

Análisis de la seguridad de la información en los protocolos de blockchain PoW (Proof of Work) y PoS (Proof of Stake) como alternativa para el manejo de información confidencial en el sector financiero público del Ecuador

Analysis of information security in the PoW (Proof of Work) and PoS (Proof of Stake) blockchain protocols as an alternative for handling confidential nformation in the public finance ecuadorian sector

Silvana Abigail Yacchirema Chicaiza, Ciro Napoleon Saguay Chafla, Luis Fernando Enríquez Álvarez, Polo

Fabian Iñiguez Matute

Universidad UTE, Facultad de Ciencias de la Ingeniería e Industrias

Quito, Ecuador

silvidim.23@gmail.com,

csaguay@ute.edu.ec, luisenriquez@fosslawyers.org, fabianiniguez@hotmail.com

Ramiro Delgado Rodriguez

Departamento Ciencias Computación,
Universidad de las Fuerzas Armadas ESPE

Sangolquí, Ecuador

rndelgado@espe.edu.ec

Resumen — La tecnología blockchain se fundamenta en un creciente número de registros distribuidos globalmente conocidos como cadena de bloques. Esta tecnología fue utilizada para la creación de la criptomoneda conocida como bitcoin que permite realizar de forma rápida y sencilla transacciones, sin la necesidad de utilizar un intermediario “entidad financiera”. La información se envía a través de los protocolos conocidos como: PoW (Proof of Work) y PoS (Proof of Stake) mismos que deben garantizar confidencialidad, integridad y disponibilidad de la información. El presente trabajo muestra el resultado de una revisión bibliográfica sobre la evolución del blockchain, los protocolos PoW y PoS; así como la aplicación de estas en el marco de la legislación ecuatoriana con énfasis en la evolución de riesgos del protocolo PoW.

Palabras Clave – blockchain, PoW, PoS, protocolo, bitcoin

Abstract — Blockchain technology relies on a growing number of globally distributed ledgers known as blockchain. This technology was used for the creation of the cryptocurrency known as bitcoin that allows transactions to be carried out quickly and easily, without the need to use an intermediary “financial institution”.

The information is sent through the protocols known as: PoW (Proof of Work) and PoS (Proof of Stake), which must guarantee confidentiality, integrity and availability of the information. The present work shows the result of a bibliographic review on the evolution of the blockchain, the PoW and PoS protocols; as well as the application of these within the framework of Ecuadorian legislation with emphasis on the evolution of risks of the PoW protocol.

Keywords - blockchain, PoW, PoS, protocol, bitcoin

I. INTRODUCCIÓN

Con la adopción de las tecnologías de la información y comunicación en el ámbito financiero, la información se ve expuesta a múltiples ciberataques [1] cada vez más específicos y complejos y esto crece a medida que aparecen nuevas tecnologías como es el caso de blockchain [2], introducida por una persona o serie de personas, con el pseudónimo Satoshi Nakamoto en el año 2008 [3], la cual propone transaccionar con moneda digital directamente de un ente a otro sin tener que pasar por una institución financiera, creando así un nuevo sistema de

pago electrónico directo y entre pares P2P (peer-to-peer) [4] que actualmente usa “bitcoin” [5]. Bitcoin es una criptomoneda que funciona bajo el protocolo PoW (Proof of Work) [6] que permite descifrar algoritmos criptográficos utilizando un alto poder computacional tales como: procesador, memoria, almacenamiento, entre otros, ya que toda la red de mineros simultáneamente realiza el trabajo que consiste en descifrar el algoritmo criptográfico [7]. Por otro lado la criptomoneda “Dash” [8] emplea el protocolo PoS (Proof of Stake) [9] en el cual los mineros deben cumplir determinadas condiciones para acceder a descifrar el algoritmo criptográfico. El presente trabajo describe la tecnología blockchain, los protocolos que utiliza, la legislación ecuatoriana que regula su uso y una evaluación de riesgos del protocolo PoW.

