

# Bitzuma

BLOG KURZY KNIHY ZPRAVODAJ O

## Kompletní průvodce multibitovou bitcoinovou peněženkou

Autor: Rich Apodaca | Aktualizováno 21. listopadu 2017

[MultiBit](#) je [oblíbený](#) program bitcoinové peněženky, jehož cílem je kombinovat rychlé spouštění, zjednodušenou sadu funkcí a podporu více jazyků.

**Poznámka: MultiBit již [není podporován](#). Tento příspěvek byl napsán v roce 2014 a od té doby byl jen mírně upraven. Zůstává pro ty, kteří mohou potřebovat používat MultiBit Classic, ale neměli by je používat začátečníci.**

Tato příručka dokumentuje MultiBit prostřednictvím podrobných příkladů napsaných z pohledu čtenáře nového v MultiBitu i Bitcoinu. Přístup k malému množství bitcoinů usnadní zde uvedené příklady [srozumitelnější](#). mnoho [možností nákupu](#); Obyvatelé USA mohou dokonce [platit za bitcoiny hotovostí u pokladní banky](#).

### MultiBit Classic a MultiBit HD

práce na nové variantě peněženky MultiBit, „MultiBit HD“ [Nedávno byla oznámena](#). MultiBit HD implementuje návrh [HD Wallet, který](#) se nachází v peněženkách, jako je [Electrum](#).

Tým MultiBit navrhl, že aktualizace aktuálně dostupné verze softwaru

budou nadále vydávány pod názvem „MultiBit Classic“. Zde uvedené informace platí pro tuto verzi MultiBit (0.5.17).

## Instalace

Stáhněte si instalační program pro váš operační systém ze [stránky ke stažení](#). „Podpis“ a „Ověřit“ se týkají funkcí zabezpečení, které budou vysvětleny v dalším článku.

### Instalace na Windows

Dvakrát klikněte na stahování MultiBit.

MultiBit vyžaduje [Javu](#). Pokud tento software na vašem počítači není, instalační program se zeptá, zda jej chcete přidat. Klikněte na „Ano“ a postupujte podle pokynů na webové stránce, na kterou jste přesměrováni. Po instalaci Javy spusťte znovu stahování MultiBit.

Instalační program vás provede zbytkem instalace.

### Instalace na Mac

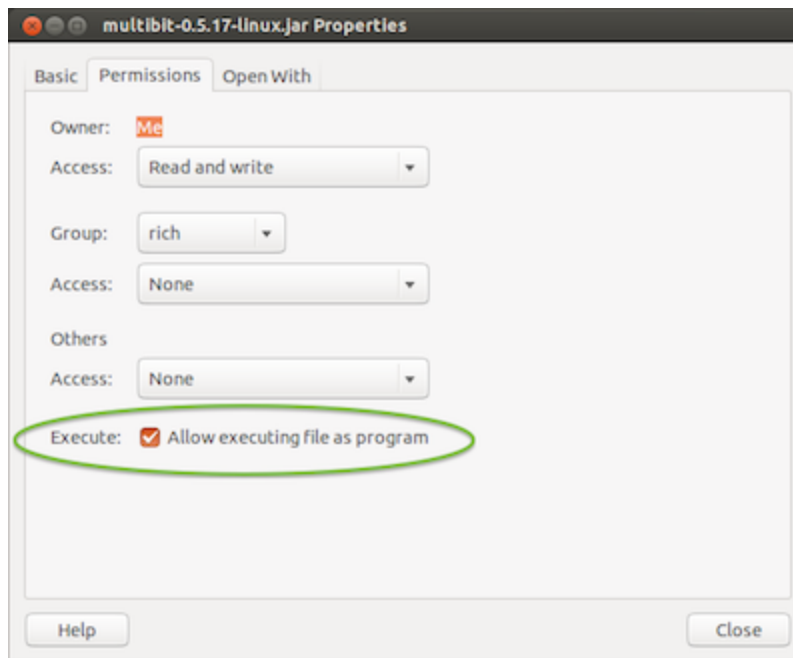
Dvakrát klikněte na stahování MultiBit. Přetáhněte ikonu MultiBit do složky „Applicatoins“.

### Instalace na Ubuntu Linux

Pokud stahujete MultiBit z prohlížeče, ujistěte se, že jste si instalační program uložili a nepokoušeli se jej otevřít pomocí správce balíčků.

MultiBit vyžaduje [Javu](#). Nainstalujte jej ze softwarového centra Ubuntu vyhledáním „openjdk“. Vyberte „OpenJDK Java 7 Runtime“.

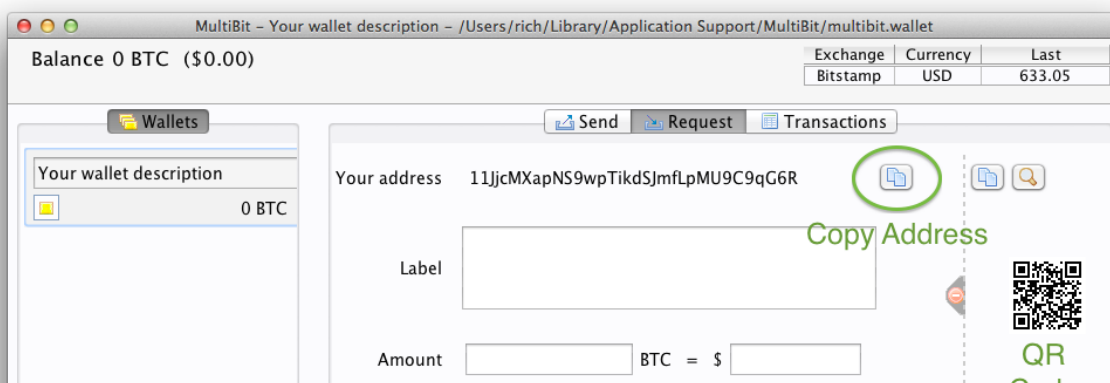
Po stažení MultiBitu a případné instalaci Javy přejděte do složky Downloads, klikněte pravým tlačítkem myši na instalační program MultiBit a vyberte možnost nabídky „Vlastnosti“. Klikněte na kartu „Oprávnění“ a zaškrtněte políčko „Provést“, poté okno zavřete.

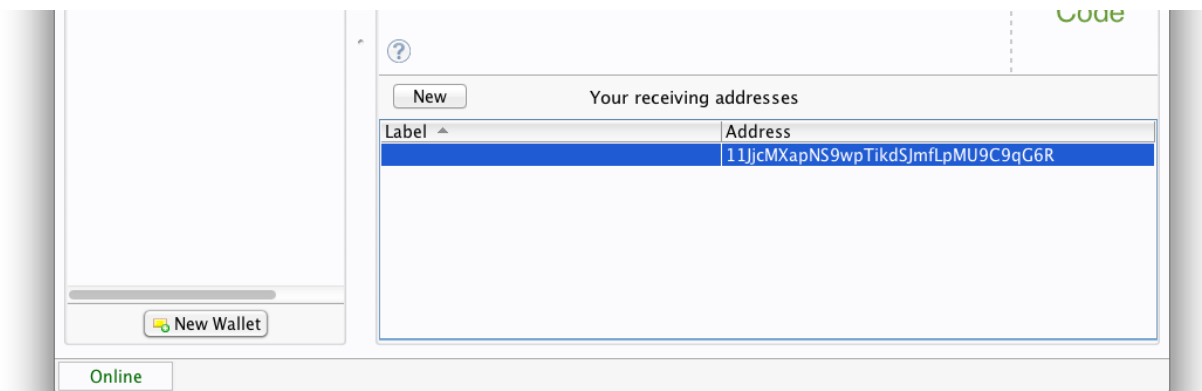


Znovu klikněte pravým tlačítkem myši na stažení MultiBit a vyberte možnost „OpenJDK Java 7 Runtime“. Instalátor vás odtud povede. Po dokončení instalace bude MultiBit dostupný po tlačítku „vyhledat váš počítač“.

