea agregado a la cadena, más de un tercio de delegados alcanzan un acuerdo y validan (Comben, 2019).

PBFT presenta una latencia promedio entre 15 y 20 segundos para la creación de bloques (Comben, 2019). NEO es una criptomoneda que utiliza este algoritmo (Zheng et al., 2018) y actualmente realiza 10.000 TPS con una latencia de 15 segundos (Frumkin, 2019).

- ***Protocolo de consenso estelar***

Stellar Consensus Protocol (SCP) Se basa en una variación de PBFT conocida como tolerancia de falla bizantina federada (FBFT) y brinda servicios de microfinanzas en plataformas BC. Sus nodos llamados federados, ejecutan un protocolo de consenso local entre sus integrantes. Es descentralizado, abierto al público y tiene una latencia muy baja, unos

segundos como máximo, haciéndola similar a las transacciones web (Salimitari & Chatterjee, 2019); es el primer protocolo basado en Acuerdos Bizantinos Federados (FBA) que proporciona a los usuarios la libertad para seleccionar entre diferentes combinaciones de otros nodos en los que puede confiar para llegar a un acuerdo (Koller, 2017).

Posee un alto rendimiento, baja latencia, uso de recursos computacionales relativamente bajo (Dinh et al., 2018) y brinda seguridad aun cuando los nodos fallan o nodos maliciosos se unen a la red (Blockchain Support, 2019).

Materiales y Métodos

Esta investigación usó un método exploratorio de carácter secundario (QuestionPro, 2020). En función de los métodos de consenso existentes, se identificaron sus principales características para posteriormente realizar una comparación y determinar aquel protocolo que posee las mejores propiedades. El proceso de estudio se conformó de los siguientes pasos:

- Selección de métodos de consenso: Permitió reducir el número de protocolos de consenso analizados previamente mediante la identificación de información que sustenten las propiedades Seguridad, Validez y Tolerancia a fallas.
- Definición de criterios de análisis: Además del cumplimiento de las tres propiedades principales, se determinaron otros aspectos a evaluar para su comparación.
- Comparación de los protocolos: Se determinó cada uno de los valores para los parámetros correspondientes a los Método de Consenso.

En este último paso, adicionalmente se realizaron otras tareas:

- Estandarización de datos a valores cualitativos: Algunas características lograron mostrar valores numéricos en diferentes escalas; de tal manera, mediante criterios se transformaron los datos numéricos a valores cualitativos.
- Ponderación de características: Mediante la escala Likert se cambiaron los valores cualitativos a valores numéricos en la escala de 1 a 3, lo que permitió sumar sus valores y determinar aquel método que posee mejores características.
- Ponderación por convenio: Se consideró si todas las características tienen la misma relevancia, para lo cual, se hizo uso de ponderación por convenio, cuyo objetivo fue asignar pesos a los parámetros de acuerdo a un criterio.

Selección de Métodos de Consenso

Las principales propiedades que debe cumplir un protocolo de consenso para su aplicabilidad y eficiencia son seguridad, validez y tolerancia a fallas (Viriyasitavat & Hoonsopon, 2018), por lo cual, se descartaron los métodos en los que no se pudo validar tales propiedades.

Al analizar los protocolos para definir la presencia o ausencia de las características antes mencionadas, se determinó que los métodos que cumplieron con las tres condiciones principales fueron: Prueba de trabajo, Prueba de participación, Prueba de participación delegada, Tolerancia práctica de fallas bizantinas y Tolerancia delegada de fallas bizantinas. Para los parámetros Seguridad y Tolerancia a Fallas, se consideró la presencia de estas características aun cuando sus niveles sean bajos.

Selección de Criterios de Análisis

Existen otras características consideradas relevantes al momento de utilizar un algoritmo de consenso. En la Tabla 1 se describen las principales cualidades mencionadas en varios artículos científicos:

Tabla 1

Características de los Métodos de Consenso

CARACTERÍSTICAS	CONCEPTO
Rendimiento	Número de transacciones que se pueden procesar por unidad de tiempo.
Escalabilidad	Tamaño de una red blockchain, es decir, el número de usuarios que puede aceptar.
Disponibilidad	Muestra la accesibilidad de los mineros a la red.
Latencia	Indica la cantidad de tiempo que tardan los mineros en llegar a un acuerdo, es decir, el tiempo de transacción.
Consumo energético	La cantidad de recursos computacionales usados por los métodos de consenso.
Descentralización	Nivel de acceso a la información para todos los nodos o mineros.
Tamaño de bloque	Su valor depende de la estructura de la cadena de bloques.
Generación de bloques	Persona encargada de agregar el siguiente bloque a blockchain.
Nivel de seguridad	Garantía que los datos no sean alterados o modificados.
Tolerancia a fallas	Resistencia a errores producidos por nodos maliciosos.

