1 **CÁNDIDO CABALLERO-GIL,**

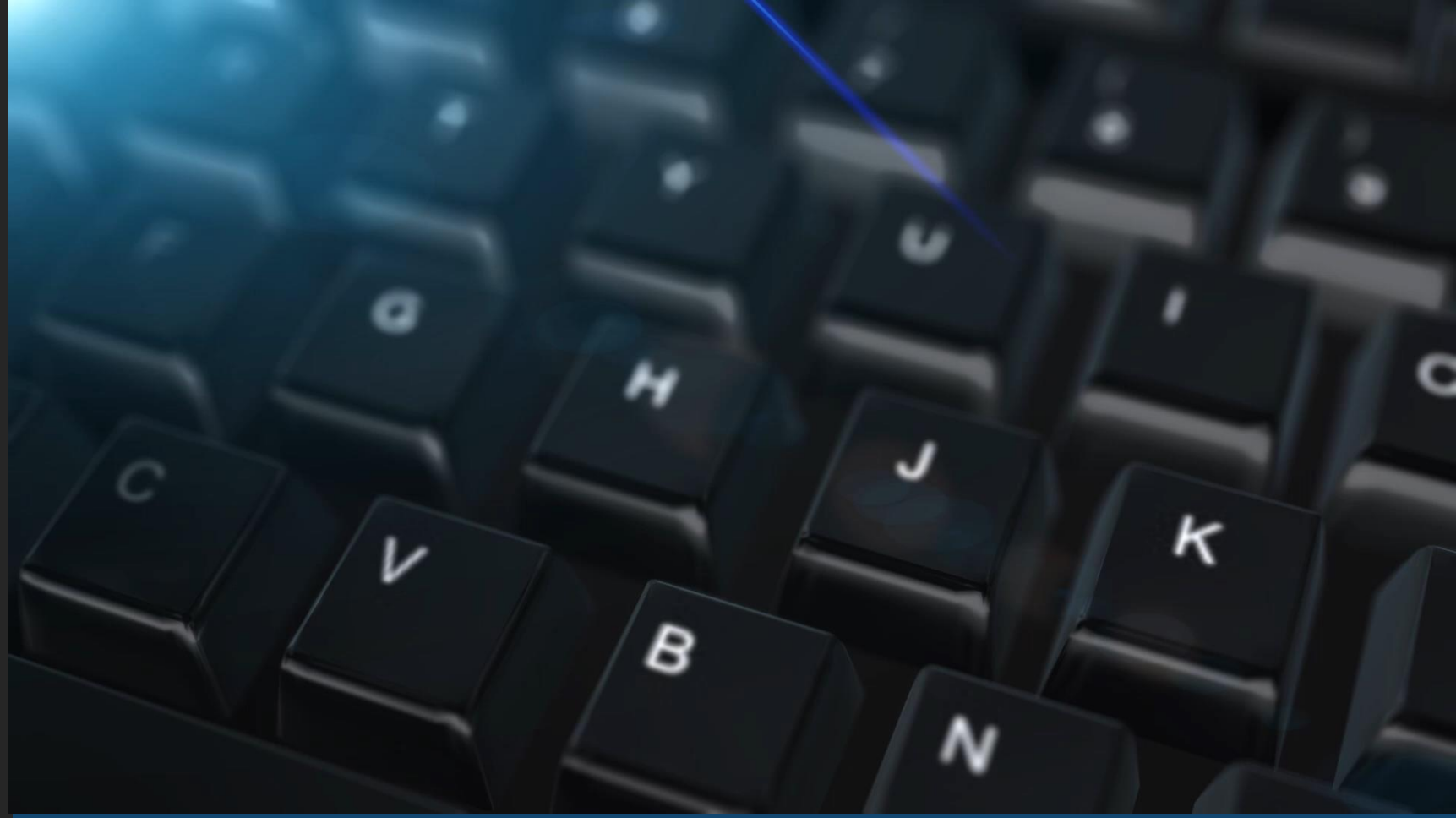
1 PINO CABALLERO-GIL,

1 NÉSTOR ALVAREZ-DIAZ,

2 **MOTI YUNG**

1 UNIVERSITY OF LA LAGUNA, TENERIFE, SPAIN

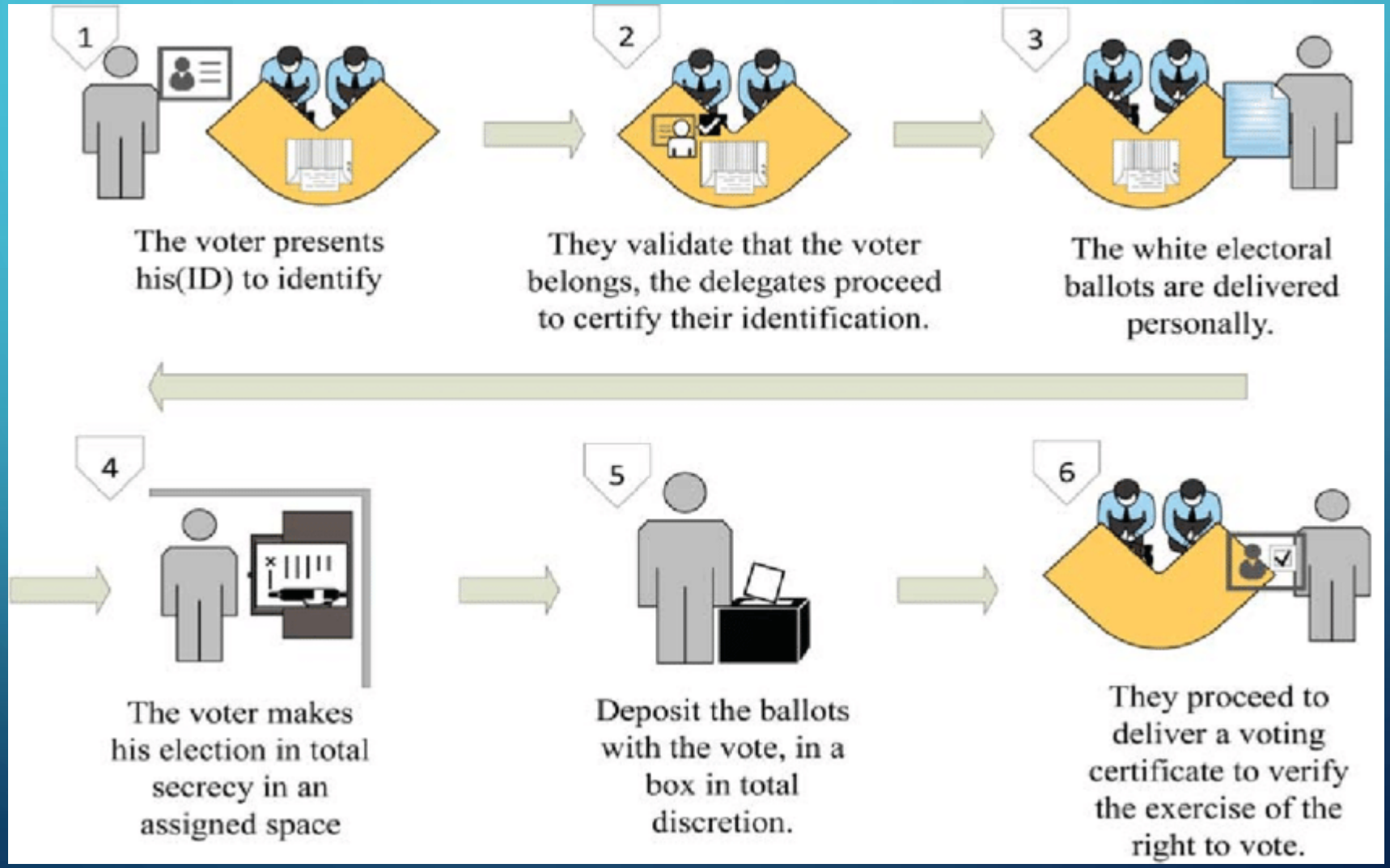
2 UNIVERSITY OF COLUMBIA, NEW YORK, USA



SISTEMA DE VOTACIÓN ELECTRÓNICA BASADO EN BLOCKCHAIN CON ENCRIPTACIÓN HOMOMÓRFICA

