



**Introducción al uso de librerías
y exploradores de Blockchain
para Bitcoin, Ethereum
y otras criptomonedas.**

BLOCKMAD



Juan Antonio Lleó – BlockMAD
COMMIT CONF 2018

INTRODUCCION: OBJETIVOS DEL TALLER

- Con un enfoque eminentemente práctico se va a trabajar con varias herramientas para explorar el blockchain y manejar distintas criptomonedas y tokens, ya sea desde páginas web o mediante librerías.
- Durante el mismo vamos a crear una cuenta en un exchange y a obtener, gratuitamente pequeñas cantidades de criptomonedas que nos ayudarán a entender mejor los diferentes aspectos del mecanismo de su funcionamiento.
- Conviene tener en cuenta que se trata de un tema muy amplio, de carácter multidisciplinar y cuyo conocimiento en profundidad, incluso en ámbitos concretos, requiere considerable esfuerzo y sobre todo tiempo.

INTRODUCCION: EXPLORADORES DE BLOCKCHAIN

Existen muchos sitios que nos permiten explorar las distintas blockchain, sin necesidad de instalarnos la aplicación y tener que bajarnos toda la cadena de bloques. Algunos **ejemplos** son:

- **Blockchain.com:** www.blockchain.com

- <https://www.blockchain.com/es/explorer>

- <https://www.blockchain.com/es/api>

- **API para Python (disponible en otros lenguajes):**

- <https://github.com/blockchain/api-v1-client-python>

- **Blockcypher.com:** www.blockcypher.com

- <https://live.blockcypher.com>

- **API para Bitcoin:**

- <https://www.blockcypher.com/dev/bitcoin/#introduction>

- **API para Ethereum:**

- <https://www.blockcypher.com/dev/ethereum/>

INTRODUCCION: CREACION DE CUENTA EN EXCHANGE

Nuestro primer paso va a ser la creación de una cuenta en un sitio de cambio de criptomonedas (exchange).

- PARA CREAR UNA CUENTA CON CREX24:
<https://bit.ly/2zmlcZv>
- APUNTA A LA DIRECCIÓN, REFERIDO DE:
DraconianRun20 / taller@blockmad.lleo.net:
<https://crex24.com/?refid=jglpdi3ob3flkxhr5wpo>
- En este caso, en vez de apuntarnos directamente en el sitio, vamos a hacerlo desde un enlace de invitación, lo que se conoce como referido.
- He escogido este exchange pues ofrece la posibilidad de obtener (unas pocas) criptomonedas gratuitamente.

CREX24: CREAR UNA NUEVA CUENTA

Pasos para registrarse:

- Copiar el enlace y pegar en el navegador:
<https://bit.ly/2zmlcZv>
- Seleccionar: **aceptar cookies** y pulsar el boton: **registrarse**
- Introducir una **dirección de correo** válida
- Introducir (2 veces) una **contraseña**
- **Validar el captcha**: Se genera un aviso de envio a la direccion de la cuenta recién creada
- Ir a la cuenta de correo usada y **abrir el correo** recibido
- Copiar y pegar el **enlace** en el navegador, o pulsar sobre él
- Saldrá un mensaje de que la dirección ha sido **confirmada**
- ...Y ya se puede **acceder** a nuestra cuenta

CREX24: INTRODUCCION AL INTERFAZ

INTERFAZ DE CREX24:

Dispone de las siguientes pestañas de menú:

- **MERCADOS:** Pantalla por defecto, ofrece la evolución de las criptomonedas y tokens, instrumentos, historial, comprar o vender, y las órdenes, tanto propias como del mercado.
- **CUENTA:** Muestra, en **BTC** o **USD**, los saldos de las monedas que tenemos en nuestra cartera. También podemos ingresar (depósitos) o retirar monedas. **Mejor:** No mostrar saldos cero
- **INFORMES:** Nos muestra el estado de nuestras órdenes de compra y/o ventas de criptomonedas.
Pestañas: Mis órdenes, Mis operaciones, Historial de pagos
- **GRIFOS (FAUCETS):** Esta pantalla es la que nos permite obtener monedas gratis. Muestra el valor en **BTC** o **USD**.

