

Technische Grundlagen für fortgeschrittene DeFi-Nutzer

➡ Dieses Modul richtet sich an Nutzer, die sich für das Thema DeFi interessieren. Wir gehen auf die grundlegenden Funktionalitäten von der Blockchain ein, sprechen über Wallets und Sicherheitsmassnahmen. Wir kratzen hier bewusst nur an der Oberfläche.

Grundprinzip Private und Public Key

Wie funktionieren Adressen & Schlüssel?

- **Public Key:** Deine öffentliche Adresse – kann jeder sehen & nutzen, um dir Coins zu senden.
- **Private Key:** Dein persönlicher Schlüssel – ermöglicht vollen Zugriff auf deine Coins.

⚠ **Nie den Private Key weitergeben! Wer diesen hat, hat deine Coins.**

Seed Phrase (Recovery Phrase)

- Eine 12- oder 24-Wort-Phrase, die deine Private Keys wiederherstellt.
- Wenn du sie verlierst, gibt es keinen Weg, deine Coins zurückzubekommen.
- Bewahre sie offline auf – am besten auf Papier oder Metallplatten.

💡 **Private Keys sind wie deine Bank-PIN – Seed Phrases sind dein Master-Schlüssel.**

Hot und Cold Wallets

Hot Wallets (z. B. MetaMask, Trust Wallet)

✅ Vorteile:

- Schnell & einfach für tägliche Transaktionen.
- Direkter Zugriff auf dezentrale Anwendungen (DApps).
- Kostenlos in der Nutzung.

⚠ Nachteile:

- Online verbunden → Höheres Risiko für Hacks & Scams.

- Private Keys sind anfälliger für Phishing & Malware.

Cold Wallets (z. B. Ledger, Trezor, Bitbox, etc.)

✓ Vorteile:

- Private Keys sind **offline** und nicht angreifbar durch Hacker.
- Beste Wahl für langfristige Aufbewahrung größerer Beträge.
- Schutz vor Phishing und betrügerischen DApps.

⚠ Nachteile:

- Umständlicher für schnelle Transaktionen.
- Hardware-Wallets kosten Geld (ca. 50–150 €).
- Verlust des Geräts oder der Seed Phrase = Totalverlust.

📌 Regel:

- **Hot Wallets** sind praktisch für kleine Beträge & tägliches Trading.
 - **Cold Wallets** sind essenziell für langfristige Sicherheit und größere Investments.
-

Zentralisiert vs. Dezentralisiert

📌 CEFI (Zentralisierte Plattformen, Custodial Wallets)

- Börsen wie Binance, Kraken, Coinbase verwalten deine Coins für dich.
- + Einfach für Anfänger
- - Kein direkter Zugriff auf deine Private Keys („Not your keys, not your coins“) – Plattform kann gehackt oder reguliert werden.

📌 DeFi (Dezentrale Plattformen, Non-Custodial Wallets)

- Wallets wie MetaMask, Trust Wallet, Rabby geben dir volle Kontrolle.
- + Du bist dein eigener Bank.
- - Höhere Verantwortung: Kein Support, keine Rückholoptionen bei Fehlern.

📌 Fazit:

- **CEX** für einfaches Kaufen, Handeln & Fiat-Zugänge.
 - **DeFi** für Fortgeschrittene gut, da erhöhte Sicherheit & weniger Gebühren.
-

Blockchains und Netzwerke

➡ Eine Blockchain ist eine dezentrale, digitale Datenbank, die aus einer Kette von Blöcken besteht. Jeder Block enthält eine Liste von Transaktionen und ist kryptografisch mit dem vorherigen Block verbunden. Dadurch entsteht eine unveränderliche und transparente Aufzeichnung aller Transaktionen.

💡 Wie funktioniert sie?

- Transaktionen werden gesammelt und in einem neuen Block gespeichert.
- Dieser Block wird mit einem kryptografischen Hash gesichert und an die Kette angehängt.
- Das Netzwerk verifiziert die Daten dezentral, wodurch Manipulation nahezu unmöglich wird.

💡 Warum ist das wichtig?

Die Blockchain-Technologie ermöglicht Vertrauenslose und sichere Transaktionen, da keine zentrale Instanz benötigt wird. Sie bildet die Grundlage für Bitcoin, Ethereum und viele andere Kryptowährungen sowie Anwendungen in Finanzwesen, Logistik und Smart Contracts.

💡 Warum, gibt es verschiedene Chains?

Nicht alle Blockchains sind kompatibel – du kannst nicht einfach BTC auf Ethereum senden.

