Guía

1

CALCTOPIA

Demostraciones de Identidad en Conocimiento Cero

Guía de Registro de Nodos de Minería

DEMOSTRACIONES DE IDENTIDAD EN CONOCIMIENTO CERO

Guía de Registro de Nodos de Minería

Tabla de Contenidos

Capítulo 1

Requisitos Técnicos

Un nodo de minería con un procesador Intel® SGX

Tu nodo de minería debe tener al menos las siguientes características:

- CPU con Intel® SGX2 / SGX1 con FLC (*Flexible Launch Control)*
- Disponibilidad 24/7
- 1 GB de RAM y 10 GB de disco duro libres
- Una dirección IP pública y dos puertos abiertos

Tu procesador debe soportar las instrucciones Intel SGX2 o SGX1 con FLC. Comprueba la documentación oficial:

- Detectando y Habilitando Intel® SGX (Vídeo de Youtube)
- Busca tu procesador en el Intel Ark
- En Linux:

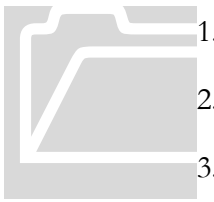
  cat /proc/cpuinfo | grep sgx2

  cat /proc/cpuinfo | grep sgx_lc

Además, recuerda que la presencia de SGX CPUID no es suficiente, la configuración de SGX en la BIOS debe estar activada.

Guía de Instalación

Sigue los siguientes pasos:



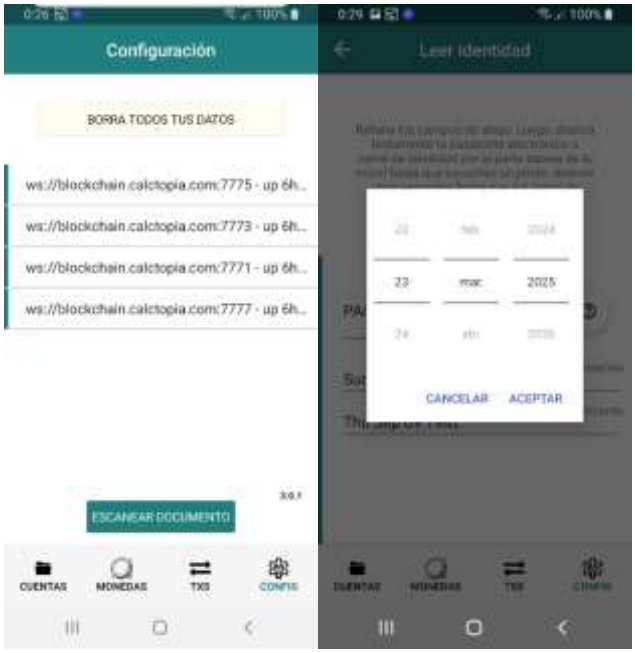
1. Instala Docker
2. Instala Occlum
3. Descarga Zero-Knowledge Proof of Identity
4. Descomprime dentro de un container docker habilitado para SGX
5. Sigue los siguientes pasos

Certificado de Confianza del Pasaporte Electrónico (Monedero Raziel - Android)

Sigue los siguientes pasos:

1. En Android, instala la aplicación Monedero Raziel de Google Play:

2. En Config>Escanear Documento, configura clave BAC de pasaporte: *Document Number* (Número pasaporte), *Date of Birth* (Fecha de Nacimiento) y *Date of Expiry* (Fecha de Expiración).



3. Lee el chip del pasaporte: debes mover muy lentamente el pasaporte por debajo de tu móvil hasta que escuches un pitido, tras el cual éste deberá permanecer quieto hasta que se lea el pasaporte.

4. Si tus datos de identidad se leen con éxito, aparecerá un mensaje de información.

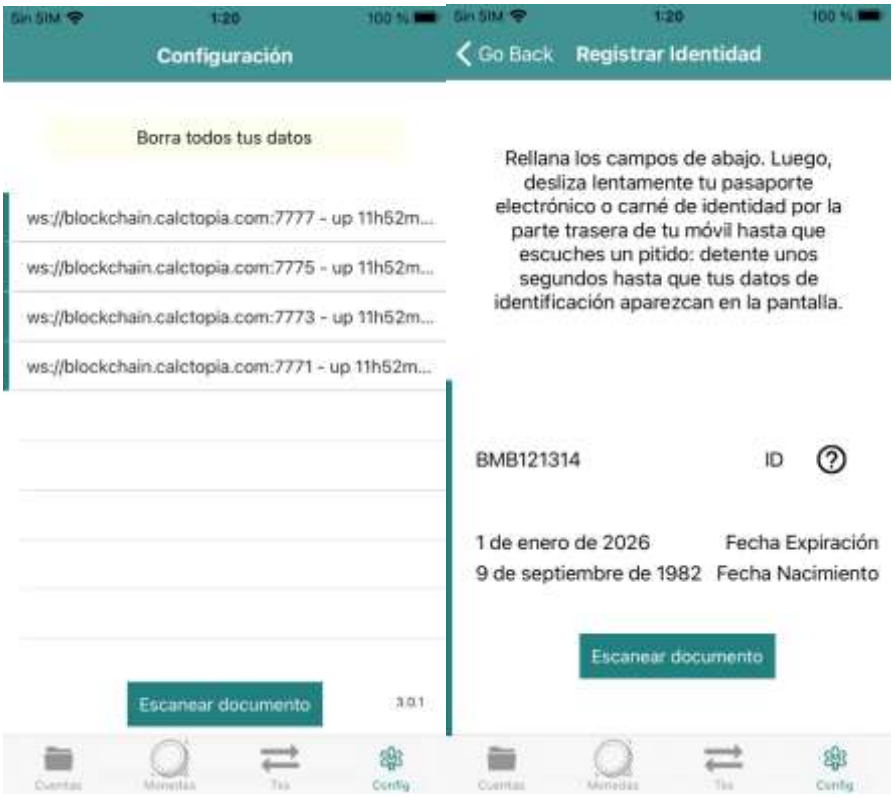
5. Copia los datos de identidad salvados desde el almacenamiento USB a tu ordenador.