## Přijmout platbu

Aby vám mohl plátce poslat peníze, vyžaduje vaši bitcoinovou adresu. Na kartě „Požadavek“ najdete řádek textu začínající „1“ a označený „Vaše adresa“. Zkopírujte tuto adresu do systémové schránky pomocí tlačítka „Kopírovat“. Alternativně může být QR kód vaší přijímací adresy naskenován ručním zařízením.





Dále proveďte platbu ze softwaru nebo služby, která aktuálně hostuje vaši financovanou peněženku, do vaší nefinancované peněženky MultiBit. Pokud jste například nakoupili přes Localbitcoins, přejděte do své peněženky tam. Vložte svou MultiBit přijímací adresu do pole označeného „Přijímání bitcoinové adresy“. Vyplňte částku. Pro tento příklad převedte 0,001 bitcoinu (1 mBTC, nebo přibližně 0,64 USD při aktuálním směnném kurzu). Zadejte své heslo pro místní bitcoiny a klikněte na „Odeslat z peněženky“.

## Send bitcoins

This is your LocalBitcoins.com bitcoin wallet.

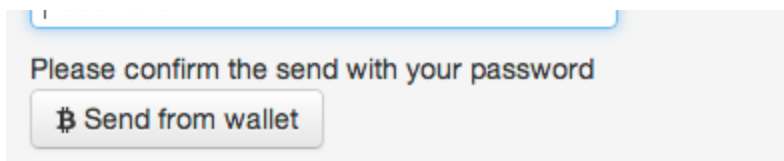
**Please note: outgoing transactions can have lengthened processing times, because of some issues with the bitcoin network. These should be fixed within days.**  
[Read more here](#)

Spendable balance: **0.00473** BTC

Receiving bitcoin address:

Amount in bitcoins:

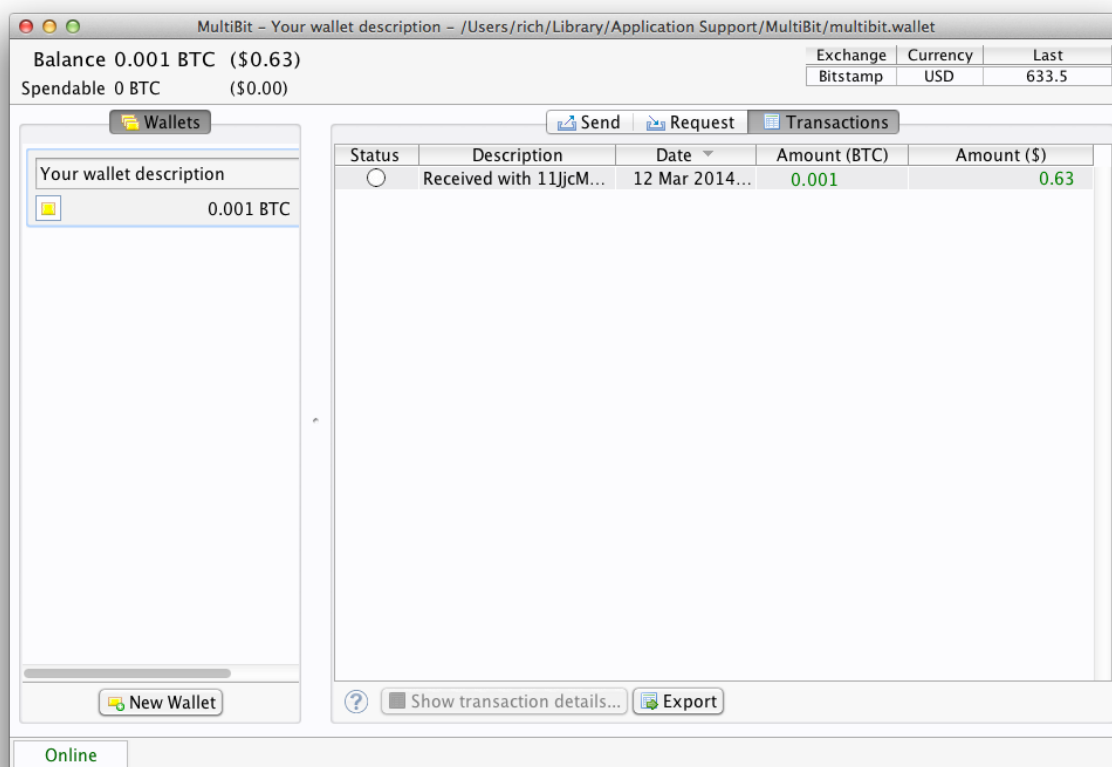
Your password:



Localbitcoiny, stejně jako jiné burzy, neposílají prostředky vždy okamžitě. Je třeba počítat se zpožděním několika minut, protože převody jsou často dávkové, aby se minimalizovaly poplatky. V mých testech trvalo Localbitcoinům zpracování výběru v průměru deset minut.

## Sledujte transakce

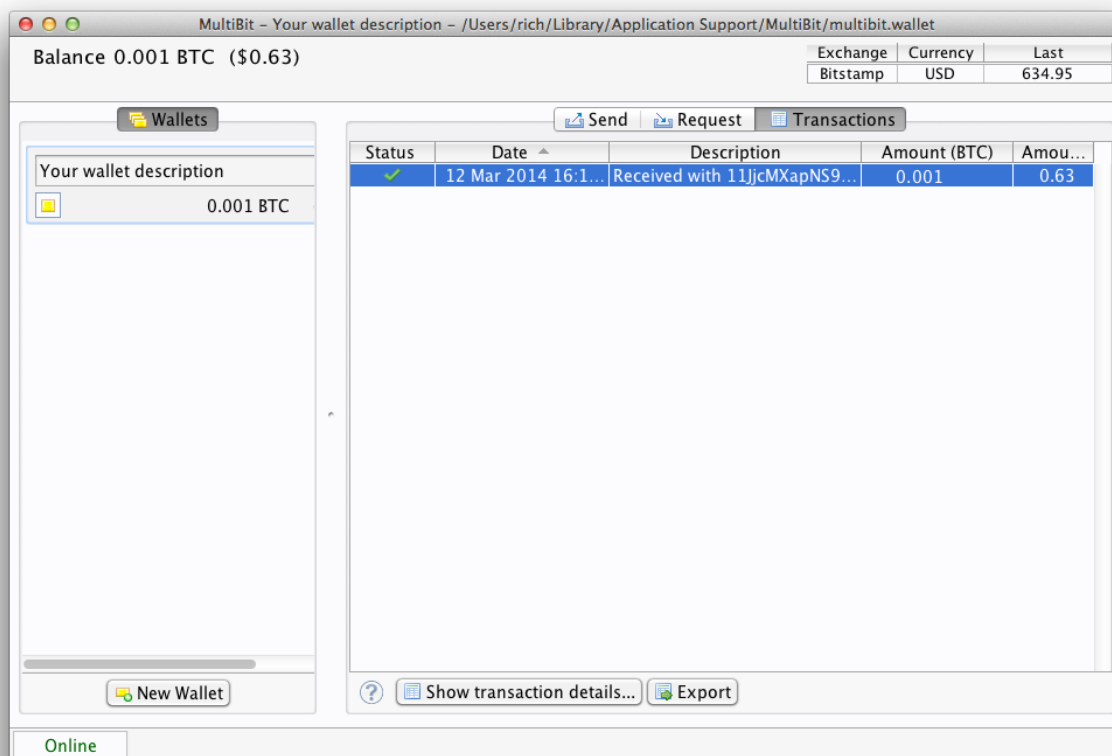
Na kartě „Transakce“ jsou uvedeny všechny aktuální a čekající transakce. „Stav“ nově přijaté nevyřízené platby by měl být označen prázdným kroužkem.



