Uživatelská dokumentace:

Úvod

Jedná se o bitcoinovou peněženku spravující privátní klíče k bitcoinovým adresám (hash veřejného klíče v kódování Base58) a zároveň zprostředkovává komunikaci mezi uživatelem a bitcoinovou sítí za pomocí připojeného RPC klienta (přijímání a odesílání transakcí). Peněženka je oddělena na jednotlivé účty, kdy jeden účet vždy reprezentuje sadu deterministicky generovaných adres pro příjem bitcoinových mincí a drobných z transakce.

Peněženka

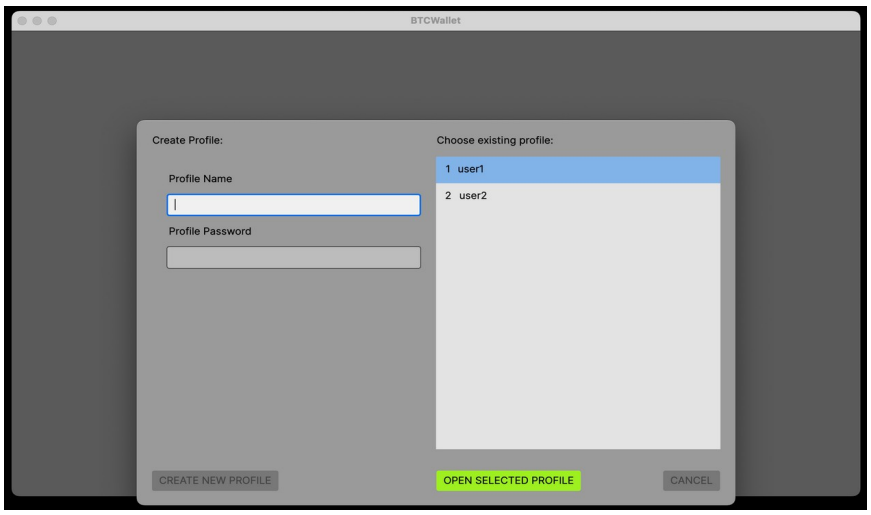
Jsou dva hlavní druhy peněženek, jedna reprezentuje sadu vzájemně nesouvisejících privátních klíčů. Druhá se nazývá hierarchicky deterministická, tedy z jednoho hlavniho klíče se deterministicky odvozují ostatní privátní klíče. Hlavní klíč je možné reprezentovat 12 slovy z normalizovaného slovníku (BIP-39), passphrase. Dále se dle “derivation path” odvodí nekonečná posloupnost klíčů.

Hierarchicky deterministická peněženka může být jak read-only (uživatel nevlastní privátní klíče a tedy může pouze pozorovat obsah peněženky a její adresy), tak i klasická varianta, která pomocí privátních klíčů podepíše jednotlivé mince (ověří vlastnictví) a tím dovolí jejich utracení ve vytvořené transakci.

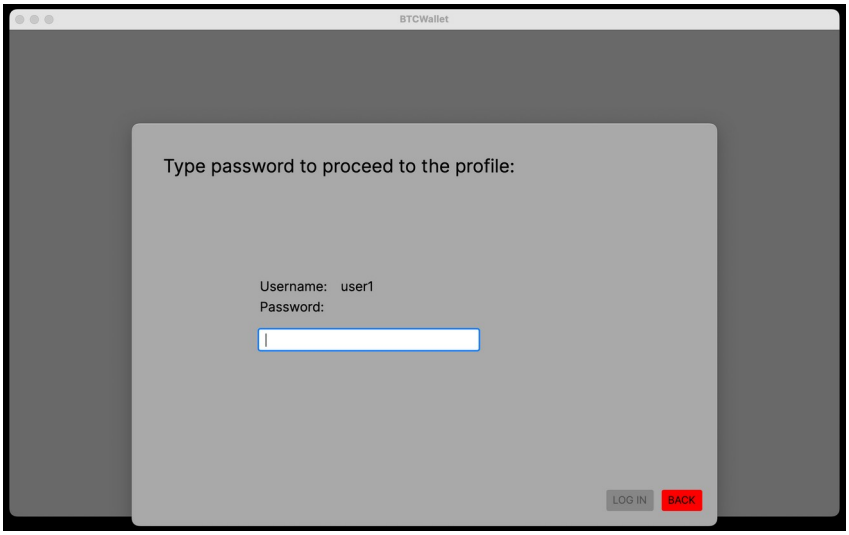
Aplikace umožňuje uživateli jak importovat již existující **Legacy** pěněženku za pomocí zmíněných 12 slov, či read-only pomocí takzvaného xpub formátu (mimojiné reprezentace veřejného klíče a chaincode, s nimiž je možné odvodit hierachii adres dané peněženky, čímž zjistíme zústatky), tak vytvořit novou.

