

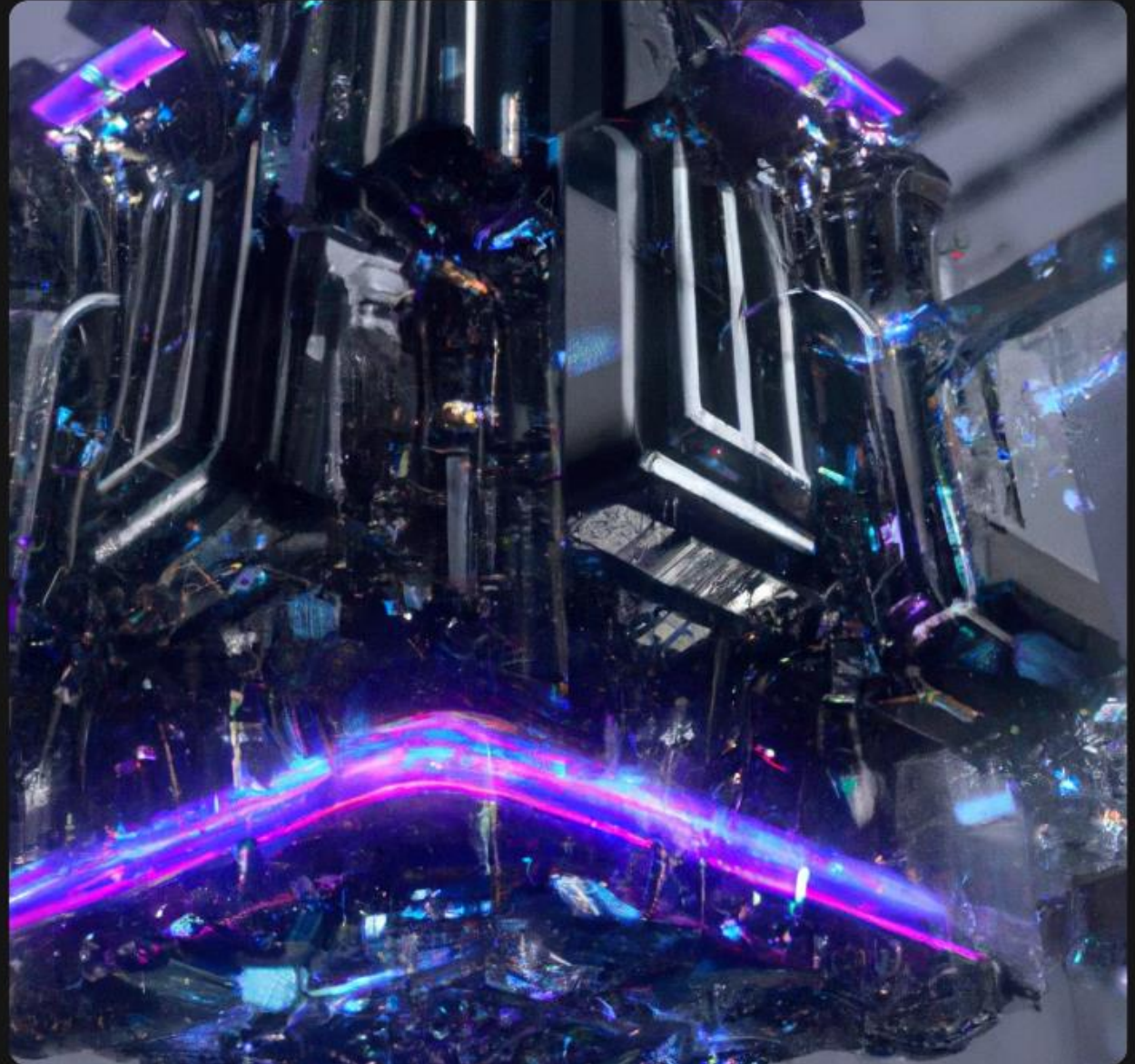
# Contratos inteligentes en la era blockchain: el futuro de la ingeniería en computación



## Introducción

Blockchain es una tecnología que ha revolucionado la forma en que se manejan las transacciones financieras y su aplicación en contratos inteligentes promete ser igual de disruptiva. En esta presentación, abordaremos los aspectos más relevantes de esta tecnología y cómo puede ser aplicada en la ingeniería en computación.

