

# Tecnología Blockchain aplicada a la Ciberdefensa Crypto-BC

Marcelo Cipriano<sup>1,2</sup>, Edith García<sup>1</sup>, Ariel Maiorano<sup>1</sup>, Eduardo Malvacio<sup>1</sup>

<sup>1</sup> Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática. Facultad de Ingeniería del Ejército (FIE), Universidad de la Defensa Nacional – UNDEF.

<sup>2</sup> Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.  
{marcelocipriano,egarcia,maiorano,emalvacio}@fie.undef.edu.ar

**Abstract.** El objetivo del proyecto “Tecnología Blockchain aplicada a la Ciberdefensa” CRYPTO BC, es investigar, en el contexto de la criptología y en el ámbito de la ciberdefensa (civil y militar, es decir de uso dual), las ventajas, aplicaciones y desafíos de este nuevo paradigma. En los últimos años la tecnología Blockchain se ha vuelto cada vez más popular, proporcionando una forma confiable y descentralizada de ejecutar transacciones y acuerdos. En este proyecto, se analizan diversos casos de uso en el ecosistema blockchain, desarrollados e implementados para diferentes dominios, orientados a la Ciberdefensa Nacional. Se estudia el rol de la criptografía para garantizar la seguridad y privacidad de los datos dentro de la cadena de bloques, la cual podría aplicarse a propósitos diferentes. Asimismo, se considera indagar y desarrollar soluciones que permitan mejorar la articulación entre los distintos mecanismos criptográficos.

**Keywords:** Ciberdefensa, Tecnología Blockchain, Contrato Inteligente, Criptografía.

## 1 Antecedentes y Descripción General.

Los autores Lee-Kim [1] definen a la Ciberdefensa como “la práctica de proteger activos nacionales de las amenazas internas o externas propias de las tecnologías de la información y las comunicaciones (TICs)”, o sea es la actividad que permite garantizar la seguridad de cualquier Estado o Nación frente a las ciberamenazas.

La Tecnología Blockchain o Tecnología Contable Distribuida (DLT Distributed Ledger Technology en inglés) fue inicialmente considerada para implementar e-cash y criptomonedas [2]. Sin embargo, las características y propiedades de este modelo de cadena de bloques, tales como su resiliencia, seguridad criptográfica e inmutabilidad, mayormente asociadas con su naturaleza descentralizada, la hacen sumamente atractiva y, particularmente útil, en el ámbito de la ciberdefensa. Asimismo, dentro del ecosistema blockchain, los Contratos Inteligentes (Smart Contracts) se entienden

como programas, que se auto-verifican, se ejecutan automáticamente y son resistentes a posibles manipulaciones [3].

Con el auge de la tecnología blockchain, se ha observado que los smart contracts tienen varias áreas de aplicación. La integración de la tecnología blockchain y los contratos inteligentes brindan flexibilidad para desarrollar, diseñar e implementar soluciones a algunos problemas del mundo real, en menos costo y tiempo sin involucrar terceras partes en el proceso [4].

Las aplicaciones [5-6] pueden ser categorizadas en distintos dominios de acuerdo con su uso, desde las que requieren Integridad de datos hasta aquellas que refieren a Redes de Datos Descentralizadas (civiles o militares), Gerenciamiento de Cadena de Suministros, Internet de las Cosas (Internet-of-Things IoT), Internet de las Cosas Industrial (Industrial-Internet-of-Things IIoT), Comunicaciones, Identificación y Autenticación, Control de Acceso, escenarios propios al ámbito de la ciberdefensa.

La Criptografía es un componente esencial de la tecnología blockchain y en particular, de los contratos inteligentes, los cuales implican la ejecución de transacciones digitales en una red blockchain descentralizada, donde la confianza se establece a través de algoritmos y protocolos criptográficos. Primitivas criptográficas robustas establecen una comunicación segura entre las partes, garantizando que los datos y la información compartidas dentro de un contrato inteligente estén protegidas [6]. Además, la criptografía también se utiliza para verificar la *Identidad* de las partes involucradas, mediante firmas digitales y mecanismos de clave pública, permitiendo la *Autenticación* de las transacciones y el *No Repudio*, asegurando que las partes no puedan negar su participación en una transacción [7].

Cualquiera sea el escenario o la plataforma seleccionada para desarrollar un contrato inteligente, para que éste se pueda ejecutar en forma confiable y segura, se requiere contar entre otras cosas, con adecuados Mecanismos de Consenso [8].

