Writing Smart Contracts
Assignment 14: Security

Peter H. Gruber

December 6, 2022

IMPORTANT:

- Most assignments are handed in via the blockchain.
- Read the instructions carefully and use the appropriate accounts.
- Be careful to choose the required network: Testnet or Mainnet.
- Tip: verify your transactions on Algoexplorer.

Compulsory Exercises

Exercise 1. (a) Research the internet and list three different products for cold storage for you recovery phrase. (b) How can you (slightly) simplify the storage of your recovery phrase?

Exercise 2. Using the material available in class, create your own cryptosteel-like cold storage.

Exercise 3. (a) Research the internet, especially Github, and try to find private keys, API-keys or recovery phareses that are (accidentally) available openly. Contact the owner to warn them. Document your efforts with screenshots and/or PDF printouts of emails. *Hint:* first think of ways how to search for the above-mentioned types of credentials. (b) Go to `https://www.gitguardian.com` and create a free account to watch over your credentials.

Exercise 4. Create a honeypot in the form of a (new and separate) wallet with 10-20 ALGOs. "Accidently" post the recovery phrase on your public github. Wait and watch.