Krypto-Wallets – Einleitung und Überblick

Christian Baumann

Arbeitskreis Blockchain - Arbeitsgruppe Technik & Blockchain Lab

18.9.2025 (v0.4)

AUSTRIA PRO

Inhalt „Wallets“

- Aufgaben
- Funktionen
- Typen
  - Vor-/Nachteile
- Beispiele
- Hands-On

Aufgaben eines „Krypto-Wallets“

- Aus Begriff leiten sich die Funktionen/Aufgaben ab
  - kryptografische Keys
  - Verschlüsselung, digitale Signatur
  - Kryptowährungen (im Jargon „Crypto“)

- Wofür ist es **NICHT**
  - Speicherung von Kryptowährungen, Tokens & NFTs IM Wallet selbst
- Sondern: Speicherung von Keys, um auf diese Assets (auf den Blockchains) zugreifen zu können

- Analogie physische Geldbörse („speichert Geld“) vs. Kreditkarten-Etui („speichert Zugriffsinformationen“)

Kryptografische Keys - Generierung 1/2

- Eine Zufallszahl wird generiert (aus „Entropy“, „strong source of randomness“)
  - zB 128 bit = 2^128 = 3,402…e+38 Möglichkeiten
- Diese wird dargestellt als BIP39 Mnemonic (typ. 12, 18, 24 Wörter), zB:
- **slab oxygen meadow history athlete reflect royal delay prison gate right hand match jewel hundred increase lyrics drift trumpet share rifle beef south present**
- Dazu noch eine Passphrase (optional): **SuperSecret8871#**
- Ergibt den BIP39 Seed:
  `164437a6c437730d772f45998a6aaeffddf9e24e598b20452b9c8964ca29c8d04262dcf8e23d07414879f81d6f4d721f2830882b6a241517b31cd5419b9241ee`
- Auswahl einer Coin/Chain, z.B.: `ETH – Ethereum`
- Ergibt den BIP32 Root Key:
  `xprv9s21ZrQH143K4JqqiPFazEuEyqrUDMU9i4QqvKwUFJKgcWpq6ZztgNNRLMLg4KPmxZZ3tE46zHUkCbrexc2jhedpJ849s1N37a929d6sF26`
- …

Kryptografische Keys - Generierung 2/2

Ergebnis ist eine (beliebig lange) Liste mit Wallet-Adressen und deren Keys, zB.

path,**address**,public key,**private key**

m/44'/60'/0'/0/0,**0x30a889eeC026C0130AaF1ADE69264fcf845A7b91**,0x02f3874ef89768f20aa68224f1f11334db5158d385736206e6aff3bcc2045e93a9,**0xe91518e05dea2e2fee5a910d07b9fd3c83c04459826a2de2536a9f14b49157ad**

m/44'/60'/0'/0/1,**0x94E92aD32302e0Bc806c3cf1050843E041FB359F**,0x02b13c2568c27f1b29a903605434006dd0466ba99f05f627ffa6bd203eeafea13d,**0xe0a803b79b842dd58f18e697767c6608324be7044705bf1109e3b772a75fe0f8**

m/44'/60'/0'/0/2,**0x47cDE99F8159b48ae5B859B31c008a8481d5532f**,0x02a091e5852740a2e36d7bb26d884c1436753663b14081b86dfa9eb5fb0594a510,**0xa62f8b8252f16898c6dfe8e9ca9799df4ae493863cb70e8641cf73fee3f5f63e**