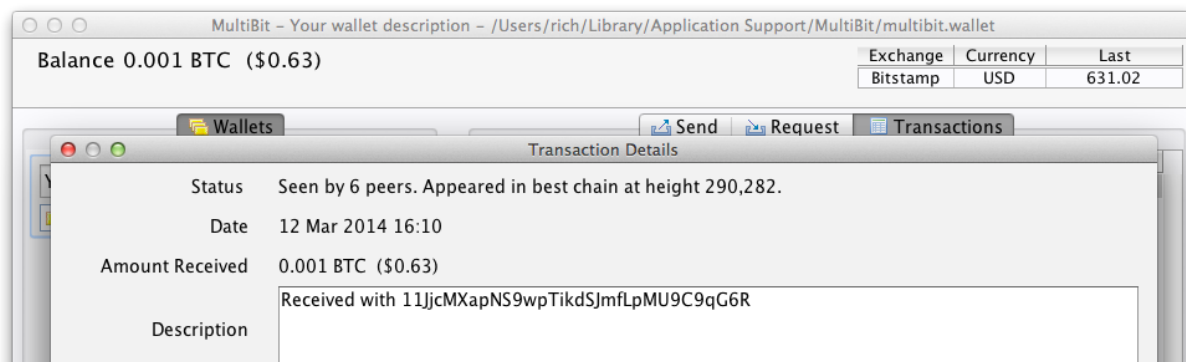
Jakmile bitcoinová síť zpracuje tuto novou transakci, její stav bude

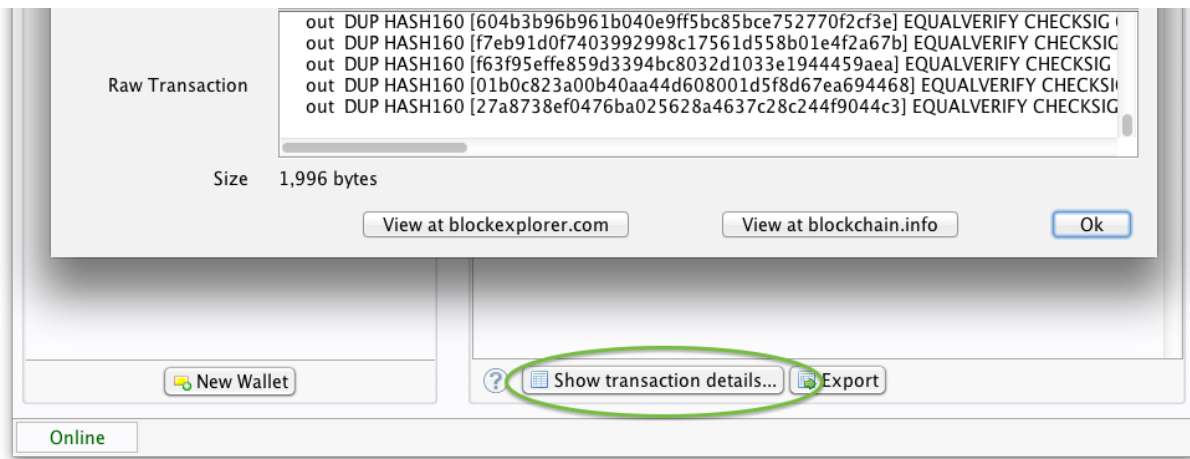
aktualizován v seznamu transakcí. Síť posílá potvrzení každých zhruba deset minut. MultiBit aktualizuje ikonu stavu transakce, kdykoli obdrží potvrzení.

MultiBit považuje transakce za plně zpracované po obdržení šesti potvrzení. Zpracované transakce jsou označeny zeleným zaškrtnutím.



Chcete-li zobrazit všechny dostupné informace o transakci, klikněte na ni a poté klikněte na tlačítko „Zobrazit podrobnosti transakce...“.

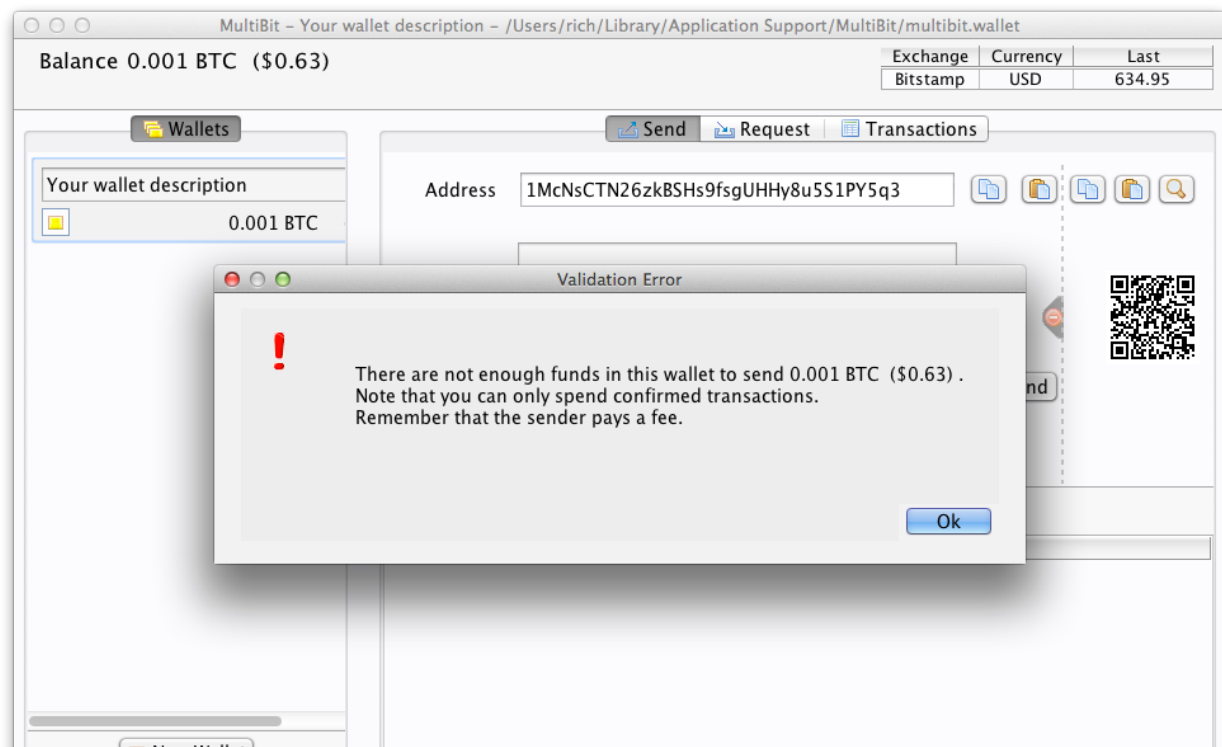


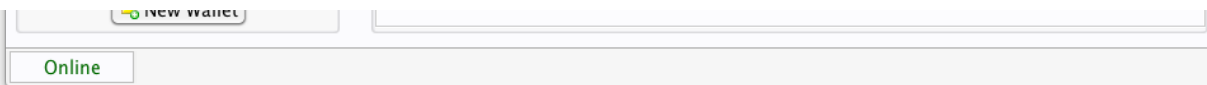


## Zaplatit

Zahajte platbu kliknutím na záložku „Odeslat“. Pro provedení platby jsou vyžadována pouze dvě pole: adresa a částka k odeslání. Pole „Adresa“ přijímá bitcoinovou adresu, jako je ta, která se používá k přijímání finančních prostředků. Částky mohou být denominovány v bitcoinech (BTC) nebo v místní měně.