Profily

Aplikace si ukládá záznamy o již vytvořených účtech. Je tedy možné si vytvořit nový, čímž přidáme novou/importujeme existující peněženku (levá část), či otevřeme již dříve vytvořený profil, který je vybrán z nabídky profilů (pravá část), viz Image1.

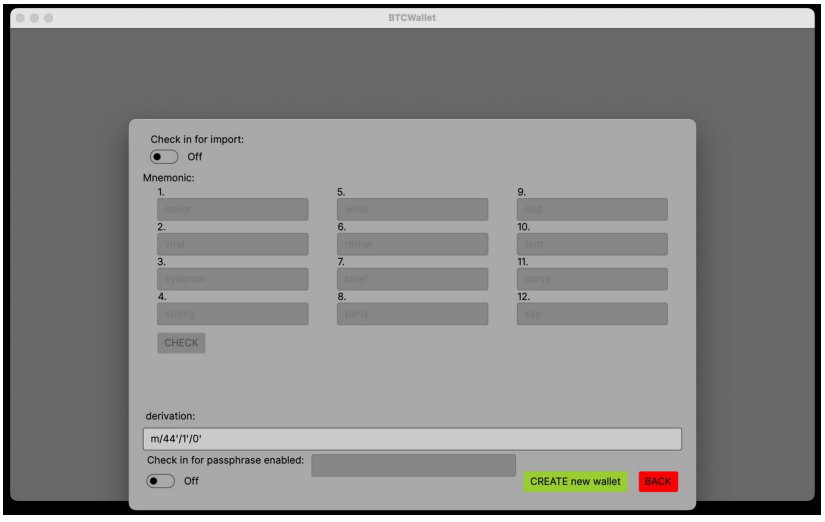


Každý profil se skládá z uživatelského jména (musí být unikátní), hesla a metadat o HD peněžence. Pro vytvoření nového profilu je nutné vyplnit uživatelské jméno a heslo, načež se aktivuje tlačítko “Create new profile”. Pro otevření existujícího profilu vybereme daný profil reprezentovaný uživatelským jménem a klikneme na “Open selected profile”, což uživatele přesměruje na obrazovku pro ověření hesla, viz Image2.



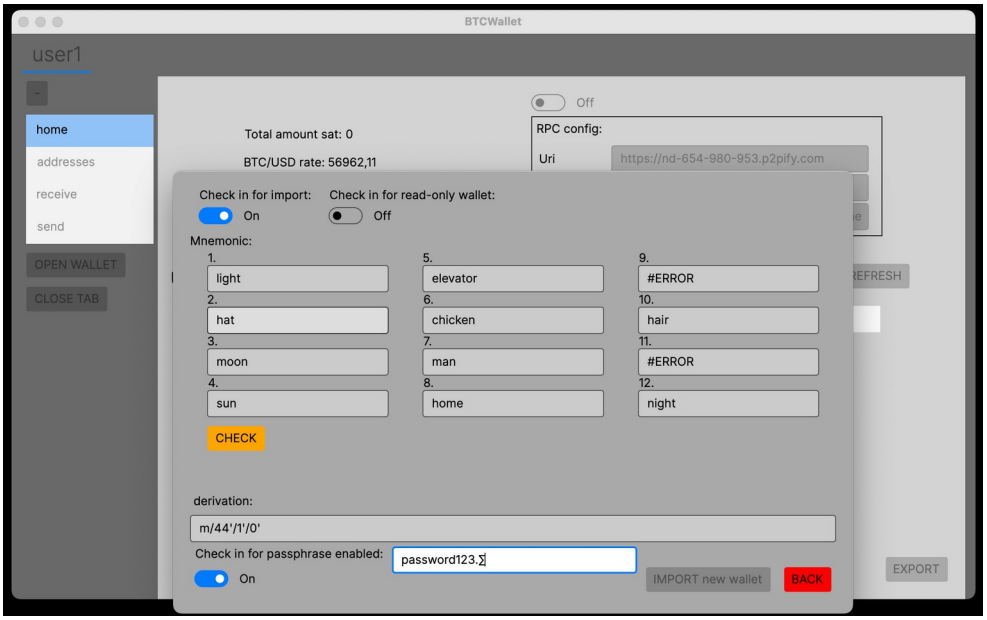
Po zadání správného hesla, se aktivuje tlačítko “Log in”, které dále přesměruje uživatele do základního rozhraní peněženky.

