Questions

What is this?

A way to hold your own Bitcoin. You make three keys at home. Any two of them can spend. No hardware company has to stay in business for that to remain true.

Why not only a hardware wallet?

A hardware wallet is a tool. It is not the backup. One company, one device, or one house is a single point of failure. Dice, two boots, and three plates come first. A signer can come later, from more than one maker.

Where does the trust sit?

Dice make the randomness. Not the laptop. Tails, networking off. Shutdown forgets the session. verify_kit.sh checks file hashes. It does not check signatures. A mismatch means format the drive and stop. Three plates. Three places. Any two spend.

What if the map is lost?

The map is not a seed. Encrypt it with gpg. Do not invent a paper cipher. If that passphrase is lost, the coins are not gone. Two plates can rebuild the map. The path is m/48'/0'/0'/2'. Write it on the inheritance sheet. It is not a secret.

Can my family recover the coins?

Yes. Give them sheet 12. They need two plates and the map. They buy a Jade and a BitBox from the makers. One plate goes in each device. They do not boot Tails. They do not type the words into a phone.