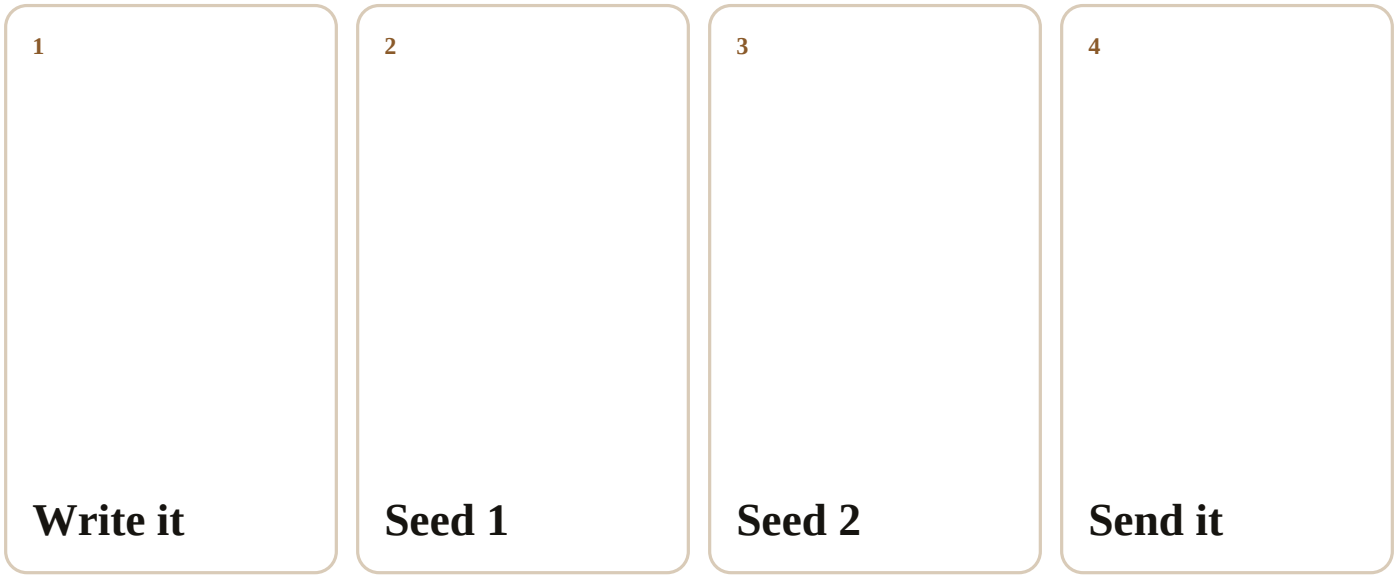
A small amount moves before any savings. The payment file walks. The seed stays seated. Savings stay where they are until a small amount has gone out and come back.



Build, then sign once

The wallet is built only after no seed is loaded. One public key is copied per boot. A public key is not the 24 words. The path has to read m/48'/0'/0'/2'. If it shows anything else, the work stops.

The map is exported. It watches. It cannot spend. The everyday computer imports that map as watch-only.

The destination, the amount, and the fee are written on paper before the unsigned file is exported. The first seed signs that file on Tails, with networking off. Then the computer is shut down fully. The screen goes dark before the drive is unplugged.