El uso de contratos inteligentes permitirá automatizar procesos y reducir costos en diversos sectores, lo que hace que sea una herramienta muy atractiva para empresas y organizaciones que buscan mejorar su eficiencia y productividad.







## Contexto histórico

La tecnología Blockchain fue creada en 2008 por Satoshi Nakamoto como parte del diseño de la criptomoneda Bitcoin. Desde entonces, ha evolucionado y se ha convertido en una herramienta muy versátil para gestionar transacciones seguras y descentralizadas.

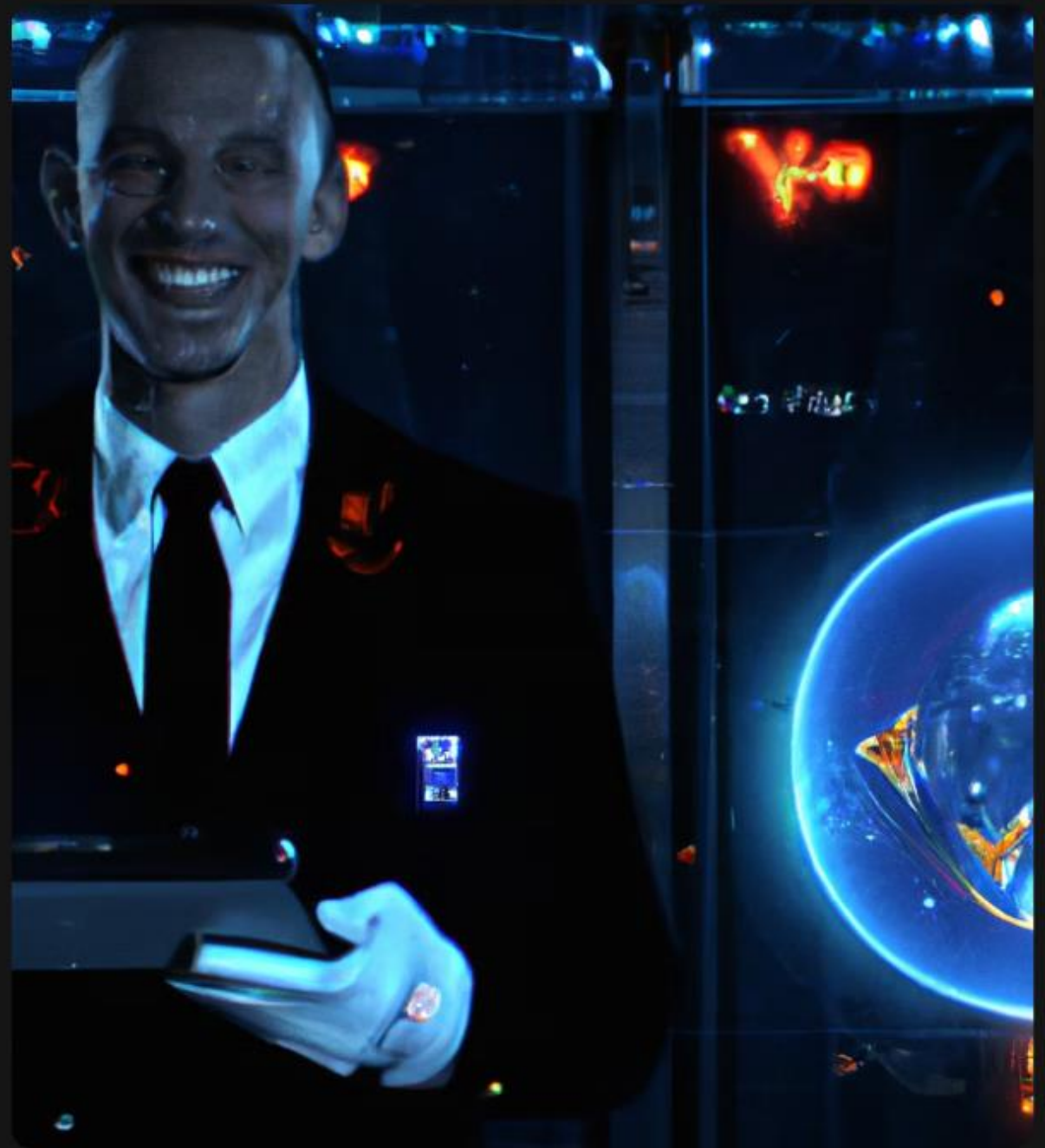
En cuanto a los contratos inteligentes, estos fueron propuestos por primera vez por Nick Szabo en 1994, aunque no fue hasta la creación de Ethereum en 2015 que se hizo posible su implementación en la práctica.