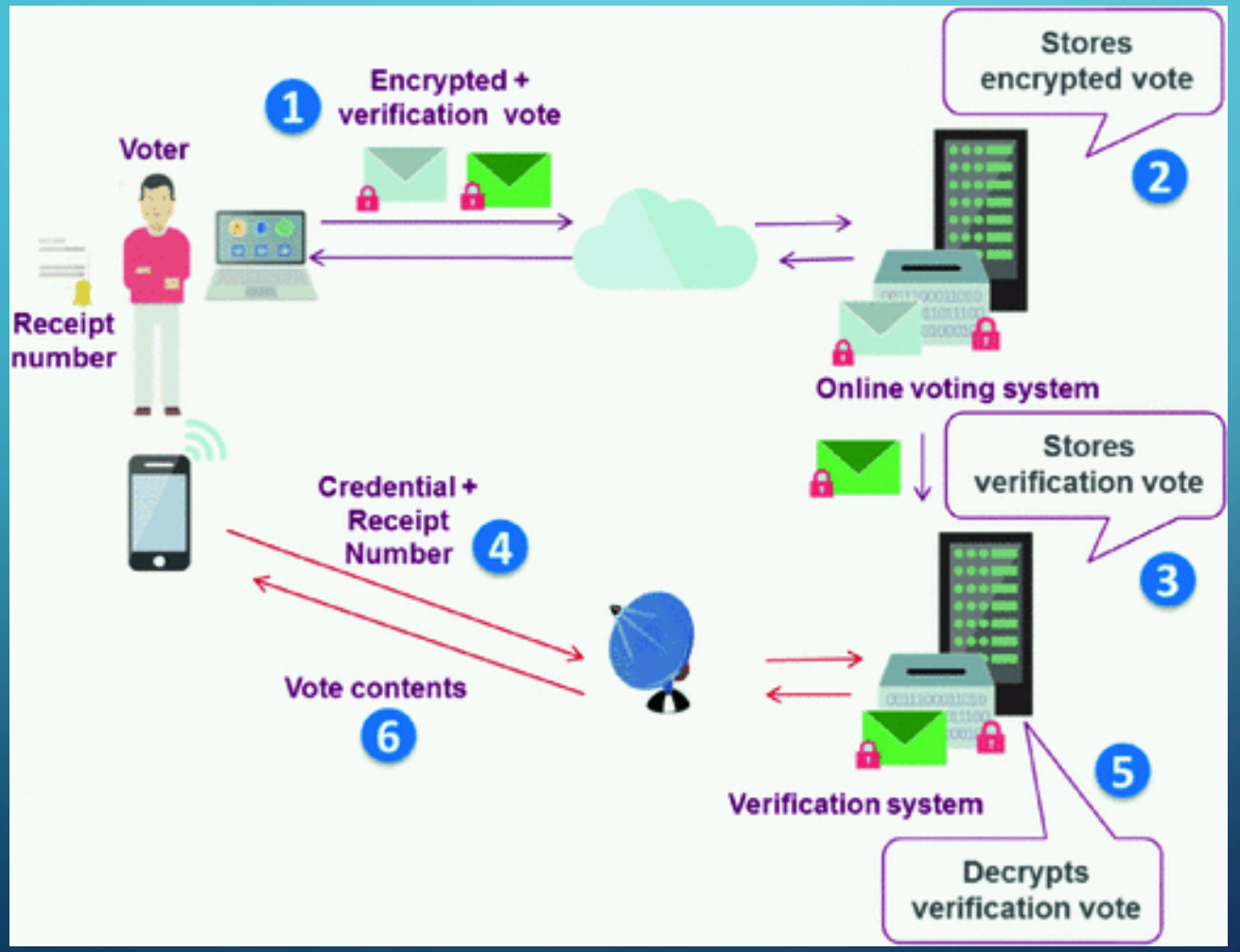

BlockVote
Create simple and secure elections
SIGN IN
REGISTER

PROCESO DE VOTACIÓN EN PERSONA



Fuente: Traditional voting process a) The voter is present at his board of the... | Download Scientific Diagram (researchgate.net)

PROCESO DE VOTACIÓN ONLINE



