



UniBlock

Elecciones de manera segura y transparente.

4 de Julio del 2025



Índice

- 01** Contexto
- 02** Problema
- 03** Solución
- 04** Arquitectura
- 05** ¿Sistema Distribuido?
- 06** Escalamiento y Sincronización
- 07** Seguridad
- 08** Protocolos de Comunicación
- 09** Blockchain



Contexto

Los sistemas de votación tradicionales presentan:

- Falta de transparencia
- Riesgo de fraude
- Altos costos logísticos

En el contexto universitario, el uso de herramientas como Google Forms no garantiza:

- La autenticidad del votante
- Ni la integridad del proceso

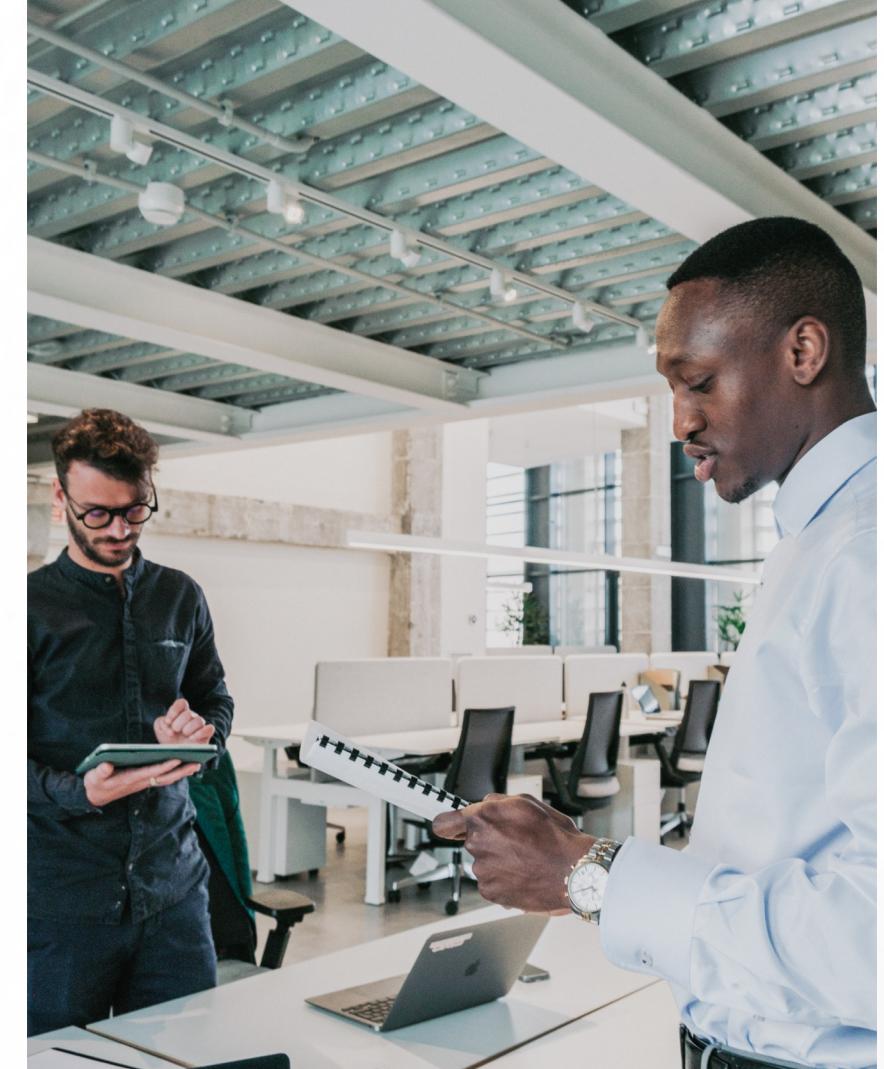
Para solucionar esto, se propone un sistema distribuido de votación electrónica, basado en tecnología blockchain, que garantice:

- Seguridad e inmutabilidad de los votos
- Transparencia total
- Verificabilidad y participación confiable

Problema

Los sistemas de votación actuales enfrentan serias limitaciones que afectan la confianza y eficacia del proceso electoral estudiantil:

- **Falta de transparencia:** Los estudiantes no pueden verificar que su voto fue correctamente registrado.
- **Riesgo de manipulación:** Con herramientas como Google Forms, los resultados pueden ser modificados sin dejar rastro.
- **Verificación compleja:** No hay mecanismos claros para auditar el proceso ni validar la identidad de los votantes.
- **Baja participación:** Procesos poco confiables y desorganizados reducen la motivación estudiantil para votar.
- **Riesgos de suplantación:** Es difícil asegurar que quien vota sea realmente estudiante de la universidad.



