Bitcoin Test

Public Address (účet)

tb1q8pc5t53prcm784rq3az86kxyjpjt2sshp5t5j9

SHARE (ke sdílení)

Private Key (heslo)

SECRET (tajné)

Toto je je zcela "Funkční" **papírová peněženka**, jen její **privátní klíč** bude časem "zdiskreditovaný". Co to znamená? Postupně si vysvětlíme:

QR kód už asi znáte. (Quick Response) *pro rychlé a bezchybné načtení řetězce znaků.*

Veřejný klíč (adresa/účet), slouží k **přijímání** plateb. Adresu ukazujeme. Na rozdíl od privátního klíče (hesla), který bychom měli držet v maximální tajnosti. Zde je privátního klíč zveřejněn (což by se v běžné praxi dít nemělo). Kdokoli si totiž může veškeré prostředky importovat!
Zvolili jsme testovací Bitcoin, který je zadarmo, ale přesto **zdůrazňujeme riziko,** že žádný obnos se na takovéto **zveřejněné** papírové peněžence dlouho neohřeje!

Elektronické aplikace 1/6 generují lépe zaznamenatelný **tajný klíč** ve tvaru několika slov - nazývá se **seed.**

SECRET drastic violin illegal acoustic into secret hip satisfy south deposit radar enable (seed)

Pomocí **seedu** (například 12 anglických slov) si můžeme svojí peněženku opět obnovit. Stejně tak ale i kdokoli cizí, kdo ho získá!

1 Nainstalujte si elektronickou peněženku, například **coinomi.**
Co je na celé proceduře nejdůležitější? Je to právě **bezpečné uchování seedu!**
Bitcoiny **NIKDY** nejsou v zařízení!
To se pouze pomocí klíče prokazuje, že jimi můžeme disponovat.

Vyzkoušejte si pár základů nanečisto s volně dostupnými **Bitcoin Test**. Jak zcela zadarmo nějaké "mince" získat (stejně tak i další podrobnosti) se dozvíte na:
www.agamapoint.com/tahak.

Zkuste něco málo **poslat** 2 na papírovku a pak si to zase celé **importovat** 3 zpět pomocí: ⊕

Zkuste pak pro změnu **poslat** něco známému 4 a podobně od známého zase **přijmout** 5.

→ přijmout v jednom zařízení zamená
← odeslat z jiného

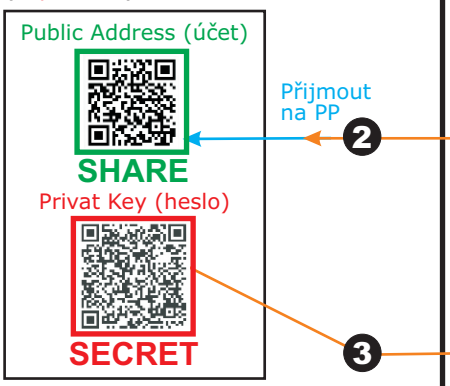
Celý proces několikrát opakujte, koukejte do **blockchainu**, snažte se pochopit, co a jak se děje. Pak můžete přejít na ostré Bitcoiny (třeba z bankomatu).

Použití **Trezor**u je až další úrovně, na kterou už zde nemáme místo.

Papírová peněženka

PP - Cold storage

Zpravidla je to na papír "vytištěná" dvojice QR kódů: Adresa (účet), na kterou se dá přijmout a k ní je jeden privátní klíč, kterým se dá jako celek celý obsah přijmout v jiném zařízení (importovat).



Privat Key → Jediná adresa

Každý, kdo uvidí nebo umí "zachytit" tajné heslo (SECTRET), má přístup k obsahu. Z toho plyne **doporučení** použít "papírovku" jednorázově!

Tímto způsobem můžete získat svojí první část Bitcoinů z **Bitcoinového automatu** (když nemáte elektronickou peněženku).

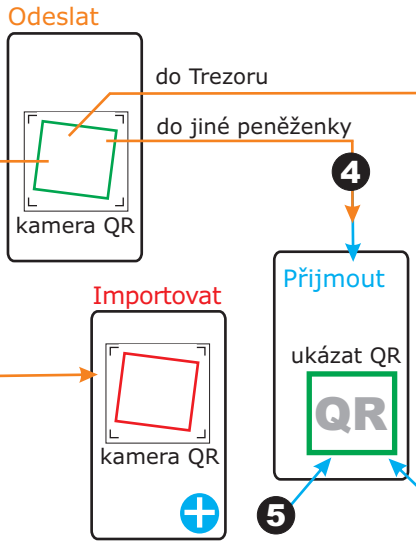
Stejně tak **čip** nebo RFID **klíčenka** obsahuje Privátní klíč (k podpisu transakcí).

Coinomi

1

mobilní aplikace (jedna z mnoha)

Elektronická peněženka ve Vašem chytrém telefonu či tabletu využívá wifi a vestavěnou **kameru** pro čtení **QR** kódů.

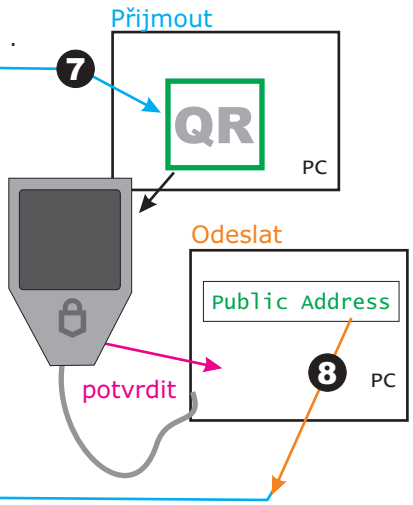


Trezor

6

hardwarová peněženka

HW zařízení připojené k PC, které "podepisuje transakce". **Privátní klíč** Trezor NIKDY neopustí a pokud uživatel ochrání svůj **seed**, jsou jeho mince v bezpečí.



Elektronická zařízení (Mobilní telefon nebo Trezor) přímo generují lépe zaznamenatelný Privat Key (PK) ve formě 12/24 slov (seed).

Bitcoiny NIKDY nejsou v zařízení! Zařízení se pouze pomocí klíče prokazuje, že jimi můžeme disponovat.
Seed neztratit a nenechat si vzít!