System Setup & Access Guide

This section provides a clear step-by-step setup for your **Start9 server, Bitcoin node, Lightning, Electrum, and related tools**. It's designed so you (or family members) can easily follow along to get fully set up and manage your infrastructure.

Start9 Server & Node Access

Your **Start9 Server** runs Bitcoin, Electrum, Lightning (LND/CLN), and BTCPay. You can access it locally or remotely.

- **Tor Dashboard (remote access):**
  `https://toraddress.onion/`
- **Local Network (same WiFi/LAN):**
  https://two-words.local
- **Local IP (IPv4, enp2so):**
  `192.000.0.00`

Electrum RPC (for Bitcoin wallets)

- **Tor RPC URL:** toraddress`.onion`
- **Port:** `50001`

Use this to connect **Sparrow** or other wallets to your own Bitcoin node over Tor.

Nick's Electrum Bitcoin Node Access

- **Nick's Node (my personal electrum server you can find and connect to on the website, with other info like DEFI):**
  https://defi.muscadine.box/
- **Tor Bitcoin Electrum RPC URL:** lyfocxl3fgg3if65jo32apupd2adzmm772vsqrtwpmdn4ndoug6gwnyd.onion
- **Port:** `50001`
- `Nick's email: nickconnelly10@gmail.com`

Credentials (Store Securely)

- **Start9 Admin Password:** password
- **Start9 application instances** (sparrow, RTL, lightning application): Username (if given): Username Password: password
- **Ledger Live / Sparrow / Rabby / Computer logins:** password
- **Ledger Device PIN:** PIN
- **Coldcard PIN:** *PIN*
- **Coldcard Anti-Phishing Phrase:** `phrase-phase`
- **Safe Box Combination:** PIN
- **Email:** *(main family member's email used for any accounts)*

Master / Child Key Strategy (Bitcoin improvement proposal 85)

- **Family Master Seed** → generate child master keys (BIP-85).
- Assign each family member a **unique index** (e.g. 1 = Dad, 2 = Mom, 3 = You, etc.).
- Each person can derive their **child wallet** with SeedSigner/Coldcard and back it up separately.
- Always keep a **clear diagram** mapping Master → Child → Wallet indices.

Emergency Recovery Plan

- **Lost child seed/device**: use parent key + index → re-derive seed → move funds to a new child index (eg child key was #3, make a #4).
- **Lost Family Master**: generate new master → re-derive children (same index mapping) → migrate funds.
- **Best practice**: after re-derivation, treat the old key as compromised and move funds to a fresh child index.

Quick Security Checklist

- Store seed phrases on **metal or paper**, not digital.
- Maintain **2+ backups** of master seed in different safe places.
- Label **devices & SD cards** clearly (e.g., "Bob Coldcard Q", "Dad Seed #0").
- Keep firmware/software updated (Start9, Sparrow, Ledger Live, Rabby, Coldcard).
- Run annual **restore drills** from backups.
- Keep **hardware in good condition** (test powering on periodically).

Device & Software Setup

1. SeedSigner (DIY Bitcoin Signer) - creates child keys from master keys and can sign bitcoin transactions

- Website: seedsigner.com
- Store: BTC Hardware Solutions - https://btc-hardware-solutions.square.site/
- Tutorials: SeedSigner Playlist - https://www.youtube.com/playlist?list=PLnLbWFZdPSbKk65dt_e0NJyHIEA7zLlo

Steps:

1. Download latest firmware from **seedsigner.com**.
2. Flash it to a microSD via USB stick.
3. Generate a **new seed** (dice rolls or QR) or import existing 12/24 words.
4. Write seed down on paper/metal backup.
5. To create family wallets → use **BIP-85 child seeds** from master key (record index numbers).