Solución

Se propone un sistema de votación electrónica distribuida, basado en una blockchain privada, accesible solo para miembros de la universidad autenticados con su correo institucional.

INMUTABILIDAD Y TRANSPARENCIA

Cada voto queda registrado de forma segura y verificable, sin posibilidad de alteración.

ACCESO RESTRINGIDO

Solo estudiantes y miembros validados institucionalmente pueden participar.

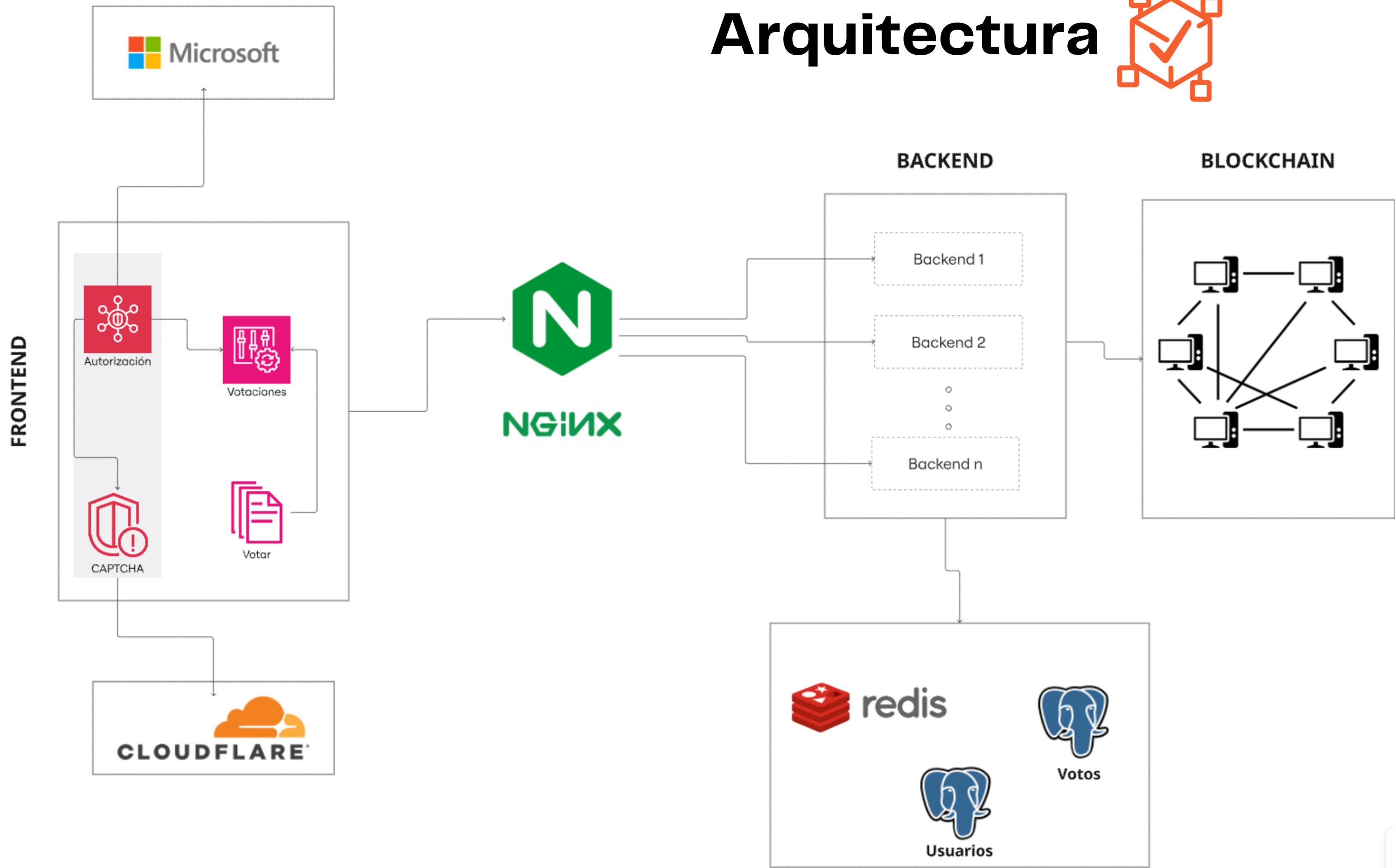
SUPERVISIÓN EN TIEMPO REAL

Los resultados pueden auditarse durante el proceso sin comprometer la privacidad.

EFICIENCIA DIGITAL

Elimina papeletas, filas y logística física, facilitando una participación más ágil y masiva.

Arquitectura





¿Sistema Distribuido?

Nuestro sistema de votación es distribuido porque:

-  No depende de un solo servidor o entidad central.
-  Las votaciones se almacenan como bloques en una blockchain, permitiendo que múltiples nodos verifiquen su validez.
-  Esto reduce riesgos de manipulación, mejora la confiabilidad y fortalece la transparencia del proceso.
-  Varias bases de datos separadas (una para usuarios, otra para votos, otra para OTP).

```
{  
    "index": 0,  
    "timestamp": "2025-06-30T23:20:05.425Z",  
    "idVotacion": "GENESIS",  
    "votos": [],  
    "hashAnterior": "0",  
    "publicKey": "-----BEGIN RSA PUBLIC KEY-----\nMIIBCgKCAQEAiA  
    "hashPropio": "49006cc70474b4e7a850a50a3eda8f6e6eeaa76fedc0:  
    "firmaDigital": "45de85d1ca635e7c6e5bba2e90982dc59953d62dce:  