Zvolil-li uživatel tvorbu nového profilu, po kliknutí na tlačítko “Create new profile”, viz Image1, je přesměrován na obrazovku tvorby/importování peněženky, viz Image3.



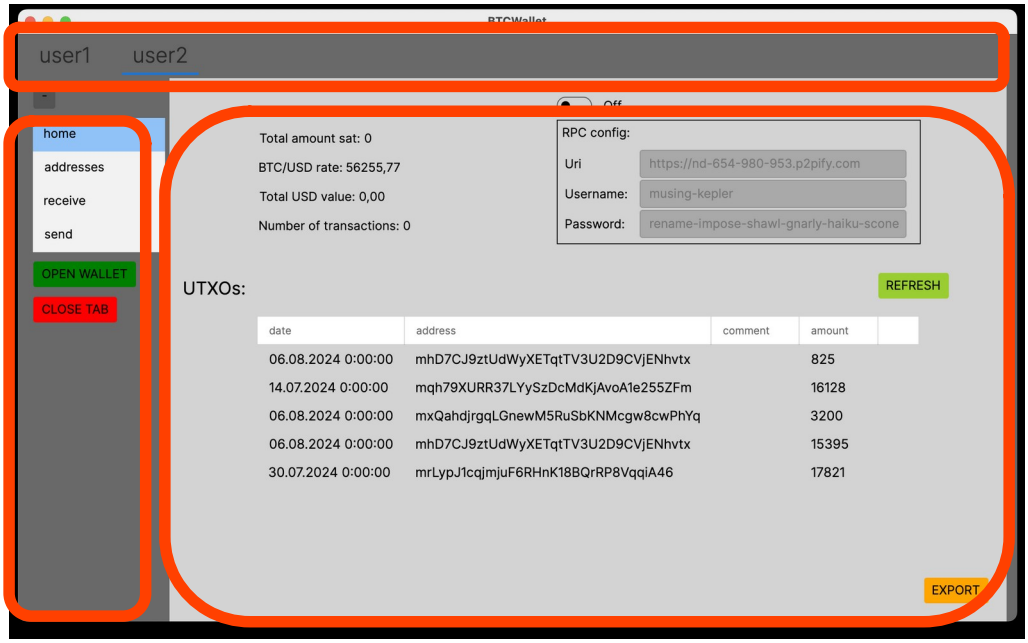
Jako základní je nastaveno, že si uživatel bude tvořit úplně novou peněženku, chce-li ale importovat již existující, zaklikne první toggle box pod nápisem “Check in for import”, čímž se zpřístupní a vynulují pole pro zadání 12 slov, reprezentující peněženku. Vyplněná slova musí být pro aktivaci tlačitka “Import new wallet” správná, a tedy zkontrolována tlačítkem “Check”, při nesprávném slově či chybě se objeví v daném poli text #ERROR. Zároveň se objeví nový toggle box, který při aktivaci signalizuje importování read-only peněženky a deaktivuje se možnost

Create/Import new wallet, dokud není zadán validní vstup do aktivních polí. Důležité je zadat správnou “Derivation path” pro nalezení správného hlavního derivačního klíče peněženky. Toggle box pod nápisem “Check in for passphrase enabled” při aktivaci zajistí, že hlavní klíč peněženky se skládá nejen z kombinace 12 slov, ale navíc přidává ochranu hesla.



Rozhraní peněženky

Při každém otevření nové honebo existujícího účtu se zobrazí náhled aktuální peněženky v okně “Home”, kde se nachází hlavní souhrn dat. Obrazovka se dělí na tři hlavní části: otevřené profily (záložky s uživatelským jménem profilu), menu rozhraní peněženky patřící aktuálně otevřenému profilu a obsahu zvoleného menu daného profilu, viz Image4.

