12 Seed cracker

¿Cómo obtener las 12 palabras de una wallet desconocida?

En primer lugar, entender que esto se trata de un código educativo que se comparte a modo únicamente educativo. Rechazando cualquier actividad malintencionada que se pueda hacer con este conocimiento.
Desde CABS no queremos fomentar el uso malintencionado del conocimiento pero tampoco limitarlo, por eso nos quedamos al margen de cualquier uso que quiera darse.

¿Qué vamos a aprender?: Vamos a aprender a desarrollar un código completo que pruebe combinaciones de palabras hasta obtener una wallet con (o sin) Ethereum.

Descripción

Esta lista vendrá compuesta por las 2048 palabras de la lista BIP39 (ENG us GB) y se tomarán de forma aleatoria para probar combinaciones de accesos a Wallet.

El código es un sencillo ejemplo de **fuerza bruta*** con algo de ingenio básico en programación 😊

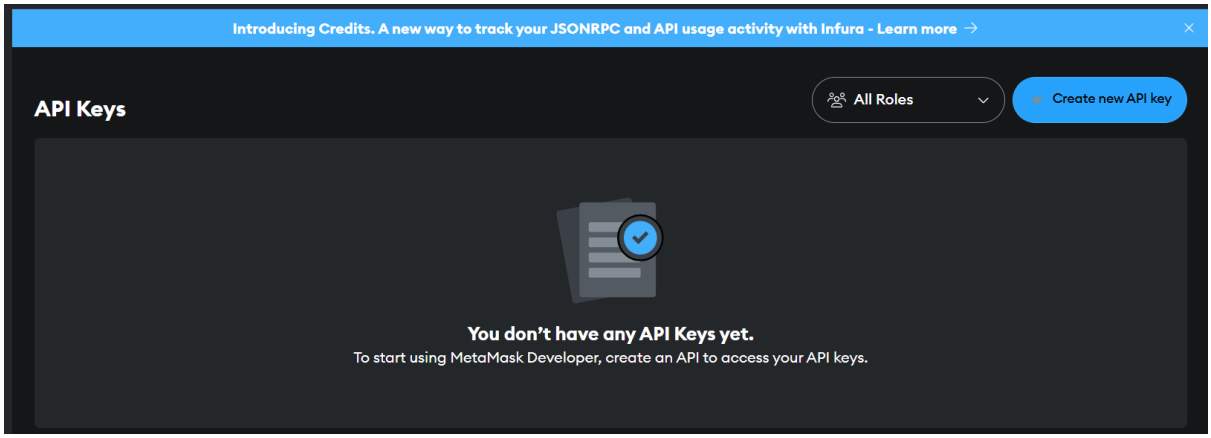
El código está totalmente comentado para ser entendido y modificado para mejoras.