CREX24: GRIFOS (FAUCETS)

GRIFOS PARA GENERAR CRIPTOMONEDAS:

- Ir a la opción **cuenta** y seleccionar la opción:
 - **Ocultar saldos cero**
- Ir a la opción **Grifos (faucets)**:
- Pulsar sobre todos los **botones en verde**
- Validar los **captchas** que vayan saliendo
- Una vez hecho, **comprobar el saldo** generado:
 - Ir a la **opcion: cuenta**
 - **Aparece el saldo** de las criptomonedas que acabamos de conseguir
 - **Por defecto:** en fracciones de bitcoin **BTC**. También podemos ver su valor en **USD**, cambiando el botón en la parte superior derecha.

CREX24: ICONO: MI CUENTA

INTERFAZ DE CREX24, ICONO: MI CUENTA

El **Nombre** de nuestra cuenta, generado automáticamente, puede verse en la parte superior izq. de la pantalla de **Grifos**.

En la parte superior derecha, hay un icono interesante, con información sobre **nuestra cuenta**, con las siguientes pestañas:

- **Seguridad:** Incluye la **Autenticación de dos factores** con Google Authenticator, el **Código QR**, la **Clave Privada**, **código de seguridad** y **cambio de contraseña**.
- **Verificación:** Para algunas operaciones, es necesario un **Código de verificación**.
- **Claves API:** Genera una o varias **claves API**, con distintos permisos, para poder realizar **operaciones automatizadas**.
- **Programa de afiliación:** o **Referidos**, si damos a alguien este enlace, conseguimos una **comisión** de sus operaciones.

CREX24: AFILIACION (REFERIDOS)

AFILIACION (REFERIDOS) PARA CREX24:

- Para crear un **Enlace de referidos**:
 - Hay que pulsar el enlace: **GENERAR ENLACE** en la parte inferior derecha.
 - Ir a la opción **Mi cuenta** (icono superior derecho)
 - Seleccionar la pestaña: **Programa de afiliacion**
 - En la parte inferior, pulsar sobre el icono: **generar enlace**
- Copiar el **enlace generado** y mandar a quien queramos invitar
- Se pueden crear **múltiples enlaces**, con lo cual podemos discriminar por su procedencia
- A continuación aparece el **listado** de todos los enlaces de referidos y si han sido usados (registros) y cuanto retorno han generado en total. **Por ejemplo, para:** draconianrun20 / taller@blockmad.lleo.net El enlace es el siguiente:
<https://crex24.com/?refid=jglpdi3ob3flkxhr5wpo>

CLAVE DE TRANSACCIONES (API KEY) I

Para obtener una clave (API key) que nos permita hacer transacciones con la API:

- En **Mi cuenta**, ir a la opción: **Claves API**
- Seleccionar: **Nueva clave API**
- **Manda un correo** con una **clave**, que hay que introducir para que la pueda generar.
- **Copiar** la clave recibida en el correo e introducir en la **ventana de verificación**.
- Una vez **validada**, sale un **listado** con (todas) las **claves secretas** (con los pares: **API key** y **secret**).
- **Atencion:** ¡¡¡**Proteged** estas claves, pues dan acceso a hacer transacciones sobre la **wallet** a todo aquel que las obtenga!!!
- **Ejemplo de Clave temporal:**

API KEY: e0e51546-77f5-4c49-b3ac-b11f4ee6e3ed

SECRET: O3tipCH0mb61uY1EZrq3Fo5Jb17R7+XXXXXXXXXXXXXXXXXXXXXXXXXXXXXJDPU51mxCvnjU5Y3rw==

CLAVE DE TRANSACCIONES (API KEY) II

Para poder **operar** con la **API key**, tenemos que activarla, poniendo el **Estado** en **On**:

- Una buena idea es **activarla sólo cuando lo necesitemos**
- También podemos **limitar la operativa**, los derechos de acceso, según estos **bloques**:
 - **R1**: libro de órdenes, historial, saldo de trading
 - **R2**: realizar/cancelar órdenes
 - **R3**: información de pago
 - **R4**: retirada de criptomonedas
- **Atencion**: hay que fijarse en el **tipo de permisos** de acceso que se necesitan, según el **comando** que se quiera usar.

Para **probar** las **claves API** hay que crear un **programa**, por ejemplo en **Python** (también hay ejemplos en **C#, Nodejs y php**).

CREX24 - API:

CREX24 - API 2.0 BETA:

<https://docs.crex24.com/trade-api/v2/#trade-api-2-0-beta>

Instrucciones en español:

<https://crex24.com/es/trade-api>

Algunos de los **comandos** que aparecen con **get**, pueden **ejecutarse** directamente desde el **navegador**.