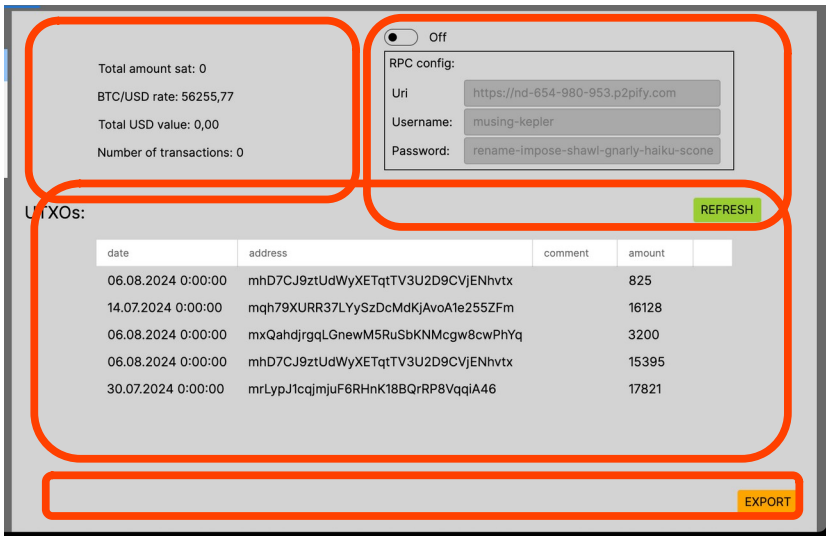


Otevřené profily (záložky)
Záložky s otevřenými profily v horní části obrazovky se ovládají pomocí dvojice tlačítek “Open wallet” (čímž se otevře nám již známí dialog s výběrem, zda-li uživatel chce přidat uplně nový profil nebo otevřít již existující) a “Close tab” (který jednoduše zavře aktuálně aktivní záložku, pokud se ale jedná o poslední záložku, otevře dialog viz tlačítko “Open wallet”).

Menu
List box je složen z následujících tlačítek:

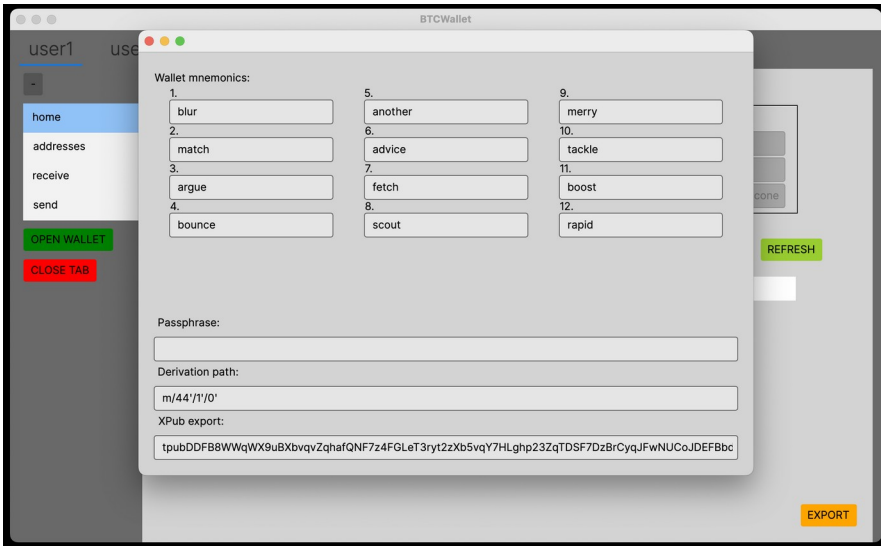
- Home – hlavní shrnutí dat a obsahu peněženky
- Addresses – vygenerované adresy patřící dané peněžence jak pro příjem tak pro odesílání vlastních zbytků transakce
- Receive – potřebná data pro přijmutí platby od jiného uživatele
- Send – potřebná data pro vytvoření a odeslání transakce do bitcoinové sítě, které není přítomné (z logických důvodů) pro read-only peněženky
- Open wallet – tlačítko pro vytvoření či importování nového profilu
- Close tab – zavření aktuální záložky

Home
Obsah okna home se dělí na základní čtyři části, viz Image6.



V prostřední části jsou všechny mince, které má peněženka k dispozici se základními metadaty jako kdy, na jakou adresu a kolik bylo odesláno.

Pod prostřední částí je tlačítko „Export“, které po kliknutí otevře okno se základními daty pro export peněženky a to buď pomocí 12 slov (pokud není peněženka read-only), derivation path a nebo xpub, který umožní exportovat read-only peněženku, viz Image7



Vlevo nahoře máme souhrn dat ohledně peněženky, tedy celková hodnota mincí v jednotkách satoshi, kurz jednoho bitcoinu v dolarech, hodnota mincí v dolarech a počet mincí v peněžence.