## Contexto actual

Actualmente, la tecnología Blockchain está siendo utilizada en una amplia variedad de sectores, desde finanzas hasta logística y salud. La posibilidad de tener transacciones seguras y transparentes sin necesidad de intermediarios es muy atractiva para muchas empresas.

En cuanto a los contratos inteligentes, ya existen diversas aplicaciones en el mercado, como por ejemplo contratos de alquiler de viviendas o de compra-venta de bienes inmuebles. Sin embargo, aún queda mucho por explorar en este campo y se espera que surjan nuevas formas de utilizar esta tecnología en el futuro.



## Relevancia en el sector de la Ingeniería en Computación

La aplicación de la tecnología Blockchain en la ingeniería en computación tiene un gran potencial. Por un lado, permite la creación de sistemas más seguros y descentralizados, lo que es especialmente importante en el ámbito de la ciberseguridad.

Por otro lado, los contratos inteligentes pueden ser utilizados para automatizar procesos y reducir costos en diversas áreas, como por ejemplo en la gestión de proyectos de software. Además, el uso de esta tecnología puede mejorar la trazabilidad y transparencia de los procesos, lo que es fundamental en cualquier proyecto de ingeniería.





## Relación con el Cómputo Móvil

La relación entre Blockchain y el cómputo móvil se ve fortalecida por la aparición de las dAPPs. Las dAPPs son aplicaciones descentralizadas que utilizan la tecnología Blockchain para su funcionamiento. Estas aplicaciones permiten a los usuarios interactuar directamente en la red, sin necesidad de intermediarios. Además, las dAPPs pueden ser ejecutadas desde dispositivos móviles, lo que permite una mayor accesibilidad y comodidad para los usuarios.

Las dAPPs son cada vez más populares y están siendo utilizadas en diversos ámbitos, como en la gestión de contratos inteligentes o en la creación de mercados descentralizados. Estas aplicaciones ofrecen un alto grado de seguridad y transparencia, gracias a la tecnología Blockchain en la que se basan.





# Contrato inteligente para un token ERC-20 básico

Un contrato inteligente para un token ERC-20 básico es una aplicación de la tecnología blockchain que permite la creación y gestión de tokens digitales. Estos tokens pueden ser utilizados como moneda digital o como representación de activos físicos o virtuales. Además, el contrato inteligente garantiza la seguridad y transparencia en las transacciones realizadas con estos tokens.