Por ejemplo:

- **Currencias:** Devuelve la lista de todas las monedas disponibles (incluyendo monedas y tokens...) con información detallada.

GET <https://api.crex24.com/v2/public/currencias>

- Sería:

<https://api.crex24.com/v2/public/currencias>

CREX24 - API: Métodos API públicos I

CREX24 - Métodos API públicos (no requieren autenticación):

Instrucciones en español:

<https://crex24.com/es/trade-api>

Hay seis métodos públicos que aceptan solicitudes **HTTP GET** y devuelven la respuesta en formato **JSON**:

- **ReturnTicker**
- **Return24Volume**
- **ReturnOrderBook**
- **ReturnTradeHistoryPub**
- **ReturnChartData**
- **ReturnCurrencies**

En la página cuyo enlace está arriba pueden verse cuales son y distintos ejemplos.

CREX24 - API: Métodos API públicos II

CREX24 - Métodos API públicos (no requieren autenticación):

Instrucciones en español:

<https://crex24.com/es/trade-api>

EJEMPLO:

- **ReturnTicker:**

El método devuelve tickers para todos/específicos mercados; ejemplos de solicitudes y respuestas:

Ejemplo 1. Devolución de todos los tickers.

Solicitud:

<https://api.crex24.com/CryptoExchangeService/BotPublic/ReturnTicker>

EJERCICIO:

A continuación, probar el resto de los métodos.

CREX24 - API: Datos del mercado (Market Data)

CREX24 - API 2.0 BETA:

También podemos usar una API más avanzada, su documentación actualmente sólo está disponible en inglés.

Los **metodos** para acceder a los **datos del mercado** no exigen ninguna **autenticacion**. La documentación está disponible en:

<https://docs.crex24.com/trade-api/v2/#market-data>

- Se incluye los siguientes tipos de **métodos**:
 - **Currencias** (monedas)
 - **Trade instruments** (Instrumentos de transacciones)
 - **Quotes** (tickers)
 - **Recent trades** (Transacciones recientes)
 - **Order book** (Libro de órdenes)

CREX24 - API: EJEMPLOS (Market Data)

- **Para saber las transacciones mas recientes desde ethereum (ETH) a bitcoin (BTC):**

<https://api.crex24.com/v2/public/recentTrades?instrument=ETH-BTC>

- **Solo las últimas 10:**

<https://api.crex24.com/v2/public/recentTrades?instrument=ETH-USD&limit=10>

- **O para saber las ultimas ventas de bitcoin (BTC) a dolares (USD):**

<https://api.crex24.com/v2/public/recentTrades?instrument=BTC-USD&limit=10>

- **Y entre litecoin (ltc) y bitcoin (btc):**

<https://api.crex24.com/v2/public/recentTrades?instrument=LTC-BTC&limit=10>

CREX24 - API: Métodos de trading API I

CREX24 - Métodos de trading API (requieren autenticación):

Instrucciones en español (a continuación de los anteriores):

<https://crex24.com/es/trade-api>

- **URL para la API de trading:**

<https://api.crex24.com/CryptoExchangeService/BotTrade/<MethodName>>

Es necesario crear la clave API para usar la API de trading, en:

<https://crex24.com/settings/tokens>

Ten en cuenta que el límite predeterminado es de 6 solicitudes por segundo. Si no es suficiente, por favor póngase en contacto con el Servicio de atención al cliente para aumentar dicho límite.

CREX24 - API: Métodos de trading API II

CREX24 - Métodos de trading API (requieren autenticación): Instrucciones en español (a continuación de los anteriores):

<https://crex24.com/es/trade-api>

Todas las solicitudes de trading de la API son enviadas a la dirección HTTP por el método POST y deben contener los siguientes encabezados:

- UserKey — API key.
- Firma — firma del cuerpo de solicitud del POST creado con una clave secreta a través de HMACSHA512.

Todas las solicitudes deben contener el parámetro POST Nonce. Nonce es unsigned int64 que debe ser siempre mayor que el valor anterior. Puede usar el parámetro timestamp para estos objetivos.

