risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 05/06/2023
Aceitação/Acceptance: 13/08/2023

Implementación de la tecnología blockchain: Un análisis de sus aplicaciones y beneficios en la seguridad y eficiencia de la transferencia de datos

Sergio Andrés Alba Sanguino[1], Eduar Bayona Ibanez[2], Dewar Rico-Bautista[1]

saalbas@ufpso.edu.co; ebayonai@ufpso.edu.co; dwricob@ufpso.edu.co

[1] Grupo de ingeniería en innovación, tecnología y emprendimiento (GRIITEM). Universidad Francisco de Paula Santander Ocaña. Ocaña, Colombia.

[2] Grupo de ingeniería en Ciencias y Tecnología (GRUCITE). Universidad Francisco de Paula Santander Ocaña. Ocaña, Colombia.

Pages: 219-228

Resumen: La blockchain es una tecnología relativamente nueva, la cual desde sus inicios fue incorporada al mundo financiero más concretamente a las criptodivisas, pero, gracias a su crecimiento y constante desarrollo sus aplicaciones han ido más allá hasta llegar a industrias como la cadena de suministros, la gobernanza y la administración de identidades entre otros. Todo esto por sus fortalezas en la seguridad, privacidad, integridad de datos y eficiencia en su transferencia. Gracias a esta evaluación y al auge exponencial que ha tenido en los últimos años, se posiciona como una gran alternativa para entrar a las redes de computadores, más específicamente en la capa 2 del modelo OSI "Capa de enlace de datos" con el fin de abarcar problemas como los denominados spoofing, replay, flooding y MITM. En este artículo se realiza una revisión de literatura donde se exponen más a detalle los usos que se le ha dado a esta tecnología en la capa de enlace de datos, los desafíos técnicos, de implementación y legales, y, la soluciones que a lo largo de estos años se han ido presentando para dar resolver estos obstáculos.

Palabras-clave: Blockchain; Desafios; Modelo-OSI; Privacidad Seguridad.

Implementation of technology blockchain: An analysis of its applications and benefits in terms of security and efficiency of data transfer

Abstract: The blockchain is a relatively new technology, which since its inception was incorporated into the financial world more specifically to cryptocurrencies, but, thanks to its growth and constant development its applications have gone beyond to reach industries such as supply chain, governance, and identity management among others. All this because of its strengths in security, privacy, data integrity and efficiency in its transfer. Thanks to this evaluation and the exponential boom it has had in recent years, it is positioned as a great alternative to enter computer networks, more specifically in layer 2 of the OSI model "Data Link Layer" to cover problems such as the so-called spoofing, replay, flooding and MITM. In this article

a review of the literature is carried out where the uses that have been given to this technology in the data link layer, the technical, implementation and legal challenges, and the solutions that have been presented over the years to solve these obstacles are exposed in more detail.

Keywords: Blockchain; Challenges; Model-OSI; Privacy; Security.

1. Introducción

Las nuevas tecnologías se han ido tomando el mundo a pasos agigantados, el auge y la cobertura que van obteniendo es de crecimiento exponencial, pues cada vez son más las múltiples aplicaciones y versatilidad de uso que brindan. La tecnología Blockchain es relativamente nueva, que, desde sus inicios ha generado gran impacto en el mundo digital por sus numerosas aplicaciones (Underwood, 2016), gracias a su esencia de red "peer-to-peer" con una columna vertebral criptografía que hace inmutable e inalterable la información que ahí se deposite (Bashir, 2018) y (Küsters & Müller, 2017). Dichas características son factores altamente codiciados para la resolución de problemáticas donde la transparencia, fiabilidad, integridad y persistencia de los datos son de vital importancia, que, de otra manera, dejaría en entredicho operaciones, resultados o soluciones ahí planteadas.

En esencia blockchain es un gran libro abierto, donde todos pueden escribir y leer, pero nadie puede actualizar ni borrar.