- Fuente: Verifiability Experiences in Government Online Voting Systems | SpringerLink

INTRODUCCIÓN A APLICACIONES DESCENTRALIZADAS

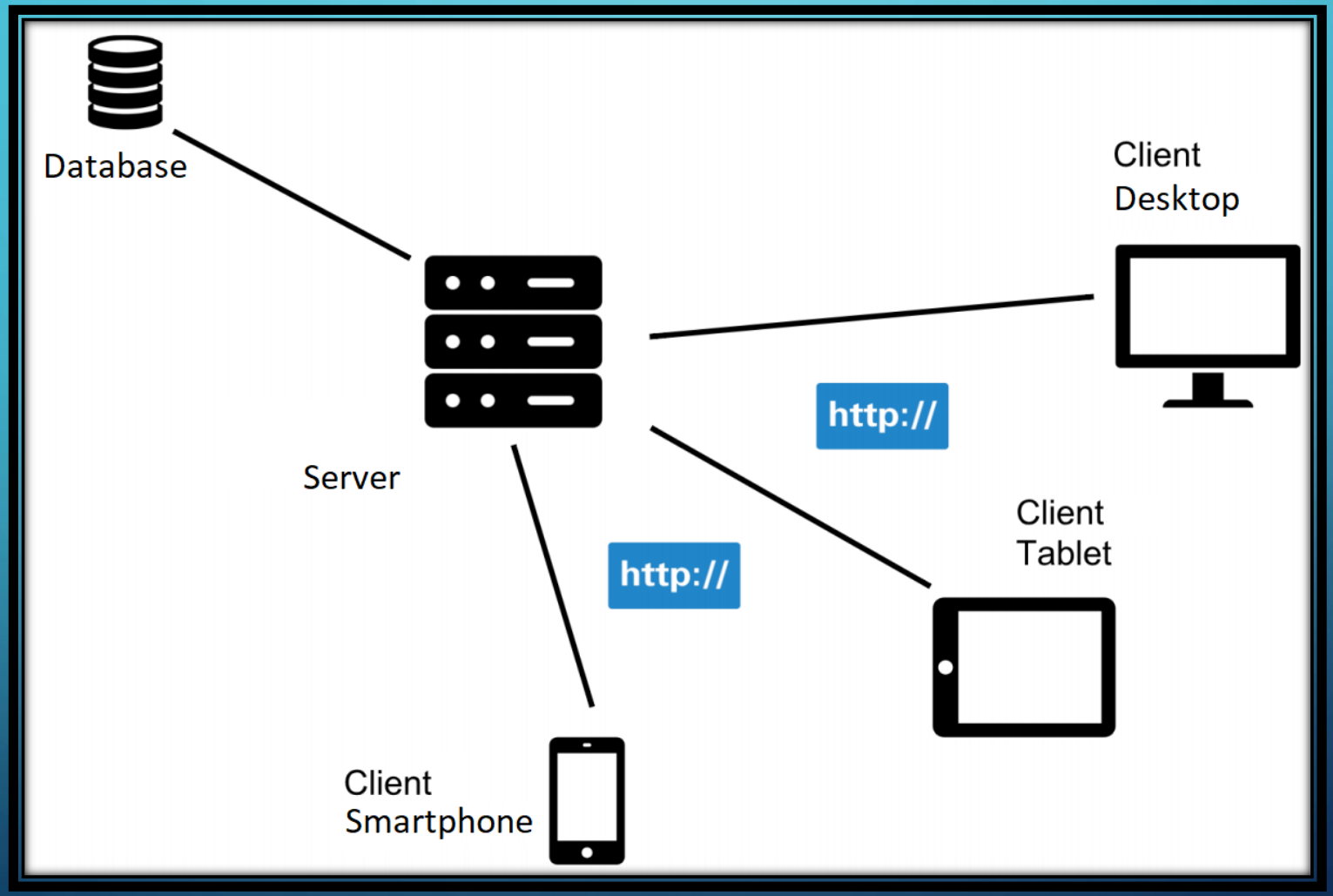


Figura: Esquema de Aplicación Centralizada

Qué es una aplicación descentralizada?

Aplicación que reemplaza el back-end con contratos inteligentes y la base de datos con la Blockchain.

