Informe sobre Contratos Inteligentes y Diseño de un Sistema de Votación en Blockchain

# 1. Introducción a los Contratos Inteligentes

Los contratos inteligentes (smart contracts) son programas informáticos que se ejecutan en una blockchain y que permiten la automatización de acuerdos sin necesidad de intermediarios. Su comportamiento está definido por código, lo que asegura que las condiciones establecidas se cumplan de manera transparente, segura e inmutable. Gracias a su diseño descentralizado, los contratos inteligentes reducen los costos, aumentan la confianza entre las partes y ofrecen nuevas posibilidades de aplicación en múltiples sectores como finanzas, logística, salud, y votaciones electrónicas.

# 2. Propósito de los Contratos Inteligentes y de un Sistema de Votación

El propósito de los contratos inteligentes es garantizar la ejecución automática de acuerdos predefinidos sin posibilidad de manipulación externa. En el caso particular de un sistema de votación, el objetivo es:  
  
- Garantizar transparencia en el proceso electoral.  
- Evitar fraudes o manipulaciones.  
- Permitir que los resultados sean verificables públicamente.  
- Reducir la dependencia de autoridades centrales en el recuento de votos.  
  
Un sistema de votación basado en contratos inteligentes permite que cada voto sea registrado de forma única e inmutable en la blockchain, ofreciendo así mayor seguridad y confianza en el proceso electoral.

# 3. Diseño de la Lógica del Contrato

El contrato inteligente de votación sigue una lógica sencilla:  
  
1. El administrador crea el contrato y registra las opciones de votación.  
2. Los usuarios autorizados pueden emitir un voto único.  
3. Cada voto se registra en la blockchain de manera inmutable.  
4. Al finalizar el proceso, se pueden consultar los resultados de manera transparente.

# 4. Diagrama de Flujo del Contrato

El flujo del contrato inteligente puede representarse de la siguiente manera:  
  
- Inicio → Creación del contrato por el administrador → Registro de candidatos u opciones.  
- Votante autorizado → Emisión de voto → Registro en blockchain.  
- Verificación de voto único (el contrato valida que un votante no pueda votar más de una vez).  
- Conteo de votos → Consulta de resultados.  
- Fin del proceso electoral.

# 5. Programación en Solidity

A continuación, se presenta un ejemplo básico de contrato inteligente en Solidity para un sistema de votación simple, programable en Remix IDE:

// SPDX-License-Identifier: MIT  
pragma solidity ^0.8.0;  
  
contract Voting {  
 address public admin;  
 mapping(address => bool) public hasVoted;  
 mapping(string => uint256) public votes;  
 string[] public candidates;  
  
 constructor(string[] memory \_candidates) {  
 admin = msg.sender;  
 candidates = \_candidates;  
 }  
  
 function vote(string memory candidate) public {  
 require(!hasVoted[msg.sender], "Ya has votado.");  
 bool validCandidate = false;  
 for (uint i = 0; i < candidates.length; i++) {  
 if (keccak256(bytes(candidates[i])) == keccak256(bytes(candidate))) {  
 validCandidate = true;  
 break;  
 }  
 }  
 require(validCandidate, "Candidato invalido.");  
 hasVoted[msg.sender] = true;  
 votes[candidate]++;  
 }  
  
 function getVotes(string memory candidate) public view returns (uint256) {  
 return votes[candidate];  
 }  
  
 function getCandidates() public view returns (string[] memory) {  
 return candidates;  
 }  
}

# 6. Informe Manual y Conclusión

Este contrato inteligente de votación representa un ejemplo funcional y sencillo de cómo implementar procesos electorales transparentes sobre blockchain. Su propósito es mostrar que mediante el uso de Solidity y una plataforma como Remix IDE, es posible diseñar y desplegar contratos que automaticen procesos con seguridad, inmutabilidad y transparencia.  
  
El sistema presentado cumple los siguientes objetivos:  
- Automatizar la votación sin intermediarios.  
- Garantizar un voto único por persona.  
- Registrar los votos en la blockchain para asegurar su inmutabilidad.  
- Permitir una consulta pública y verificable de resultados.  
  
Este tipo de soluciones sientan las bases para una mayor confianza en procesos de gobernanza digital.