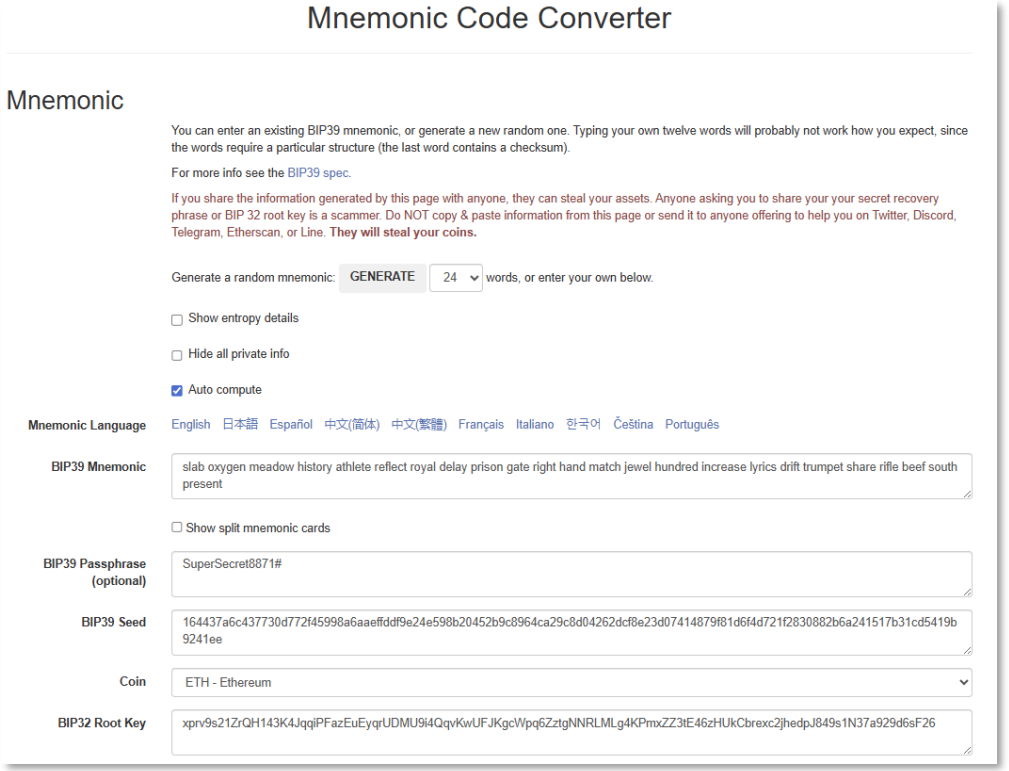
m/44'/60'/0'/0/3,**0xF40ccA9ba30362AC8FAdAd4303EC8653EE6D9f73**,0x03e9190973827ceabf8f354bf2cc8d03e3d73e230b43766a3d10b8d09690d75dd3,**0xf8447440774640e6ca32db951f11f8debefd2acca2ab13865b453672105e064e**

m/44'/60'/0'/0/4,**0x1fd4b22Fe18823Ce55A2091B9dF7A427BD9f83De**,0x035741ca1bb9551e8042ff147b746a445a346ae0dc39d98f54aa679e98ac2423cb,**0xe8a0b3b4270c85e6ab56937452a59ba6962ffe87454366a46aa66c115aeff069**

…

Quellen & Details BIP39

- Spezifikation
  - https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- Tool
  - https://iancoleman.io/bip39/
  - Mehrsprachig
  - Offline verwendbar („airgapped“)



Funktionen von Wallets

- Aus der Seed-Phrase die „Accounts“ (Adressen und deren private Keys) ableiten und verwalten.
- Die Daten passwortgeschützt verschlüsseln und am Gerät speichern
- Mehrere Chains konfigurieren und verwalten („Multichain-Wallets“)
  - früher nur Ethereum wichtig, mittlerweile werden weitere Blockchains massiv eingesetzt (Polygon, Gnosis, Binance …)
- Anwendung mit der jeweiligen Blockchain verbinden
  - Accounts identifizieren, Transaktionen signieren und absetzten
- Tokens und NFTs anzeigen
- Schnittstelle für dApps
  - Finanzbereich
  - NFT Portale (OpenSea, mintable.app …)

Sicherheit

- **„not your keys … not your coins (or NFTs)“**
- Die Seed-Phrase (Wortliste)
  - Sicher aufheben (auch auf Papier, Alternativen siehe später …)
  - NIE aus der Hand geben
  - Niemandem mitteilen (Achtung bei Phishing oder anderen Scams)
  - Am Computer gespeichert? Nur verschlüsselt (z.B. Passwort-Manager)
- Jeder, der die Wortliste kennt, kann alle Adressen, private Keys … daraus herstellen und hat somit die volle Kontrolle über alle dem Wallet zugehörigen Assets (auf allen verwendeten Blockchains)!
- Es gibt bei der Seed-Phrase keine Funktion, diese wieder herzustellen
  - wie zB. „Passwort vergessen …“ – Funktionen bei normalen Web-Anwendungen