Vpravo nahoře se nachází konfigurace RPC klienta, která je v základu nastavena na klienta provozovaného v cloudu aplikace https://console.chainstack.com. Chce-li uživatel změnit RPC klienta na vlasntího, aktivuje toggle box a změní si údaje dle vlastní potřeby. Následně, je-li klient správně nakonfigurován, po kliknutí tlačítka „Refresh“ započne aktualizace držených micí danou peněženkou zobrazením textu „Loading…“, jinak je zobrazena korespodující chybová hláška.

!! REFRESH MINCI TRVA AZ NIZKE JEDNOTKY MINUT a uzivatel nesmi odchazet z okna.

Addresses

Obshah okna Addresses se dělí na dvě části, viz Image8.

V horní části jsou adresy pro příjem mincí od „cizích“ uživatelů, které je možné přigenerovávat v menu sekci „Receive“ viz dále. Zde jsou všechny adresy patřící dané peněžence pouze zobrazeny.

V dolní části jsou adresy pro odkládání zbytků, při platbě na jiné adresy viz v menu sekci „Sent“, kdy je nová adresa přigenerována právě když dojde k odchozí transakci.

Receive

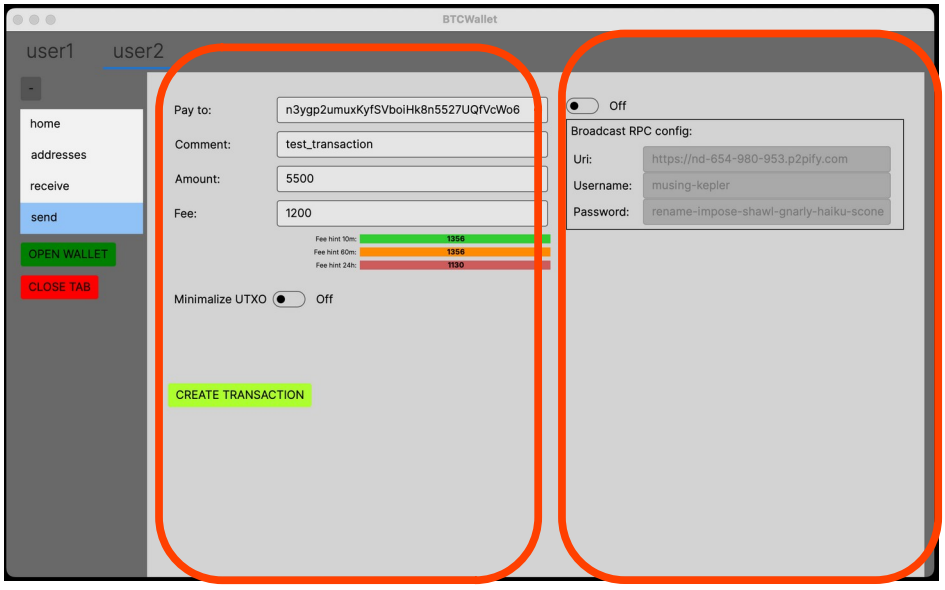
Obshah okna Receive se dělí na dvě části, viz Image9.

V horní části jsou zobrazená statická pole adresy a derivační cesta k ní od hlavního klíče a potom dvě dynamická pole pro částku, kterou chce uživatel obdržet a případnou zprávu pro odesílatele transakce, které se promítají do generování QR kódu.

V dolní části je vygenerovaný QR kód, který obsahuje adresu, částku a zprávu, jeho textová podoba je zobrazena hned pod ním. Následuje tlačítko „Next address“, které vzgeneruje a použije následující adresu pro příjem mincí, zároveň dojde i k aktualizaci QR kódu a zamykacího scriptu, který bude jako výstup transakce provedené na zobrazenou adresu.