En [10] muestra las propuestas de varias criptomonedas con mayor capitalización en el mercado, pero se enfatiza en la tecnología blockchain y en como esta puede aperturar oportunidades en el sector financiero como es el caso de la blockchain de Ripple que es capaz de verificar las transacciones mucho más rápido que la blockchain de Bitcoin. Sin embargo este trabajo hace notar que adoptar la tecnología blockchain e integrarla es un largo camino que supone diversos desafíos de integración tecnológica, ya que desde el principio el sistema blockchain no estaba diseñado para el uso corporativo (sino para el usuario de la moneda virtual Bitcoin) y no estaba considerando todas las complejidades del sector financiero.

En [11] expone las características intrínsecas de las criptomonedas: anonimidad, descentralización e independencia y describe los métodos por los cuales los criminales utilizan las criptodivisas para la ejecución de sus actividades delictivas, finalmente formula propuestas de medidas que se deben implementar para la prevención y persecución de los delitos cometidos a través del uso de las criptomonedas en donde sugiere que Ecuador considere las regulaciones implementadas por Malta y Estados Unidos como marco de referencia útil para la integración de las monedas virtuales en el Ecuador.

II. PROTOCOLOS BLOCKCHAIN

Los protocolos blockchain permiten a los mineros descifrar algoritmos criptográficos, los más utilizados son:

A. PoW (*Proof of Work*)

El concepto de PoW aún sin ese nombre fue introducido en 1992 por Cynthia Dwork y Moni Naor en la 12^a Edición Anual de la Conferencia Internacional de Criptología en donde se propuso crear un proceso que redujera el correo no deseado de Internet y los ataques DDOS, por ejemplo la resolución de captchas, años más tarde este planteamiento lo adopta la red Bitcoin como “prueba de trabajo” [12] que básicamente consiste en un tipo de consenso que genera recompensas “tokens”, es decir, requiere de un arduo trabajo por parte de los mineros para descifrar un algoritmo criptográfico y el primer minero en conseguirlo retransmite el bloque que resolvió y es recompensado. Ver Fig. 1.



Figura 1 Funcionamiento PoW

Con la particularidad que este protocolo obliga a los mineros a contar con recursos computacionales elevados respecto a las características de hardware como: memoria, CPU, almacenamiento, etc. Lo cual a su vez conlleva a un alto consumo de energía.

B. PoS (*Proof of Stake*)

Se lo conoce como “prueba de participación” que consiste en que los mineros deben cumplir con determinadas condiciones antes de descifrar el algoritmo criptográfico, por ejemplo, para poder participar es necesario medir el “stake” del minero “lo rico que sea el minero para poder participar” [9]. Ver Fig. 2.

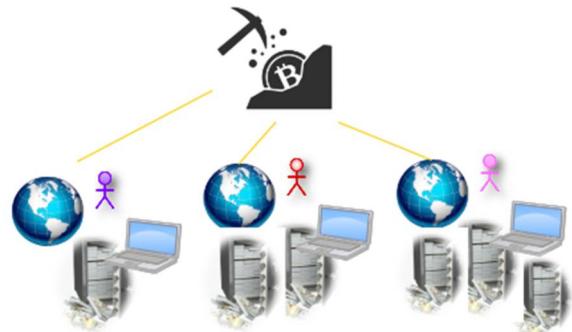


Figura 2 Funcionamiento PoS

C. PoW (*Proof of work*) vs (*Proof of stake*)

De lo anteriormente descrito los protocolos PoW y PoS se los puede diferenciar de acuerdo con lo descrito en la tabla I.

