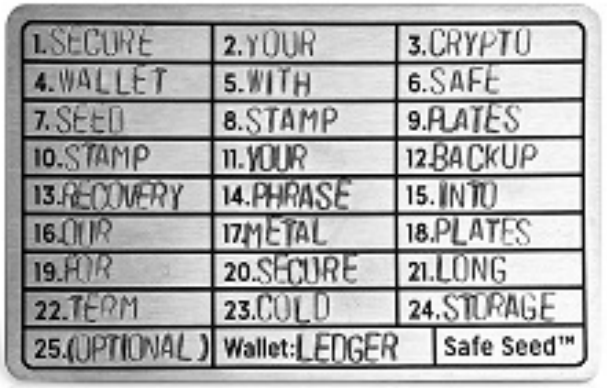
Co je Recovery seed storage?

V kryptoměnách je recovery seed, nebo zkráceně seed, seznam slov v určitém pořadí, který uchovává všechny informace potřebné k obnovení peněženky. Uchování obnovovacího seedu v soukromí a bezpečí je klíčem k dlouhodobé bezpečnosti prostředků uživatele v kryptoměně. Recovery seed storage je tedy místo, kde lze bezpečně tento kód uschovat.

Problematika

Nejrozšířenější a nejjednodušší variantou pro uchovávání seedu jsou nerezové či titanové destičky, do kterých se pomocí razníků vytlučou jednotilvá slova z kódu.

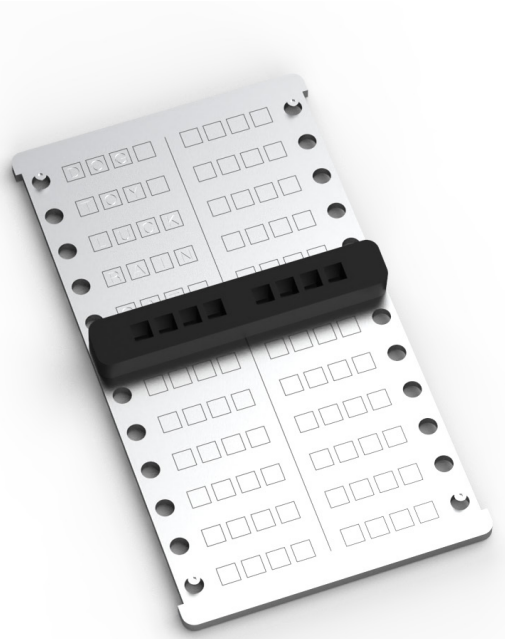
Výhodou tohoto řešení je jeho jednoduchost, odolnost a nízká výrobní cena. Problémem je pak špatná čitelnost vyražených slov kvůli často nepřesnému vyražení jednotlivých písmen.

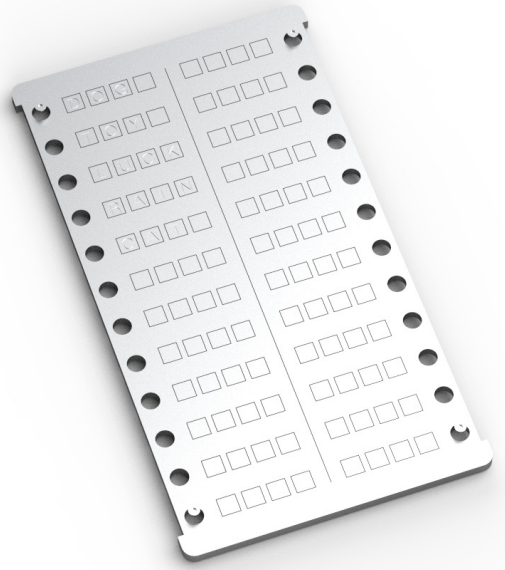


Návrh

Návrh zohledněňuje silné stránky stávajících nosičů a přináší řešení nečitelnosti pomocí posuvného nástavce, který slouží jako vodítko pro běžně prodejné raznice.

Ty se postupně prostrčí skrz otvory, které zajistí pravidelné vyražení písmen. Jeden díl je navržen pro oba druhy seedů, tedy pro 12 nebo 24 slov.