Ethereum clasifica las DApps en tres clases:

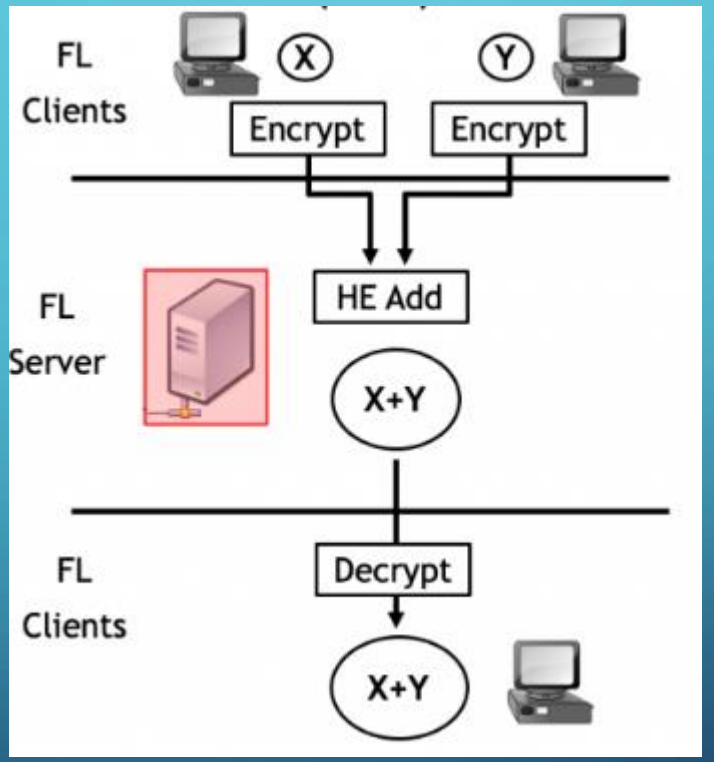
1. Aplicaciones que **gestionan dinero**.
2. Aplicaciones en las cuales hay dinero involucrado
3. **Otras. Votación,** Gobierno, etc.

Nota

Aplicaciones Descentralizadas pueden requerir ficheros estáticos o Bases de Datos tradicionales.

CIFRADO HOMOMÓRFICO

- El cifrado Homomorfico es una forma de cifrado con una capacidad adicional de evaluación para la computación sobre datos encriptados sin acceso a la clave secreta. El resultado de dicha computacion permanence cifrado.

