Kenneth G. Paterson
Editor In Chief
Journal of Cryptology
Berlin Tiergartenstrasse 17. D-69121 Heidelberg
Germany

October 23, 2019

Dra. Anabel

Gracias por tomar el tiempo de leer y analizar el avance de proyecto, después de las revisiones de los compañeros se han hecho múltiples correcciones y espero el documento adjunto a esta carta tenga una calidad mas aceptable que el entregado en la ocasión anterior.

Primer editor

Gracias por su dedicado y extensivo análisis del proyecto en cuestión, temo mucho que haya encontrado errores gramaticales y peor aún de ortografía en el documento a pesar de mis varias revisiones. A continuación responderé a sus observaciones:

En el planteamiento del problema cuando se hace referencia a la Figura 1, no se compiló de manera correcta el documento, por lo tanto, no es visible la referencia de la imagen.

Se ha hecho la corrección pertinente en el documento en la sección 1.1, ahora la referencia se ve correctamente.

En el planteamiento del problema, se hace referencia a la siguiente parte: "En este proyecto se pretende diseñar implementación de Blockchain", la redacción no es correcta.

Se ha corregido el 9º párrafo del planteamiento del problema para corregir este error de la siguiente manera:

"En este proyecto se pretende diseñar un protocolo Blockchain que utilize métodos criptográficos como alternativa a los métodos de proof-of-work por medio de esfuerzo computacional, y que al mismo tiempo logre mantener el mismo o un mejor nivel de seguridad para la validación de los nuevos bloques dentro de la cadena de transacciones".

Último párrafo de la justificación: "En base a las cualidades", debe ser expresado como: "Con base en las cualidades"

También se ha corregido la sintaxis del texto del párrafo en cuestión para que ahora se pueda leer de la siguiente manera:
"Con base en las cualidades que se proponen para el nuevo protocolo, se permitiría que la adopción de protocolos basados en Blockchain crezcan de manera mas rápida y con una infraestructura menor y con menos impacto a nivel energético".

En el objetivo general el segundo párrafo no se considera necesario, puede ser incluido en la justificación del problema o desglosado en los objetivos particulares.

Tiene razón en ese punto, el segundo párrafo del objetivo general es reiterativo una vez que se leen los objetivos específicos, por lo cual es mejor eliminarlo.

En los objetivos particulares es necesario definir el método para evaluar la velocidad del protocolo.

No hay método específico para la medición de la velocidad de un protocolo, se colocarán códigos de manejo de timestamp en el código de las versiones originales y modificadas del protocolo para medir su velocidad, las pruebas de ambos se harán en el mismo equipo para poder tener un resultado válido.

Se debió escribir explícitamente que el nombre de la metodología a usar es metodología para investigación cuantitativa.

El primer párrafo de la sección de metodología se ha modificado para tomar en cuenta las sugerencias. Además, se ha agregado un diagrama de la metodologío empleada.

"La investigación actual se considera del tipo experimental y se manejará una implementación del método de investigación cuantitativa presentada por Hernádez Sampieri[15] el cual se puede visualizar en la Figura 2. Basado en dicha metodología se generará un conjunto de pasos específicos para analizará la posibilidad de implementar un criptosistema blockchain basado en sistemas criptográficos y comprobar su funcionalidad y nivel de seguridad como alternativa a los sistemas blockchain existentes.".

Segundo Editor

Muchas gracias por sus comentarios, la mayoría de ellos se han podido tomar en cuenta, aún así hay algunos que son difíciles de analizar por ser un poco vagos, pero para poder tomarlos en cuenta se dieron lecturas adicionales al documento para poder tratar de resolverlos, espero el documento enviado

Corregir ortografía, por ejemplo: "metodologia, multiples, calculo".

Se han corregido varias errores con acentos, me encuentro corrigiendo el diccionario de la computadora donde trabajo, pues muchos de ellos no fueron tomados en cuenta.

El índice no debe ir en formato arábigo, debe ir en numeración romana.

Se ha corregido el manejo del indice y la numeración de páginas de este y el contenido principal.

Existen párrafos escritos de manera informal o presentan pleonasmos.

Se ha corregido la manera de escribir varios de los párrafos que podrían considerados reiterativos, pero si aún se encontraran algunos me sería muy util que pudiera señalar cuales encuentra con estas cualidades para analizarlos con más detalle.

La Figura no está correctamente numerada.

Se ha corregido la referencia a la Figura 1 de la página 1.

No debe usar juicios de valor en los enunciados, por ejemplo: ".al mismo tiempo logre

mantener el mismo o un mejor nivel...".

Se corrigieron los juicios de valor que se cree se encuentran en el documento.

Carece de referencias bibliográficas en algunos párrafos, por ejemplo: "Blockchain ha sido calificado como la tecnología más disruptiva del año 2017".

Se han agregado referencias adicionales a algunos párrafos no solo en el anunciado mencionado sino en algunos otros que pudieran faltar a lo largo de todo el documento.

Presenta demasiados objetivos particulares, se deben resumir algunos aspectos.

Se ha reducido en el número de objetivos particulares, principalmente se han eliminado algunos que podían considerarse obvios.

Tercer Editor

Muchas gracias no solo por sus comentarios dados en su carta, sino a los adicionales que agregó en el documento adjuntado originalmente, los cuales ayudaron bastante a encontrar de manera puntual varios de los errores por corregir en el documento. A continuación se responde a las demás anotaciones hechas por su parte:

Justificación:

¿Quiénes serán los beneficiarios y de qué modo?

Los investigadores en areas como el desarrollo de Internet de las cosas, contratos inteligentes como se describe en el párrafo de la justificación.

¿Cuál es su utilidad?

En los párrafos 2 y 3 se describen las utilidades de Blockchain en general del sistema propuesto.

¿Se podrán generalizar los resultados a principios más amplios?

Cómo se plantea un desarrollo general si se pueden generalizar los resultados para otras aplicaciones.

Objetivos:

El objetivo general se debe de redactar brevemente, debe de ser claro y preciso.

Se ha corregido el objetivo general para ser mas corto como se puede ver a continuación:

"Desarrollar un sistema de validación de transacciones tipo Blockchain basado en sistemas criptográficos post cuánticos para reducir el tiempo de cómputo utilizado para generar las pruebas de trabajo de los nuevos bloques de las cadenas."

En los objetivos específicos: Falto agregar lo que se pretende lograr en cada una de las etapas. Se puede simplificar en una cantidad menor (máximo 5 objetivos específicos)

Los objetivos específicos se han reducido como se puede ver en la sección 1.3.2 del documento corregido adjunto.

Metodología:

En esta sección se debe de redactar en futuro o pasado en caso de haber concluido cada etapa respectivamente (las etapas concluidas en pasado y las etapas faltantes en futuro).

Se corrigió el tiempo de conjugación de los pasos de la metodología

Benjamin Oribe Mendieta
Corresponding author.
Universidad Politécnica de Pachuca
Carretera Pachuca - Cd. Sahagún km 20 Ex-Hacienda de Santa Bárbara, Zempoala, Hidalgo, México.
boribem@micorreo.upp.edu.mx
+52 7711846606