Fue incorporada inicialmente en el ámbito financiero como pilar de las criptodivisas (Nakamoto, 2009) que, desde entonces su crecimiento y constante desarrollo le ha permitido hacer parte de diferentes industrias como (Nikonov, 2017): En la cadena de suministro (Kshetri, 2018), gobernanza (Ølnes, 2016), atención médica y administración de identidades (Reid & Harrigan, 2013), entre otros (Christidis & Devetsikiotis, 2016).

La implementación de la tecnología blockchain en la capa 2 del modelo OSI "capa de enlace de datos" proporciona un gran número de beneficios, como la mejora en la seguridad, privacidad y la eficiencia en la transferencia de datos, los cuales son unas de las principales preocupaciones en el canje de información en las redes de computadores (Lin & Liao, 2017), (Barrientos-Avendaño et al., 2019; Lobo & Rico-Bautista, 2012; Rico-Bautista et al., 2008). Al hacer un acercamiento se encuentra con problemas como los ataques de suplantación (spoofing) y envenenamiento de direcciones, ataques de repetición (replay), ataques de inundación (flooding) y ataques man-in-the-middle (MITM). Por lo que, al hacer una incorporación de la tecnología blockchain, se obtendría transparencia, integridad y autenticidad (Balduzzi et al., 2014), (Zohar, 2015).

No obstante, el uso de dicha tecnología en la capa 2 del modelo OSI representa desafíos técnicos, de implantación y legales. A continuación, se expone la revisión de literatura realizada para analizar los avances que existen en cuanto a la incorporación de la blockchain en la capa 2 del modelo OSI y sus aplicaciones en la seguridad y eficiencia de la transferencia de datos.

2. Metodología

Para llevar a cabo la revisión de literatura primero se definieron una serie de preguntas a las cuales se pretendía dar respuesta con los análisis hechos a los artículos, proyecto y libros (Rico-Bautista, 2019; Rico-Bautista et al., 2021; Rico-Bautista, Maestre-Gongora, et al., 2020; Rico-Bautista, Medina-Cardenas, et al., 2020).

Las preguntas de revisión de literatura planteadas son la siguientes:

1. ¿Qué medidas específicas se han implementado para mejorar la seguridad y eficiencia de la transferencia de datos en la capa 2 del modelo OSI mediante la blockchain y qué desafíos presenta?
2. ¿Cómo se han abordado los desafíos técnicos y prácticos asociados con la implementación de la blockchain en la capa 2 del modelo OSI?
3. ¿Qué oportunidades y beneficios ofrece la implementación de la blockchain en la capa 2 del modelo OSI en términos de transparencia, integridad y autenticidad de los datos, y cómo se pueden aprovechar estas ventajas para mejorar la gestión de datos?
4. ¿Cuáles son los posibles riesgos y desafíos legales y regulatorios asociados con la implementación de la blockchain en la capa 2 del modelo OSI, como la privacidad de los datos y la responsabilidad legal?

Para la revisión sistemática de literatura con el fin de dar respuesta a las preguntas planteadas anteriormente, se realizó una identificación y definición de palabras clave las cuales engloban de la manera pertinente y concreta el tema que es objeto de estudio y las preguntas de investigación ya definidas, ver Tabla 1. Las cuales fueron usada en la creación de la cadena de búsqueda para las bases de datos digitales, que a su vez son de vital importancia para la comprensión adecuada del presente escrito.

Style Name	Format
P1	Blockchain
P2	OSI-model
P3	Security
P4	Transfer
P5	Data

Tabla 1 – Palabras claves y sus definiciones

Haciendo uso de los operadores booleanos se armó la cadena de búsqueda con las anteriores palabras, la cual se presenta a continuación:

*(blockchain **and** osi-model **and** securuty **and** transfer **and** data)*

Posterior se realizó una búsqueda exhaustiva de artículos científicos, proyectos y libros de investigación relacionados con la implementación de la blockchain en la capa 2 del modelo OSI, utilizando bases de datos académicas confiables como Scopus, IEEE, ACM y ScienceDirect, para lo cual se definieron palabras clave que permitieron hacer dichas

búsquedas, las palabras clave son: Blockchain, Smart Contracts, Modelo OSI, Encale de datos, Switching, redes y telecomunicaciones.