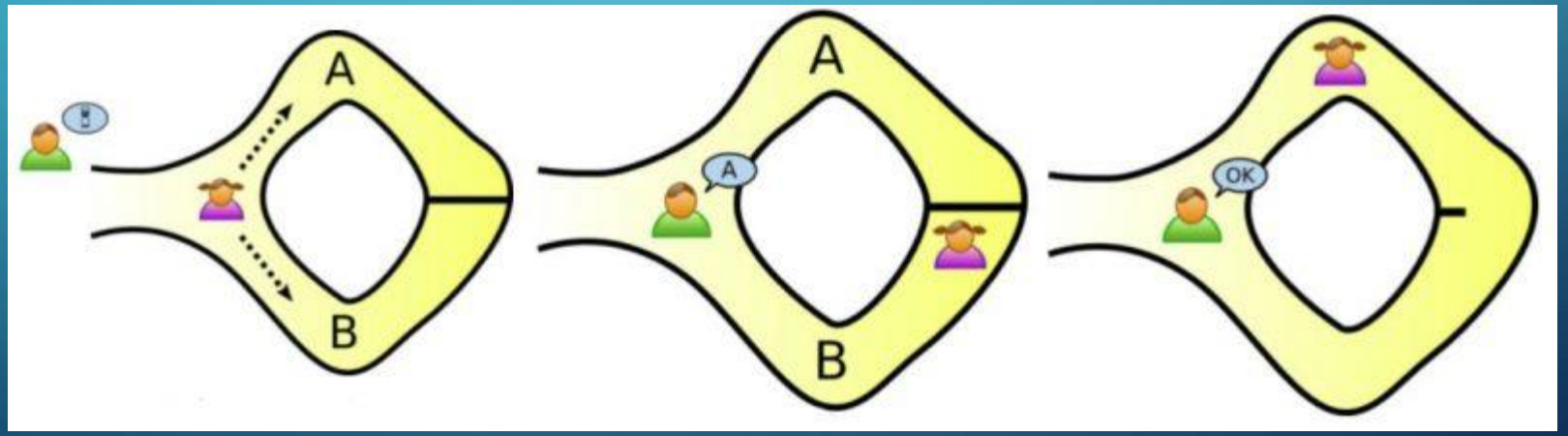


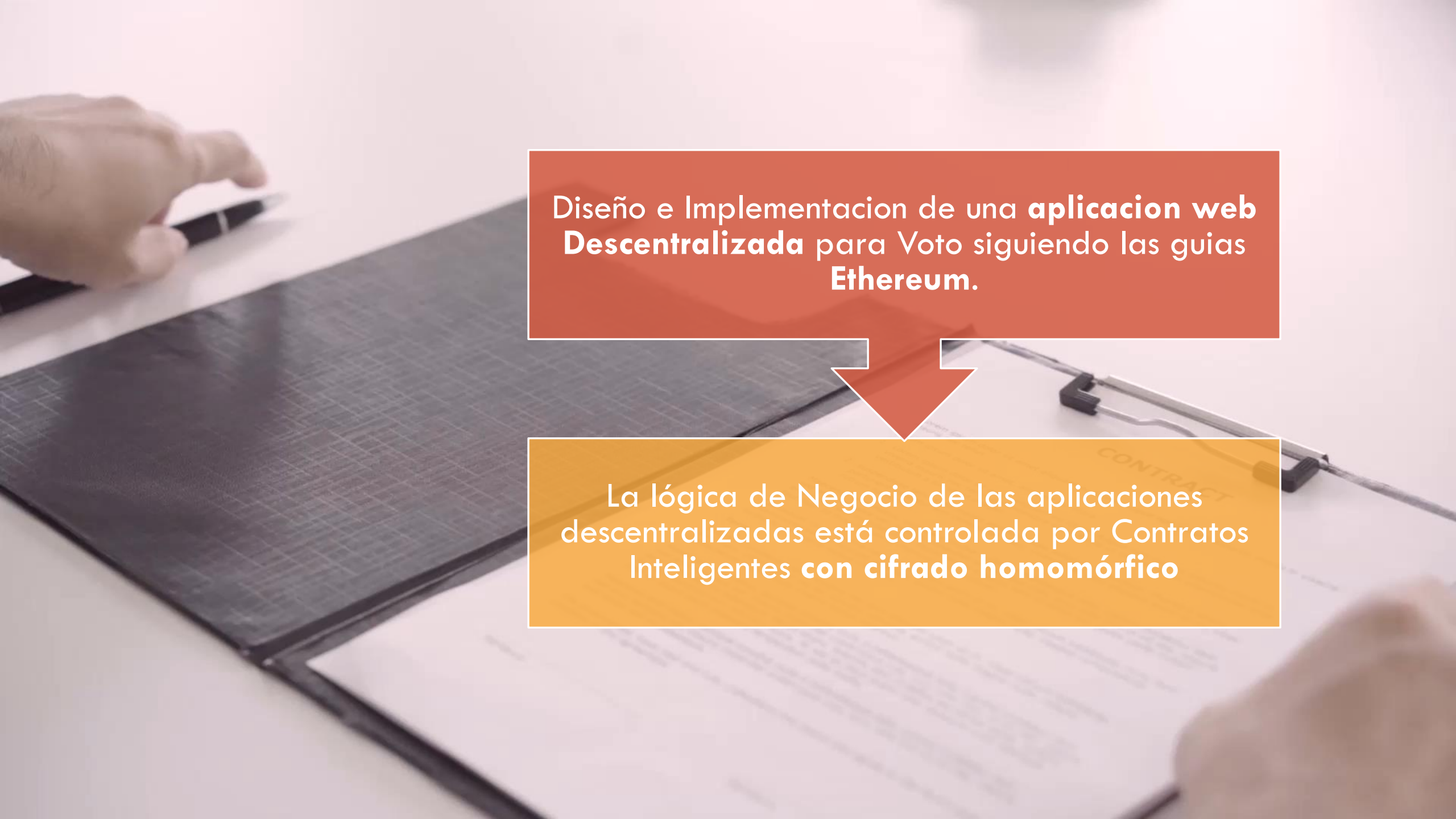
Dados dos mensajes, m1 y m2, existe una operación que satisface E(m1 + m2) = E(m1) ◦ E(m2) donde ◦ denota la función homomórfica, la cual representa una suma homomórfica en este esquema particular HE y E(), denota la función de cifrado.

Federated Learning with Homomorphic Encryption | NVIDIA Technical Blog

PRUEBAS DE CONOCIMIENTO ZERO

- La idea detrás de las **ZKP** es que un Usuario puede probar a otro usuario que conoce un valor absoluto sin realmente revelar ninguna otra información extra.