CREX24 - API: EJEMPLOS (Con autenticación) I

El resto de los métodos disponibles requiere de la autenticación correspondiente. Son los siguientes:

- **Trading:**
- **Account:**
- **Authentication:**
- **Order Types:** Tipos de Órdenes (no se incluyen ejemplos)

Tanto para operaciones con o sin autenticación, se pueden obtener distintos errores. Aquí tenemos más información:

- **Handling Errors:** Manejo de errores, listado de los errores que podemos obtener con llamadas fallidas a la API. (Ver ejemplos)

<https://api.crex24.com/v2/public/currencies?filter=ASDFASDF>

Este **método** se ejecuta con **código 400** y devuelve éste **JSON**:

```
{  
  "errorDescription": "Parameter 'filter' contains invalid value."  
}
```

CREX24 - API: EJEMPLOS (Con autenticación) II

Si intentamos ejecutar un método que requiere autenticación, por ejemplo:

<https://api.crex24.com/v2/trading/orderStatus?id=466747915>

obtendremos un error parecido a éste:

```
{"errorDescription": "Request must contain 'X-CREX24-API-KEY' header."}
```

Para poder usar métodos con autenticación, necesitamos que estén integrados dentro de un programa, con todos los requerimientos necesarios satisfechos.

A continuación veremos un ejemplo de un programa para ello, con el lenguaje Python. También podemos usar otros lenguajes:

CREX24: EJEMPLOS EN PYTHON I

Autenticación con el metodo get:

<https://docs.crex24.com/trade-api/v2/#authentication>

LISTADO:

```
-----  
import datetime  
import base64  
import hmac  
from hashlib import sha512  
from urllib.request import urlopen, Request  
from urllib.error import HTTPError  
  
baseUrl = "https://api.crex24.com"  
apiKey = "-- Your API key --"  
secret = "-- Your secret --"
```

CREX24: EJEMPLOS EN PYTHON II

LISTADO:

```
path = "/v2/account/balance?currency=BTC"
nonce = round(datetime.datetime.now().timestamp() * 1000)

key = base64.b64decode(secret)
message = str.encode(path + str(nonce), "utf-8")
hmac = hmac.new(key, message, sha512)
signature = base64.b64encode(hmac.digest()).decode()

request = Request(baseUrl + path)
request.method = "GET"
request.add_header("X-CREX24-API-KEY", apiKey)
request.add_header("X-CREX24-API-NONCE", nonce)
request.add_header("X-CREX24-API-SIGN", signature)
```


CREX24: EJEMPLOS EN PYTHON Y III

LISTADO (SIGUE):

```
try:
```

```
    response = urlopen(request)
```

```
except HTTPError as e:
```

```
    response = e
```

```
status = response.getcode()
```

```
body = bytes.decode(response.read())
```

```
print("Status code: " + str(status))
```

```
print(body)
```

```
-----
```

CREX24: EJEMPLOS DE LIBRERIAS EXTERNAS I

EJEMPLO DE PROGRAMACION CON LIBRERÍAS EXTERNAS PARA CREX24:

- **Crex24.Examples:** Ejemplos de uso de un **BotTrade** (robot de transacciones) con autenticación, a través de firmas **HMACSHA512**
- Disponible en varios lenguajes: Python 2 y 3, R, JS, Perl y PHP

<https://github.com/iiv/Crex24.Examples>

CREX24: EJEMPLOS DE LIBRERIAS EXTERNAS II

EJEMPLO PARA PYTHON 3:

<https://github.com/iiw/Crex24.Examples/blob/master/python/app.py>

INSTRUCCIONES, (Para Linux):

- Para ejecutar este ejemplo en python, sólo se necesita:
Python 3

- Ve a la carpeta python y ejecuta el comando:

```
python app.py
```

- ¡Antes hay que poner las API Keys!
- Si te sale el mensaje de error:

ModuleNotFoundError: No module named 'requests'

- Por favor, instala el módulo requests via pip:
pip install requests (en Linux, con sudo delante)

EJEMPLO PARA PYTHON 2:

<https://github.com/iiw/Crex24.Examples/tree/master/pythonv2>



COMMIT 2018 Introducción a Exploradores y Lib. Blockchain

¡Muchas Gracias!



¡Muchas Gracias!

Juan Antonio Lleó:

juan.a.lleo@gmail.com

BlockMAD

Grupo de Blockchain orientado al desarrollo:

<https://www.meetup.com/es-ES/BlockMAD/>

FIN

FIN