Se identificaron y analizaron los artículos más relevantes para abordar las preguntas de revisión de literatura planteadas. La metodología de revisión de literatura se centró en la identificación de las medidas específicas implementadas, los desafíos técnicos y prácticos abordados, las oportunidades y beneficios, así como los posibles riesgos y desafíos legales y regulatorios asociados con la implementación de la blockchain en la capa 2 del modelo OSI.

3. Resultados

3.1. Medidas específicas implementadas y los desafíos que representan

La implementación de la blockchain en la capa 2 del modelo OSI se ha venido dando mediante la utilización de sus compuestos principales de manera separada, pero que se encuentra muy presente. Como es el caso de la encriptación de extremo a extremo (Merkle, 1988), donde se utiliza para garantizar que las partes se encuentran autorizadas a acceder los recursos que solicitan (Swan, 2015). La incorporación de la criptografía simétrica (Merkle, 1988) garantiza el intercambio de claves públicas y privadas para prevalecer la integridad y la persistencia de los datos (Lamport et al., 1982).

Los principales desafíos a los que se podría enfrentar la implementación de esta tecnología en la capa de enlace de datos son:

- Escalabilidad, esto debido a la limitación en el número de transacciones que se pueden realizar en periodos determinados de tiempo, peor para ellos ya se está trabajando en soluciones como sharding o sidechains.
- Latencia, el tiempo necesario para resolver los algoritmos de consenso para validar las transacciones puede aumentar la latencia en la transmisión de información (Baird, 2018).
- Consumo energético, resolver los algoritmos de consenso como PoW requiere de un procesamiento elevado por lo que se necesita gran energía para mantener funcionando dichos dispositivos (Krause & Tolaymat, 2018).

Estos desafíos se traducen en altos costos en tiempo y recursos para su implementación, agregando también la posible incompatibilidad entre los sistemas preexistentes en el mercado, o con sistemas que no adopten dichas tecnologías como métodos de autorización y seguridad (Croman et al., 2016).

3.2. Abordando desafíos técnicos y prácticos:

Para abordar los desafíos técnicos y prácticos mencionados anteriormente, los cuales están asociados con la implementación de la blockchain en la capa 2 del modelo OSI, se han propuesto soluciones para mejorar la escalabilidad, la implementación de protocolos de consenso más eficientes y la optimización de la infraestructura y los recursos de red (Pustišek & Kos, 2018).

Una de estas soluciones que permite mejorar la escalabilidad es la implementación del denominado "concepto de canales de estado", incorporador en Lightning Network el cual permite un mayor número de transacciones de Bitcoin sin tener la necesidad que cada una de ellas sea registrada en la cadena de bloques principal (Poon & Dryja, 2016). Al lograr hacer uso de este concepto apoyado por algoritmos de consenso alternativos como el Proof-of-Stake (PoS) propuesto y analizado en el proyecto Ethereum 2.0 (Buterin, 2020), (Wood, 2022) se lograría disminuir el consumo energético pues la red es más eficiente en cada proceso y por ende se obtiene una reducción altamente notable en la latencia lo que llevaría a una velocidad de transferencia más alta de lo que se esperaría (Yu et al., 2020).

Además, se han desarrollado frameworks y herramientas para facilitar la implementación y el mantenimiento de la blockchain en diferentes entornos y aplicaciones (Zheng et al., 2017), ver Tabla 2.