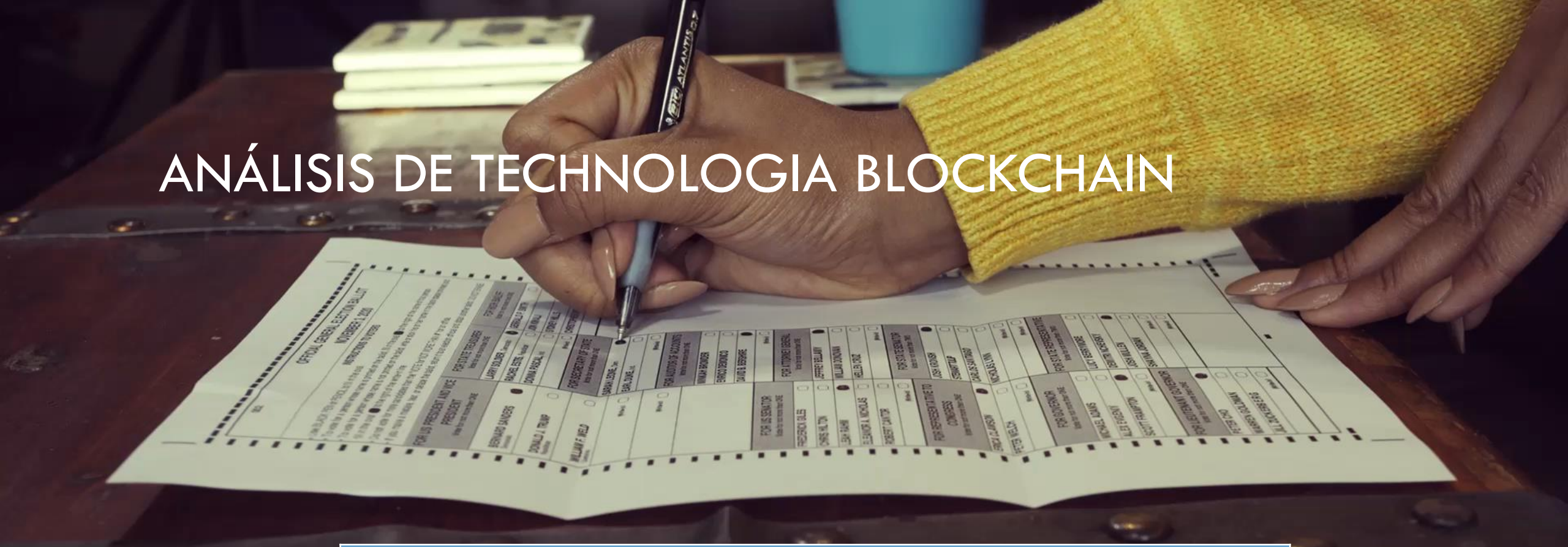




Diseño e Implementacion de una **aplicacion web Descentralizada** para Voto siguiendo las guias **Ethereum.**

La lógica de Negocio de las aplicaciones descentralizadas está controlada por Contratos Inteligentes **con cifrado homomórfico**

ANÁLISIS DE TECHNOLOGIA BLOCKCHAIN



Contrato Inteligente

- Programa que sella un pacto o acuerdo.
- Independiente
- Automático
- Escrito en Solidity (basado en C ++ / JavaScript)
- Características propias de Ethereum.

DESARROLLO DE APLICACIÓN DESCENTRALIZADA I

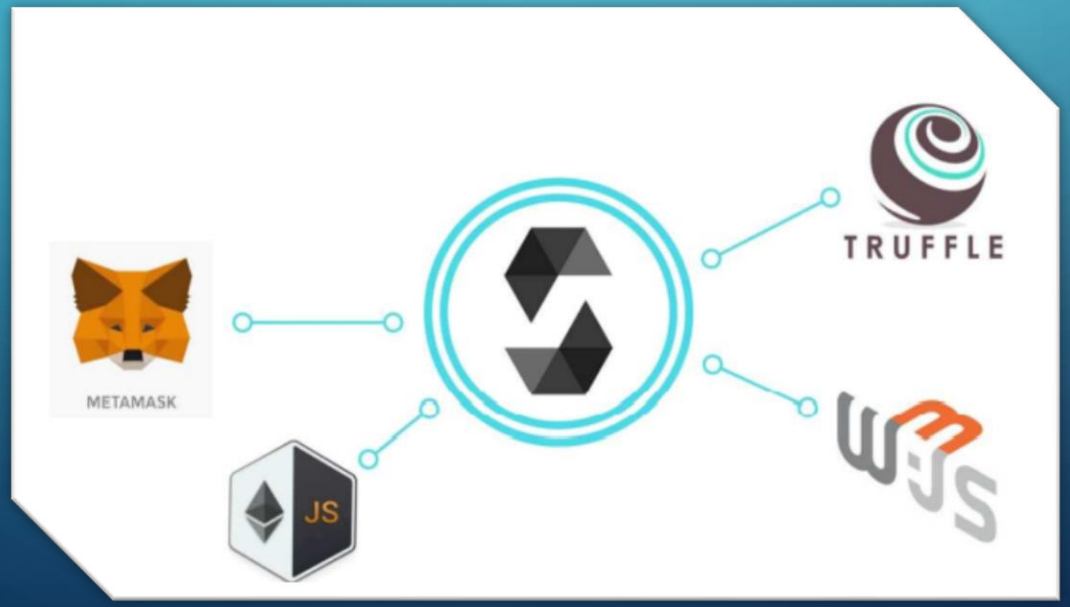
Para el desarrollo de Aplicaciones Descentralizadas DApp:

- JavaScript y Solidity para la creación de contratos inteligentes.
- Librería Web3 JavaScript para interactuar con contratos.
- Frameworks como Truffle o Embark para trabajar con Ethereum.
- Navegador propio de Ethereum como Mist o extensiones en los navegadores habituales como Metamask.