El proceso de creación de un contrato inteligente para un token ERC-20 básico implica la definición de los parámetros del token, como su nombre, símbolo, cantidad total, decimal y la dirección del contrato inteligente. Una vez definidos estos parámetros, se puede desplegar el contrato inteligente en la red Ethereum y comenzar a utilizar el token. Este tipo de contrato inteligente es utilizado por muchas empresas y proyectos en la actualidad, lo que demuestra su utilidad

```
// Indica la versión de Solidity que se utilizará para compilar el contrato
pragma solidity ^0.8.0;

// Declaración del contrato
contract Token {
    // Variables públicas del contrato
    string public name; // Nombre del token
    string public symbol; // Símbolo del token
    uint8 public decimals; // Número de decimales del token
    uint256 public totalSupply; // Suministro total del token

    // Mappings (tablas hash) para almacenar balances y aprobaciones
    mapping(address => uint256) public balanceOf; // Balances de los usuarios
    mapping(address => mapping(address => uint256)) public allowance; // Aprobaciones de transferencia de terceros

    // Eventos que se emiten al realizar transferencias o aprobaciones
    event Transfer(address indexed from, address indexed to, uint256 value); // Evento de transferencia
    event Approval(address indexed owner, address indexed spender, uint256 value); // Evento de aprobación

    // Constructor del contrato
    constructor(string memory _name, string memory _symbol, uint8 _decimals, uint256 _totalSupply) {
        name = _name; // Asigna el nombre del token
        symbol = _symbol; // Asigna el símbolo del token
        decimals = _decimals; // Asigna el número de decimales del token
        totalSupply = _totalSupply; // Asigna el suministro total del token
        balanceOf[msg.sender] = totalSupply; // Asigna todo el suministro inicial al creador del contrato
        emit Transfer(address(0), msg.sender, totalSupply); // Emite un evento de transferencia que indica que se ha transferido todo el suministro inicial al creador del contrato
    }

    // Función para transferir tokens a otro usuario
    function transfer(address _to, uint256 _value) public returns (bool success) {
        require(balanceOf[msg.sender] >= _value); // Verifica que el remitente tenga suficientes tokens para la transferencia
        balanceOf[msg.sender] -= _value; // Reduce el balance del remitente
        balanceOf[_to] += _value; // Aumenta el balance del destinatario
        emit Transfer(msg.sender, _to, _value); // Emite evento de transferencia que indica que se ha transferido un cierto número de tokens de un remitente a un destinatario
        return true; // Indica que la transferencia se ha realizado con éxito
    }

    // Función para aprobar la transferencia de tokens a un tercero
    function approve(address _spender, uint256 _value) public returns (bool success) {
        allowance[msg.sender][_spender] = _value; // Asigna una cantidad de tokens que el tercero está autorizado a transferir desde la cuenta del remitente
        emit Approval(msg.sender, _spender, _value); // Emite un evento de aprobación que indica que se ha aprobado una cierta cantidad de tokens para transferirse desde una cuenta del remitente a una cuenta del tercero
        return true; // Indica que la aprobación se ha realizado con éxito
    }
}
```



## Apps y contratos inteligentes

Las apps criptowallet son aplicaciones móviles que permiten a los usuarios almacenar, recibir y enviar criptomonedas de manera segura y eficiente. Estas aplicaciones utilizan tecnología blockchain para garantizar la seguridad y transparencia en las transacciones realizadas con criptomonedas. Además, algunas de estas apps también cuentan con contratos inteligentes integrados, lo que les permite ofrecer servicios adicionales como préstamos, intercambios y pagos programados.

Los contratos inteligentes integrados en las apps criptowallet permiten a los usuarios realizar transacciones de manera automática y sin intermediarios. Estos contratos pueden ser programados para ejecutarse cuando se cumplen ciertas condiciones, lo que aumenta la eficiencia y reduce los costos asociados a las transacciones. Además, la transparencia y la seguridad inherentes a la tecnología blockchain garantizan que todas las transacciones sean registradas de manera inmutable y accesible para todos los participantes de la red.



# Apps y contratos inteligentes



## Trust Wallet

Es una billetera de criptomonedas que permite a los usuarios almacenar, enviar y recibir criptomonedas, incluyendo tokens ERC-20



## Coinbase Wallet

Billetera de criptomonedas que también permite a los usuarios almacenar, enviar y recibir criptomonedas y tokens ERC-20



## MetaMask

Es una extensión de navegador web que permite a los usuarios interactuar con la blockchain de Ethereum y sus contratos inteligentes.



## MyEtherWallet

Es una billetera de criptomonedas que permite manipular y gestionar



## Prospectiva y Conclusiones

La tecnología Blockchain y los contratos inteligentes tienen un gran potencial para transformar diversos sectores, incluyendo la ingeniería en computación. Se espera que en el futuro surjan nuevas aplicaciones y usos para esta tecnología, lo que permitirá mejorar la eficiencia y transparencia en diversos procesos.

Sin embargo, también es importante tener en cuenta los desafíos que presenta esta tecnología, como por ejemplo la necesidad de una regulación adecuada y la protección de datos personales. A medida que la tecnología evolucione, será necesario seguir trabajando en estos aspectos para asegurar su correcto funcionamiento y beneficios para la sociedad en general.