Año	Evento	Descripción
2009	Proof of Work (PoW)	Bitcoin crea el algoritmo de consenso donde se resuelven problemas matemáticos complejos por los mineros (Antonopoulos, 2014).
2012	Algoritmo de consenso Ripple (RPCA)	Ripple crea el algoritmo de consenso Ripple (RPCA) que permite transacciones más rápitas y con consumo más bajo de energía (Schwartz et al., 2018).
2015	Ethereum y Contratos inteligentes	Ethereum introduce los contratos inteligentes que permiten la creación de aplicaciones descentralizadas en diferentes industrias (Buterin, 2020).
2016	Consorcios Blockchain	Aparición de R3 Corda y Hyperledger Fabric que permiten soluciones blockchain privadas y personalizadas (Brown et al., 2016).
2018	Sharding859*	Ethereum propone esta solución para aumentar la capacidad de procesamiento de la red (Luu et al., 2016).
2019	Canales de estado	Soluciones que permiten transacciones más rápidas y de menor costo (Bartoletti et al., 2017).
2021	Almacenamiento distribuido	Almacenamiento descentralizado y seguro basado en blockchain (Benet, 2014).

Tabla 2 – Desarrollo de soluciones a los desafíos técnicos

3.3. Oportunidades y beneficios

La implementación de la blockchain en la capa 2 del modelo OSI ofrece oportunidades y beneficios en términos de transparencia, integridad y autenticidad de los datos. Estos beneficios pueden aprovecharse para mejorar la gestión de datos y reducir los costos en áreas como la ciberseguridad, la detección y prevención de fraudes, y la protección de la privacidad de los usuarios (Casino et al., 2019). Una de las principales características de

la blockchain que daría grandes beneficios son los métodos de autenticación (Lamport, 1981), ya que, al estar basados en criptografía y tener una base descentralizada se garantiza que solo las partes autorizadas tendrán acceso a los recursos específicos.

Otro punto fuerte es la resiliencia de los datos, pues al ser de naturaleza distribuida se hace poco vulnerable a los fallos o taques facilitando también así la recuperación de información gracias a que se encuentran en múltiples nodos. Esto con la garantía de inmutabilidad que nos garantiza este tipo de tecnologías.

Al contar con una operación en tiempo real se pueden incorporar algoritmos de análisis y monitoreo que permitan la identificación de patrones y tendencias logrando así hacer un direccionamiento eficiente de los recursos de la red como la asignación del ancho de banda, la asignación de recursos de almacenamiento y la reconfiguración de nodos, o la distribución de la información agregando un balanceo de cargar y optimización del enrutamiento mejorando la eficiencia y reduciendo una posible congestión.

3.4. Riesgos y desafíos legales y regulatorios

A pesar de los beneficios y oportunidades que ofrece la implementación de la blockchain en la capa 2 del modelo OSI, también existen riesgos y desafíos legales y regulatorios que deben abordarse. Algunos de estos riesgos y desafíos incluyen la privacidad de los datos, la propiedad intelectual y la responsabilidad legal. Al ser una tecnología relativamente nueva, con un mercado aun en desarrollo pues los procesos legislativos o regulatorios aplicables son escasos o prácticamente nulos en algunos países o regiones (Radziwill, 2018).

Para abordar estos riesgos y desafíos, se han propuesto enfoques como el uso de tecnologías de preservación de la privacidad y la implementación de marcos legales y regulatorios adecuados para garantizar la protección y privacidad de los datos con conformidad a las leyes aplicables ya existentes, como en el caso de Colombia que serían: La ley estatutaria 1581 del 2012 donde se regula el derecho fundamental de habeas data y se establecen los principios, derechos y deberes para el tratamiento de datos, la resolución 0448 del 2022 donde opta las políticas de seguridad y privacidad de la información, la resolución 924 del 2020 que actualiza las políticas de tratamiento de datos personales, y el artículo 15 de la constitución política donde se reconoce el derecho a la intimidad, el habeas data y al buen nombre (Bonneau et al., 2015).