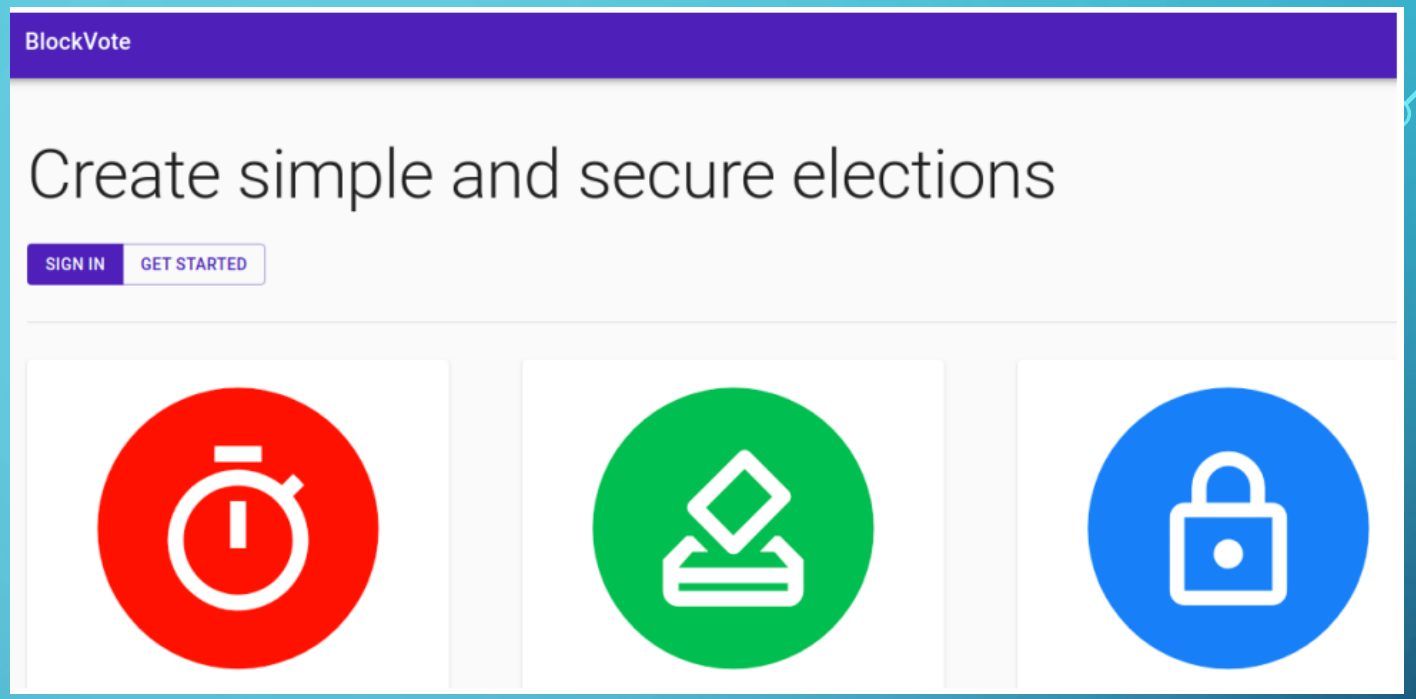
SISTEMA DE VOTACIÓN I

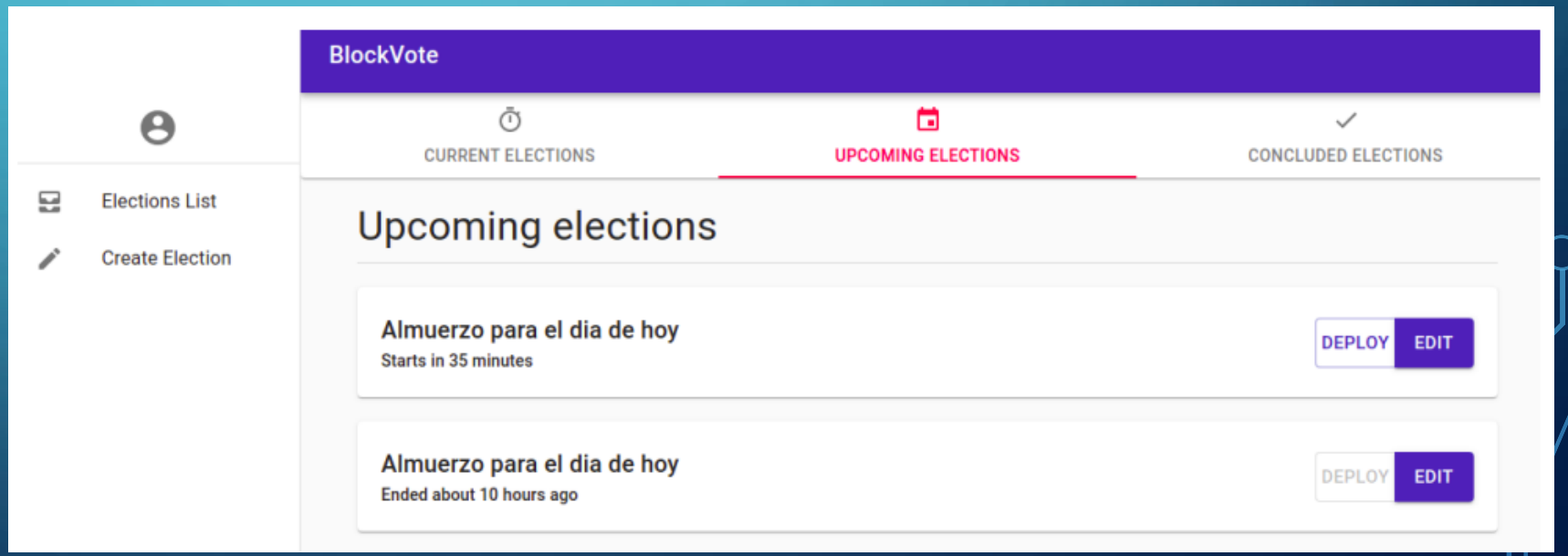
Aplicación web Descentralizada para sistemas de votación

- Cubre el proceso completo de sistemas de votación gracias a los contratos inteligentes.
- Usuarios pueden crear elecciones, Votar si están en el censo, comprobar su participación y ver los resultados de la elección.
- Dos contratos Inteligentes, uno para la creación de la elección y otro para verificar la autenticidad del Usuario, censo y voto.



INTERFAZ


BlockVote
Create simple and secure elections
SIGN IN
GET STARTED


BlockVote
CURRENT ELECTIONS
UPCOMING ELECTIONS
CONCLUDED ELECTIONS
Elections List
Create Election
Upcoming elections
Almuerzo para el dia de hoy
Starts in 35 minutes
DEPLOY
EDIT
Almuerzo para el dia de hoy
Ended about 10 hours ago
DEPLOY
EDIT

SISTEMA DE VOTACIÓN II

Características
• Diseñado siguiendo el modelo SPA (Single Page Application) gracias a VueJS • Base de datos Local para almacenar información usando MongoDB • Convierte Ether – Euros y Euros - Ether • Cambios Dinámicos en el SPA son tratados con VueX

TESTS Y RESULTADOS

Ventajas

- No tiene registro de usuario.
- Pasarela de Pago (POS) o extensiones Paypal.
- Usa el token Ethereum.
- No es una comunidad.