Fuerza bruta: En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.1

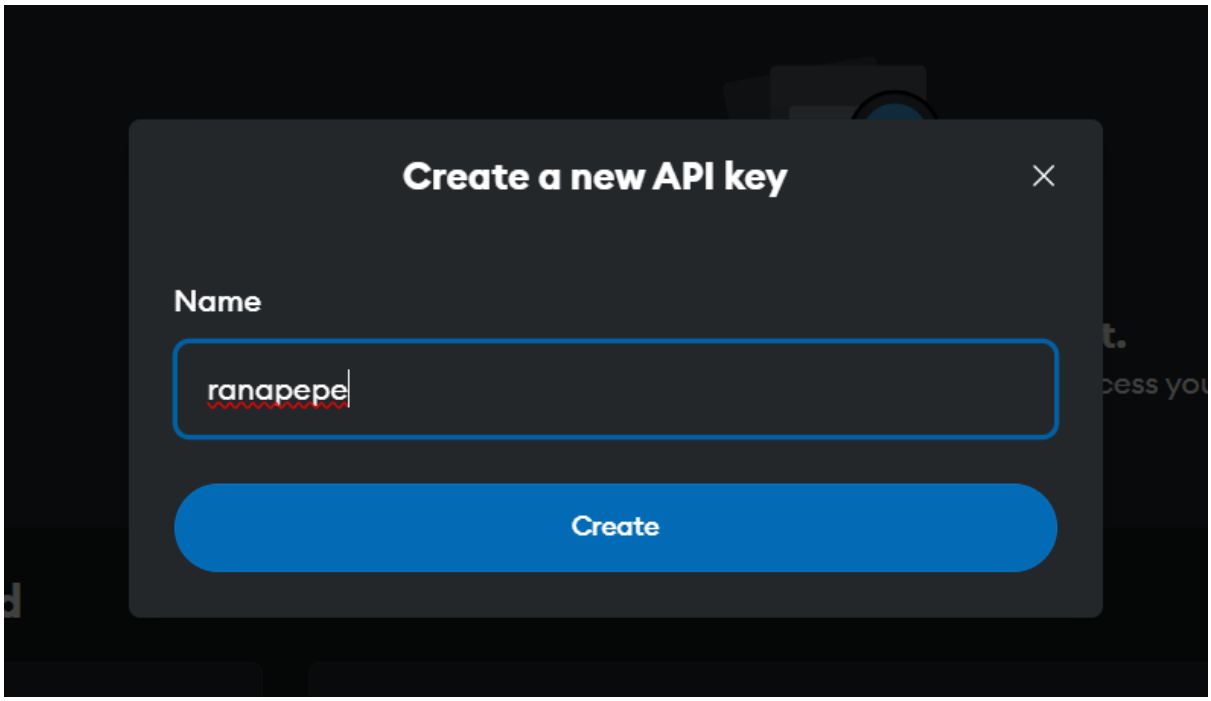
Empecemos

Deberemos registrarnos en INFURA, pudiendo utilizar nuestra Wallet de Metamask o nuestra dirección de correo electrónico.

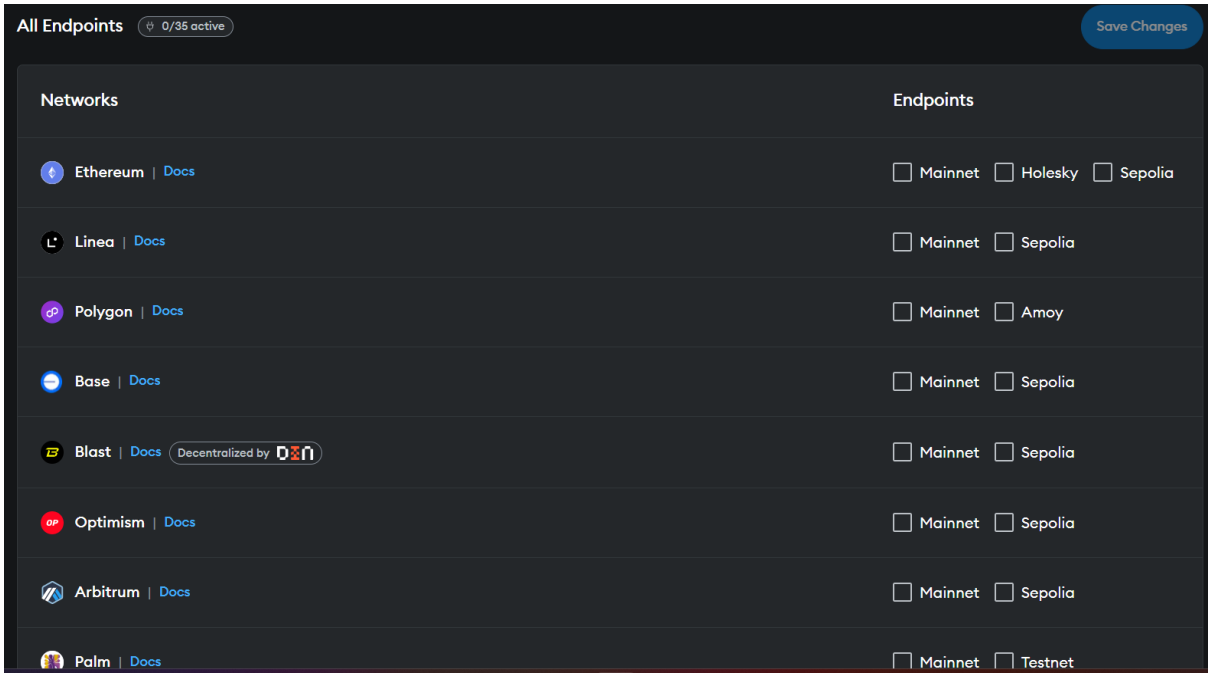
Deberemos crear una *NEW API KEY* para obtener un código "de acceso" a los servicios gratuitos de Infura.