Comparación de los Métodos de Consenso

En características tales como rendimiento, latencia, tamaño de bloque y tolerancia a fallas se identificó su valor real; sin embargo, el resto de cualidades únicamente fueron representadas por una valoración cualitativa como Alto, Medio o Bajo como es el caso de escalabilidad, consumo energético, descentralización y nivel de seguridad. En el caso del parámetro disponibilidad se consideró la facilidad de acceso al libro mayor que puede ser público o privado. En la característica generación de bloque los valores posibles fueron: cualquier persona, elección de representante y miembro autorizado. En la Tabla 2 se detalla cada una de las propiedades mencionadas con sus respectivos valores por cada método de consenso:

Tabla 2

Estandarización de Datos a Valores Cualitativos

CARACTERÍSTICA	PoW	PoS	DPoS	PBFT	dBFT
Rendimiento	7 TPS	250 TPS	5.000 TPS	2.828 TPS	10.000 TPS
Escalabilidad	Alto	Alto	Medio	Medio	Medio
Disponibilidad	Pública	Pública	Pública	Privada	Privada
Latencia	10 min.	10 min.	1.5 seg.	No disponible	15 seg.
Consumo Energético	Alto	Medio	Medio	Bajo	Medio
Descentralización	Alto	Alto	Medio	Medio	Medio
Tamaño de bloque	1 MB	1 MB	No disponible	No disponible	No disponible
Generación de Bloques	Cualquier persona	Cualquier persona	Elección de representante	Miembro Autorizado	Miembro Autorizado
Nivel de seguridad	Alto	Alto	Relativamente bajo	Relativamente bajo	Medio
Tolerancia a fallas	<51% de mineros maliciosos	<51% de mineros maliciosos	<51% de mineros maliciosos	1/3 de mineros maliciosos	1/3 de mineros maliciosos

Estandarización de datos a valores cualitativos

A base de los valores cuantitativos obtenidos en las variables rendimiento, latencia, tamaño de bloque y tolerancia a fallas, se transformaron a valores cualitativos Alto, Medio o Bajo simulando una escala de Likert (McLeod, 2019).

En el caso de la variable tamaño de bloque, se ha mostrado su valor únicamente en Prueba de Trabajo y Prueba de Participación, siendo en ambos casos 1 MB, por lo tanto, su valoración cualitativa está dado por la ausencia o presencia de esta característica.

En la Tabla 3 se observa los valores cualitativos asignados para su posterior comparación. En las características que no ha podido determinarse su valor se visualizará "No disponible".

Tabla 3

Valores Cualitativos

CARACTERÍSTICA	ESCALA	VALOR CUALITATIVO
Rendimiento	>= 5.000 – < 10.000	Alto
	>= 2000 – < 5000	Medio
	> de 1 – < 2000	Bajo
Latencia	>= 5 min	Alto
	>=15 seg. – < 60 seg	Medio
	< 15 seg	Bajo
Tolerancia a Fallas	< de 51% de nodos maliciosos	Bajo
	1/3 de nodos maliciosos	Alto
Disponibilidad		Público
		Privado
Tamaño de Bloque		Valor Presente
		Valor no Disponible

Ponderación de características

Para analizar de mejor manera los resultados e identificar qué protocolos son aquellos que cumplen con los mejores estándares en cada una de las características, conforme a la escala de Likert se puede asignar más o menos puntos (Palacios, 2002) de acuerdo a la descripción cualitativa que poseen; por lo tanto, en la Tabla 4 se determina la siguiente ponderación:

Tabla 4

Valores Cuantitativos

VALOR CUALITATIVO	PONDERACIÓN
Alto	3
Medio	2
Bajo	1
Público	2
Privado	1
Valor Presente	1
Valor no Disponible	0
Cualquier persona	3
Elección representante	2
Miembro autorizado	1

Nota: Para las variables latencia y consumo de energía estos valores varían, mientras menor tiempo o consumo posea, es mejor. Alto equivale a 1, Medio 2 y Bajo 3.