},  
{  
    "index": 1,  
    "timestamp": "2025-06-30T23:21:05.012Z",  
    "idVotacion": "1f355854-0c5a-4105-89b9-36fabd9df7f9",  
    "votos": [  
        {  
            "votation_id": "1f355854-0c5a-4105-89b9-36fabd9df7f9",  
            "candidate_id": "11",  
            "timestamp": "2025-06-30T18:09:18.242Z",  
            "firma": "YKTBDxPF9XiqBUTRIa/Mbfs+fYMUzPvQxYa3ljj96DdlTI:  
            "public_key": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqI  
        },  
        {  
            "votation_id": "1f355854-0c5a-4105-89b9-36fabd9df7f9",  
            "candidate_id": "11",  
            "timestamp": "2025-06-30T18:12:44.899Z",  
            "firma": "W3z3dTf4dgs1me9p4R9N7yE4fqU3t00FV6ZBK1MJ0Rh24:  
            "public_key": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqI  
        }  
    ],  
    "hashAnterior": "49006cc70474b4e7a850a50a3eda8f6e6eeaa76fedc0:  
    "publicKey": "-----BEGIN RSA PUBLIC KEY-----\nMIIBCgKCAQEAiA  
    "hashPropio": "2f1c6df8b4485ba25f4c48c353cf31969f3089b619bc:  
    "firmaDigital": "7b71922f352f2329f650e5cb24cf5944cb1100b764:  
}
```

¿Como funciona la votación?

- Durante el periodo de votación, los votos se guardan en una base de datos segura.
- Al finalizar el tiempo de la votación, todos los votos se agrupan y se almacenan en la blockchain privada como un único bloque inmutable.
- Esta estructura permite auditar los votos sin comprometer la identidad del votante.