4. Conclusiones

La revisión de literatura realizada en este artículo demuestra que existen diversos desafíos técnicos y de implementación presentes en la adopción de las tecnologías blockchain para la capa de enlace de datos, como los problemas de escalabilidad, latencia y consumo energético. Esto debido a que es una tecnología resiente que aún se encuentra en desarrollo con el fin de llegar a sus mejores capacidades, pero, aun así, se logró evidenciar que hay avances significativos como el “concepto de canales de estado” implementados en Lightning Network y los algoritmos de consenso alternativos como el Proof-of-Stake (PoS) propuesto y analizado en el proyecto Ethereum 2.0.

Otro de los grandes desafíos a sortear son los marcos legales y regulatorios, en donde se determinó que la legislación específica para este tipo de implementaciones es casi nula, lo que genera huecos legales y posibles problemas de integración con otras tecnologías que si están reguladas. La solución más razonable determinada gracias la revisión de literatura es la adopción de las leyes existentes en materia de políticas de seguridad y tratamiento de datos con es el caso de las mencionadas de la legislación colombiana.

Por último, las ventajas y beneficios que conlleva esta unión son de grandes proporciones en diferentes parámetros, pues los problemas técnicos y legales ya cuentan con soluciones parciales que permiten el desarrollo de pruebas piloto para ir ganando campo y adquiriendo nuevos conocimientos sobre el área, pero, la tecnología blockchain no se encuentra en la etapa adecuada para hacer una incorporación a gran escala en la capa 2 del modelo OSI.

Referencias

Antonopoulos, A. M. (2014). Mastering Bitcoin Unlocking Digital Cryptocurrencies. In *O'Reilly Media, Inc.* (Vol. 9, Issue 1).

Baird, L. (2018). The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance. In *Swirlds Tech Report* (Vol. 01).

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system. *ACM International Conference Proceeding Series*, *2014-Decem*(December), 436–445. https://doi.org/10.1145/2664243.2664257

Barrientos-Avendaño, E., Rico-Bautista, D., Coronel-Rojas, L. A., & Cuesta-Quintero, F. R. (2019). Smart farm: Defining of infrastructure based on internet of things, IpV6 and software defined networks [Granja inteligente: Definición de infraestructura basada en internet de las cosas, IpV6 y redes definidas por software]. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *E17*, 183–197. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85061174873&partnerID=40&md5=ac38dc2b5b0d67edae2c307fe67f26e3

Bartoletti, M., Lande, S., Pompianu, L., & Bracciali, A. (2017, December 11). A general framework for blockchain analytics. *SERIAL 2017 - 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*. https://doi.org/10.1145/3152824.3152831

Bashir, I. (2018). Mastering Blockchain - Second Edition. In *Paper Knowledge . Toward a Media History of Documents* (Issue 2).

Benet, J. (2014). *IPFS - Content Addressed, Versioned, P2P File System*.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. *Proceedings - IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). *Corda: An Introduction*.

Buterin, V. (2020). Ethereum Whitepaper | Ethereum.org. *Ethereum.Org*, 1–41.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–81. https://doi.org/10.1016/J.TELE.2018.11.006

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., & Wattenhofer, R. (2016). On scaling decentralized blockchains. *Lecture Notes in Computer Science*, *9604*, 106–125. https://doi.org/10.1007/978-3-662-53357-4_8

Krause, M. J., & Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. *Nature Sustainability*, *1*(11), 711–718. https://doi.org/10.1038/s41893-018-0152-7

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80–89. https://doi.org/10.1016/J.IJINFOMGT.2017.12.005

Küsters, R., & Müller, J. (2017). Cryptographic security analysis of E-voting systems: Achievements, misconceptions, and limitations. *Lecture Notes in Computer Science*, *10615 LNCS*, 21–41. https://doi.org/10.1007/978-3-319-68687-5_2/COVER

Lamport, L. (1981). Password Authentication with Insecure Communication. *Communications of the ACM*, *24*(11), 770–772. https://doi.org/10.1145/358790.358797

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401. https://doi.org/10.1145/357172.357176

Lin, I.-C., & Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, *19*(5), 653–659. https://doi.org/10.6633/IJNS.201709.19(5).01