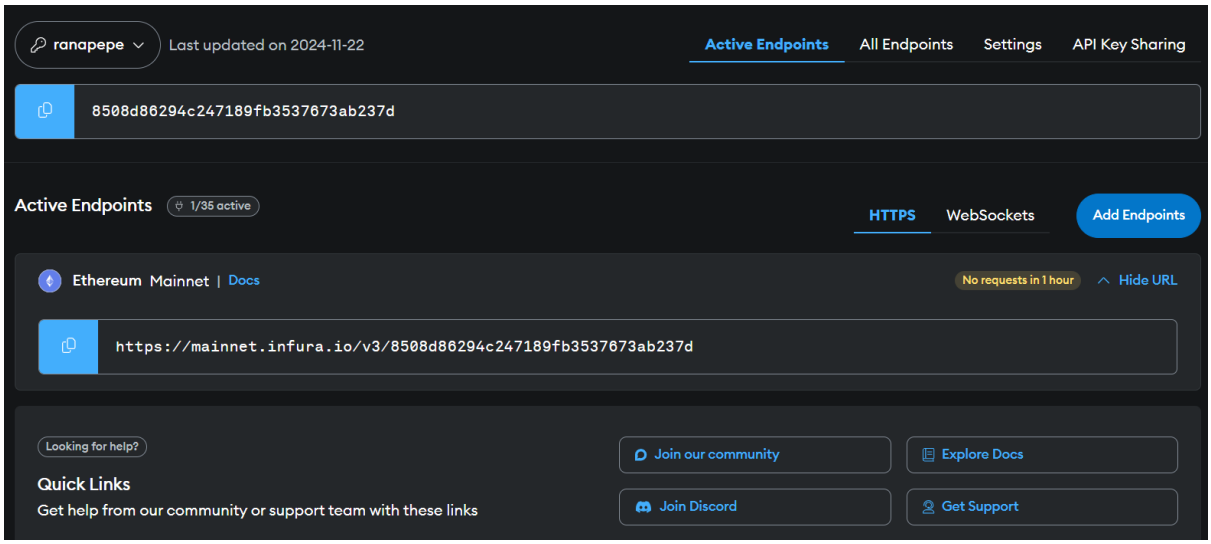
Aparecerá un Pop-Up donde deberemos asignar un nombre a este proyecto / API.



A continuación, deberemos seleccionar los ENDPOINTS (redes) donde querremos que nuestro código pueda acceder y verificar si dicha wallet tiene fondos o no.



Una vez guardados los cambios, nos entregará un API KEY (código) el cual deberemos introducir en el código proporcionado.



Nota: *Debemos tener en cuenta que el programa está diseñado para comprobar únicamente la MAINNET de Ethereum (posible mejora)*

Reflexión

Teniendo en cuenta la realidad de la BIP39, aparecía una cantidad ASTRONOMICA de combinaciones posibles:

Wallets de 12 palabras: 2048^12 ≈ 5.79 x 10^39

Wallet de 24 palabras: 2048^24 ≈ 3.36 x 10^78

Que esta cantidad sea ENORME, no hace imposible la obtención de las palabras clave adecuadas, "al menos" con wallets "simples" de 12 palabras.

- Diferentes ejercicios de seguridad que podrían aplicarse, pese a reducir o anular el anonimáto serían:
- Utilizar sistemas 2FA (Google o Microsoft Authenticator) por ejemplo.
- Utilizar sistemas OTP, sistemas de SMS / Email
- Otros sistemas que mantendrían el usuario oculto y no relacionado con sus datos personales, serían las wallets multifirma:
- Una **cartera de multifirma** es un tipo de cartera de criptomonedas que requiere múltiples firmas, en lugar de solo una, para ejecutar cada transacción. Estas firmas están asociadas con diferentes claves privadas criptográficas, y un umbral definido de claves debe firmar una transacción para validarla.

Teniendo en cuenta que utilizaramos dos firmas de 24 palabras cada una, sería un número que a día de hoy, ni la paciencia podría encontrar.

(Probablemente un ordenador cuántico, pero de momento no están en Aliexpress)

- Otras opciones, más complejas y enfocadas a la programación, consisten en desarrollar un SmartContract privado (y BIEN HECHO) donde bloquearamos nuestros fondos, añadiendo un retardo, multifirma (con wallets que ya conozcamos) u otros sitemas ya existentes para desbloquear nuestros fondos.

Seguramente existan muchas más opciones y cada uno encontrará mayor o menor facilidad con diferentes propuestas, no osbtante, recordad la **CLAVE DE ORO de ESTE MUNDO.**

🏅 **La "norma" de oro que todos sabemos, pero pocos aplicamos:**

🥇 Ten una wallet para hodlear y una wallet para conectarte a dApps.

🥈 No conectes tu wallet de hodler (donde tengas tu $) en ninguna dApp, NUNCA.

🥉 Es más tedioso, pero te ahorrará disgustos.

*Nota: Así también entenderás que ETH es una red cara :)

Recuerda que puedes seguirme en:

 CriptoFiveat