Ponderación por convenio

De acuerdo a (Palacios, 2002), los autores consideran que cada una de las características analizadas no poseen la misma relevancia; los pesos asignados se observan en la Tabla 5:

Tabla 5

Ponderación por Convenio

CARACTERÍSTICA	PONDERACIÓN
Rendimiento	15%
Escalabilidad	18%
Disponibilidad	10%
Latencia	10%
Consumo Energético	5%
Descentralización	5%
Tamaño de bloque	2%
Generación de Bloques	1%
Nivel de seguridad	18%
Tolerancia a fallas	18%
TOTAL	**100%**

De los valores recopilados en la investigación, el valor cualitativo asignado a cada uno, el peso asignado a cada métrica cualitativa y, finalmente los resultados luego de realizar la ponderación por convenio se visualizan en la Tabla 6.

Tabla 6

Resultados Análisis

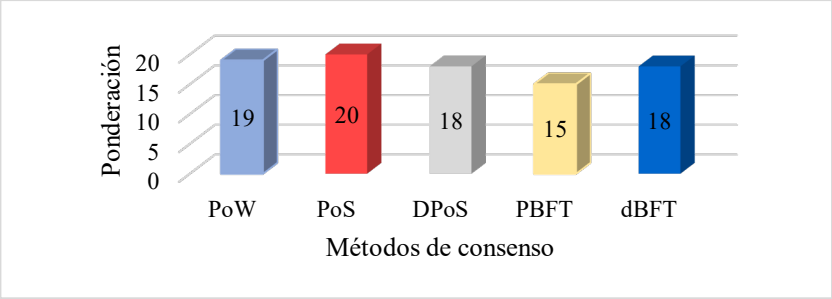
	PoW			PoS			DPoS			PBFT			dBFT		
Característica	**Valor Cualitativo**		**Val. Pond**	**Valor Cualitativo**		**Val. Pond**	**Valor Cualitativo**		**Val. Pond**	**Valor Cualitativo**		**Val. Pond**	**Valor Cualitativo**		**Val. Pond**
Rendimiento	Bajo	1	0,15	Bajo	1	0,15	Alto	3	0,45	Medio	2	0,3	Alto	3	0,45
Escalabilidad	Alto	3	0,54	Alto	3	0,54	Medio	2	0,36	Medio	2	0,36	Medio	2	0,36
Disponibilidad	Pública	2	0,2	Pública	2	0,2	Pública	2	0,2	Privada	1	0,1	Privada	1	0,1
Latencia	Alto	1	0,1	Alto	1	0,1	Bajo	3	0,3	No disponible	0	0	Medio	2	0,2
Consumo Energético	Alto	1	0,05	Medio	2	0,1	Medio	2	0,1	Bajo	3	0,15	Medio	2	0,1
Descentralización	Alto	3	0,15	Alto	3	0,15	Medio	2	0,1	Medio	2	0,1	Medio	2	0,1
Tamaño de bloque	Valor presente	1	0,02	Valor presente	1	0,2	No disponible	0	0	No disponible	0	0	No disponible	0	0
Generación de Bloques	Cualquier persona	3	0,3	Cualquier persona	3	0,3	Elección de represent.	2	0,2	Miembro Autorizado	1	0,1	Miembro Autorizado	1	0,01
Nivel de seguridad	Alto	3	0,54	Alto	3	0,54	Bajo	1	0,18	Bajo	1	0,18	Medio	2	0,36
Tolerancia a fallas	Bajo	1	0,18	Bajo	1	0,18	Bajo	1	0,18	Alto	3	0,54	Alto	3	0,54
Total Ponderación	**19**		**1,96**	**20**		**2,01**	**18**		**1,89**	**15**		**1,74**	**18**		**2,22**

Resultados y Discusión

Considerando únicamente la suma de las ponderaciones asignadas se obtiene los siguientes resultados de la Figura 1:

Figura 1

Posicionamiento de los Métodos de Consenso por su Ponderación

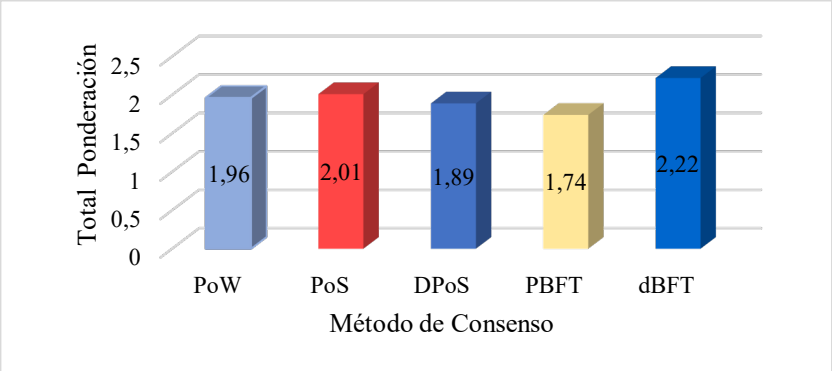


Por las características que presenta Prueba de Participación (PoS) obtiene la mejor puntuación con un total de 20 puntos. Seguido se encuentra Prueba de Trabajo (PoW) con 19 puntos. En la tercera posición está Tolerancia Delegada de Fallas Bizantinas (dBFT) con 18 puntos. Con la misma puntuación se ubica Prueba de Participación Delegada (DPoS). Finalmente, Tolerancia Práctica de Fallas Bizantinas (PBFT) obtiene 13 puntos.

Luego de asignar los pesos correspondientes considerando la relevancia de cada variable en los métodos de consenso (ver subsección Ponderación por Convenio), la Figura 2 muestra que el posicionamiento de los protocolos difiere:

Figura 2

Posicionamiento de los Métodos de Consenso por Convenio y Ponderación



En primer lugar, se ubica dBFT con un valor de 2,22 puntos. Seguido está PoS con 2,01. Con un valor no muy lejano, 1,96, se encuentra PoW. En la cuarta posición se observa a DPoS con 1,89 puntos. Por último, se visualiza que el único protocolo que no ha variado su ubicación es PBFT alcanzando un puntaje de 1,74.

En este trabajo se ha procurado obtener la mayor cantidad de información sobre los Métodos de Consenso que permita identificar su aplicabilidad en los diferentes campos. Sin embargo, existen protocolos que debido a sus características son muy usados en varias áreas como es el caso de Prueba de Trabajo que es utilizado como algoritmo criptográfico por varias plataformas como Bitcoin y Ethereum.

Una vez que se ha determinado los pesos a cada una de las características dependiendo de la importancia de las mismas en el funcionamiento de los protocolos de consenso, se identifica que el mejor resultado lo obtiene dBFT que ha incrementado significativamente las transacciones por segundo, permitiendo realizar 10.000 transacciones con una latencia de 15 segundos (Frumkin, 2019), tiene un bajo consumo de recursos; sin embargo, es un protocolo usado generalmente en BC privadas, por lo cual no todas las personas tienen acceso. Presenta mejoras en tolerancia a fallas, admitiendo únicamente un tercio de nodos maliciosos dentro de la red (Salimitari & Chatterjee, 2019).

PoS se ubica en la segunda posición, el mejoramiento que presenta es con respecto al número de transacciones que realiza por segundo en comparación a PoW y al no generar una competencia entre nodos, el consumo energético es menor; no obstante, su latencia no presenta una reducción relevante. De la misma forma mantiene la descentralización, por lo tanto, su tolerancia a fallas es baja pero su nivel de seguridad garantiza la inmutabilidad de los datos. Por otro lado, se conoce que Peercoin fue la primera criptomoneda en usar este protocolo de consenso, muestra una capitalización de mercado baja (Criptonario, 2019).

PoW es el método de consenso más utilizado; sin embargo, se posiciona en el tercer lugar al poseer un alto consumo de recursos computacionales. Entre sus principales características se conoce que brinda un alto nivel de seguridad y mantiene la descentralización que es una característica fundamental en la tecnología Blockchain. A pesar de que su latencia se encuentra en un nivel alto y su tolerancia a fallas es más baja frente a los otros métodos, es un algoritmo que posee una buena escalabilidad (Zhang & Lee, 2019). Su uso en criptomonedas ha colaborado para que éstas se encuentren en las tres primeras posiciones de la capitalización de mercado.

