

# Lab Session: Wallet Setup and First Transaction

## BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

By the end of this lab session, you will be able to:

- Install and configure MetaMask wallet extension
- Understand seed phrase importance and backup procedures
- Connect to Ethereum testnets (Sepolia)
- Obtain testnet ETH from faucets
- Send and receive testnet transactions
- Navigate wallet features: account management, network switching
- Apply security best practices for wallet protection

## Structure:

- 1 MetaMask installation (10 minutes)
- 2 Wallet creation and seed phrase backup (15 minutes)
- 3 Testnet configuration (10 minutes)
- 4 Obtaining testnet ETH (15 minutes)
- 5 First transaction (20 minutes)
- 6 Advanced features exploration (15 minutes)
- 7 Security review and best practices (15 minutes)

**Total Duration:** 90 minutes

## Prerequisites:

- Web browser: Chrome, Firefox, Brave, or Edge
- Basic understanding of public-private key cryptography
- Secure location for seed phrase backup (physical storage)

# What is MetaMask?

## Overview:

- Browser extension and mobile app cryptocurrency wallet
- Supports Ethereum and EVM-compatible blockchains
- Non-custodial: you control private keys
- Free and open-source
- Most popular Ethereum wallet ( 30 million users)

## Key Features:

- Send and receive ETH and ERC-20 tokens
- Interact with decentralized applications (dApps)
- Multiple account management
- Network switching (Mainnet, testnets, custom networks)
- Hardware wallet integration (Ledger, Trezor)

## Alternatives:

- Browser: Coinbase Wallet, Rabby, Frame
- Mobile: Trust Wallet, Rainbow, Argent
- Hardware: Ledger, Trezor (highest security)

# Exercise 1: Installing MetaMask

## Installation Steps:

- ① Visit official website: <https://metamask.io>
- ② Click “Download” and select your browser
- ③ Install extension from official browser store:
  - Chrome: Chrome Web Store
  - Firefox: Firefox Add-ons
  - Brave: Chrome Web Store
  - Edge: Microsoft Edge Add-ons
- ④ Pin extension to browser toolbar for easy access
- ⑤ Click MetaMask icon to launch setup wizard

## Security Warning:

- Only install from official sources
- Beware of phishing sites (check URL carefully)
- Official website uses HTTPS and `metamask.io` domain
- Fake extensions exist in browser stores (verify developer name)

## Exercise 2: Creating Your Wallet

### Setup Wizard Steps:

- 1 Click "Create a new wallet"
- 2 Agree to terms of service
- 3 Set a strong password (8+ characters, mix of letters/numbers/symbols)
- 4 Watch the seed phrase explanation video
- 5 Reveal and record your 12-word seed phrase
- 6 Confirm seed phrase by selecting words in correct order
- 7 Wallet creation complete

### Password Purpose:

- Encrypts wallet on your device
- Required each time you access wallet
- Does NOT recover wallet if you forget it
- Password protects seed phrase on local device only

### Critical: Seed Phrase vs. Password

- Seed phrase = master backup (recovers wallet on any device)
- Password = local device protection (cannot recover wallet)
- Lose seed phrase -> lose wallet permanently

# Seed Phrase Security: Critical Importance

## What is a Seed Phrase?

- 12-word mnemonic (BIP-39 standard)
- Encodes master private key
- Deterministically generates all wallet addresses
- Anyone with seed phrase has FULL control of wallet

## Backup Best Practices:

- 1 Write down on paper (never digital storage)
- 2 Verify correct spelling and order
- 3 Store in secure physical location (safe, safety deposit box)
- 4 Consider multiple redundant copies in separate locations
- 5 Never share with anyone (no support staff will ask for it)
- 6 Do not store in:
  - Email, cloud storage, screenshots, text files
  - Password managers (controversial, higher risk)

## Advanced: Steel Backup

- Engrave seed phrase on metal plate (fireproof, waterproof)
- Products: Cryptosteel, Billfodl, Blockplate
- Protects against physical disasters

## Exercise 3: Understanding Your Wallet Interface

### Main Wallet Screen:

- **Account Name:** Default “Account 1” (customizable)
- **Public Address:** 0x... (click to copy)
- **Balance:** ETH amount (and USD value if on mainnet)
- **Network Selector:** Top-right dropdown (Ethereum Mainnet by default)
- **Account Menu:** Click circular icon for account management

### Tabs:

- **Assets:** View tokens and NFTs
- **Activity:** Transaction history

### Action Buttons:

- **Buy:** Purchase crypto with fiat (mainnet only)
- **Send:** Transfer tokens to another address
- **Swap:** Exchange tokens (decentralized exchange integration)
- **Receive:** Display QR code and address for receiving funds