Lobo, J., & Rico-Bautista, Dewar. (2012). Implementación de la seguridad del protocolo de internet versión 6. *Gerencia Tecnológica Informática*, *11*(29), 35–46. https://biblat.unam.mx/es/revista/gerencia-tecnologica-informatica/articulo/implementacion-de-la-seguridad-del-protocolo-de-internet-version-6

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

Merkle, R. C. (1988). A digital signature based on a conventional encryption function. *Lecture Notes in Computer Science*, *293*, 369–378. https://doi.org/10.1007/3-540-48184-2_32/COVER

Nakamoto, Satoshi. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://doi.org/10.2139/ssrn.3977007

Nikonov, A. V. (2017). Generation of testing actions for electronic packages. *Dynamics of Systems, Mechanisms and Machines (Dynamics)*, *2017-Novem*, 1–9. https://doi.org/10.1109/DYNAMICS.2017.8239490

Ølnes, S. (2016). Beyond Bitcoin enabling smart government using blockchain technology. *Lecture Notes in Computer Science*, *9820*, 253–264. https://doi.org/10.1007/978-3-319-44421-5_20

Poon, J., & Dryja, T. (2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*.

Pustišek, M., & Kos, A. (2018). Approaches to Front-End IoT Application Development for the Ethereum Blockchain. *Procedia Computer Science*, *129*, 410–419. https://doi.org/10.1016/j.procs.2018.03.017

Radziwill, N. (2018). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. *Quality Management Journal*, *25*(1), 64–65. https://doi.org/10.1080/10686967.2018.1404373

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. *Security and Privacy in Social Networks*, 197–223. https://doi.org/10.1007/978-1-4614-4139-7_10/COVER

Rico-Bautista, D. (2019). Conceptual framework for smart university. *Journal of Physics: Conference Series*.

Rico-Bautista, D., Guerrero, C. D., Collazos, C. A., Maestre-Góngora, G., Hurtado-Alegría, J. A., Medina-Cárdenas, Y., & Swaminathan, J. (2021). Smart University: a vision of technology adoption. *Revista Colombiana de Computación*, *22*(1), 44–55. https://doi.org/10.29375/25392115.4153

Rico-Bautista, D., Maestre-Gongora, G., & Guerrero, C. D. (2020). Smart University:IoT adoption model. *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 821–826. https://doi.org/10.1109/WorldS450073.2020.9210369

Rico-Bautista, D., Medina-Cardenas, Y., Areniz-Arevalo, Y., Barrientos-Avendano, E., Maestre-Gongora, G., & Guerrero, C. D. (2020). Smart University: Big Data adoption model. *2020 9th International Conference On Software Process Improvement (CIMPS)*, 52–60. https://doi.org/10.1109/CIMPS52057.2020.9390151

Rico-Bautista, Dewar., Medina-Cárdenas, Y., & Santos Jaimes, L. M. (2008). Ipsec de Ipv6 en la universidad de Pamplona. *Scientia Et Technica*, *2*(39), 320–325. https://doi.org/10.22517/23447214.3239

Schwartz, D., Youngs, N., & Britto, A. (2018). *The Ripple Protocol Consensus Algorithm*.

Swan, M. (2015). *Blockchain: Blueprint for a new economy* (Vol. 55, Issue 6). O'Reilly Media, Inc.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17. https://doi.org/10.1145/2994581

Wood, G. (2022). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 1–41.

Yu, X. L., Al-Bataineh, O., Lo, D., & Roychoudhury, A. (2020). Smart Contract Repair. *ACM Transactions on Software Engineering and Methodology*, *29*(4), 1–32. https://doi.org/10.1145/3402450

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Zohar, A. (2015). Bitcoin: Under the hood. In *Communications of the ACM* (Vol. 58, Issue 9, pp. 104–113). ACM PUB27 New York, NY, USA. https://doi.org/10.1145/2701411

© 2023. This work is published under https://creativecommons.org/licenses/by-nc-nd/4.0/(the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.