**Argumentación #1**

Los estudios realizados por [1] revelan que las redes privadas basadas en blockchain tiene las características de descentralización, no manipulación, trazabilidad, alta credibilidad y consenso multipartito que mejoran la seguridad, convirtiéndolas en redes virtualmente imposible de hackear, esta afirmación se fortalece en el artículo [2] donde indican que gracias a las ventajas de seguridad que brinda el blockchain, bancos como J.P. Morgan Chase (EEUU) y Santander (España) han introducido esta tecnología en sus sistemas bancarios.

|  |  |
| --- | --- |
| Tesis | La implementación Blockchain en una red privada es virtualmente imposible de hackear. |
| Evidencia | Dado a las ventajas de seguridad que brinda el blockchain, bancos como J.P. Morgan Chase (EEUU) y Santander (España) han introducido esta tecnología en sus sistemas bancarios [2]. |
| Garantía o justificación | Las redes privadas basadas en blockchain tiene las características de descentralización, no manipulación, trazabilidad, alta credibilidad y consenso multipartito que mejoran la seguridad [1]. |
| Respaldo | Las investigaciones realizadas por [2] y [1]. |
| Cualificador modal | Siempre |
| Refutación | Ninguna |

**Argumentación #2**

El uso de la tecnología blockchain contribuye a la gestión y verificación de la identificación digital de manera más segura, debido a que los datos digitales se comparten y se autentican mediante el empleo de técnicas criptográficas, como funciones hash, firmas digitales y pruebas de zero-knowledge [3], estas ventajas han permitido que empresas como BID Lab implementen proyectos para desarrollar una identidad digital para habitantes de barrios vulnerables del Área Metropolitana de Buenos Aires [4] o se desarrollen aplicaciones como uPort y Sovrin que garantizan que la identidad sea soberana, segura, confiable y genérica. A pesar de todas estas ventajas, la mayoría de Gobiernos actualmente aún no implementan esta tecnología como método de verificación digital.

|  |  |
| --- | --- |
| Tesis | El uso de la tecnología blockchain contribuye a la gestión y verificación de la identificación digital de manera más segura. |
| Evidencia | BID Lab, en conjunto con la Asociación Civil para el Desarrollo de Ecosistemas Descentralizados, está implementando un proyecto cuyo objetivo es desarrollar una identidad digital para habitantes de barrios vulnerables del Área Metropolitana de Buenos Aires a través de la tecnología blockchain [4].  La utilización del blockchain para identificar usuarios en un entorno de ciudad inteligente (IOT) [5].  uPort y Sovrin son sistemas de IDM emergente que incorporan varias características que garantizan que la identidad sea soberana, segura, confiable y genérica [6]. |
| Garantía o justificación | Los datos digitales se comparten y se autentican mediante el empleo de técnicas criptográficas, como funciones hash, firmas digitales y pruebas de zero-knowledge (pruebas de conocimiento cero) [3]. |
| Respaldo | Las investigaciones realizadas por [4], [5], [6] Y [3]. |
| Cualificador modal | Probablemente. |
| Refutación | La mayoría de Gobiernos actualmente aún no implementan la tecnología blockchain como método de verificación digital. |

**Argumentación #3**

Los smart contracts aseguran que ciertas acciones ocurran en un marco de un conjunto de condiciones establecidas, permitiendo mitigar el riesgo de estafas en transacciones comerciales, esto se evidencia debido a que el protocolo de smart contract del blockchain fue diseñado pensando en la mitigación de fraudes y estafas ocasionadas por el surgimiento del internet, pero a pesar de esto existen ciertas estafas que no se pueden solucionar con los smart contracts.

|  |  |
| --- | --- |
| Tesis | Los smart Contracts mitigan el riesgo de estafas en transacciones comerciales. |
| Evidencia | El protocolo de smart contract del blockchain fue diseñado pensando en la mitigación de fraudes y estafas ocasionadas por el surgimiento del internet [7]. |
| Garantía o justificación | Aseguran que ciertas acciones ocurran en un marco de un conjunto de condiciones establecidas [8]. |
| Respaldo | Las investigaciones realizadas por [7] y [8]. |
| Cualificador modal | Probablemente |
| Refutación | Existen ciertas estafas que no se solucionan con los smart contracts , pueden existir casos como comprar algún artículo en internet, el vendedor envía el producto pero este no cumple con las expectativas del cliente, se cumple el contrato inteligente pero existe una sensación de estafa por parte del cliente. |

# Bibliografía

|  |  |
| --- | --- |
| [1] | K. Yang, H.-m. Liao, L.-h. Zhao, S.-z. Zheng y H.-w. Li, «Research on network security protection technology of energy industry based on blockchain,» *IEEE/CIC International Conference on Communications in China (ICCC Workshops),* pp. 162-166, 2020. |
| [2] | N. A. Popova y N. G. Butakova, «Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions,» *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus),* pp. 1764-1768, 2019. |
| [3] | H. Gulati y C.-T. Huang, «Self-Sovereign Dynamic Digital Identities based on Blockchain Technology,» *IEEE,* pp. 1-6, 2019. |
| [4] | B. LAB, «Bid Lab,» [En línea]. Available: https://bidlab.org/es. [Último acceso: 30 03 2021]. |
| [5] | R. Rivera, J. G. Robledo, V. M. Larios y J. M. Avalos, «How digital identity on blockchain can contribute in a smart city environment,» *International Smart Cities Conference (ISC2),* pp. 1-4, 2017. |
| [6] | N. Naik y P. Jenkins, «Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems,» *IEEE International Symposium on Systems Engineering (ISSE),* pp. 1-6, 2020. |