En la cuarta posición se encuentra DPoS. Este protocolo ha presentado mejoras con respecto al número de transacciones y su tiempo de latencia ha disminuido significativamente (Frumkin, 2019). La incorporación de un bloque a la BC está determinada por la elección a un representante reduciendo así la descentralización. Su nivel de seguridad se mantiene siendo alto con respecto a PoW pero aún los nodos pueden comportarse de manera maliciosa. Su nivel de escalabilidad no es igual que en PoS pero con referencia al consumo energético si presenta mejoras.

Finalmente, en última posición se encuentra PBFT. Aunque siendo del mismo grupo de protocolos junto con dBFT, se observa que en este método de consenso no ha sido posible determinar su valor de latencia, pero se visualiza que ha presentado mejoras en el parámetro de rendimiento (Frumkin, 2019). Este método, comúnmente es aplicado en BC con lo cual admite el comportamiento malicioso de solo un tercio de los nodos y su escalabilidad es limitada debido a que es adecuada para una red de alto rendimiento con un pequeño número de nodos (Zhang & Lee, 2019). Además, al ser usada en cadenas privadas pierde su valor de descentralización.

La primera aplicación de la tecnología Blockchain fue la moneda virtual y, la fiabilidad y seguridad de sus transacciones están determinadas por los Métodos de Consenso usados para validarlas y lograr un acuerdo para agregar un nuevo bloque a la cadena. BC brinda transparencia en la supervisión de las operaciones; sin embargo, esta transparencia puede comprometer la privacidad en particular cuando se refiere a datos personales y puede resultar beneficiosa para aquellas personas dedicadas a realizar actividades ilícitas como el lavado de dinero, venta de mercancías ilegales, delitos informáticos, etc. Actualmente, existe una carencia generalizada de leyes que regulen el comercio de criptomonedas y carteras digitales,

lo cual causa vulnerabilidades en los derechos legales de los consumidores y población en general (Mora et al., 2019).

En un futuro, es probable que la seguridad de los métodos de consenso pueda ser vulnerada debido a los avances computacionales. La intervención de la computación cuántica en este ámbito puede descubrir un método que permita vulnerar un cifrado debido a que tal tecnología podría resolver problemas que ahora resultan imprácticos con la computación tradicional (Mora et al., 2021).

Conclusiones

Se han identificado las principales características que constituyen un método de consenso, entre ellas están rendimiento, escalabilidad, latencia, seguridad y tolerancia a fallas. La fortaleza de cada una de estas características determina el mejor aprovechamiento de los protocolos de consenso.

Con el crecimiento actual de nuevas tecnologías basadas en BC, se puede aplicar en ámbitos más allá de las criptomonedas. Esta tecnología provee una forma segura y encriptada para que las transacciones no puedan ser modificadas, garantizando así la inalterabilidad e inmutabilidad de los datos. Si bien la primera aplicación de BC fue las criptomonedas, su uso se ha extendido hacia los contratos inteligentes y últimamente ha llamado la atención en ámbitos como la industria, salud, IoT, bienes raíces, entre otros.

Para que un nuevo bloque pueda ser incluido en la cadena es necesario que los nodos lleguen a un acuerdo único dentro de la red y, este acuerdo lo consiguen a través del uso de métodos o protocolos de consenso. Usualmente estos métodos de consenso son conocidos como el núcleo de cualquier aplicación basada en la tecnología *Blockchain* y su seguridad depende de estos protocolos. La importancia de estos métodos es que los diferentes nodos o mineros que participan en la red, deben poseer la capacidad de enviar mensajes entre sí con altos niveles de confianza para garantizar una comunicación segura y efectiva entre pares.

Los métodos de consenso usados con mayor frecuencia son PoW y PoS. PoW es el algoritmo usado por Bitcoin y a pesar de realizar un número bajo de transacciones por segundo posee una buena escalabilidad y un alto nivel de descentralización; además asegura la tolerancia a fallas y brinda seguridad en la red; es el protocolo de consenso que usa gran cantidad de energía al realizar complejos cálculos para la verificación en el proceso de minería. PoS a diferencia de PoW, no genera una competencia entre nodos; al contrario, un nodo es seleccionado de acuerdo a su participación en la red y será el encargado de resolver el siguiente bloque. En lugar de resolver un hash criptográfico, el nodo usa una firma digital para demostrar su participación.