2. Coldcard (Mk4 or Q) - signs bitcoin transactions from being loaded, sd card, or qr code

- Store: coldcard.com - https://coldcard.com/
- Tutorials: Coldcard Playlist - https://www.youtube.com/playlist?list=PLnLbWFZdPSbJFo0nQ0DVR4udq_WFijilM

Steps:

1. Power on Coldcard.
2. Set **4-digit PIN** + confirm **anti-phishing phrase**.
3. Initialize new 24-word seed (or import your BIP-39 words).
4. Export **xpub/descriptor** to microSD (or QRcode) for watch-only wallet setup.
5. Use **Sparrow Wallet** to view balances and build/sign transactions.

-If you import a seed from SD card, you have to have an extra 12-word password in order to use it!
For maximum safety: keep Coldcard airgapped (use microSD or QR with Q model).

3. Sparrow Wallet (Desktop) - application used for air gapped devices to sign transactions, wallet tracker

- Download: sparrowwallet.com - https://sparrowwallet.com/
- Tutorials: Sparrow Playlist - https://www.youtube.com/playlist?list=PLnLbWFZdPSbLHIGb8stnl1qno4VJlIfPg

Steps:

1. Install Sparrow on your computer.
2. Go to **Settings → Server →** set to **Electrum over Tor**.
   - Host: toraddress`.onion`
   - Port: `50001`
3. Create **watch-only wallets** from xpubs exported via SeedSigner or Coldcard.
4. Use **Taproot addresses** (`bc1p...`) for new deposits.

4. Ledger Live (Desktop) - signs all types of crypto transactions + DeFi

- Download: ledger.com - https://www.ledger.com/ledger-live

Steps:

1. Install Ledger Live and create profile.
2. Connect Ledger device, unlock with PIN.
3. Install apps: **BTC, ETH, XRP** (and others you use).
4. Use with **Rabby** or **Sparrow** as needed.

5. Rabby Wallet (in Browser) - Secure wallet with features that can connect to Ledger to make DeFi easier

- Download: rabby.io (use **Brave** for privacy). - https://rabby.io/

Steps:

1. Install Rabby extension in Brave.
2. Create two profiles:
   - `my-DeFi Cold` → connect Ledger hardware wallet
   - `my-Hot Wallet` → software EOA (for daily DeFi & spending)
3. Ensure **Base network** is used for both profiles.

6. Browser Access

- **Tor Browser** → remote access to Start9 services (via onion URL).
- **Brave Browser** → private, safe DeFi interactions with Rabby extension.

7. DeFi Tracker

- **Zerion** → easy lookup of wallet to track coins wallet holds + DeFi positions
- **Debank** → easy lookup of wallet to track coins wallet holds + DeFi positions
- **Excel sheet** → Keep everything on a spreadsheet, update periodically to view your holdings

Bitcoin Paper/Hardware Wallet (Cold)

Purpose: Generational, set-and-forget Bitcoin storage.

Setup & Storage - on system setup page

1. **Choose a signer:** SeedSigner **or** Coldcard (Mk4/Q).
2. **Create/Import seed:**
    - *SeedSigner:* flash from seedsigner.com → generate a new seed (dice or camera) or import 12/24 words.
    - *Coldcard:* power on offline → "New Wallet" (or import 24 words).
3. **Backups:** Write **24 words** on metal/paper. Store duplicate copies in separate safes. **Never** photograph seeds.
4. **(Optional) BIP-85 plan:** From a master key, derive child wallets by index (#0, #1, …). Record which index belongs to which person/purpose through the seedsigner. Make sure on seedisgner settings on advance BIP-85 is turned on.
5. **Connect to a watch-only wallet:** Export the **xpub**/descriptor (public keys, not private) to **Sparrow** so you can view balances without exposing the seed. Use Taproot as your bitcoin script.

You can use the same seed on both SeedSigner and Coldcard; just never type it into an online computer.

