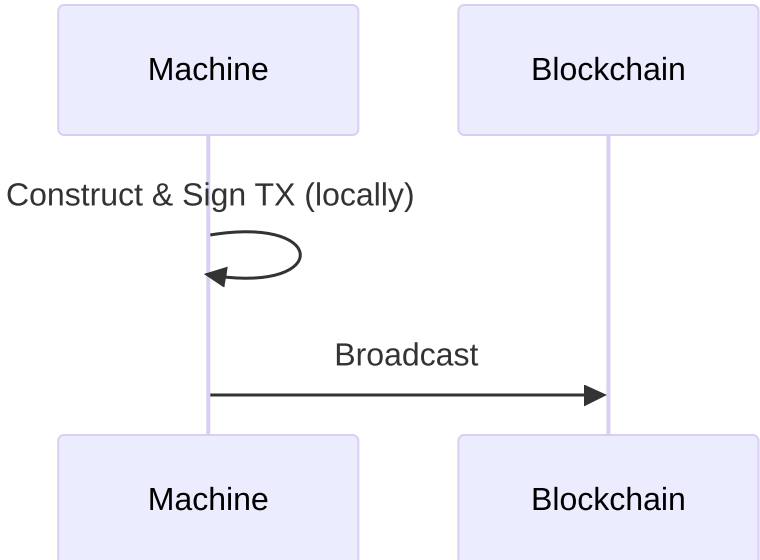
🛠️ Secure transaction

Airgap transaction and Hardware key

🔑 How to do a Transactions?



Why using safe transaction?

Risks of Signing in an Online environment: Malware ⚠️

- 🔑 Memory scraping attacks
- ⌨️ Keyloggers capturing passwords
- 🌐 MITM transaction hijacking
- 📧 Phishing fake transaction prompts
- etc...

🔒 Airgap Transactions

Hardware Keys

Hardware key + Airgap Security

🛡️ Hardware key + Airgap Security

Advantages ✅	Limitations ⚠️
Isolation (No USB/Bluetooth)	**Slower** (Manual transfers)
Physical verification (On-device display)	**Complex setup** (QR workflow)
Immune to malware (No driver exploits)	**Dependent on device security** (Firmware risks remain)

⚠️ **Airgap ≠ Perfect Security**

- Always verify TX details **on the hardware key's screen**.

Hardware Key vs Airgap Environment

🛡️ Hardware Key

Pros:

- **Instant signing process**
- **Tamper-proof hardware**
- Private keys never exposed
- Portable (works with any computer)
- Physical confirmation required

Cons:

- **Hardware cost** 💰
- **Limited to supported blockchains**
- Firmware updates needed

🔒 Airgap Environment

Pros:

- **Works with any offline device**
- **No special hardware needed**
- Flexible for any blockchain
- Complete network isolation
- Can store multiple key types

Cons:

- **Multi-step process**
- Requires data transfer method
- Dependent on offline device security
- Manual setup complexity

What you should go for

Hardware Key - Most Secure + Convenient

Recommended way ✅

- Ledger **(Gno compatible)**, Trezor, YubiKey, ...

AirGap Vault - Secure but inconvenient 🔒

Must be offline ⚠️

- **Virtual Machine** - QEMU/KVM – Or lighter with container
- **USB** - Tails OS (Amnesic system)
- **Hardware based** - Old smartphone, Old Laptop, dedicated Raspberry Pi
- **Mobile (IOS/Android)** - e.g.: AirGap

Native Way - Convenient but vulnerable 👾

✍️ Multi-Signature Setup