## Exercise 4: Adding Sepolia Testnet

### Why Use Testnets?

- Practice without risking real money
- Free testnet ETH available from faucets
- Identical functionality to mainnet
- Experiment with smart contracts and dApps safely

### Adding Sepolia Network:

- 1 Click network selector (top-right dropdown)
- 2 Toggle “Show test networks” in settings:
  - Click three dots (top-right) -> Settings
  - Advanced -> Show test networks (enable)
- 3 Return to network selector
- 4 Select “Sepolia test network”
- 5 Wallet now displays Sepolia ETH balance (initially 0)

### Alternative Testnets:

- Goerli (deprecated, use Sepolia instead)
- Holesky (validator testing)

# Exercise 5: Obtaining Testnet ETH

## What are Faucets?

- Free services that distribute small amounts of testnet cryptocurrency
- Rate-limited to prevent abuse (e.g., 0.5 ETH per 24 hours)
- No real value (cannot be exchanged for mainnet ETH)

## Sepolia Faucets:

- 1 **Alchemy Sepolia Faucet:** <https://sepoliafaucet.com>
  - Requires Alchemy account (free)
  - Provides 0.5 Sepolia ETH per day
- 2 **Infura Sepolia Faucet:** <https://www.infura.io/faucet/sepolia>
  - Requires Infura account (free)
  - Provides 0.5 Sepolia ETH per day
- 3 **QuickNode Faucet:** <https://faucet.quicknode.com/ethereum/sepolia>
  - Requires Twitter account verification
  - Provides 0.1 Sepolia ETH

## Steps:

- Copy your MetaMask address (click address to copy)
- Visit faucet website
- Paste address and request ETH
- Wait 30-60 seconds for transaction confirmation

# Exercise 6: Sending Your First Transaction

## Transaction Steps:

- ❶ Ensure you have Sepolia ETH (from faucet)
- ❷ Click “Send” button in MetaMask
- ❸ Enter recipient address:
  - Option 1: Create second account in MetaMask (send to yourself)
  - Option 2: Use classmate’s address (coordinate in pairs)
  - Option 3: Use burn address: 0x0000...0000 (test only)
- ❹ Enter amount (e.g., 0.1 Sepolia ETH)
- ❺ Review transaction details:
  - Gas fee estimate (varies by network congestion)
  - Total amount (amount + gas fee)
- ❻ Click “Confirm”
- ❼ Wait for transaction confirmation ( 15 seconds on Sepolia)
- ❽ View in Activity tab (shows pending -> confirmed)

## Understanding Gas Fees:

- Gas = computational effort to execute transaction
- Fee = gas units × gas price (in gwei)
- Higher gas price = faster confirmation (priority)
- Sepolia: fees are negligible (testnet)
- Mainnet: fees vary widely (1-50+ USD during congestion)

# Exercise 7: Viewing Transaction on Block Explorer

## What is a Block Explorer?

- Web interface to view blockchain data
- Shows transactions, blocks, addresses, contracts
- Publicly accessible (blockchain is transparent)

## Sepolia Block Explorer:

- Etherscan Sepolia: <https://sepolia.etherscan.io>

## Viewing Your Transaction:

- 1 In MetaMask Activity tab, click on your transaction
- 2 Click “View on block explorer” (opens Etherscan)
- 3 Observe transaction details:
  - Transaction hash (unique identifier)
  - Status (Success / Pending / Failed)
  - Block number (which block included transaction)
  - From address (your address)
  - To address (recipient)
  - Value (amount sent)
  - Gas fee paid
  - Timestamp

## Exercise 8: Creating Additional Accounts

### Why Multiple Accounts?

- Organize funds by purpose (personal, business, savings)
- Privacy (different addresses not easily linked)
- Security (isolate risky activities)

### Creating New Account:

- 1 Click account menu (circular icon, top-right)
- 2 Click "Add account or hardware wallet"
- 3 Select "Add a new account"
- 4 Name account (e.g., "Account 2")
- 5 New account created with new address

### Important Notes:

- All accounts derived from same seed phrase
- Seed phrase recovers ALL accounts
- Accounts use BIP-44 derivation path: `m/44'/60'/0'/0/index`
- Switching accounts: click account menu, select account

### Task:

- Create second account
- Send Sepolia ETH from Account 1 to Account 2
- Verify transaction in block explorer

# Exercise 9: Importing Existing Account

## Import Methods:

### 1 Private Key Import:

- Account menu -> Add account -> Import account
- Paste private key (64 hexadecimal characters)
- Account added (NOT derived from seed phrase)
- Warning: imported accounts NOT backed up by seed phrase

### 2 Hardware Wallet:

- Account menu -> Add account -> Connect hardware wallet
- Select Ledger or Trezor
- Follow on-screen instructions
- Most secure method (private key never leaves device)