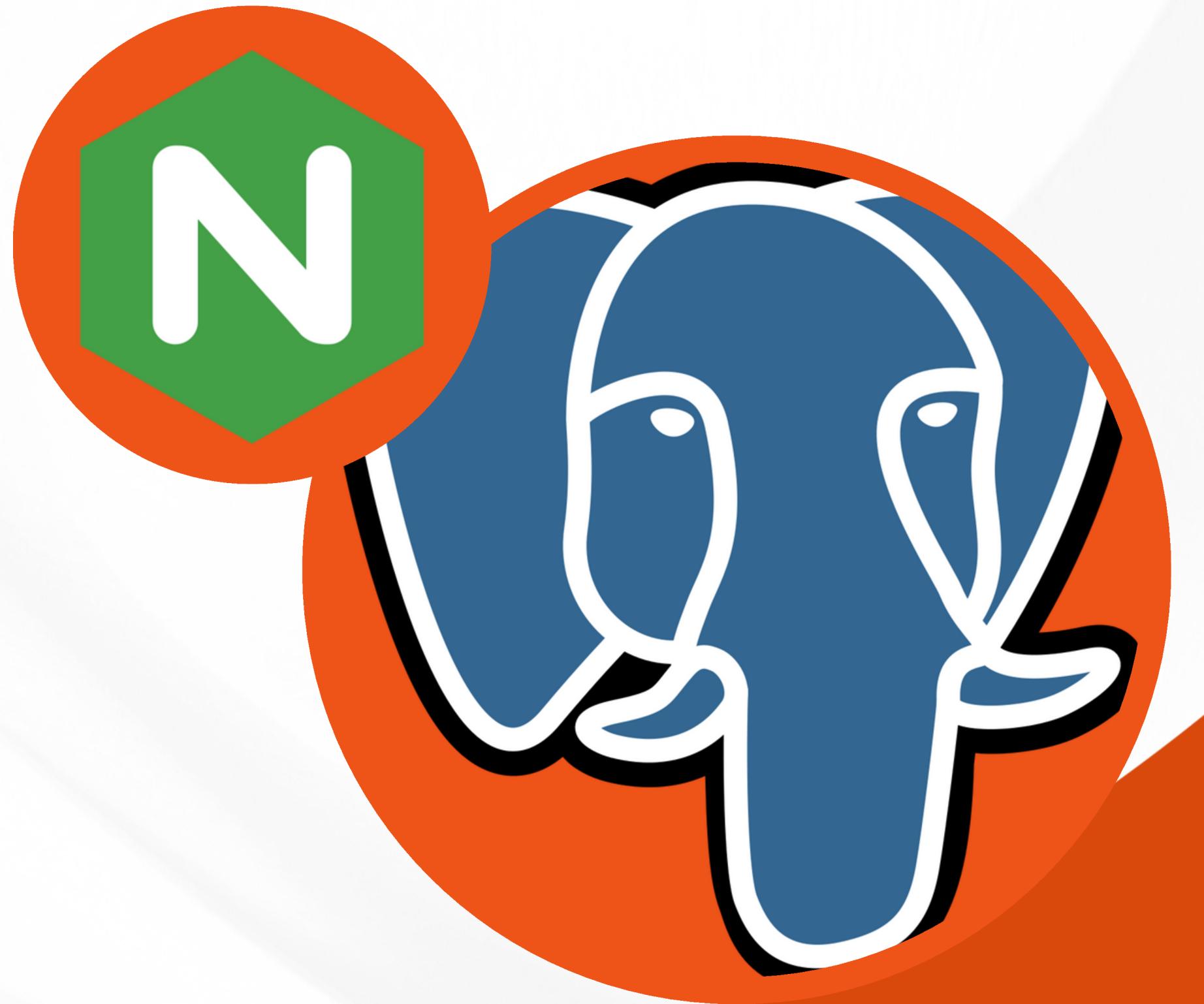
Escalamiento

Escalable horizontalmente:

Se puede añadir más instancias de backend y configurar Nginx para balancear el tráfico entre ellas, usando round-robin

Bases de datos:

- Base de datos de usuarios
- Base de datos de votos
- Base de datos para verificación





Seguridad

Microsoft Azure es la plataforma en la nube de Microsoft que ofrece servicios como Azure Active Directory para gestionar identidades y autenticación, permitiendo integrar fácilmente el login de Microsoft en aplicaciones sin manejar contraseñas directamente.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Buscar recursos, servicios y documentos (G+/-)". Below the header, the breadcrumb navigation shows "Inicio > UniBlock". The main title is "UniBlock | Autenticación". On the left, there's a sidebar with icons for "Información general", "Inicio rápido", "Asistente para integración", and "Diagnosticar y solucionar problemas". The main content area has a search bar and a comment section asking if there are any comments. Below that, it lists "Tipos de cuenta compatibles" with two options: "Solo cuentas de este directorio organizativo (solo de Universidad Austral de Chile: inquilino único)" (selected) and "Cuentas en cualquier directorio organizativo (cualquier inquilino de id. de Microsoft Entra - multiinquilino)". At the bottom, there's a large button with the Microsoft logo and the text "Continuar con cuenta Microsoft UACH".