Hay varios tipos de algoritmos de consenso como ser: Prueba de Trabajo (Proof of Work, Bitcoin), Prueba de Participación (Proof of Stake, Ethereum), Prueba de Historial (Proof of History, Solana), Prueba de Autoridad (Proof of Authority, Quorum Blockchain Service). Cada una tiene sus propias ventajas y desventajas en términos de escalabilidad, seguridad, velocidad y consumo de energía [9-10]. En [11-13] los autores presentan aplicaciones de contratos inteligentes inherentes al dominio de IoT, donde la plataforma utilizada es Ethereum con PoW y PoS como algoritmos de consenso.

Un ejemplo muy interesante de aplicaciones de contratos inteligentes, sobre el dominio de las Comunicaciones, es el que se puede ver en el trabajo de Koulianos y Litke [14], donde Solidity ha sido usado para crear un contrato inteligente compacto, liviano y efectivo que automatiza el proceso de elección de una posición en cierta estructura de formación de drones. En cada caso, se destacan las librerías criptográficas utilizadas: Criptografía en Solidity [15].

## **2 Resultados obtenidos y esperados.**

De acuerdo con lo planteado, las contribuciones serían las siguientes:

- Determinar los roles fundamentales que cumple la tecnología blockchain para ser aplicados a la ciberdefensa, considerando los aspectos de visibilidad, verificabilidad, resiliencia y auditabilidad.
- Estudiar diferentes trabajos *en proceso*, de sistemas blockchain para ciberdefensa, incluyendo aquellos que respondan a investigación y desarrollo[1].
- Establecer y disponer en dominios específicos, los límites y desafíos de la tecnología blockchain aplicada a la ciberdefensa.

## Referencias

1. Lee, Suhyeon & Kim, Seungjoo. (2021). Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3136328.
2. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system,". En línea: <https://bitcoin.org/bitcoin.pdf>, 2008.
3. Szabo, Nick. "Formalizing and securing relationships on public networks." First Monday 2.9 (1997).
4. Banerjee, A., Clear, M., & Tewari, H. (2021). "zkHawk: Practical Private Smart Contracts from MPC-based Hawk". 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 245-248.
5. Mohanta, Bhabendu & Panda, Soumyashree & Jena, Debasish. (2018). "An Overview of Smart Contract and Use Cases in Blockchain Technology". 10.1109/ICCCNT.2018.8494045.
6. "Smart Contracts: 10 Use Cases. Ambisafe". En línea: <https://perma.cc/2LBT-9SMB>.
7. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts". In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.
8. Lashkari, B., & Musilek, P. (2021). "A comprehensive review of blockchain consensus mechanisms." IEEE Access, 9, 43620-43652.
9. Zhang, P., Schmidt, D. C., White, J., & Dubey, A. (2019). "Consensus mechanisms and information security technologies. Advances in Computers" 115, 181-209.
10. Aggarwal, S., & Kumar, N. (2021). "Cryptographic consensus mechanisms". In Advances in Computers (Vol. 121, pp. 211-226). Elsevier.
11. G. Papadodimas, G. Palaiokrasas, A. Litke and T. Varvarigou, "Implementation of smart contracts for blockchain based IoT applications" 2018 9th International Conference on the Network of the Future (NOF), Poznan, Poland, 2018, pp. 60-67, doi: 10.1109/NOF.2018.8597718.
12. Mateen Ashraf, Cathal Heavey, "A Prototype of Supply Chain Traceability using Solana as blockchain and IoT", Procedia Computer Science, Volume 7,2023,Pages 948-959,ISSN 1877-0509
13. Omar, Ilhaam & Jayaraman, Raja & Debe, Mazin & Hasan, Haya & Salah, Khaled & Omar, Mohammed. (2021). "Supply Chain Inventory Sharing Using Ethereum Blockchain and Smart Contracts". IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3139829
14. Koulianos A, Litke "A Blockchain Technology for Secure Communication and Formation Control in Smart Drone Swarms". Future Internet. 2023; 15(10):344. <https://doi.org/10.3390/fi15100344>
15. Solidity Academy, "Cryptography in Solidity: Key management, encryption, and digital signatures". En línea:<https://medium.com/@solidity101/cryptography-in-solidity-key-management-encryption-and-digital-signatures-3cd933038b4e>.