## Practice Task (Optional):

- Export private key from Account 2:
  - Account menu -> Account details -> Show private key
  - Enter password to reveal
  - Copy private key
- Create new MetaMask wallet (different browser profile)
- Import private key
- Verify same address appears

## Adding Custom Network (Example: Polygon):

- ❶ Click network selector -> Add network
- ❷ Enter network details:
  - Network Name: Polygon Mainnet
  - RPC URL: <https://polygon-rpc.com>
  - Chain ID: 137
  - Currency Symbol: MATIC
  - Block Explorer: <https://polygonscan.com>
- ❸ Save and switch to network

## Popular EVM Networks:

- Binance Smart Chain (BSC)
- Avalanche C-Chain
- Arbitrum (Ethereum Layer 2)
- Optimism (Ethereum Layer 2)
- Fantom

## Network Resources:

- Chainlist: <https://chainlist.org> (one-click network addition)
- Lists 1000+ EVM-compatible networks with verified parameters

## Critical Security Rules:

### 1 Seed Phrase:

- Never share with anyone (no exceptions)
- Never enter on websites (phishing)
- Never store digitally (paper only)
- Never photograph or screenshot

### 2 Phishing Protection:

- Bookmark MetaMask extension (avoid typing URL)
- Verify website URLs before connecting wallet
- Beware of fake support contacts (MetaMask never DMs first)
- Check transaction details before confirming

### 3 Network Verification:

- Always confirm correct network before transacting
- Mainnet transactions use real money (double-check)
- Testnet assets have no value (safe to experiment)

### 4 Transaction Approval:

- Review recipient address carefully (irreversible)
- Check amount and gas fees
- Start with small test transactions
- Revoke unnecessary token approvals (debank.com, revoke.cash)



## Attack Vectors:

### 1 Phishing Websites:

- Fake dApp sites request seed phrase
- Look-alike domains (metamask.com vs metarnask.com)
- Mitigation: bookmark trusted sites, verify URLs

### 2 Malicious dApps:

- Request unlimited token spending approval
- Drain wallet after approval
- Mitigation: review permissions, limit approvals

### 3 Clipboard Malware:

- Replaces copied address with attacker's address
- Victim sends funds to wrong address
- Mitigation: verify first/last characters after pasting

### 4 Fake Support Scams:

- Impersonators offer help via DM
- Ask for seed phrase or remote access
- Mitigation: never respond, MetaMask has no live support DMs

## Submit the following:

### ❶ Screenshot Collection (single PDF):

- MetaMask wallet main screen showing Sepolia network
- Transaction details from MetaMask Activity tab
- Etherscan transaction page showing confirmed transaction
- Account list showing at least 2 accounts

### ❷ Lab Report (1-2 pages):

- Your Sepolia address (Account 1)
- Transaction hash of sent transaction
- Reflection questions:
  - ❶ Why is seed phrase security more critical than password security?
  - ❷ How does testnet differ from mainnet in practice?
  - ❸ What are three ways to protect against phishing attacks?
  - ❹ Why are blockchain transactions irreversible?

### ❸ Bonus (Optional):

- Add Polygon testnet (Mumbai) and obtain testnet MATIC
- Demonstrate cross-chain address consistency (same address on different chains)

**Submission Deadline:** One week from lab session date

- MetaMask is a non-custodial wallet (you control private keys)
- Seed phrase is the master backup (protects access to all accounts)
- Testnets provide safe environment for learning and experimentation
- Gas fees vary by network congestion (testnet fees negligible)
- Block explorers provide transparency into all blockchain activity
- Security requires vigilance against phishing, malware, and scams
- Blockchain transactions are irreversible (verify before sending)

## Next Steps:

- Keep wallet active for future labs
- Explore dApps on testnets (Uniswap, Aave, OpenSea testnet versions)
- Practice safe wallet habits
- Never use testnet wallet for mainnet funds (create separate wallet for real funds)

- ❶ What would happen if you lost both your password and seed phrase?
- ❷ Why do imported private keys not get backed up by the seed phrase?
- ❸ How does MetaMask generate multiple accounts from a single seed phrase?
- ❹ What is the purpose of requiring gas fees for transactions?
- ❺ Why are hardware wallets considered more secure than browser extensions?
- ❻ How can you verify that a website is safe to connect your wallet to?

### Topics to be covered:

- Proof-of-stake fundamentals and comparison with proof-of-work
- Validator mechanics: staking, attestation, block proposal
- Slashing conditions and penalties
- Ethereum 2.0 Beacon Chain architecture
- Finality and checkpoint mechanisms
- Staking economics and rewards
- Centralization risks in proof-of-stake systems

### Preparation:

- Review proof-of-work consensus (Lesson 7)
- Read about Ethereum's transition to proof-of-stake (The Merge, 2022)
- Explore current staking statistics ([beaconcha.in](https://beaconcha.in))