Seguridad

Cloudflare es una plataforma en la nube que protege y optimiza sitios web, ofreciendo servicios como firewall, CDN y mitigación de ataques. Usamos su servicio de captcha para verificar que los usuarios que ingresan a la aplicación son humanos y así prevenir accesos automatizados o maliciosos.

a@gmail.com's Account

Go to... ctrl + K

Support ▾

+ Add ▾

English ▾



Turnstile

Overview

Turnstile can be embedded into any website without sending traffic through Cloudflare and works without showing visitors a CAPTCHA

[Turnstile documentation](#)

Turnstile widgets

[+ Add widget](#)

Search...

Search

Show filters

Widget Name	Number of hostnames	Likely human <small> ⓘ</small>	Widget Mode	Pre-Clearance	
uniblock 0x4AAAAAAvVVMaEmNpS814	1	50%	Managed	No pre-clearance	View analytics



¡Operación exitosa!



Seguridad

Implementamos un sistema **OTP (One-Time Password)** que envía un código de verificación al correo del usuario que desea registrarse. Esto asegura que solo usuarios con acceso al correo puedan completar el proceso de registro. Usamos su servicio de captcha para verificar que los usuarios que ingresan a la aplicación son humanos y así prevenir accesos automatizados o maliciosos.

Ingrresa tu nombre

Luis Veas

Correo electrónico

felipe.cordova@alumnos.uach.cl

¡El OTP ha sido enviado al correo!

Código OTP

Verificar OTP

¡Hola!

Tu código de verificación es:

65833

Válido por 5 minutos.

Ingresa tu nombre

Luis Veas

Correo electrónico

felipe.cordova@alumnos.uach.cl

OTP verificado exitosamente.

Contraseña



¡Operación exitosa!