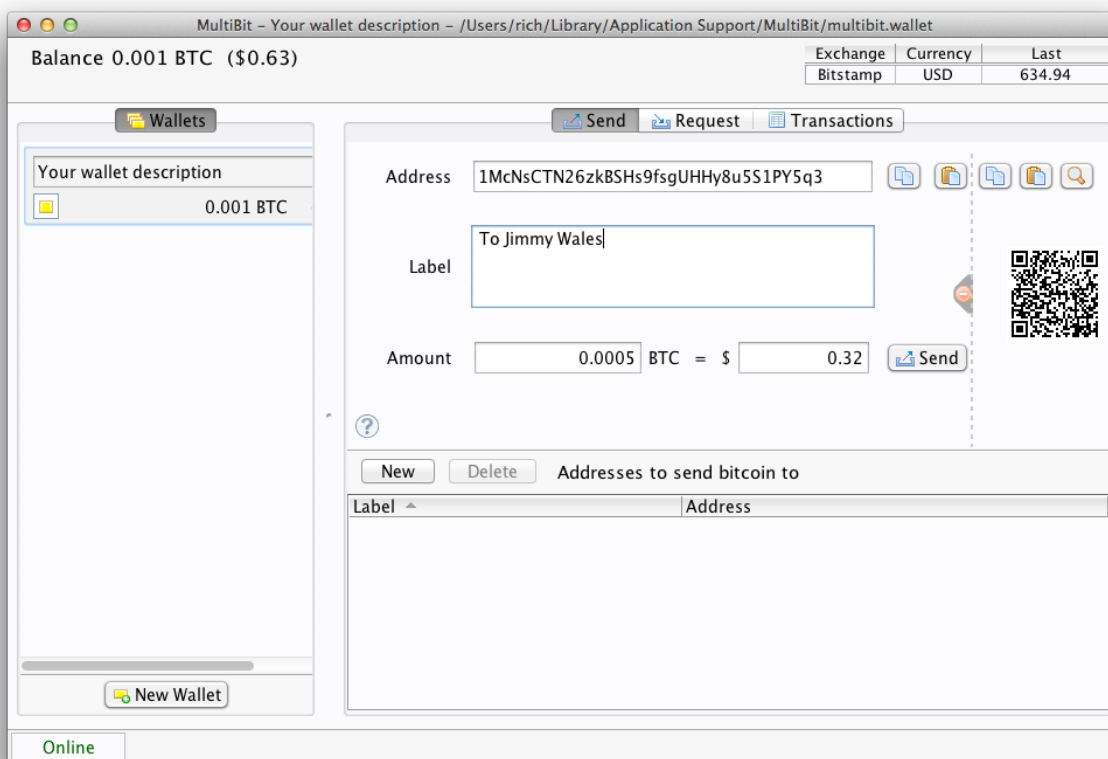
Poplatky musí být zaúčtovány při každé transakci. Pokud se například pokusíte utratit celý zůstatek peněženky, zobrazí se chybová zpráva.





Sít očekává transakční poplatek 0,1 mBTC za každou platbu. K odeslání této platby s ohledem na prostředky, které mám aktuálně v peněženke (1 mBTC), budu muset poslat 0,9 mBTC nebo méně.

V tomto příkladu daruji 0,5 mBTC (0,0005 BTC) [Jimmymu Walesovi](#) v naději, že přesvědčí správní radu Wikipedie, aby přijala dary bitcoinů. „Štítek“ pomáhá při vedení osobních záznamů, ale tyto informace nejsou viditelné mimo aktuální peněženku. Kliknutím na „Odeslat“ se zobrazí dialogové okno s žádostí o potvrzení. Kliknutím na „Odeslat“ v tomto dialogu odešlete platbu do sítě.



Kliknutím na kartu „Transakce“ můžete sledovat průběh platby.



## Zamette papírovou peněžku

Papírové peněženky jsou někdy přijímány jako dárky od jiného uživatele bitcoinů. Zde popsáný postup pro **bezpečný import papírových peněženek do MultiBitu je bohužel komplikovaný**. Pokud jste dostali papírovou peněžku a chcete ji jednoduše utratit, zvažte použití jiného programu bitcoinové peněženky – například [Electrum](#).

Postup zametání se bude skládat z těchto kroků:

1. Přidejte soukromý klíč papírové peněženky do souboru importu.
2. Vytvořte novou peněžku s názvem „Paper Wallet“.
3. Importujte soukromý klíč papírové peněženky do „Papírové peněženky“
4. Převeďte celý zůstatek z „Papírové peněženky“.
5. Smazat „Papírovou peněžku“

Před utrácením finančních prostředků do papírové peněženky je třeba importovat „soukromý klíč“ do peněženky MultiBit. Tento klíč obvykle začíná číslem „5“ a je často označen slovy „soukromý klíč“, „tajný“, „vykoupit“ nebo „utratit“.



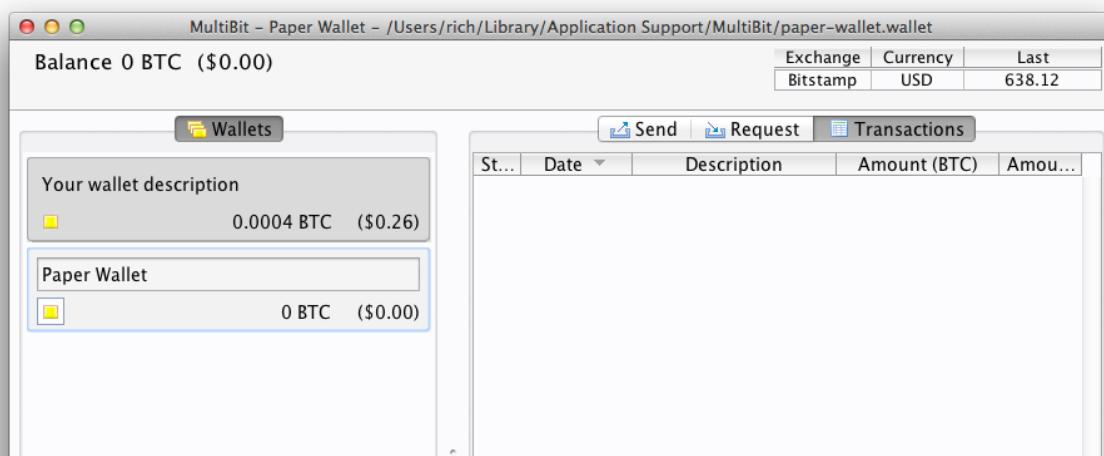
Vytvořte textový soubor s názvem `import.key` pomocí textového editoru, jako je Poznámkový blok. Zkopírujte soukromý klíč Peněženky a vložte jej do prvního řádku. Přidejte znak mezery a poté přidejte časové razítko ve [formátu ISO 8601](#) ( `YYYY-MM-DDTHH:MM:SSZ` ). Časové razítko by mělo *bezpečně představovat čas před* provedením první platby do peněženky. Toto datum lze získat zadáním adresy papírové peněženky na [blockchain.info](#) . Příklad souboru může vypadat takto:

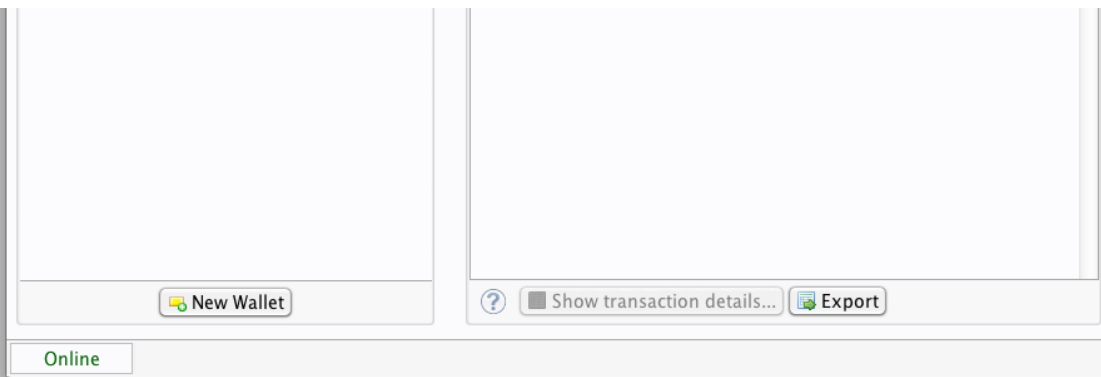
```
#sample multibit private key import file
5Jw4mJMfm6HySiqG5ndM1fYEiHZZNGpJqLr57qCptaU7JR6K5JX 2014-01-01T12:00:00Z
```

Bohužel nesprávné přiřazení časového razítka v importovaném souboru je snadné a může způsobit matoucí chování MultiBit. Pokud by MultiBit po importu soukromého klíče nezobrazoval zůstatky očekávaným způsobem, podívejte se do [Zaseknuté transakce](#) .

Dále vytvoříme samostatnou MultiBit peněženku pro uložení finančních prostředků z papírové peněženky. Začněte kliknutím na tlačítko „Nová peněženka“ v levé dolní části hlavní obrazovky. Až budete vyzváni k zadání názvu souboru, zadejte `paper-wallet.wallet` . Uložte soubor do výchozího umístění kliknutím na „Uložit“.

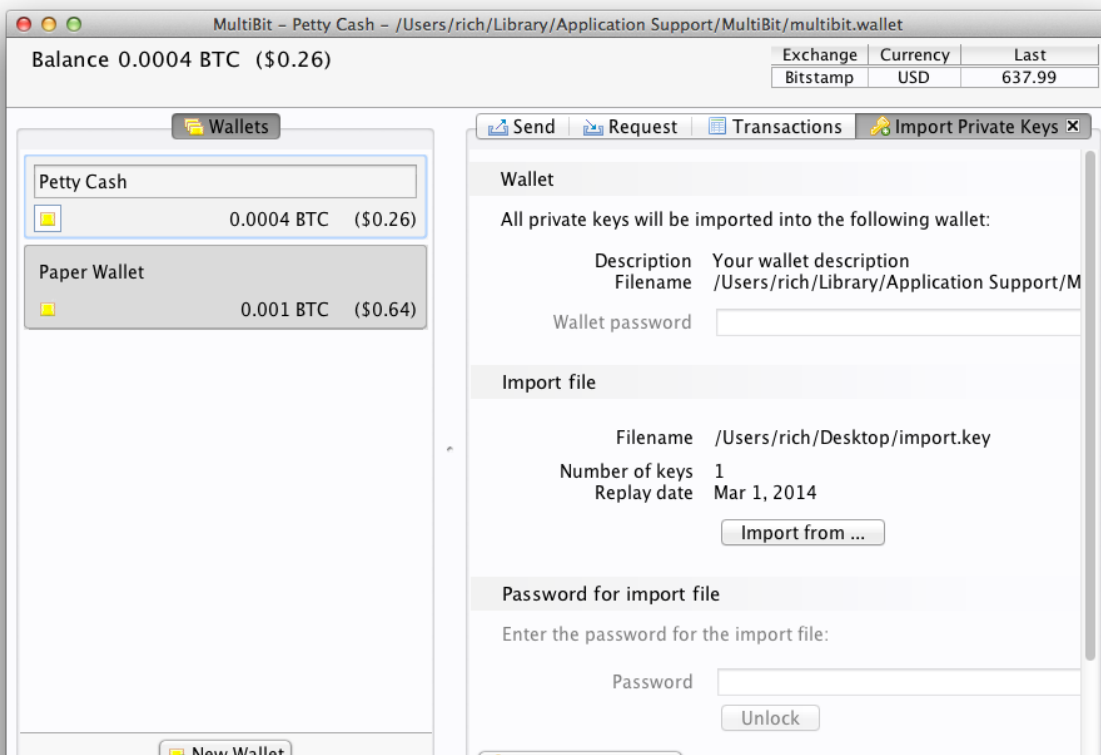
Nově vytvořená peněženka by měla být prázdná. Přejmenujte ji dvojitým kliknutím na „Popis vaší peněženky“ a zadáním „Papírová peněženka“.

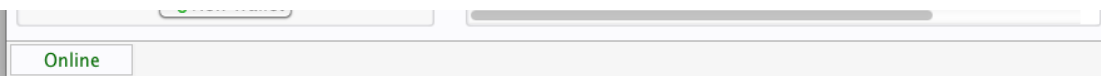




Dále importujte papírovou peněženkou. Ujistěte se, že peněženko s názvem „Paper Wallet“ je vybrána v sekci MultiBit „Wallets“. Poté vyberte z hlavní nabídky možnost nabídky Nástroje > Importovat soukromé klíče. Klikněte na tlačítko „Importovat z...“ a vyberte dříve vytvořený soubor s názvem `import.key`.

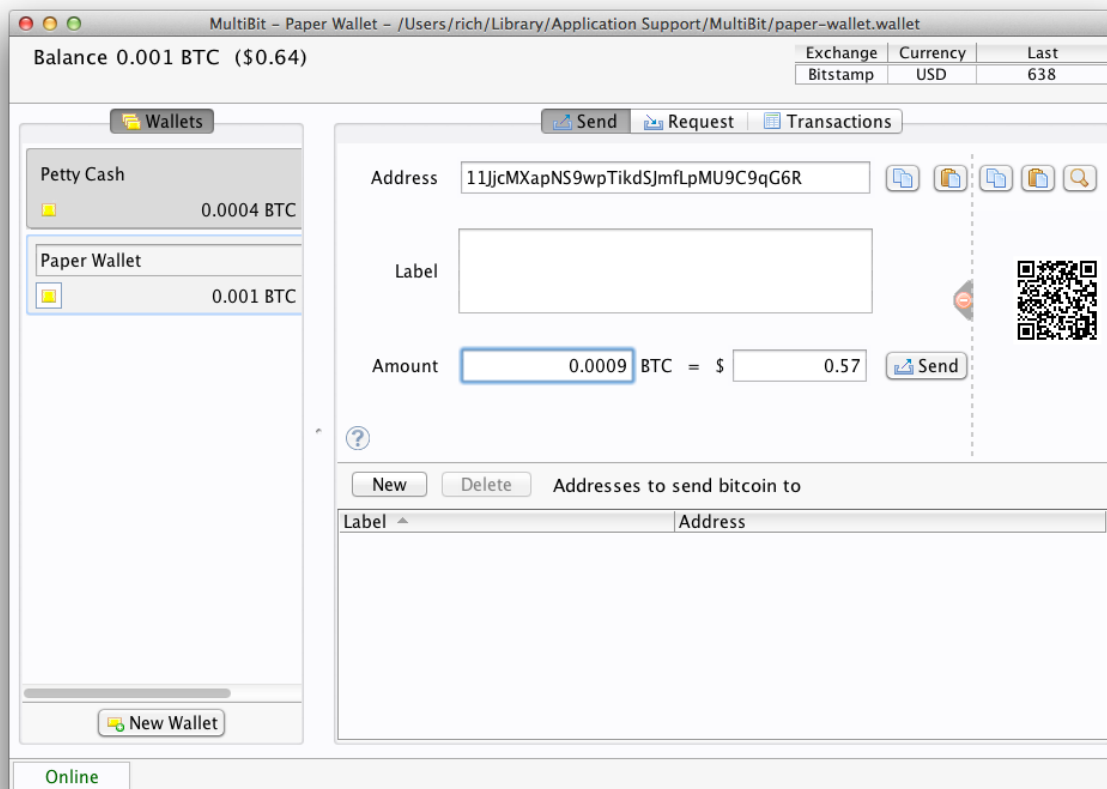
Po synchronizaci byste měli vidět dvě peněženky, z nichž jedna obsahuje zůstatek nově importované papírové peněženky. Abyste předešli nejasnostem, označte původní MultiBit peněženko jako „Petty Cash“.



