Writing Smart Contracts
14 Security

Peter H. Gruber

Supported by the Algorand Foundation

Elements of security

1. Mindset
2. Organizational
3. Physical

Your passphrase (2)

Irreversible transactions (!)

You may loose . . .

- Assets (tokens, NFTs)
- Voting rights / control over organization
- Identity, home . . .

Dangers

1. Loss (loose, forget, become incapacitated)
2. Theft (physical, cyber)
3. Robbery
4. Destruction (fire, water, . . .)

Considerations

- Cost vs. maximal damage
- Useful: mindset of data backup

Your passphrase (2)

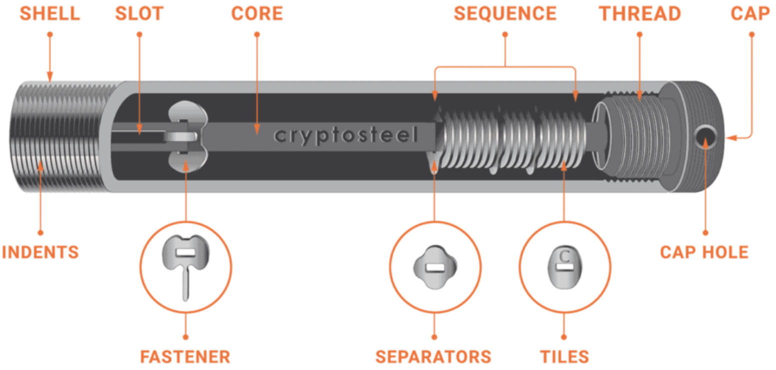
Don't

- Digital cop<u>ies</u> (backups, hacks, . . .)
- Especially in the cloud (no google docs, dropbox)
- Store credentials in code (Github)
- Leave credentials in old hardware (phone, SSD, laptop)

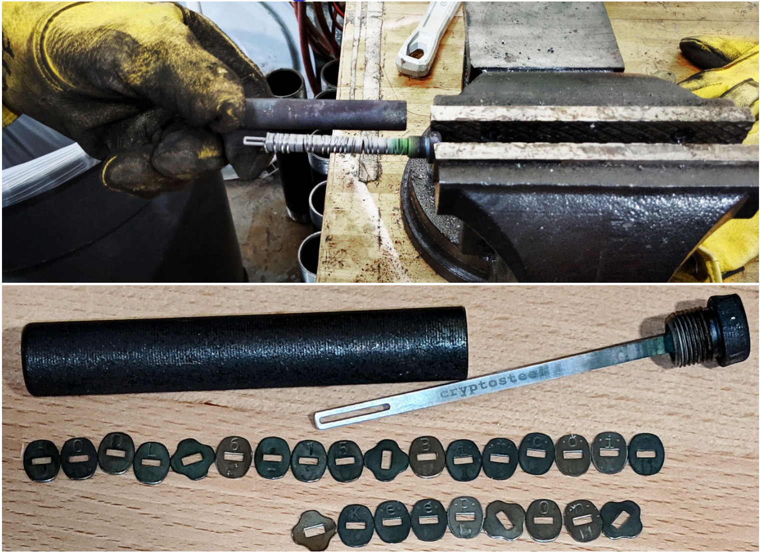
Do

- Store passphrase, not private key
- Keep small wallet online and large wallet offline ("cold")
- Physical storage of passphrase
  - Limited durability of paper storage (paper, ink, lamination)
  - Alternative materials (stone, metal), e.g. Cryptosteel
- Split passphrase in two
- Consider multisig
- Consider including passphrase in your will
- Regularly verify cold storage

Cryptosteel



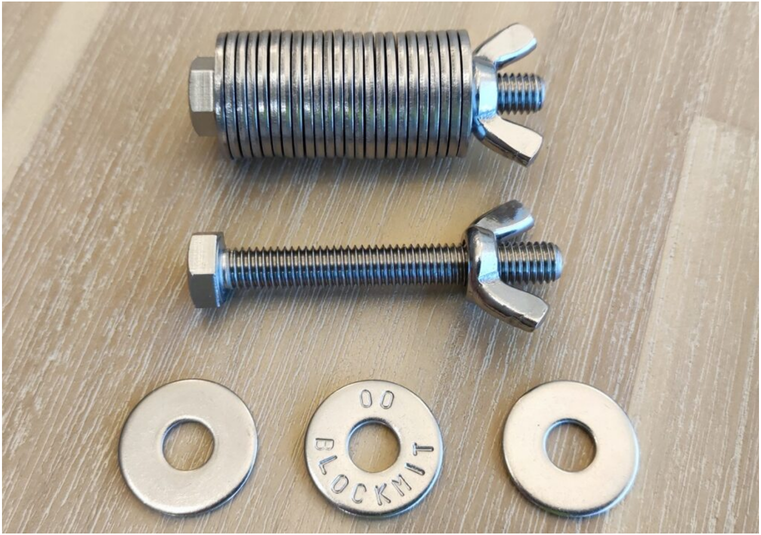
Cryptosteel after burning



Source:

https://medium.com/@cryptosteel/independent-heat-test-of-the-cryptosteel-capsule-e9de0c3ea534

Home-made cryptosteel



Source: https://blockmit.com/english/guides/diy/make-cold-wallet-washers/

Credentials in the code

Don't

- Store credentials in main code
  - Problem 1: loss/theft (Github etc)
  - Problem 2: updates

Do (depending on security requirements)

- Store in separate `.key` file, use `gitignore`
- Enter directly into code
- Use system variable (in the RAM)
- Connect to wallet app in browser
- Connect to phone wallet via QR code

  `https://algorand.github.io/walletconnect-example-dapp/`