DA51 Lab session 5

MetaMask
J. Gaber, gaber@utbm.fr

Target set of this session:
After completion of this session, you will successfully know:
- how to use MetaMask
- how to recover your account addresses as well as their keys
- how to load some Ether.

Installing MetaMask

MetaMask is one of the most popular Ethereum clients. MetaMask serves as a wallet for Ethereum accounts.

As a browser extension, it meant to access Ethereum enabled applications from your browser. The extension is available for Chrome, for Internet Explorer as well as Firefox browsers

1. Get access to the extensions page of your favorite browser to search for MetaMask and then to add it to your browser.

As a result, you should see MetaMask, identified by the fox logo available on top right corner of your browser.

2. Click on the fox logo and create your MetaMask account.

Among the steps, you will reach a page titled Secret Backup Phrase with a box and lock icon. A 12-word phrase will be generated for your account. And this is something which you need to make a note of for you to access the Ethereum accounts which will be generated by MetaMask on your behalf. The password you created just a few moments ago will help you log into MetaMask from your current installation in your browser.
This 12-word phrase is referred to as a seed phrase, or a mnemonic code. In conjunction with the BIP39 standard, it will map to a specific set of key pairs. These key pairs correspond to Ethereum accounts. You must memorize and save this phrase, to be able to access your Ethereum accounts from anywhere.

The BIP39 standard defines This mapping of a Mnemonic code or a seed phrase, to an account address and key pairs.

You will be given the option to deposit Ether into the account which has just been created. You can do so by either directly depositing Ether from some other account which you have. Alternatively, you could purchase some Ether from Coinbase, which is an online digital currency exchange where you can purchase Ether, Bitcoin, and other cryptocurrencies. ShapeShift is another option available to load your accounts with Ether.

Exploring MetaMask
many of the options available using the MetaMask interface, as well as the details for an account available on etherscan.io.

3. Use the interface of the MetaMask tool to check the available options.

A default account called Account number 1 is configured for you. You can click on the fox logo and then by clicking on button with an image in the top right, you can create and input additional accounts using this interface and define some of the settings for your MetaMask account.

If you would like to view information regarding Account number 1, you can click on the three dots to view the account information on Etherscan. This brings up a web page which corresponds to your account on etherscan.io.
etherscan.io website shows all the publicly available information for an Ethereum account.

by default, MetaMask will connect us to the main Ethereum network. However, by clicking on the dropdown, you will see all of the other options which are available: Main Ethereum Network, Linea Mainnet, Sepolia test network, Goerli test network, Localhost 8545 and Custom RPC (see Lab 6).

Sepolia and Goerli are test networks (testnets). They are primarily used for development on the blockchain testing out applications and smart contracts. You can also connect MetaMask to a private Ethereum network using the custom RPC option, where you will need to define a URL endpoint where the network can be connected to.

Note that the same account address can map to multiple Ethereum networks.

What if you ever happen to lose your account addresses as well as their keys?

When creating a MetaMask account, a key phrase or a seed phrase was generated. That seed phrase maps to a particular set of Ethereum account addresses.

If you were to forget the account addresses or lose the keys which map to them, you can recover them by making use of that seed phrase.

4. navigate to a website with the URL https://iancoleman.io/. which will help recover the Ethereum account addresses from the seed phrase.

This website provides several different tools, and the one we are interested in, is the BIP39 Mnemonic Code Converter.

5. Click on the Site option to open the Mnemonic Code Converter page. It has three sections: Mnemonic, Derivation Path, and Derived Addresses.

6. to recover the account addresses as well as the key pairs corresponding to our own Ethereum wallet, enter the 12 words in the input box for BIP39 Mnemonic.

Once entered, the BIP39 Seed will be generated and the QR code which maps to your Ethereum wallet visible when you hover over this field.

selects ETH - Ethereum from the list of options of the Coin dropdown which is the type of wallet the seed phrase maps onto.
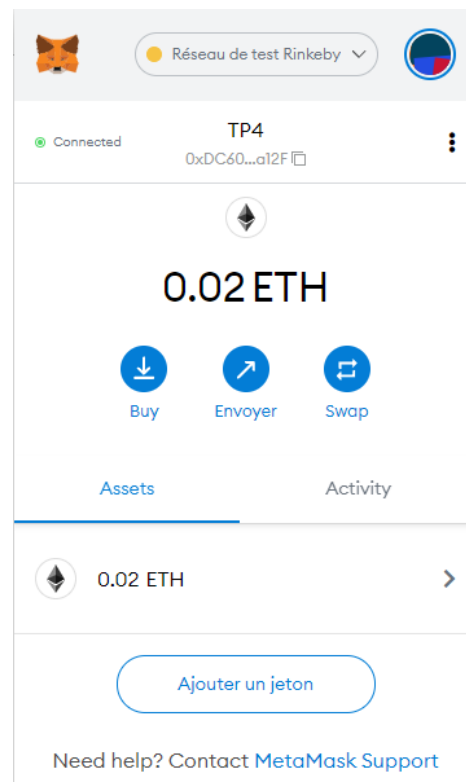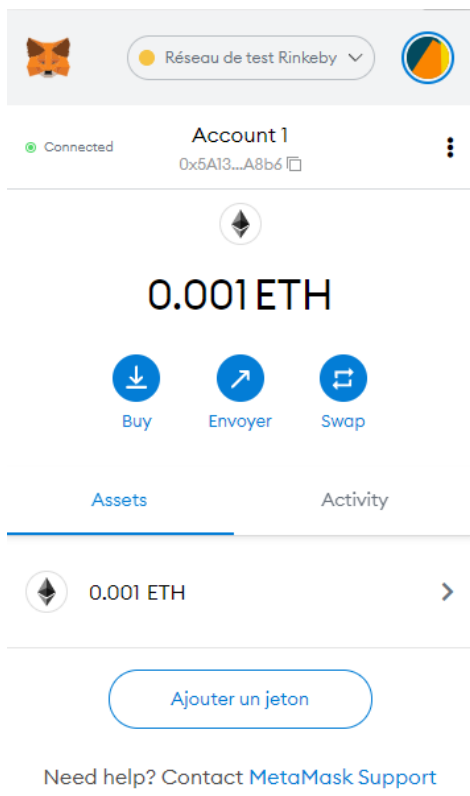
7. Then scrolls down the page to the Derived Addresses section to see all the different account addresses, as well as their private and public keys, which mapped to the Mnemonic phrase you entered.

The Sepolia Network

To be able to use this account to invoke transactions, you will need to load it with some Ether, whether on the main network or on the test networks.

The Sepolia test network, allows you to generate some Ether to be used on that network alone. This can be done by turning on a faucet via making a social media post. In other words, the Sepolia Network, allows you to generate Ether by making posts on Twitter.

8. Head to https://sepoliafaucet.com/ to request funds via Twitter (see instructions, you should create an Alchemy account)

9. Check etherscan link to follow your transaction.

10. What is Alchemy?

Check here for the most up to date faucets: https://docs.chain.link/resources/link-token-contracts to get some ChainLink Tokens.

11. What is chainlink?