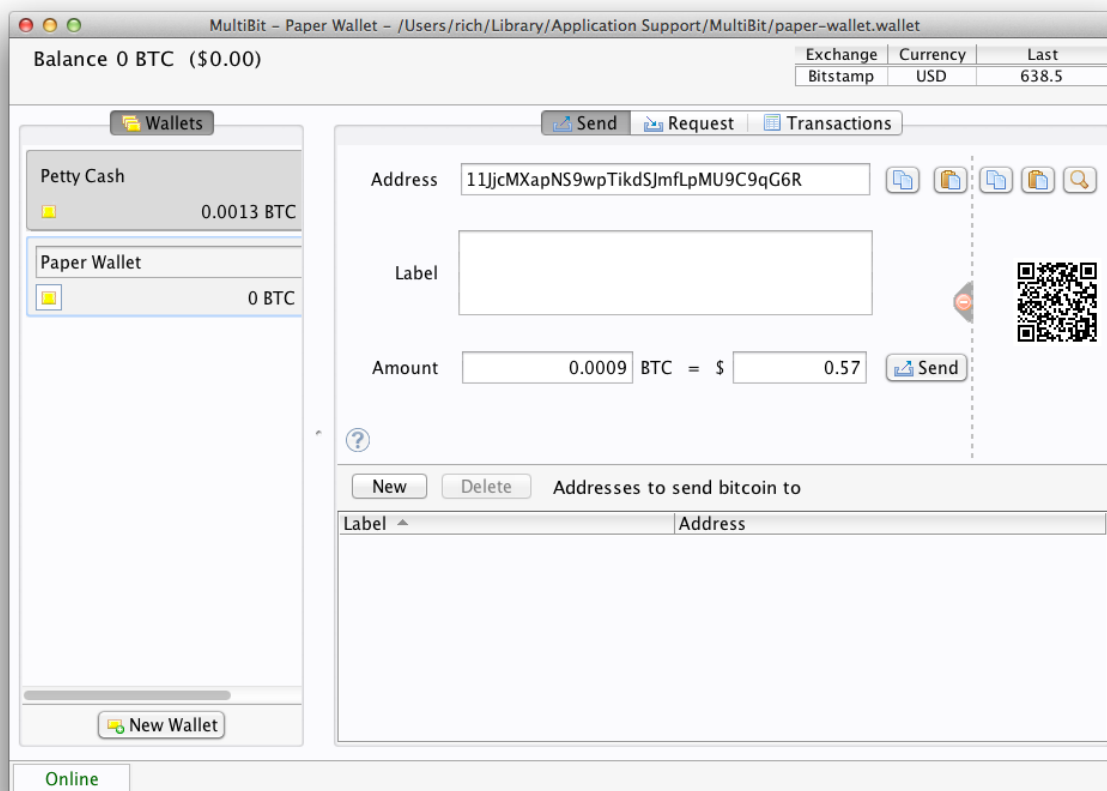


Dále převedte všechny prostředky z peněženky označené „Paper Wallet“ do peněženky označené „Petty Cash“. Začněte zkopírováním adresy požadavku z peněženky „Petty Cash“ do systémové schránky. Aktivujte „Papírovou peněženkou“ kliknutím na ni a poté klikněte na kartu „Odeslat“. Vložte dříve zkopírovanou adresu „Petty Cash“, která je aktuálně v systémové schránce. Zadejte částku, která plně převede prostředky z papírové peněženky, když jsou zohledněny transakční poplatky.

Protože v tomto příkladu je částka na „Paper Wallet“ 1 mBTC, částka, kterou převedu, je 0,9 mBTC.



Po odeslání transakce by měl mít „Papírová peněženka“ nulový zůstatek. Zůstatek „Petty Cash“ by měl odrážet převod prostředků „Paper Wallet“.



V tomto okamžiku je bezpečné odstranit „Paper Wallet“. Klikněte na něj a poté z hlavní nabídky vyberte možnost Soubor > Zavřít peněženku.

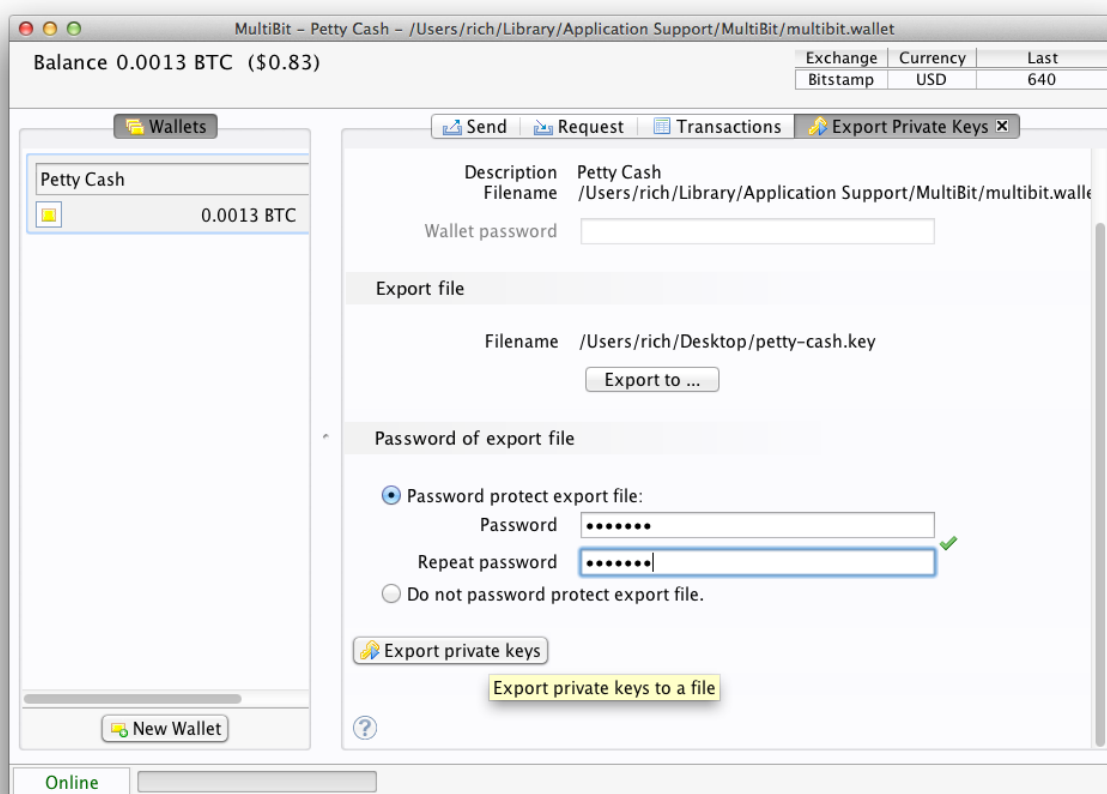
Možná se ptáte, proč byla použita přechodná peněženka („Paper Wallet“). Proč neimportovat soukromý klíč přímo do výchozí peněženky?