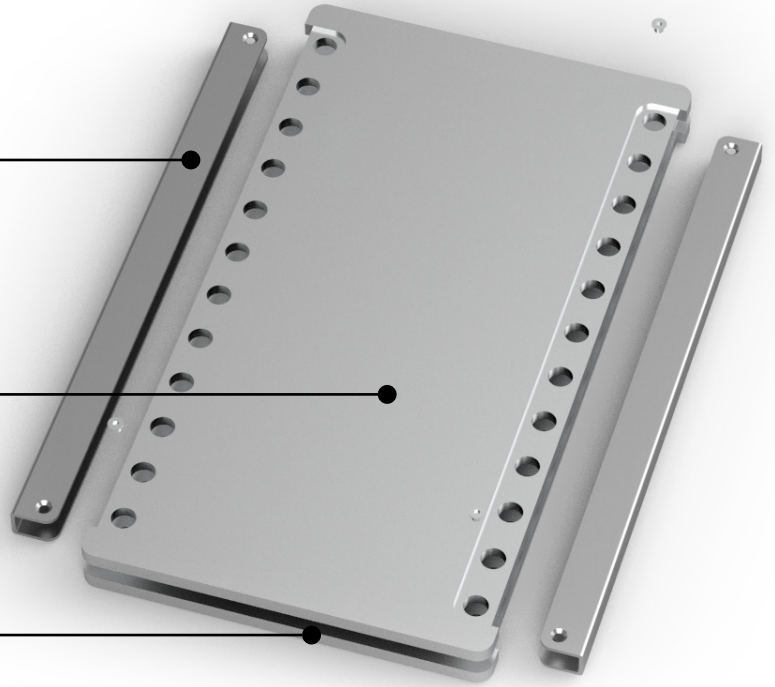


Pojistné šroubky pro spojení dílů

Lišta pro uchycení dílů

Vrchní díl pro ražbu

Spodní díl pro ražbu / překrytí

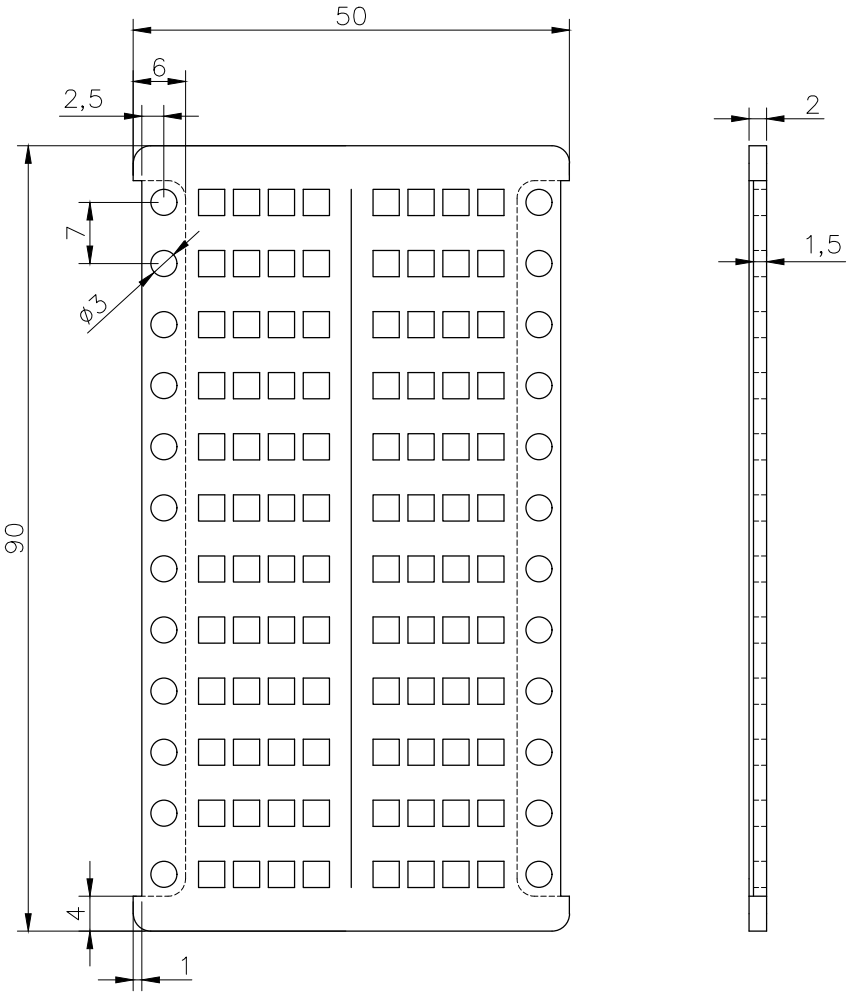


Komplet

Destičky pro ražbu jsou dodávané v páru spolu s úchytnými lištami. Po samotném vyražení kódu se destičky kódy k sobě sešroubují a tvoří tak komplexní nosič, u kterého není na první pohled vidět ani kód, ani smamotná funkce.

Rozměry

Jedna přenosná destička má rozměry kreditní karty. Komplet lze tedy bez větších obtíží přenášet v peněžence či ho mít uložený mezi ostatními dokumenty na bezpečném místě.



Vít Bednář
FA ČVUT
Ateliér Jaroš / Bednář
ZS 2021/2022