TABLA I. CUADRO COMPARATIVO POW Y POS

	SEGURIDAD	ESCALABILIDAD	COSTO
PoW	El protocolo puede ser sabotead por el 51% de mineros.	Es limitada para aquellas regiones del mundo donde los costos de hardware son elevados	Depende de la región en la que se encuentre el minero ya que el consumo de energía es abundante y el costo por región varía en este servicio.
POS	El protocolo puede ser sabotead por el	Es ilimitado ya que no demanda características de	No requiere de ordenadores costosos

	51% de la posesión total de la criptomoneda.	hardware potentes	
--	--	-------------------	--

III. LEGISLACIÓN ECUATORIANA EN EL USO DE BLOCKCHAIN

En el Ecuador en el año 2002 la “Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos” define a los datos personales como “*aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley*”, definición ambigua y con falta de especificidad [13]. En el 2004 la “Ley Orgánica de Transparencia y Acceso a la Información Pública” describe a la información confidencial como “*(...) aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República [14]*”.

En el 2014 la Ley del Sistema Nacional de Registro de Datos Públicos respecto a la accesibilidad y confidencialidad de los datos señala que “*Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales. (...)*”. En este mismo año el COIP “Código Orgánico Integral Penal” hace referencia a los delitos contra la información pública reservada legalmente en donde señala que “*(...) Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.*

En el año 2019 el presidente constitucional del Ecuador presentó ante la asamblea nacional el “Proyecto de ley Orgánica de Protección de Datos Personales” que tiene como finalidad regular el tratamiento y la protección de datos personales, genéticos, crediticios e inclusive aquellos datos personales de carácter sensible como religión, ideología entre otros, sin embargo a la fecha este proyecto de ley no ha sido aprobado.

Respecto al ámbito financiero el “Código Orgánico Monetario y Financiero” señala que “*Todas las transacciones, operaciones monetarias, financieras y sus registros contables, realizados en la República del Ecuador, se expresarán en dólares de los Estados Unidos de América, de conformidad con este Código. La circulación, canje, retiro y desmonetización de dólares de los Estados Unidos de América, moneda en la República del Ecuador, corresponden exclusivamente al Banco Central del Ecuador (...)*”. En este sentido el 14 de febrero de 2018 el Banco Central del Ecuador recuerda a los ecuatorianos que “*(...) las criptomonedas no son un medio de pago autorizado en el país y no cuentan con respaldo, pues sustentan su valor en la especulación (...)*”

Bajo estas consideraciones el Ecuador aún no reconoce en su marco regulatorio el uso de la criptomoneda como medio de pago digital así como tampoco protege los datos que aseguren este tipo de transacciones, lo cual significa que la utilización de este medio de pago y los posibles riesgos financieros que generan queda a exclusiva responsabilidad de quienes la adopten como medio de pago.

IV. EVALUACIÓN DE RIESGOS DE LOS PROTOCOLOS POW Y POS

A. Criterios de Evaluación

- Los criterios de evaluación están dados en función del CID: Confidencialidad, Integridad y Disponibilidad.
- Se considera la pérdida del CID para ponderar el impacto y establecer un criterio. tabla II, III y IV.

TABLA II. VALORACIÓN PERDIDA DE CONFIDENCIALIDAD

Confidencialidad	
Ponderación	Criterio
Alto (3)	La divulgación no autorizada de información a personas o procesos produce pérdida total de una transacción.
Medio (2)	La divulgación no autorizada de información a personas o procesos produce pérdida parcial de una transacción.
Bajo (1)	La divulgación no autorizada de información a personas o procesos no produce pérdida de la transacción.

TABLA III. VALORACIÓN PÉRDIDA DE INTEGRIDAD

Integridad	
Ponderación	Criterio
Alto (3)	La alteración o modificación de la información de una transacción que origina pérdida total de uno de los bloques de la cadena.
Medio (2)	La alteración o modificación de la información de una transacción que origina pérdida parcial de uno de los bloques de la cadena.
Bajo (1)	La alteración o modificación de la información de una transacción que no altera la cadena de bloques.

