BCT

Practical 2

Problem Statement

Create your own wallet using Metamask for crypto transactions.

Objectives

- To understand the concept of crypto wallets and how they function.
- To install and configure MetaMask on a system or mobile device.
- To learn how to create and secure a wallet using a seed phrase.
- To perform basic crypto transactions (send and receive).
- To explore how to connect MetaMask with blockchain networks and dApps.

Hardware Requirements

- Computer or laptop with minimum 4 GB RAM.
- Stable internet connection (Wi-Fi or broadband).
- Smartphone (optional) for MetaMask mobile app.
- USB or paper/metal backup for seed phrase storage.

Software Requirements

- Windows 10+/macOS/Linux or Android/iOS OS.
- Web browser – Chrome, Firefox, Brave, or Edge.
- MetaMask extension or mobile app.
- Antivirus/VPN for security and privacy.

Theory

(a) Concept of Crypto Wallet

- A crypto wallet stores private keys — digital signatures required to access and transfer cryptocurrency.
- Wallets are non-custodial (user-controlled) or custodial (exchange-controlled).

(b) Types of Wallets

1. Hot Wallets: Connected to the internet (e.g., MetaMask, Trust Wallet).
2. Cold Wallets: Offline storage (e.g., hardware wallets, paper wallets).

(c) Public and Private Keys

- Public Key / Address: Used to receive funds; can be shared openly.
- Private Key: Used to sign transactions; must be kept secret.

(d) Seed Phrase (Recovery Phrase)

- A 12- or 24-word mnemonic generated when creating a wallet.
- It can recover all associated accounts and tokens if the wallet is lost.

(e) Hierarchical Deterministic (HD) Wallet

- Uses a single seed phrase to derive multiple wallet addresses deterministically (BIP-39 standard).

(f) Transaction Signing

- A transaction includes recipient address, amount, gas fees, and data.
- The wallet signs this using the private key to authenticate ownership.

(g) Gas Fees

- Fee paid to miners/validators for processing a transaction.
- Measured in Gwei (a fraction of ETH).

(h) Blockchain Networks

- MetaMask supports Ethereum Mainnet and other EVM-compatible chains (Polygon, BSC, Avalanche, etc.).
- Custom networks can be added via RPC URLs.

(i) Smart Contracts

- Programs stored on the blockchain that execute automatically.
- MetaMask interacts with these through dApps.

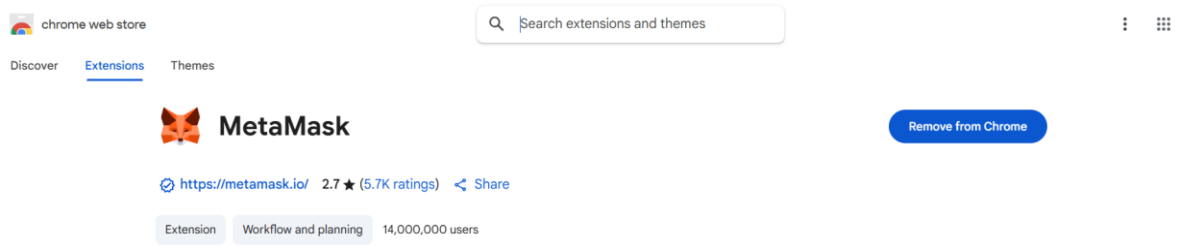
(j) Security Model

- Funds are protected by private keys.
- If a private key or seed phrase is lost or leaked, funds are unrecoverable.

Step-by-Step Procedure

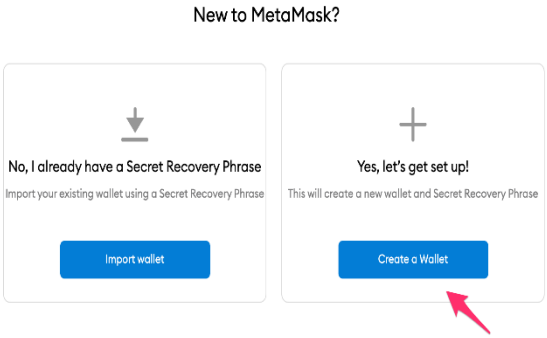
Step 1: Install MetaMask

- Open https://metamask.io.
- Download for your browser (Chrome, Firefox, Edge, Brave).
- Add the MetaMask extension or install the mobile app.