Send

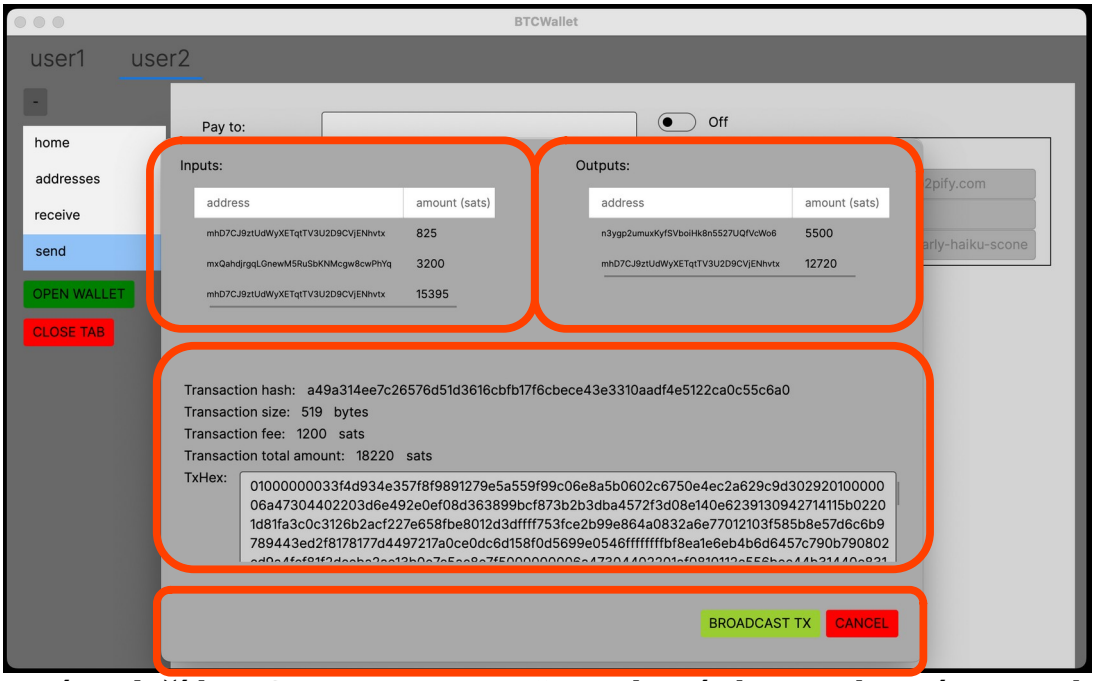
Obshah okna Send se dělí na dvě části, viz Image10.



V pravé části se opět nachází konfigurace (vlastního) RPC clienta, který slouží pro odeslání validní transakce do bitcoinové sítě. Více viz obsah Menu Home.

V levé části obrazovky se nachází informace, které je nutno vyplnit pro odeslání transakce, tedy adresu příjemnce, částku a poplatek těžaři (motivace, aby zařadil transakci do bloku a tím jí potvrdil za platnou). Pole komentáře je zcela nepovinné, slouží pouze jako informace pro peněženku, která bude zobrazena uživateli. Pod zmíněnými text boxy se nachází orientační nápověda pro velikost průměrného transakčního poplatku vzhledem k ostatním stále nepotvrzeným transakcím. Následuje toggle box s nápisem „Minimalize UTXO“, který slouží k modifikovatelnosti transakce. Uživatel má tedy na výběr mezi použitím co nejvíce malých mincí, tak aby dohromady daly požadovanou sumu (**ne**aktivní toggle box) a nebo naopak pokud aktivujeme toggle box, potom je transakce složena z co nejvíce velkých mincí, tedy transakce bude pravděpodobně mít méně vstupů (bude menší).

Při validním vyplnění polí se aktivuje tlačítko „Create transaction“, které vytvoří již podepsanou transakci a zobrazí jí v novém okně, viz dále Image11. Jnak se zobrazí chybová hláška s konkrétním problémem.



Po kliknutí na tlačítko „Create transaction“ se zobrazí okno se shrnutím transakce, která je intuitivní. V levém horním rohu se nachází naše mince (adresa a hodnota), které slouží jako vstup pro transakci. V pravém horním rohu se nachází výstupy transakce, tedy na jakou adresu bude suma zaslána a případně suma zbytku mincí, která bude odeslána na naše adresy pro zbytky. V prostřední části máme identifikátor transakce (hash sha256 celé transakce), její velikost, sumu poplatku, a celkovou výstupní sumu transakce za kterou následuje samotná podepsaná transakce v hexadecimálním formátu, která může být případně použita ke zveřejnění v jiném

internetovém API. Ve spodní části se nachází tlačítko pro zvřejnění transakce do bitcoinové sítě, či jeji zrušení.

V případě, že jsou použity špatné vstupy pro transakci (např. již utracené mince), dojde místo ke zveřejnění transakce k chybové hlášce a je nutno obnovit mince peněženky v sekci Home tlačítkem „Refresh“.