5️⃣

Lecture 05: Seed Phrase and SPV

Bitcoin 12 Word Generation

https://github.com/bitcoin/bips/tree/master/bip-0039

https://bitcoin.org/bitcoin.pdf

🪙 Bitcoin Wallets & Seed Phrase (Easy Notes)

💼 Crypto Wallet Basics

A **crypto wallet** stores your **private key** and **public key** to interact with blockchain.

Examples:

- 🌐 Apps like **MetaMask**, **Phantom**
- 📱 Mobile wallets
- 🖥️ Hardware wallets

🔗 KYC → App → Wallet

✅ When you use an app:

- You may complete **KYC** (Know Your Customer)
- The app creates your **wallet**, which generates:

  - 🔒 **Private Key** (kept secret)
  - 🔓 **Public Key** (shared)

📝 12-word Seed Phrase

When creating a wallet, you get a **12-word seed phrase** (also called **mnemonic phrase**) which is a human-readable backup of your wallet keys.

📊 How it works:

✅ The seed phrase is generated from a **wordlist of 2048 words (2^{11})**.

✅ The total number of combinations: **2^{132} possible seed phrases**.

🔗 Reference:

📜 BIP-39 Standard

📄 Bitcoin Whitepaper

🧾 UTXO: Unspent Transaction Output

- Bitcoin uses a system called **UTXO**:

  ✅ Every transaction output is either *spent* or *unspent*.

  ✅ Your wallet balance = sum of all your UTXOs.

🧪 SPV: Simplified Payment Verification

SPV = a way for **lightweight wallets** (like mobile wallets) to work **without downloading the full blockchain**.

✅ How?

- Instead of downloading all data, it only downloads **block headers** and verifies transactions by checking proofs.

📲 Used in:

- Mobile wallets
- Hardware wallets

- Any lightweight client

📚 Key Concepts Recap:

- 📝 **12-word seed phrase** → backup for wallet keys
- 🔒 **Private key** → signs transactions
- 🔓 **Public key** → used to receive funds
- 🧾 **UTXO** → system for managing balances
- ⚡ **SPV** → fast, lightweight verification