Sparrow Wallet (watch-only + PSBT)

1. **Download Sparrow:** sparrowwallet.com. Keep it updated.
2. **Server settings:** *Settings* → *Server* → *Electrum over Tor*.
    - Host: your electrum server .onion address
    - Port: `50001`
3. **Create wallet:** Import **xpub/descriptor** from your Cold signer. Use **Taproot** (addresses start with `bc1p...`).
4. **Verify fingerprint:** Sparrow's wallet fingerprint should match the device/paper fingerprint before using.

Receive Bitcoin (cold)

1. Open wallet in Sparrow → **Addresses** tab.
2. Copy the **first unused** `bc1p...` address.
3. **Verify address** on the device (Coldcard: *Address Explorer*) and in Sparrow (match **first/last 4** chars).
4. From your exchange (e.g., Coinbase), **withdraw BTC on Bitcoin mainnet** to that address.

Send Bitcoin (via PSBT(partially signed bitcoin transaction))

Build in Sparrow → sign offline → broadcast in Sparrow

1. **Build PSBT:** Click **Send** → paste recipient address → set amount/fee → **Finalize PSBT** (it needs keys to broadcast).
2. **Move PSBT to signer:**
    - *Coldcard:* save to microSD, insert into Coldcard. Or scan PSBT QR code to Coldcard.
    - *SeedSigner:* scan Sparrow's PSBT QR on the device.
3. **Sign offline:** On the device, review the transaction and **sign** the PSBT. Device must already have the seed loaded in.
4. **Return signed PSBT:**
    - *Coldcard:* bring signed file back on microSD and **Import** in Sparrow. Or scan the QR code on your computer
    - *SeedSigner:* have Sparrow **scan signed QR**.
5. **Broadcast:** Sparrow → **Broadcast Transaction**. Save the TXID.
6. **Verify:** Check confirmation on a block explorer (e.g., mempool.space).

Monitoring

- Keep Sparrow as **watch-only**. Check balances **weekly/monthly**.
- Rotate to a **new child index** if any key exposure is suspected.

Emergency Recovery

1. If a **child wallet** is lost/compromised: re-derive from its **parent** (BIP-85 index) → move funds to a **new** child index → update records.
2. If the **Family Master** is lost/compromised: generate a **new master** on SeedSigner → re-derive all children with the same labeling → migrate funds.

DeFi Cold & Hot Wallets (Base Network)

General Rule

- Use **Base** (BASE CHAIN) a layer 2 network on Ethereum for all EVM activity.
- Always confirm your wallet address (starts with **0x…**) matches across dApps and explorers before transacting.

Recommended dApps on Base

1. Morpho
https://app.morpho.org/
- **Purpose:** Borrow against your assets at optimized rates (somewhat complex, rates more optimal).

2. Moonwell
https://moonwell.fi/
- **Purpose:** Lending/borrowing (powered by Morpho in the backend, alot of functionality such as AI agents).

3. Aave
https://app.aave.com/
- **Purpose:** Lend and borrow assets (easy to manage, not as much optional rates).

4. Aerodrome
https://aerodrome.finance/
- **Purpose:** Swap tokens and provide liquidity.

5. Uniswap
https://app.uniswap.org/
- **Purpose:** Swap tokens easily on Base.

Use Defillama to find the best protocols on-chain. https://defillama.com/
Top DeFi sectors (anything in defi can be done on centralized finance + more):
- Decentralized Exchanges (DEXs)
- Lending & Borrowing
- Perpetual Futures, Derivatives & Orderbook DEXs
- Liquid Staking & LSDfi
- Real-World Assets (RWA) & On-Chain Credit
- Yield Aggregators & Vaults
- Insurance & Risk Protocols

Sending From Exchange to wallet

1. Copy wallet address you want to send crypto to (USDC, cbBTC) as a 0x…w39 or a basename (nick.base.eth)
2. On coinbase, press send, copy the address into coinbase, press the token you want to send, than the network (base), submit and amount you want to send, than review the transaction before you send
3. Once sent, it should arrive quickly into your wallet.