Typen von Wallets

- Softwarewallets
  - Als Browser-Plugin
  - Als Browser App
  - Als PC/Mac Programm
  - Am Smartphone
  - (Wallet Connect)
- Hardwarewallets
- Paper-, Cardwallets
  - „Cold Storage“

Wallet Provider	Easy Sign-Up	Purchase Crypto with Credit Card	Notes
MetaMask		✓	○
Coinbase Wallet			
TrustWallet		✓	
Portis	✓	✓	
Fortmatic/ Magic	✓	✓	
Venly	✓		
Authereum	✓	✓	●
Bitski	✓		
Dapper		✓	
Kaikas			
MetaMask Mobile		✓	○
OperaTouch			
Torus	✓	✓	
WalletConnect	✓		
WalletLink (Coinbase Wallet)	✓		

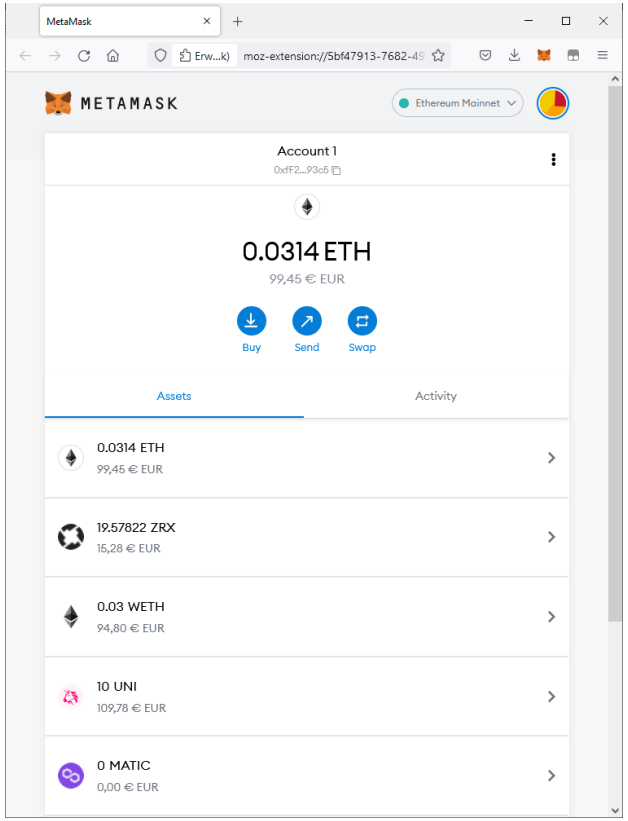
○ ETH is purchasable via third-parties in some regions

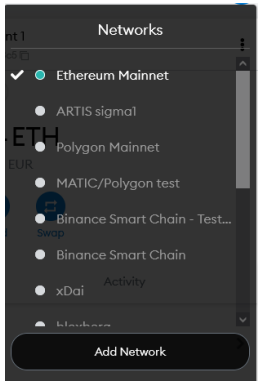
● Only available in USA

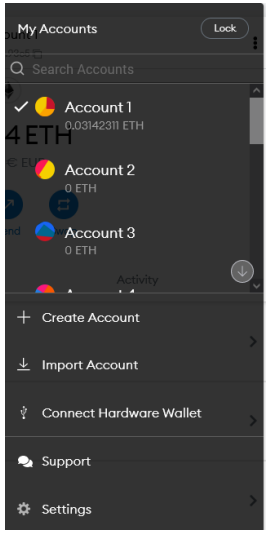
AUSTRIA PRO

Browser-Plugin

- MetaMask
  - Größte Verbreitung
  - Für Chrome, Firefox, Brave, Edge, ~~Safari~~
  - Mehrere Chains (auch Testchains)
  - Viele Accounts
  - Kompatibel zu allen gängigen dApps
  - Unterstützung von Hardware-Wallets
  - NFT Unterstützung
    - „Portfolio“
    - Oder nur manueller Import