Certificado de Confianza del Pasaporte Electrónico (Monedero Raziel - iOS)

Sigue los siguientes pasos:

1. En iPhone, instala la aplicación Monedero Raziel del Apple Store.

2. En Config>Escanear Documento, configura clave BAC de pasaporte: *Document Number* (Número pasaporte), *Date of Birth* (Fecha de Nacimiento) y *Date of Expiry* (Fecha de Expiración).

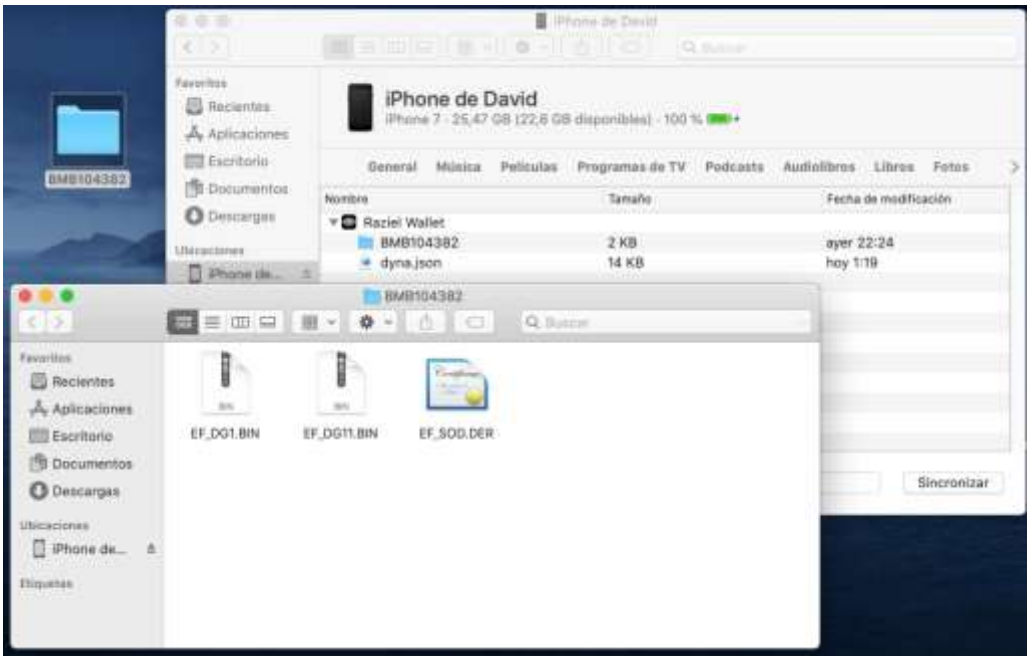


3. Lee el chip del pasaporte: presiona el botón "Escanear documento", y mueve muy lentamente el pasaporte por debajo de tu móvil hasta que escuches un pitido, tras el cual éste deberá permanecer quieto hasta que se lea el pasaporte.

4. Si tus datos de identidad se leen con éxito, aparecerá un mensaje de información.

5. Copia los datos de identidad salvados a tu ordenador: desde Finder > tu iPhone como Ubicación > Archivos > expande el directorio "Raziel Wallet" > pincha y arrastra el directorio con tu número de documento al Escritorio, tal y como se muestra en la siguiente imagen.

Si todo ha ido correctamente, deberías obtener un directorio como archivos que representan Grupos de Datos (*Data Groups*) extraídos de tu pasaporte electrónico, tal y como se muestra más abajo:



Registro

Registrar una identidad de un Pasaporte Electrónico/Biométrico:

1. Copia los archivos EF_SOD.DER, EF_DG1.BIN y EF_DG11.BIN al directorio de la instancia zkPOI para Occlum
2. Ejecuta la siguiente linea de comando:

   ```
   occlum run /bin/client --userPassword 12345  --address
   tls://conode.yourhost.com:7770 --url tls://conode.yournode.com:7771
   ```

3. Si el registro concluyó satisfactoriamente, se habrán creados dos archivos (**public.toml** y **private.toml**) que deben utilizarse como configuración para tu nodo blockchain

Índice