Sending From wallet to Exchange

1. On coinbase, press receive, click the asset, than the network you want to receive from (base) and copy the address coinbase sends you.
2. On your wallet (rabby), click send, than the token you want to send, amount and copy the address coinbase sent you. Review the transaction than send.
3. Once sent, it should arrive quickly into your wallet.

Records to Keep (offline)

- Device label (e.g., "Dad – BTC Coldcard Q").
- Wallet name in Sparrow + **fingerprint**.
- BIP-85 **index number** per person/purpose.
- SD card label & location for each encrypted backup.

Emergency (DeFi)

1. If **DeFi Cold** seed lost: derive a **new child** → repay borrow from Hot/Stable buffer → withdraw collateral → redeposit under new DeFi Cold.
2. If protocol-level risk spikes: reduce LTV, repay, or fully unwind to **USDC/cbBTC**.

Cold Wallet (Ledger-backed)

Purpose: Larger positions; lending/borrowing with strict risk limits.
Setup

1. Initialize **Ledger** with your **DeFi Cold** seed.
2. On **Ledger live** add token accounts (Apps) on "My Ledger" (Bitcoin, Solana, Ethereum, XRP). Than on accounts add the network (BTC, ETH, SOL), make a name and click what address to use.
3. On accounts, you can click send/receive for any asset (always double check the network and token) and see your addresses and amount of tokens.
4. You can even stake some assets, or connect to other browser wallets for more functionality like phantom (on Solana) or rabby (ethereum and layer 2s like BASE).
5. In **Rabby (Brave)**, add Ledger account; select **Base** network. Make sure ledger is plugged in, and your in the ethereum account on the ledger
6. Keep device **offline** except when signing.

Standard Lending Flow (AAVE on Base)

1. **Fund the wallet:** Hold **USDC** or **cbBTC** in your Ledger account on **Base**.
   - *BTC → cbBTC:* use Coinbase's official wrap/on-ramp to **cbBTC on Base** (or verified bridge). Test with small amount first.
2. **Open AAVE:** https://app.aave.com/ (go to dashboard, than BASE instance, not ethereum).
3. **Connect Ledger via Rabby.**
4. **Deposit collateral:** Select asset (e.g., **cbBTC** or **USDC**) → **Enable/Approve** → **Supply/Deposit**.
5. **Toggle as Collateral** (optional) (if you intend to borrow, allows smart contract to liquidate if under-collateralized).
6. **Borrow (optional):** Borrow **USDC** at a **conservative LTV** (≤ **40%**). Target **Health Factor ≥ 1.6**.
7. **Confirm & sign** on Ledger/rabby.

Repay / Unwind

1. Repay **USDC** debt → wait for confirmation.
2. Untoggle collateral if needed → **Withdraw** collateral (cbBTC/USDC) back to wallet.

Monitoring

- Create read-only profiles in **Zerion/DeBank**.
- Check **Health Factor** daily if borrowing; set alert thresholds (HF < 1.5).
- Only use **official/verified bridges & token addresses**.
- Avoid volatile LTVs; liquidation risk rises quickly during market moves.
- If **cbBTC** or other tokens are **not** supported in a given protocol, do **not** force deposits; stick to supported assets.

Hot Wallet (Rabby software wallet)

Purpose: Day-to-day swaps, payments, repayments.
Setup

1. Create a **Hot Wallet** in Rabby (software EOA).
2. Network = **Base**. Keep only a **working balance, pretend your carrying cash**.
3. (Optional) Enable **Account Abstraction** tools (EIP-4337/7702) for batching & gas sponsorship.

Daily Use (Examples)

- **Top up USDC** → repay borrow on AAVE.
- **Send USDC** to Friends or Family
- **Swap** small amounts on Aerodrome/Uniswap (Base) → send to DeFi Cold if needed.

Hygiene

- Always revoke approvals (Rabby → **Approval Manager**).
- Maintain enough **ETH/SOL for a gas buffer** (e.g., $20–$50 worth).
- never go on random sites, or never re-put your keys on your computer in browser, if it ask you while your on a website it's a scam.