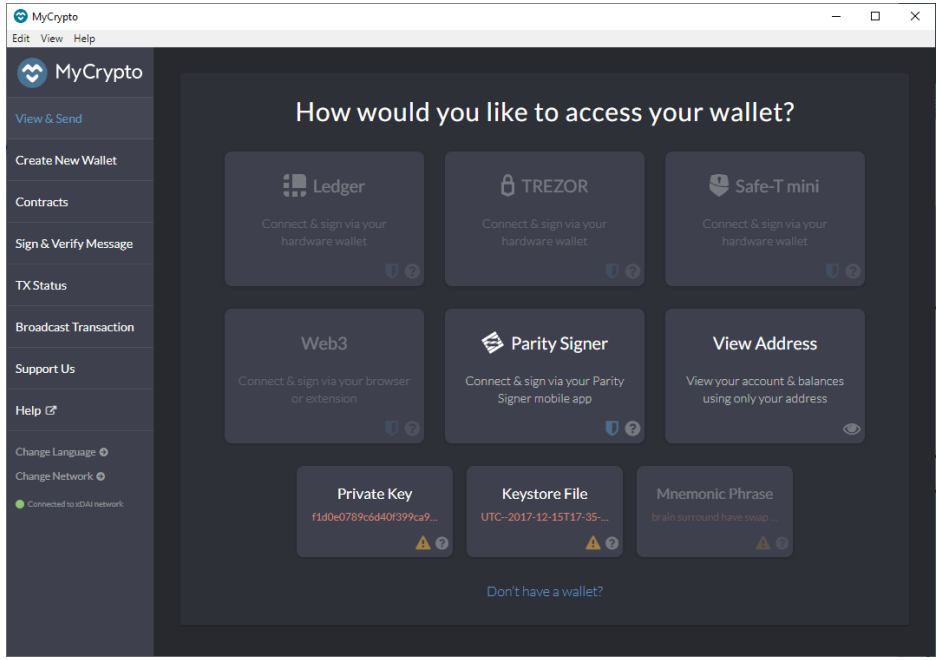




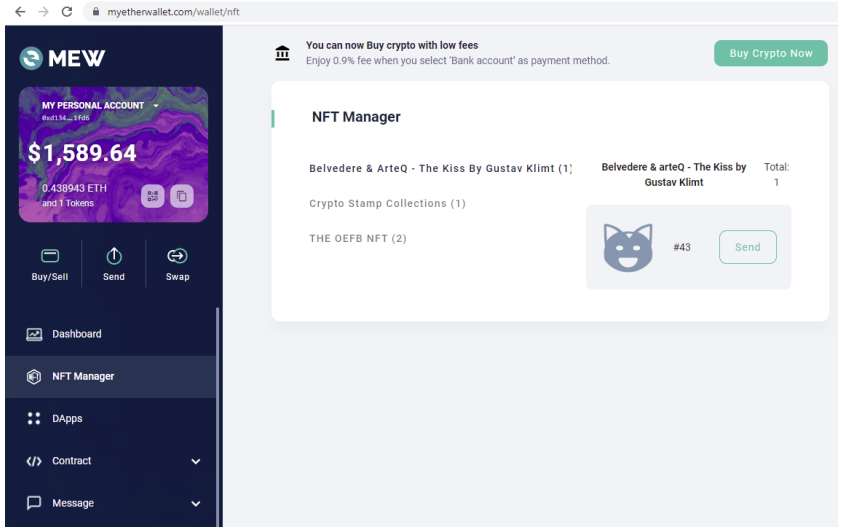


Browser-Apps

- MyCrypto – Web & installiert
  - Alle gängigen Wallets: Hardware, Web3 …
  - View Address
  - Contract Interaction, Message Signing
  - „Tools“ für private Keys, Keystores, Seed-Phrases