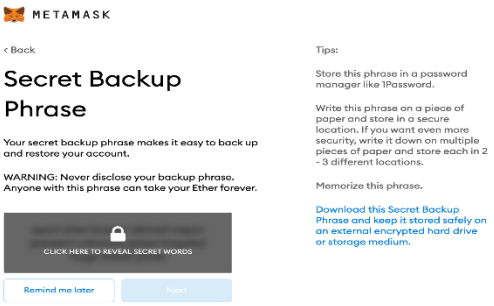
Step 2: Create a New Wallet

- Click Get Started → Create a Wallet.
- Set a strong password.
- Agree to terms and continue.



Step 3: Backup Seed Phrase

- Note down the 12-word Secret Recovery Phrase offline.
- Store it securely (paper or metal backup).
- Confirm the phrase in correct order.

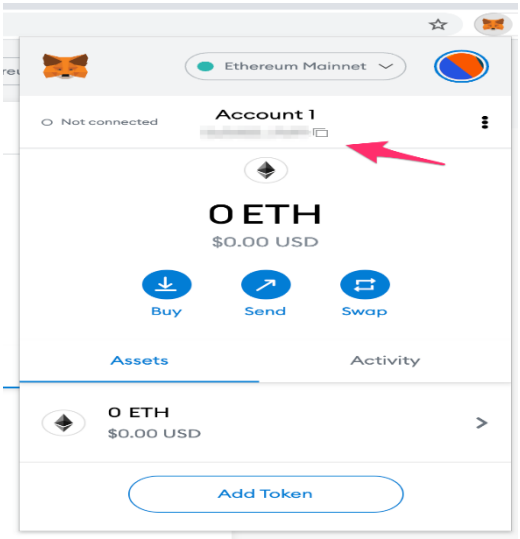


Step 4: Access Wallet

- View your Ethereum address (starts with "0x…").
- Share only this address to receive crypto.

Step 5: Receive Crypto

- Click Receive → Copy wallet address.
- Share or receive funds from other wallets/exchanges.

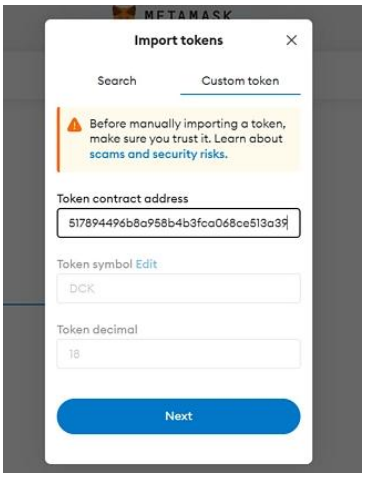


Step 6: Send Crypto

- Click Send → Paste recipient address.
- Enter amount and confirm gas fee.
- Review and click Confirm.

Step 7: Add Tokens

- Click Import Tokens → Paste token contract address → Add.
- Manage all your tokens from the wallet.



Step 8: Connect to a dApp

- Visit a decentralized app (e.g., Uniswap, OpenSea).
- Click Connect Wallet → Approve connection.
- Interact with smart contracts safely.

Step 9: Add Custom Network

- Go to Settings → Networks → Add Network.
- Enter RPC URL, Chain ID, Symbol, Explorer URL.
- Save and switch between networks.
-

Security Practices

1. Never share your seed phrase or private key with anyone.
2. Backup your seed phrase offline in multiple secure places.
3. Use a hardware wallet (Ledger/Trezor) for storing large funds.
4. Always download MetaMask from the official website only.
5. Avoid using public Wi-Fi for transactions.
6. Lock your wallet when not in use.
7. Keep your browser, OS, and antivirus updated.
8. Use limited token approvals when interacting with dApps.
9. Regularly revoke unused approvals using trusted sites (e.g., Etherscan).
10. Verify URLs carefully to avoid phishing (bookmark trusted sites).
11. Use a different wallet for testing or small transactions.
12. Never store your seed phrase digitally (email, screenshot, drive).

Common Errors & Solutions

Problem	Cause	Solution
Wallet not syncing	Outdated app	Update MetaMask
Lost password	Forgot MetaMask password	Recover using seed phrase
Token not visible	Not added manually	Import token contract address
Transaction pending	Low gas fee	Speed up or cancel transaction
Wrong network	Using different chain	Switch to correct network

Conclusion

In conclusion, MetaMask provides a simple and secure way to create and manage a personal cryptocurrency wallet. Through this project, we learned how to install MetaMask, create a wallet, back up the recovery phrase, and perform crypto transactions safely. It helps users understand the working of blockchain, private keys, and decentralized applications (dApps). By following proper security practices like keeping the seed phrase safe and verifying all transactions, users can securely explore the world of digital currencies. Thus, MetaMask serves as an essential tool for entering and understanding the decentralized Web3 ecosystem.