Protocolos de Comunicación

01

HTTP/HTTPS

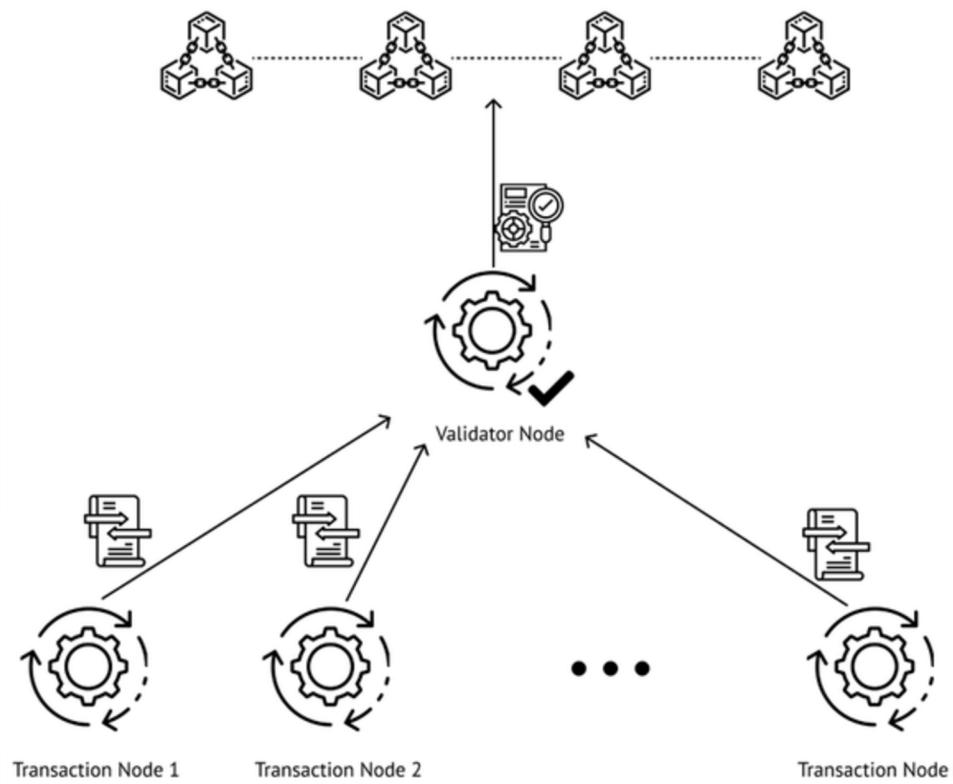
02

RESP (REdis Serialization Protocol)
PostgreSQL Wire Protocol

03

SMTP (Simple Mail Transfer Protocol)

Mecanismo de consenso de la Blockchain: POA



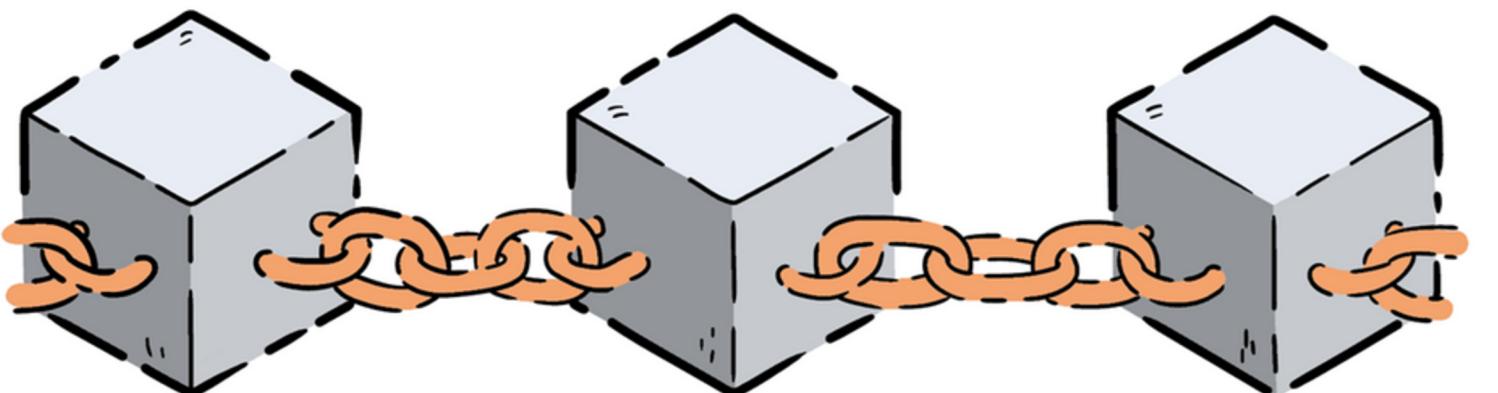
Solo nodos validadores autorizados pueden agregar bloques con votos.

No usamos minería ni prueba de trabajo , por lo cual el sistema es más eficiente y rápido.

Los validadores están definidos previamente, lo que garantiza que la institución a cargo controla quienes participan

Que contiene cada bloque?

Cada bloque representa una votación completa enviados desde el backend, firmados por el nodo validador para prevenir fraudes y asegurarnos de que ningún dato sea modificado



Cada bloque contiene:

index

timestamp

idVotacion

votos

hashAnterior

publicKey

hashPropio

firmaDigital

¿Por que nuestra blockchain es segura?

Hash correcto

Verificamos que el contenido del bloque no haya sido modificado. Si cambia algo, el hash ya no coincide y se rechaza.



Hash anterior válido

Cada bloque debe enlazarse correctamente con el anterior. Esto asegura la continuidad e integridad de la cadena.