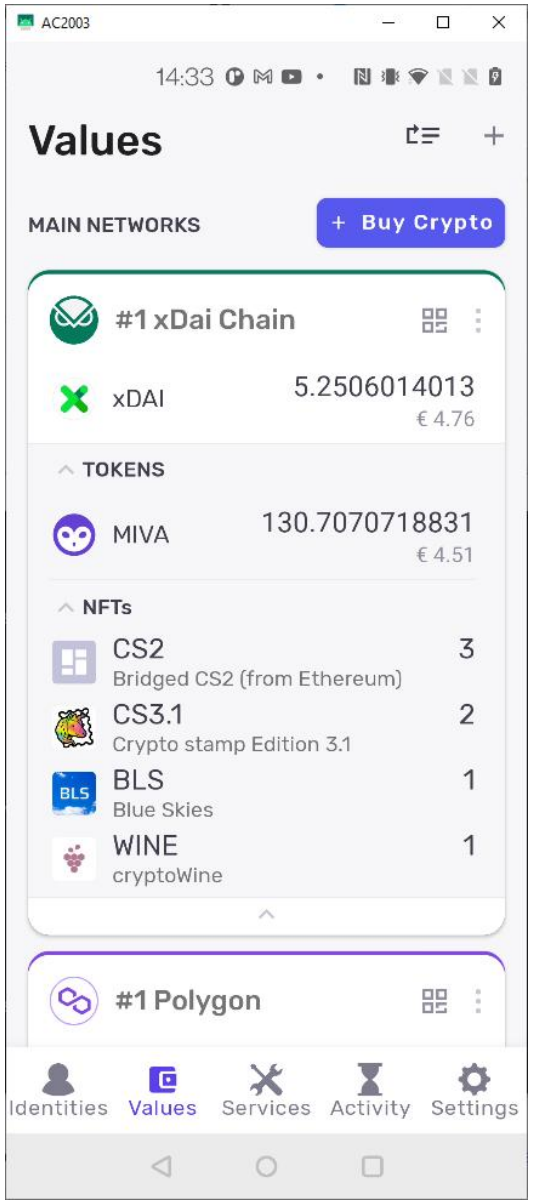


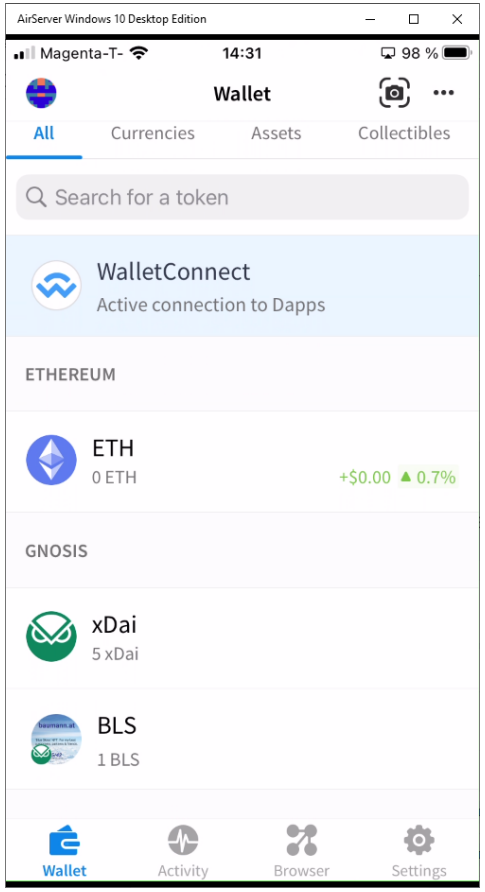
- MEW - MyEtherWallet
  - Eigenes Wallet oder Web3 …
  - Übliche Funktionen
  - Rudimentäre NFT Unterstützung



Mobile Wallets

- MetaMask mobile
  - Übliche Funktionen (wie Browser Plugin)
  - Rudimentäre NFT Funktionen
- Android: Minerva Wallet
  - Mehrere Chains
  - Mehrere Accounts
  - NFT Unterstützung
  - https://minerva.digital/
- iOS: AlphaWallet
  - Mehrere Chains
  - NFT Unterstützung

