Digital Lisa Club – ANCHOR’ s

ENC-Wallet.json — Erklärung & Nutzung

1. Was ist die ENC-Wallet.json?

Die ENC-Wallet.json ist kein echtes Wallet, sondern eine Hilfsdatei, die innerhalb des Anchor-Systems benötigt wird, um verschlüsselte HQ-Dateien (HQ-ENC) sicher zu verwalten. Sie dient als Schnittstelle zwischen der Bitcoin-Signatur (BIP-322) des Besitzers und den verschlüsselten Dateien (ENCs), die zu einem Anchor gehören.

Kurz gesagt:

Die ENC-Wallet.json ist eine technische Identitätsdatei, die es ermöglicht, dass das System weiß, welcher Public Key zur Entschlüsselung eines verschlüsselten Assets verwendet werden darf.

2. Wann und warum braucht man eine ENC-Wallet?

Eine ENC-Wallet.json wird immer dann benötigt, wenn man:

- einen Anchor mintet oder kauft, der eine HQ-ENC-Datei nutzt oder enthält,
- oder wenn man einen solchen Anchor verkaufen möchte.

Mit ENC-Wallet.json kann das System sichere Schlüsselübergaben (Keywraps) durchführen ohne das man sein Harwarewallet auslesen muss.

3. Warum ist sie notwendig?

Wenn ein Anchor mit einer verschlüsselten HQ-Datei verkauft wird, muss beim Besitzerwechsel ein neuer Verschlüsselungsschlüssel (Keywrap) erzeugt werden. Dieser Keywrap basiert auf einer Signatur des Käufers (canonical message), die später den Content Encryption Key (CEK) entschlüsseln kann.

Damit das sicher funktioniert:

- darf diese Signatur des Käufers niemals öffentlich werden,
- wird sie daher verschlüsselt auf den Public Key des Verkäufers (aus dessen ENC-Wallet.json) geschrieben.
  Nur der Verkäufer kann mit Hilfe der Dapp diese verschlüsselte Signatur wieder entschlüsseln.

So bleibt gewährleistet, dass nur der aktuelle Besitzer Zugriff auf die sensiblen Daten erhält.

4. Warum keine Hardware-Wallet?

Die ENC-Wallet.json darf nicht auf einer Hardware-Wallet (Ledger, Trezor usw.) basieren, denn:

- Sie müssen Zugriff auf den PrivKey des erzeugten Public Keys** haben**,
- und Hardware-Wallets geben diesen niemals heraus.

Darum wird der ENC-Wallet-Key immer mit dem AnchorKey Generator erstellt – entweder offline oder online.

5. Erstellung einer ENC-Wallet.json (Schritt-für-Schritt)

Teil 1 — Offline Keypair generieren

1. Öffnen Sie AnchorKey OFFLINE.html (läuft komplett ohne Internetverbindung).

2. Klicken Sie auf Generate Keypair.

--> Es wird ein voll funktionsfähiges Bitcoin BIP-322 Keypair erzeugt:

- Address
- Public Key
- Private Key

3. Klicken Sie anschließend auf Download Encrypted Keypair.

- Wählen oder generieren Sie ein sicheres Passwort.
- Klicken Sie auf Encrypt & Download.

  Ihr Browser lädt nun 3 Dateien herunter:

PubKey+Address-for-Import_YYYY-MM-DD.txt

Password_For_Encrypted_Key_YYYY-MM-DD.txt

Encrypted_Private_Key_YYYY-MM-DD.txt

4. Sicherung der Dateien:

- Bewahren Sie Password_For_Encrypted_Key... und Encrypted_Private_Key...auf zwei verschiedenen USB-Sticks auf.
- Die Sticks müssen getrennt voneinander gelagert werden.
- Mit dem verschlüsselten Private Key kann niemand etwas anfangen, solange das Passwort unbekannt ist.

Teil 2 — ENC-Wallet.json erstellen

1. Öffnen Sie AnchorKey ONLINE.
2. Klicken Sie auf Import Data und wählen Sie die Datei
   PubKey+Address-for-Import_YYYY-MM-DD.txt aus.
3. Geben Sie unter “ Enter your BTC address” Ihre eigene Bitcoin-Adresse ein.
4. Klicken Sie auf Generate ENC-Wallet.json.
   --> Das System erzeugt eine Signatur-Nachricht.
5. Signieren Sie diese Nachricht in Ihrer Bitcoin-Wallet (z. B. Sparrow) per BIP-322.
6. Fügen Sie die erzeugte Signatur in das Feld“ Enter BIP322 signature…” ein.
7. Klicken Sie auf Verify Signature.
   Wenn die Signatur gültig ist, erscheint der Button:
   Upload ENC-Wallet-TX
   --> Mit diesem Button wird die ENC -Wallet. json auf Arweave hochgeladen.

6. Was passiert, wenn man Daten verliert?

- Wenn Sie Ihre ENC-Wallet-Dateien oder das Passwort verlieren,
  können Sie jederzeit eine neue ENC-Wallet.json erstellen.
- Die neue Version wird automatisch verwendet, sobald Sie ein neues Angebot erhalten
  oder ein Anchor minten.
- Wichtig: Wenn Sie bereits ein Kaufangebot (Offer) mit einer verschlüsselten Signatur
  erhalten haben, diese Signatur aber mit Ihrer alten ENC-Wallet erstellt wurde, dann kann
  sie mit einer neuen nicht mehr entschlüsselt werden.

In diesem Fall muss der Käufer das Angebot erneut erstellen, damit Ihre neue ENC-Wallet genutzt werden kann.

7. Gültigkeit und Wiederverwendung

Eine einzige ENC-Wallet.json genügt, egal wie viele Kollektionen oder Anchors Sie besitzen oder minten.

Sie dient nur dazu, dass das System weiß:

„ Dieser Nutzer besitzt einen verifizierten Key, mit dem sicher verschlüsselt und entschlüsselt werden kann.“

8. Sicherheit und Empfehlung

- Verwenden Sie für Ihre echten Anchors immer eine Hardware-Wallet (Ledger, Trezor usw.).
- Nutzen Sie die ENC-Wallet.json ausschließlich als technische Brücke zwischen Ihrer Besitzadresse und den verschlüsselten Dateien.
- Speichern Sie Passwörter und verschlüsselte Schlüssel getrennt.
- Signaturen sollten niemals langfristig gespeichert, sondern bei Bedarf neu erstellt werden.

9. Zusammenfassung

Punkt	Beschreibung
Was	Technische JSON-Datei zur Verwaltung von verschlüsselten HQ-Dateien
Wann nötig	Beim Minten, Kaufen oder Verkaufen von Anchors mit HQ-ENC
Warum	Damit Schlüssel sicher zwischen Besitzern übertragen werden können
Erstellt mit	AnchorKey OFFLINE (Keypair) + AnchorKey ONLINE (ENC-Wallet.json)
Verknüpfung mit Wallet	Keine echte Wallet! Nur Namensähnlichkeit
Sicherheit	PrivKey verschlüsselt, Signaturprüfung per BIP-322, keine Hardware-Wallet nötig
Wiederverwendung	Eine ENC-Wallet.json reicht für alle Anchors desselben Besitzers