- **Bitcoin (BTC):** Sicherstes Netzwerk, aber langsam & teuer für Transaktionen.
- **Ethereum (ETH):** Smart-Contract-Plattform, hohe Adoption, aber oft hohe Gebühren.
- **Layer 2 (z. B. Arbitrum, Optimism):** Skalierungslösungen für Ethereum.
- **Binance Smart Chain (BSC):** Günstig & schnell, aber stärker zentralisiert.
- **Solana (SOL):** Hohe Geschwindigkeit, aber nicht so dezentral wie Ethereum.
- **Cosmos & Polkadot:** Interoperabilität zwischen Blockchains.

⚠ **Wichtig:** Immer prüfen, auf welcher Chain deine Assets liegen – falsche Netzwerknutzung kann zum Verlust der Coins führen.

Verwahrung & Wallet-Grundlagen

➡ Bevor du DeFi-Anwendungen sicher nutzt, musst du dein Kapital richtig verwahren.

✅ Empfohlene Wallets für DeFi:

- **Trust Wallet** → Mobile-First-Option mit breiter Unterstützung.
- **MetaMask** → Beste Option für Browser- & Desktop-Nutzung.

💡 Kurz erklärt:

- **MetaMask & Trust Wallet sind non-custodial**, das heißt, du bist für deine Private Keys verantwortlich.
- **Wenn du deine Seed Phrase verlierst**, gibt es keine "Passwort vergessen".
- **Updates sind extrem wichtig**: Dein Browser und deine Wallet-Erweiterung sollten **immer aktuell** sein, da ältere Versionen Sicherheitslücken aufweisen können.

⚠ **Regel**: Halte deine Software immer auf dem neuesten Stand, um Exploits zu vermeiden!

Das beste Wallet-Setup für maximale Sicherheit

💡 Hot Wallets vs. Cold Wallets

- Hot Wallet (z. B. MetaMask, Trust Wallet) → Nutze es für tägliche Transaktionen.
- Cold Wallet (Ledger, Trezor) → Für langfristige Aufbewahrung & höhere Sicherheit.

📌 Empfohlene Kombination:

- ✅ Metamask für den täglichen DeFi-Gebrauch
- ✅ Ledger als zusätzlichen Schutz für grössere Beträge

💡 Warum ein Hardware Wallet?

- Ein Ledger oder Trezor speichert deine Private Keys offline – Hacker haben keinen Zugriff.
 - Selbst wenn dein PC kompromittiert wird, kann niemand ohne dein physisches Gerät Transaktionen bestätigen.
 - Bei jeder Transaktion musst du die Bestätigung auf deinem Hardware-Wallet geben – du hast die volle Kontrolle.
-

Wichtige Sicherheitsannahmen bei der Nutzung von DeFi-Protokollen

⚠️ Nutze immer die richtigen Links

- Pass auf, wenn du über Google-Suchergebnisse auf DeFi-Plattformen gehst!
- Phishing-Websites sehen oft genau aus wie das Original, haben aber manipulierte Smart Contracts.

✅ Lösung:

- Erstelle eine Lesezeichenleiste mit den offiziellen Links deiner DeFi-Protokolle.
 - Nutze Debank (<https://debank.com/>) zur Übersicht deiner Wallet-Aktivitäten.
-

⚠️ Sei vorsichtig mit Wallet-Berechtigungen (Allowances)

➡ Beim Nutzen von DeFi-Protokollen gibst du oft Smart Contracts eine Erlaubnis (Allowance), deine Coins zu bewegen.

⚠️ Das Problem:

- Manche Plattformen verlangen unbegrenzte Berechtigungen (Infinite Approvals).
- Das bedeutet, dass sie theoretisch deine kompletten Token bewegen könnten, ohne weitere Bestätigung.

✅ Lösung:

- Überprüfe immer die Allowances bevor du sie bestätigst!
- Nutze Debank (<https://debank.com/>) oder Revoke.cash (<https://revoke.cash/>), um bestehende Berechtigungen zu überprüfen und zurückzunehmen.
- Setze manuelle Limits, z. B. nur den Betrag genehmigen, den du tatsächlich handeln möchtest.

⚠️ **Regel:** Eine Plattform sollte niemals die vollständige Kontrolle über deine Coins haben – diese muss immer in deiner Hand bleiben!

Die wichtigsten DeFi-Plattformen für fortgeschrittene Nutzer

Hier sind die essenziellen DeFi-Tools und Protokolle, die du nutzen kannst:

 Summer.fi (ehemals Oasis App) → Dezentralisierte Kreditplattform
 [Hier klicken](#)

 Aave → Liquiditätsmarkt für Lending & Borrowing
 [Hier klicken](#)

 Jumper → Cross-Chain Bridge für schnelle Asset-Übertragungen
 [Hier klicken](#)

 1inch → DEX-Aggregator für das beste Swap-Preisangebot
 [Hier klicken](#)

 Debank → DeFi-Wallet-Tracking und Allowance-Überprüfung
 [Hier klicken](#)

 **Schütze dich:** *Nutze nur offizielle Links und baue diese bestenfalls in deine Lesezeichenleiste ein, um Scams zu vermeiden.*