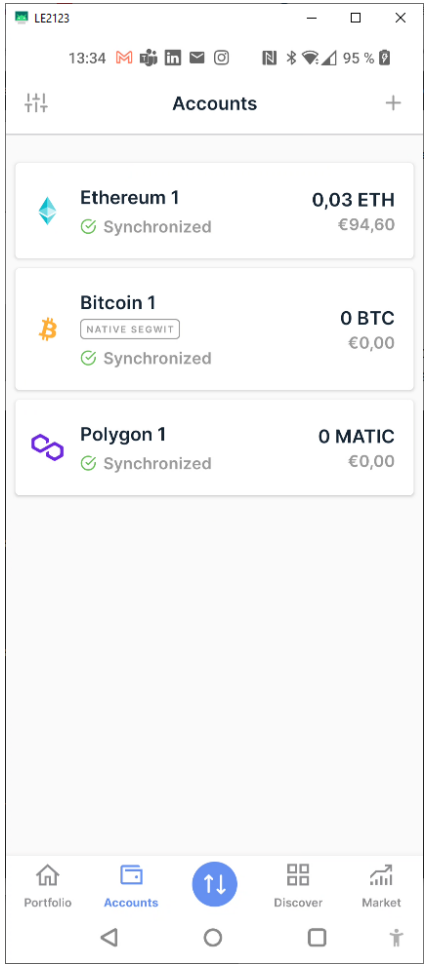




Hardware Wallets

- Extrem sicher
  - Physischer Besitz & PIN
- Alle kryptografischen Funktionen auf eigener Hardware
- Interaktion mit Software am PC oder Smartphone, Kabel oder Bluetooth
- Weitere Infos: siehe „Crypto-Wallets (Hardware) – Übersicht“ (AustriaPro & bc-init.at)

- „Plausible deniability“ kann verwendet werden, d.h. andere Passwörter leiten andere Walletadressen ab
- https://en.wikipedia.org/wiki/Plausible_deniability#Use_in_cryptography



Offline Wallets – „Cold Storage“

- Paperwallet
  - Public & private Key eines Accounts
    - Gedruckt, meist mit QR-Code
  - Sicheres Speichern von großen Beträgen
  - Kartenform
- „Steel-Wallets“
  - Bis zu 24 Wörter Seed-Phrase
- Card-Wallets
  - Crypto-Chip
  - Private Key nicht auslesbar

Weitere Begriffe

- Custodial / non custodial Wallets
  - Custodial: Keys nicht unter eigener Kontrolle
  - Vertrauen in Betreiber vorausgesetzt
  - Bei Krypto-Exchanges verwendet
    - Frühere Hacks, zB. Mt. Gox, 60% des Bitcoin Handels, 2014: 650.000 BTC „verschwunden“, damals 800 Mio USD, offiziell 7000 durch einen Hacker, 643.000 „unterschlagen“
    - D.h. „Hacks“ betreffen nicht die Blockchain-Technologie selbst, sondern unzureichende Sicherheitsmaßnahmen von Betreibern (von zB. Krypto-Exchanges)
  - „not your keys … not your coins“
  - Aber: Exchanges notwendig, Wechseln von FIAT in Crypto u.a.
    - In EU streng überwacht (KYC laut Bankgesetzen)
    - Beispiel in AT: Bitpanda, Coinfinity
- Watch Only Wallets
  - Nur Walletadresse nötig (kein private Keys)
  - Um bestimmte (auch fremde) Accounts anzuzeigen
  - Und deren Tokens und NFTs

Beispiele, Hands on

- Beispiele für Workshops
  - Siehe „Wallet-Setup_20250916_v08“ (AustriaPro)

- Am PC/Mac (in Chrome, neues Profil)
  - MetaMask installieren und konfigurieren (zweites network Polygon einrichten)
  - https://metamask.io/ - https://chainlist.org/
  - Verbindung zu einer dApp herstellen am Beispiel OpenSea

- Android
  - MetaMask mobile
  - Minerva Wallet
- iOS
  - MetaMask mobile
  - AlphaWallet

AUSTRIA PRO

Kontakt

www.austriapro.at

austriapro@wko.at

DI Dr. Christian Baumann
c.baumann@baumann.at
+43 664 43 24 243