Odpověď souvisí se [změnou adresy](#). Ponechání importovaného soukromého klíče v MultiBit peněžence umožňuje v budoucnu odcizení bitcoinů. Od verze 0.5.17 zůstal MultiBit náchylný k tomuto druhu krádeže. Tato obava však nemusí platit, pokud importujete pouze soukromé klíče, které jste bezpečně vytvořili.

## Vytvořte zálohu

Záloha umožňuje obnovu finančních prostředků v případě, že jsou soubory MultiBitu poškozeny nebo náhodně odstraněny.

Začněte zálohování výběrem možnosti **Nástroje > Exportovat soukromé klíče** z hlavní nabídky. Vyberte vhodný název souboru pro zálohu (v tomto případě `petty-cash.key`) a přidejte heslo pro soubor. Až budete připraveni, stiskněte tlačítko **Exportovat soukromé klíče**.



Mnoho případů krádeže bylo způsobeno tím, že uživatelé MultiBit ukládali nešifrované zálohy do cloudového úložiště. Každý, kdo najde takový záložní soubor, může vzít peníze z vaší peněženky – s přístupem k vašemu počítači nebo bez něj. Přidejte bezpečné heslo do jakékoli zálohy peněženky obsahující netrivalní množství bitcoinů.

## Obnovte zálohu

Pouhé vytvoření zálohy nezaručuje bezpečnost vašich peněz – budete se muset ujistit, že můžete zálohu v případě potřeby obnovit. Bohužel testování obnovy zálohy není v MultiBitu jednoduché. Následující dva odstavce popisují postup pro simulaci čisté instalace MultiBit. **Použijte jej pouze na zálohovanou peněženkou obsahující triviální množství bitcoinů a pouze v případě, že se cítíte dobře upravovat systémové soubory.**

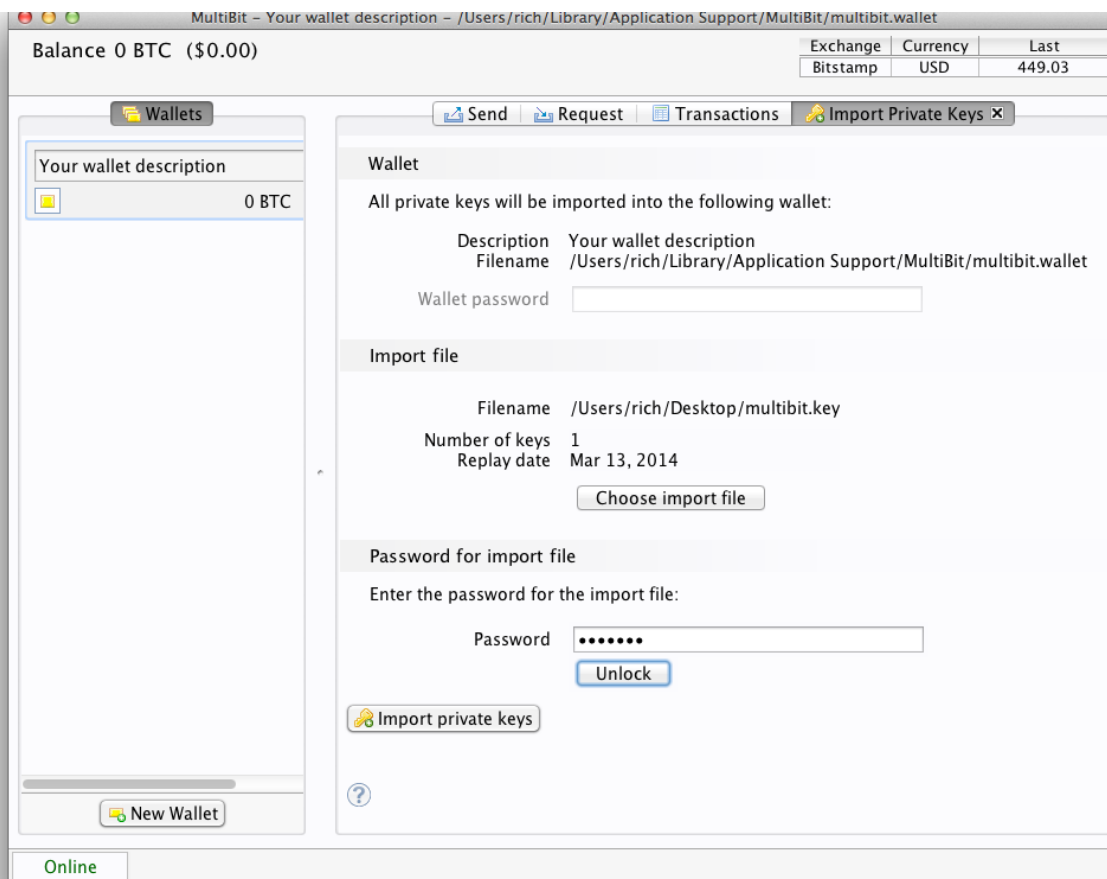
Datový adresář MultiBit se nachází na cestě specifické pro operační systém, která je také zobrazena v horní části hlavního okna MultiBit. Výchozí cesty jsou:

- **Okna** `C:\Users\<<UserName>\AppData\Roaming\MultiBit`
- **Mac** `~/Library/Application Support/MultiBit`
- **Linux** `~/MultiBit`

Po nalezení tohoto datového adresáře zavřete MultiBit. Dále smažte datový adresář. Při restartování MultiBitu bude vaše předchozí peněženko nahrazena novou, nefinancovanou peněženkou. Tím je procedura pro simulaci čisté instalace MultiBit ukončena.

Počínaje čistou instalací MultiBitu je postup obnovení zálohy podobný postupu popsánému v části [Sweep a Paper Wallet](#). Záložní soubor hraje roli ručně vytvořeného `import.key` soubor.

V nově otevřené multibitové instanci vyberte v hlavní nabídce možnost **Nástroje > Importovat soukromé klíče**. Klikněte na tlačítko „Vybrat soubor importu“, přejděte do umístění zálohy a vyberte soubor. Pokud byla záloha zašifrována, zadejte její heslo a klikněte na tlačítko „Odemknout“. Pokud zadáte špatné heslo, MultiBit odpoví zprávou v tomto smyslu.