En los protocolos de consenso existen características como rendimiento, escalabilidad, latencia, entre otras, que ayudan a determinar qué protocolo de consenso posee las mejores cualidades. Como resultado de analizar cada una de éstas, se concluye que Tolerancia Delegada de Fallas Bizantinas (dBFT), con 2,22 puntos, es el método de consenso que brinda los valores más altos en cada uno de los parámetros analizados. Este protocolo de consenso ha incrementado el número de transacciones que se pueden realizar por segundo con una latencia relativamente baja en comparación al tiempo que posee tanto PoW como PoS. Además, tiene una baja tolerancia a fallas. No obstante, este protocolo de consenso es usado generalmente en redes privadas, con lo cual se pierde la descentralización.

Por las características que presenta, en segundo y tercer lugar se posicionan los métodos de consenso más utilizados, Prueba de Participación con 2,01 puntos y Prueba de Trabajo con 1,96 respetivamente. En la cuarta posición se observa a DPoS con 1,89 pese a ser una variación de PoS, se diferencia por presentar niveles bajos de escalabilidad, descentralización y seguridad son. En última posición se muestra PBFT alcanzando un puntaje de 1,74 que posee un rendimiento y nivel de seguridad bajo.

La centralización es el principal problema por el cual los sistemas actuales no logran garantizar la transparencia de las transacciones. *Blockchain* por su lado, proporciona la descentralización, es decir, ninguna autoridad controla la información y la misma se encuentra distribuida en todos los nodos o computadores pertenecientes a la red. Los nodos son los encargados de realizar transacciones, validarlas y agregarlas a la cadena de bloques brindado de esta manera una mejora significativa a este inconveniente.

En la investigación realizada se identifican estudios similares que se enfocan en el uso de métodos de consenso en distintos ámbitos como cadenas de suministro o IoT. En cada campo de implementación las características de interés difieren; en el caso de redes de IoT, por ejemplo, la baja latencia es una de las variables más importante. Entre los métodos de consenso aptos para este uso están PoET y PBFT y, aquellos parcialmente aptos son PoS, DPoS o dBFT (Salimitari & Chatterjee, 2019).

Este estudio resume los componentes más importantes desarrollados en su totalidad en el trabajo de (Campaña & Zumba, 2020).

Referencias

Algorand. (2019). *Algorand*. 12 de enero de 2020, https://www.algorand.com/what-we-do/technology/algorand-protocol

Blagojevic, D. (21 de marzo de 2019). *Captainaltcoin.co*. 24 de enero de 2020, https://captainaltcoin.com/what-is-practical-byzantine-fault-tolerance-pbft/

Blockchain Support. (30 de noviembre de 2019). 12 de enero de 2020, https://support.blockchain.com/hc/en-us/articles/360019105391-Stellar-consensus

Buterin, V., & Griffith, V. (2019). Casper the Friendly Finality Gadget. arXiv:1710.09437v4

Cachin, C., & Vukolić, M. (17 de Julio de 2017). Blockchain Consensus Protocols in the Wild. *IBM Research - Zurich*, 24. doi:arXiv:1707.01873v2

Campaña Iza, X. M., & Zumba Sampedro, W. X. (2020). Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo. 80. http://www.dspace.uce.edu.ec/handle/25000/21832

Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On Security Analysis of Proof-of-Elapsed-Time (PoET). 282-297. doi:10.1007/978-3-319-69084-1_19

CoinsTelegram. (30 de octubre de 2018). *CoinsTelegram*. 11 de enero de 2020, https://coinstelegram.com/2018/10/30/what-is-leased-proof-of-stake-lpos/

Comben, C. (14 de marzo de 2019). *Coin Rivet*. 11 de enero de 2020, https://coinrivet.com/es/delegated-byzantine-fault-tolerance-dbft-explained/

Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 39. doi:doi 10.1109/COMST.2018.2842460,

Criptonario. (febrero de 2019). 25 de febrero de 2020, https://criptotario.com/que-es-la-capitalizacion-de-mercados-en-criptomonedas

Curran, B. (24 de julio de 2018). 13 de enero de 2020, https://blockonomi.com/iota-tangle/

Danezis, G., & Meiklejohn, S. (2016). Centrally Banked Cryptocurrencies. doi:dx.doi.org/10.14722/ndss.2016.23187

Debus, J. (2017). Consensus methods in blockchain systems. *Frankfurt School of Finance & Management*.

Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., & Hamida, E. (2018). Consortium Blockchains: Overview, Applications and Challenges. *International Journal On Advances in Telecommunications, 11*(1 &2), 51-64.

Dinh, T. T., Liu, R., Zhang, M., Chen, G., & Chin, B. (01 de julio de 2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering, 30*(7), 1366-1385. doi:doi: 10.1109/TKDE.2017.2781227

DistrictOx Education Portal. (s.f.). *DistrictOx Education Portal*. 11 de enero de 2020, https://education.district0x.io/general-topics/ethereum-scaling/what-is-casper/

Duchenne, J. (2018). Blockchain and Smart Contracts: Complementing Climate Finance, Legislative Frameworks, and Renewable Energy Projects. *Transforming Climate Finance and Green Investment with Blockchains*, 303-317. https://doi.org/10.1016/B978-0-12-814447-3.00022-7

Fadhil, M., Owen, G., & Adda, M. (junio de 2017). Proximity Awareness Approach to Enhance Propagation Delay on the Bitcoin Peer-to-Peer Network. *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, 2411–2416. doi:10.1109/ICDCS.2017.53

Fairley, P. (Octubre de 2017). Feeding the Blockchain Beast - If Bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous. *Blockchain World*, 36, 37, 58, 59. http://spectrum.ieee.org/beast1017

Frumkin, D. (08 de abril de 2019). *Invest in Blockchain*. 24 de emero de 2020, https://www.investinblockchain.com/transactions-per-second-and-consensus-mechanisms-of-the-top-50-cryptocurrencies/

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. *In Proceedings of the 26th Symposium on Operating Systems*, 52-68. doi:doi.org/10.1145/3132747.3132757

Gramoli, V. (2017). From blockchain consensus back to Byzantine consensus. *Future Generation Computer Systems*, 10. doi:doi.org/10.1016/j.future.2017.09.023

Grobys, K., Ahmed, S., & Sapkota, N. (05 de Diciembre de 2019). Technical trading rules in the cryptocurrency market. *Finance Research Letters*, 20. doi.org/10.1016/j.frl.2019.101396

Hanke, T., Movahedi, M., & William, D. (2018). Dfinity technology overview series, consensus system. doi:arXiv:1805.04548v1

Islam, N., Mäntymäkib, M., & Turunenc, M. (2019). Why do blockchains split? An actor-network perspective on Bitcoin splits. *Technological Forecasting & Social Change, 148*, 10. doi:doi.org/10.1016/j.techfore.2019.119743

Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018). OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. *In 2018 IEEE Symposium on*, 583-598. doi:10.1109/SP.2018.000-5

Koller, M. (25 de octubre de 2017). *ItNext*. 12 de enero de 2020, https://itnext.io/the-stellar-consensus-protocol-decentralization-explained-338b374d0d72

Larimer, D. (2014). Delegated proof-of-stake (dpos). *Bitshare whitepaper*.

Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A secure sharding protocol for open blockchains. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 17-30. doi:dx.doi.org/10.1145/2976749.2978389

McLeod, S. (2019). *SymplyPsychology*. 28 de enero de 2020, https://www.simplypsychology.org/likert-scale.html

Milutinovic, M., He, W., Wu, H., & Kanwal, M. (s.f.). Proof of Luck: an Efficient Blockchain Consensus Protocol. *Proceedings of the 1st Workshop on System Software for Trusted Execution (SysTEX '16)*, 1–6. doi:doi.org/10.1145/3007788.3007790

Mitar's Point. (21 de marzo de 2017). *Mitar's Point*. 13 de enero de 2020, https://mitar.tnode.com/post/proof-of-luck-consensus-protocol-and-luckychain/

Mora, H., Morales M., M. R., Pujol López, F. A., & Mollá Sirvent, R. (2021). Social cryptocurrencies as model for enhancing sustainable development. *Kybernetes*, 34. doi:10.1108/K-05-2020-0259

Mora, H., Pujol López, F. A., Mendoza Tello, J. C., & Morales, M. R. (2019). Virtual Currencies in Modern Societies: Challenges and Opportunities. *Politics and Technology in the Post-Truth Era*, 171-185. doi:10.1108/978-1-78756-983-620191012

Mora, H., Pujol López, F. A., Morales, M. R., & Mollá Sirvent, R. (2020). Disruptive Technologies for Enabling Smart Government in Reserach and Innovation Forum 2020. *Disruptive Technologies in Times of Change*, 57-69.