- Truffle incluye testeo de aplicaciones.
- Todas las funciones del contrato inteligente son cubiertas para chequear si la operación es correcta.

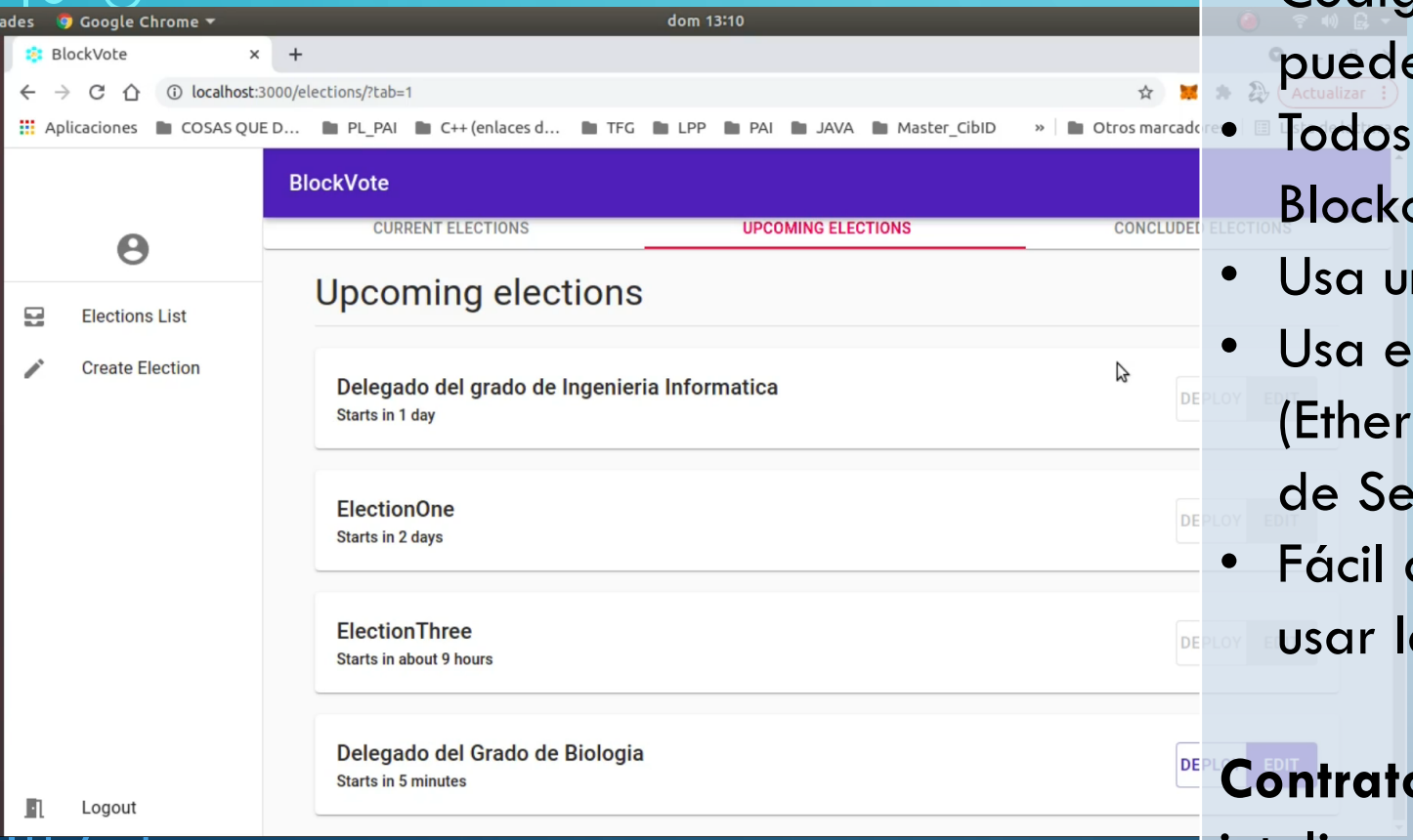
Nota

- El Sistema de Voto está en una red de pruebas.

SEGURIDAD

- Los beneficios principales en términos de ciberseguridad gracias a la tecnología Blockchain son:
  - No hay base de datos ➡ no información vulnerable.
  - Descentralizada ➡ inmune a ataques DDoS.
  - No es posible modificar la Blockchain para alterar los datos de la aplicación.
  - Sin pasarela de pago ➡ es muy difícil robar criptomonedas de billeteras.
  - No hay suplantación de identidad de terceras partes de confianza.

Un Sistema de Votación Electrónica ha sido desarrollado siguiendo los siguientes standards



- Código abierto y ni la empresa/gobierno puede controlar los tokens
- Todos los datos son almacenados en un Sistema Blockchain descentralizado basado en Ethereum
- Usa un token criptográfico
- Usa el algoritmo prueba de participación (Ethereum II completo “the merge” desde el 15 de Septiembre)
- Fácil de crear nuevas encuestas/votaciones y usar la aplicación

Contratos Inteligentes dan a la app autonomía e inteligencia. Están a cargo de la plataforma de voto

Trabajos Futuros

- Buscar un proceso válido de cifrado homomórfico e implementarlo con Smart-contracts con Solidity
- Lanzarlo en la red Ethereum real, o hacer una simulación realista para comprobar costes, y tiempos para completarse las transacciones.
- Hacer el sistema más flexible, que permita diferente tipo de votaciones.
- …