TABLA IV. VALORACIÓN PÉRDIDA DE DISPONIBILIDAD

Disponibilidad	
Ponderación	Criterio
Alto (3)	El acceso a la información tiene una interrupción de efecto crítico para todos los actores de la tecnología blockchain
Medio (2)	El acceso a la información tiene una interrupción de efecto considerable para todos los actores de la tecnología blockchain
Bajo (1)	El acceso a la información tiene una interrupción de efecto mínimo para todos los actores de la tecnología blockchain

B. Estimación de Amenazas

La tabla V presenta una ponderación bajo un criterio de probabilidad que la amenaza ocurra.

TABLA V. ESTIMACIÓN DE AMENAZAS

Ponderación de amenaza	Criterio por probabilidad
Alto (3)	La ocurrencia es muy probable (probabilidad > 75% <=100%)
Medio (2)	La ocurrencia es probable (probabilidad >40% <= 75%)
Bajo (1)	La ocurrencia es menos probable (probabilidad > 0 y <=40%)

C. Estimación de Vulnerabilidades

La tabla VI presenta una ponderación bajo un criterio que la vulnerabilidad se presente.

TABLA VI. ESTIMACIÓN DE VULNERABILIDADES

Ponderación de vulnerabilidad	Criterio
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la amenaza.
Medio (2)	La medida de seguridad implementada no reduce la probabilidad de ocurrencia de la amenaza.
Bajo (1)	La medida de seguridad implementada es adecuada.

D. Criterio de evaluación del activo

La tabla VII resume los criterios de evaluación CID y la estimación de amenazas y vulnerabilidades que da como resultado el nivel de riesgo.

TABLA VII. EVALUACIÓN DEL ACTIVO

Nivel de amenaza		Bajo			Medio			Alto		
Nivel de vulnerabilidad		Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)
Valor del impacto en términos de la pérdida de CID en los activos.	Bajo (1)	1	2	3	2	4	6	3	6	9
	Medio (2)	2	4	6	4	8	12	6	12	18
	Alto (3)	3	6	9	6	12	18	9	18	27

El nivel de riesgo se muestra en la tabla VIII. Será empleado para evaluar un activo; definido como todo elemento importante con valor para la organización.

TABLA VIII. NIVEL DE RIESGO

Nivel de riesgo		
1	3	BAJO
4	8	MÉDIO
9	27	ALTO

E. Valoración del activo

La tabla IX muestra un ejemplo de valoración de un activo

TABLA IX. VALORACIÓN DEL ACTIVO

No. Activ o	Proceso macro	Tipo de activ o	Nombre del activo	Descripción del activo	Impacto (pérdida)			V A
					C	I	D	
A1	Cadena de blockchain	Datos	Base de datos (blockchain) empleando PoW	Base de datos compartida entre todos los participantes de la red blockchain en donde se registran operaciones de compraventa o cualquier otra transacción	3	3	3	12

F. Evaluación de Riesgos

La evaluación de riesgos, tabla X muestra el análisis de riesgos del activo del literal E.

TABLA X. ANÁLISIS DE RIESGO

Análisis de riesgo				
Proceso Macro	No. de Activo	Nombre del Activo	Amenaza	Vulnerabilidad
Cadena de blockchain	A1	Base de datos empleando el protocolo PoW	Perdida de energía eléctrica	Duplicidad en la cadena de bloques

Una vez realizado el análisis de riesgo del activo identificado, la evaluación permite determinar un nivel cuantitativo de riesgo al que se expone el activo. Ver tabla XI.

TABLA XI. EVALUACIÓN DE RIESGOS

Evaluación de riesgo					
Impacto	Probabilidad	Nivel de vulnerabilidad	Controles implementados existentes	Cálculo de evaluación riesgo	Nivel de riesgo
CID	Nivel de amenaza				
3,00	2	1	Cifrado	6,00	Medio

I. CONCLUSIONES Y RECOMENDACIONES

La tecnología blockchain hace posible la eliminación de un tercero de confianza que en el sistema financiero convencional se conoce como entidad financiera, lo que significa que quien envíe y reciba la transferencia no pague algún tipo de comisión por la transacción realizada.