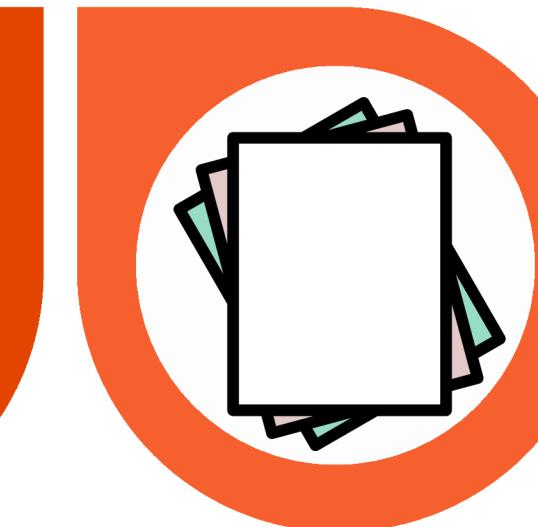
Firma digital válida

El bloque debe estar firmado con la clave privada del validador. Así comprobamos que fue generado por alguien autorizado.



Clave pública autorizada

Solo se aceptan bloques firmados por claves registradas. Evita que externos creen bloques falsos



Demostración del sistema



UniBlock

Bienvenido al sistema de votación basado en blockchain. Aquí puedes participar en elecciones de manera segura y transparente.

Votar

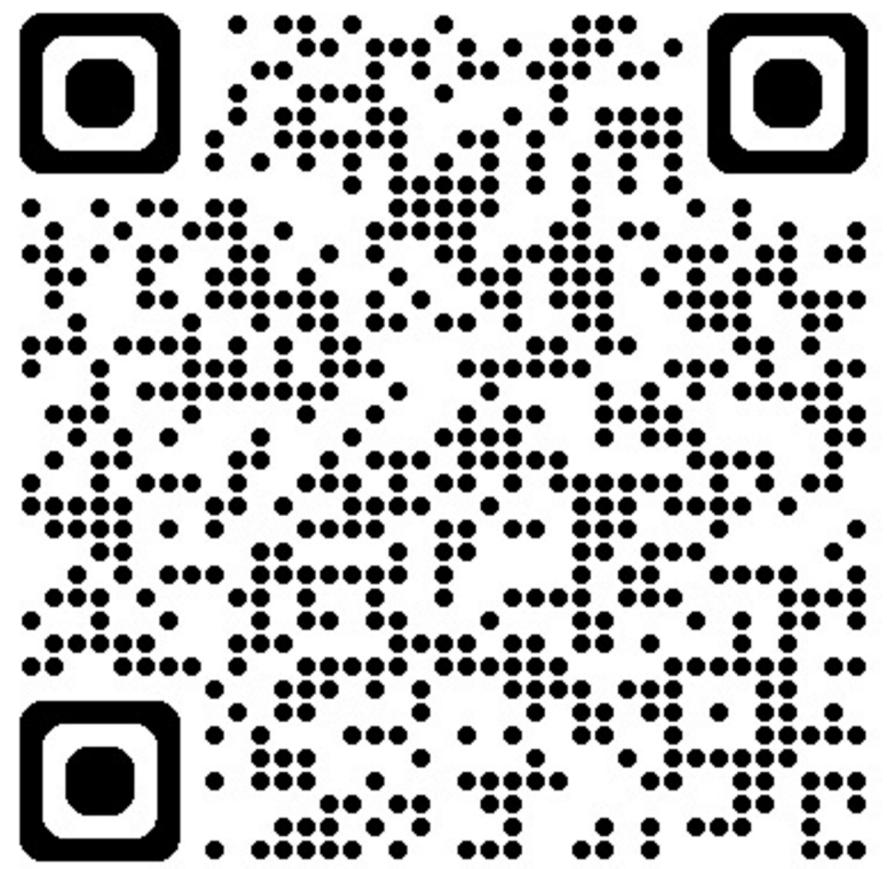
UniBlock

Demostración del sistema



Screenshot of the UniBlock voting system interface:

- Header:** UniBlock logo, navigation menu (Acerca De, Como Votar, Proximas Votaciones, Noticias, Preguntas Frecuentes, Usuarios), user icons.
- Main Content:**
 - Section Title:** UniBlock
 - Text:** Bienvenido al sistema de votación basado en blockchain. Aquí puedes participar en elecciones de manera segura y transparente.
 - Call-to-Action:** Botón "Votar".
 - Visual Elements:** A central graphic illustrating the voting process: hands placing colored ballot boxes (green with checkmark, orange with checkmark) into a ballot box, a smartphone displaying a voting interface with a checkmark, and hands interacting with digital representations of voters.



<https://uniblock-frontend.vercel.app/>