Morales, S., Morales, M., Trujillo, W., & Paucar, J. (2020). Tecnología blockchain en la optimización de una cadena de sumistro. *Revista Arbitrada Interdisciplinada Koinonia, 5(2)*, 161-180.

Nawari, N. O., & Ravindran, S. (04 de Junio de 2019). Blockchain and the built environment: Potentials and limitations. *Journal of Building Engineering, 25*, 16. doi:doi.org/10.1016/j.jobe.2019.100832

Nem. (s.f.). 11 de enero de 2020, de https://nem.io/technology/

Ongaro, D., & Ousterhout, J. (2014). In Search of an Understandable Consensus Algorithm. *In 2014 USENIX Annual Technical Conference (USENIXATC 14)*, 305-319.

Option Finance. (s.f.). 11 de enero de 2020, https://option.finance/proof-importance-algorithm

Palacios Gómez, J. L. (2002). Estrategias de Ponderación de la respuesta en encuestas de satisfacción de usuarios de servicio. *Metodología de Encuestas, 4*(2), 175-193.

Papadopoulos, G. (2015). Blockchain and Digital Payments:An Institutionalist Analysis ofCryptocurrencies. *Handbook of Digital Currency*, 153-172. doi:doi.org/10.1016/B978-0-12-802117-0.00007-2

peercoinDocs. (s.f.). 24 de enero de 2020, https://docs.peercoin.net/

Porta, M. (17 de agosto de 2019). *The Cryptonomist*. 11 de enero de 2020, https://en.cryptonomist.ch/2019/08/17/proof-of-capacity-poc-consensus-algorithm/

Prasanna. (25 de septiembre de 2019). *Cryptoticker*. 11 de enero de 2020, https://cryptoticker.io/en/proof-of-burn/

QuestionPro. (2020). 28 de enero de 2020, https://www.questionpro.com/blog/es/investigacion-exploratoria/

Ruozhou, L., Shanfeng, W., Zilib, Z., & Xuejun, Z. (2019). Is the introduction of futures responsible for the crash of Bitcoin? *Finance Research Letters*, 7. doi:doi.org/10.1016/j.frl.2019.08.007

Salimitari, M., & Chatterjee, M. (19 de Junio de 2019). A Survey on Consensus Protocols in Blockchain for IoT Networks. doi:15. arXiv:1809.05613v4

Seth, S. (04 de abril de 2018). *Golden*. 11 de enero de 2020, https://golden.com/wiki/Proof-of-activity_(PoA)

Swan, M. (2018). Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems. *Advances in Computers*, 42. doi:doi.org/10.1016/bs.adcom.2018.03.013

Tahar Hammi, M., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A descentralized blockchain-based authentication system for IoT. *Computers & Security, 78*, 126-142. doi:doi.org/10.1016/j.cose.2018.06.004

Viriyasitavat, W., & Hoonsopon, D. (29 de Julio de 2018). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration, 13*, 32-39. doi:https://doi.org/10.1016/j.jii.2018.07.004

WavesDocs. (s.f.). 11 de enero de 2020, https://docs.wavesplatform.com/en/blockchain/leasing.html

Young Lee, J. (2019). A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Kelley School of Business, Indiana University, 62*, 773-784. doi:doi.org/10.1016/j.bushor.2019.08.003

Zamani, M., Movahedi, M., & Raykova, M. (2018). RapidChain: Scaling Blockchain via Full Sharding. *In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 931-948.

Zhang, S., & Lee, J.-H. (2019). Analysis of the main consensus protocols of blockchain. *The Korean Institute of Communications and Information Sciences*. doi.org/10.1016/j.icte.2019.08.001

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (Octubre de 2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services, 14*(4), 352-375. doi: 10.1504/IJWGS.2018.10016848