La inexistencia de un marco regulatorio respecto al uso de la criptomoneda como medio de pago y a la protección de datos en las transacciones por este medio, pueden ocasionar una elevada perdida financiera en sus usuarios ya que la capitalización de esta moneda varía en el mercado conforme el tipo de criptomoneda Bitcoin, Dash, entre otras.

De la evaluación de riesgos realizada al protocolo PoW dio como resultado un nivel de riesgo medio que a criterio del autor este podría ser mitigado ya que las CID (Confidencialidad, Integridad y Disponibilidad) tienen la ponderación más alta y esto se debe a que la pérdida total o parcial de energía eléctrica puede producir latencia en el proceso de restablecer la conectividad de los mineros, asumiendo que estos se encuentran en una misma región y que no disponen de equipos tecnológicos capaces brindar alta disponibilidad para que se reintegren a la blockchain que están participando. En Ecuador adoptar la tecnología blockchain es aún una realidad lejana ya que sin la existencia de un marco regulatorio las instituciones financieras no la van adoptar por los riesgos financieros y tecnológicos que su adopción significaría.

REFERÊNCIAS BIBLIOGRÁFICA

- [1] B. I. d. Desarrollo, «Ciberseguridad 2020,» 2020.
- [2] P. M. N. R. K. S. Dylan Yaga, «Blockchain Technology Overview,» 2018. [En línea]. Available: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>.
- [3] A. T. Don Tapscott, La Revolución Blockchain, Colombia, 2019.
- [4] I. M. G. Urbini, *Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada*, Argentina: Universidad Nacional de la Plata, 2018.
- [5] C. D. Retamal, J. B. Roig y J. L. M. Tapia, «La blockchain : fundamentos, aplicaciones y relación con otras tecnologías disruptivas.» *Economia Industrial*, nº 405-2017, pp. 33-40, 2017.
- [6] D. Z. Aggelos Kiayias, «Proof-of-Work Sidechains,» *International Conference on Financial Cryptography and Data Security*, pp. 21-34, 2020.
- [7] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» *unpublished*.
- [8] A. B. Aguado, de *Monedas Digitales: Origen y perspectiva desde un punto de vida social*, Valencia, Universidad Politécnica de Valencia, 2018, pp. 9-25.
- [9] Z. S. W. X. Campaña Iza Ximena Marcela, «Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo,» [En línea]. Available: <http://www.dspace.uce.edu.ec/bitstream/25000/21832/1/T-UCE-0011-ICF-256.pdf>. [Último acceso: 14 2021].
- [10] A. Zemlianskaia, Tecnología blockchain como palanca de cambio en sector financiero y bancario, Sevilla: Universidad de Sevilla, 2017.
- [11] R. G. Salvador, «Repositorio Digital USFQ,» 28 05 2019. [En línea]. Available: <https://repositorio.usfq.edu.ec/bitstream/23000/8401/1/143605.pdf>.
- [12] N. G. J. Daniel, «Estudio de Factibilidad de un sistema de voto electrónico basado en la tecnología blockchain para los procesos electorales de la facultad de ingeniería industrial de la Universidad de Guayaquil,» Guayaquil, Universidad de Guayaquil, 2018, pp. 39-41.
- [13] L. Enriquez, «Observatorio Ciberderechos y Tecnosociedad,» UASB, 10 1 2020. [En línea]. Available: <https://www.uasb.edu.ec/web/ciberderechos/la-proteccion-de-datos-en-america-latina-influencia-del-rgpd>.
- [14] C. d. I. R. d. E. 2008. [En línea]. Available: https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf. [Último acceso: 14 2021].
- [15] V. Betancourt, «Observatorio Ciberderechos y Tecnosociedad,» UASB, 1 6 2020. [En línea]. Available: <https://www.uasb.edu.ec/web/ciberderechos/proteccion-de-datos-personales-un-tema-aun-pendiente-en-ecuador>.