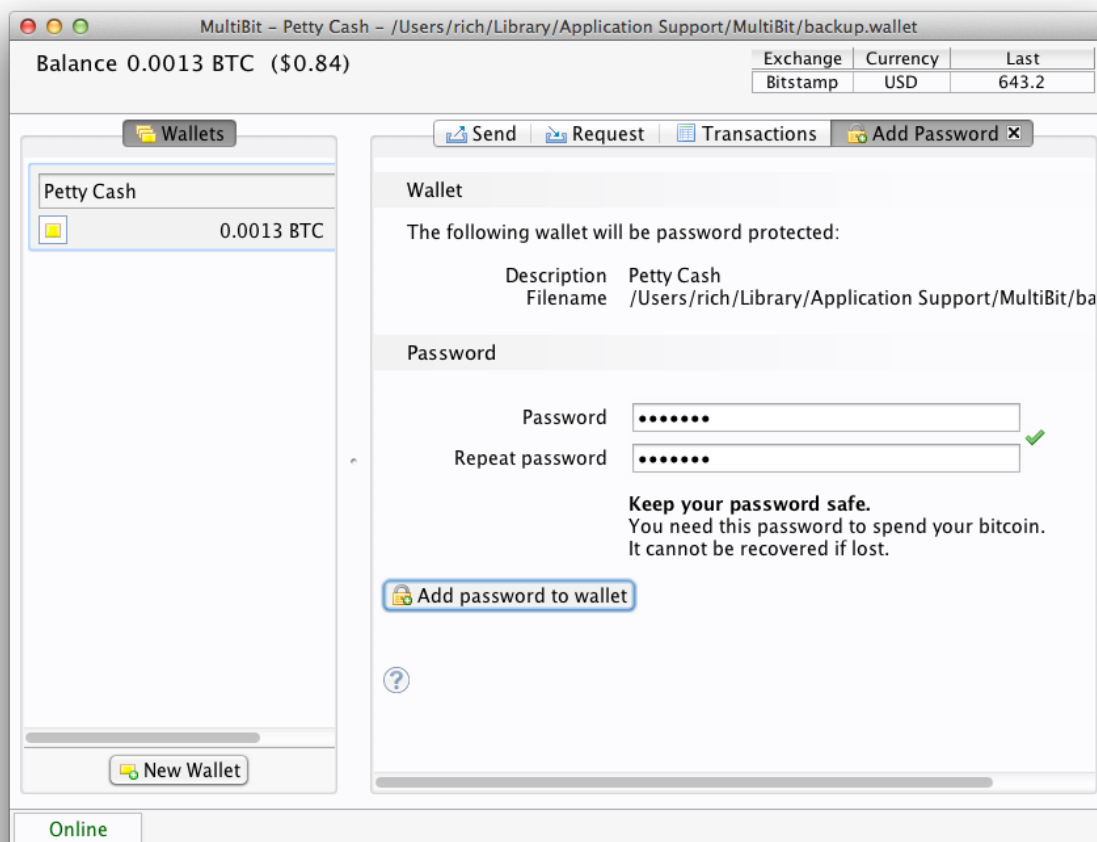
S vybraným a v případě potřeby odemčeným záložním souborem klikněte na tlačítko „Importovat soukromé klíče“. MultiBit se synchronizuje se sítí, což může trvat minutu nebo dvě. Po dokončení synchronizace by měla být vaše peněženka uvedena do původního stavu.

## Bezpečnostní

Dosud používané MultiBit peněženky nebyly chráněny heslem. Bez hesla může v zásadě ukrást bitcoiny z peněženky kdokoli, kdo má přístup k vašemu počítači nebo může číst z vašeho disku. Přidání hesla ztěžuje takovou krádež.

Chcete-li přidat heslo, vyberte v hlavní nabídce možnost Soubor > Přidat heslo.





Penženky chráněné heslem se chovají jinak než penženky nechráněné. Před utrácením nebo zálohováním je třeba je odemknout. Zobrazují také ikonu zámku v zobrazení penženky. Obnovení ztraceného hesla penženky je pro většinu praktických účelů nemožné, proto je důležité zvolit zapamatovatelné a bezpečné heslo.

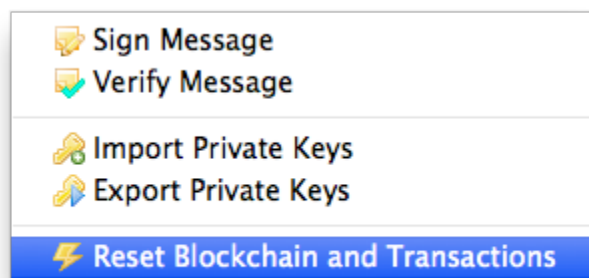
## Zaseknuté transakce

MultiBit platby se někdy nepodaří potvrdit. Příznaky mohou zahrnovat:

- odchozí platba, která se nikdy nepotvrdí, ukazuje čtverec nebo trojúhelník déle než hodinu
- zobrazí se nesprávné vyvážení

Pokud k tomu dojde, je [doporučeným postupem](#) použít funkci resetování,

kteřá je přístupná prostřednictvím možnosti hlavní nabídky **Nástroje** > **Resetovat blockchain a transakce**.



Ačkoli tato oprava často problém vyřeší, existují případy, kdy ne. Tento stav může být způsoben například použitím nesprávně naformátovaného importního souboru papírové peněženky. Jak je popsáno v [Sweep a Paper Wallet](#), při přiřazování časového razítka pro soukromý klíč je třeba postupovat opatrně. Pokud se zvolené časové razítko objeví *po* první transakci, MultiBit může trvale zobrazovat nesprávný zůstatek.

Pokud by se tento problém objevil, řešení je přímočaré. Exportujte soukromé klíče peněženky výběrem možnosti „Nechránit soubor exportu heslem“. Otevřete exportovaný soubor pomocí textového editoru a poté soukromý klíč přeneste do jiného programu peněženky.

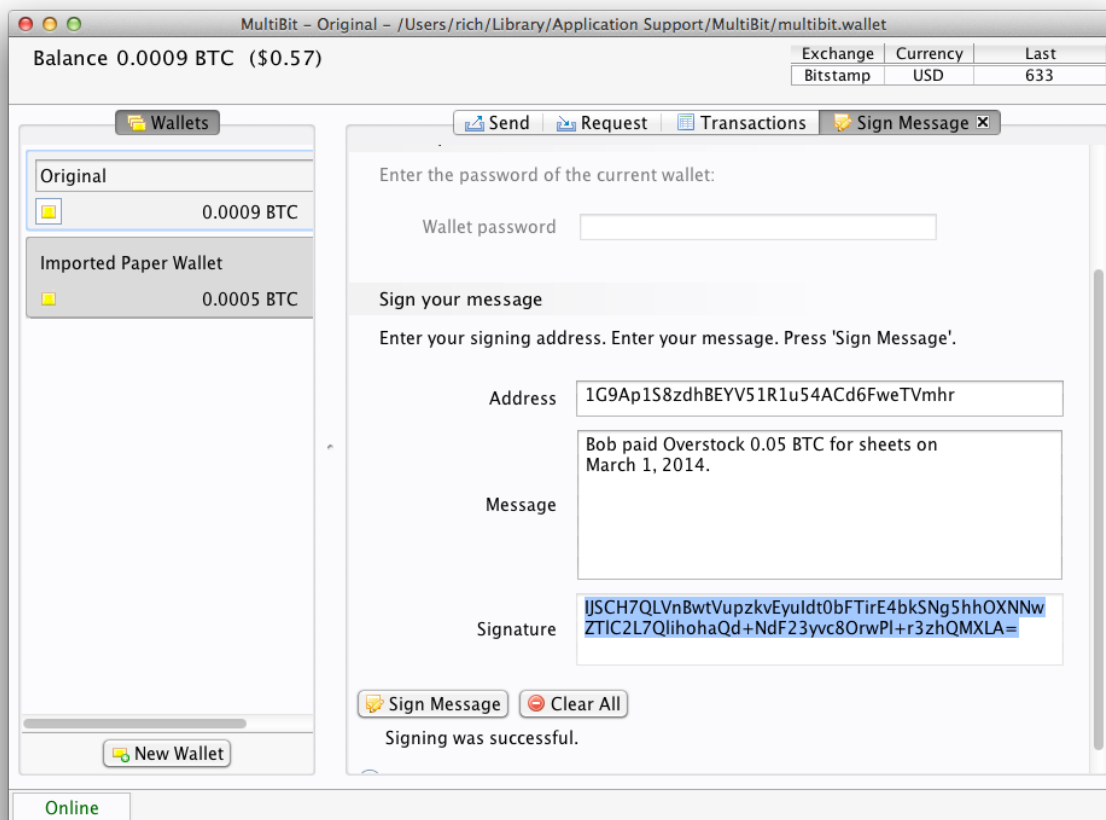
## **Podepisujte a ověřujte zprávy**

Někdy je užitečné dokázat druhé straně, že ovládáte adresu, ale bez převodu prostředků. Představte si, že mezi kupujícím a prodávajícím vznikne spor. Prodejce tvrdí, že nebyly zaplacený. Kupující ukáže na transakci block chain, která ukazuje platbu. Proávající tvrdí, že platba nepřišla od kupujícího, ale od někoho jiného.

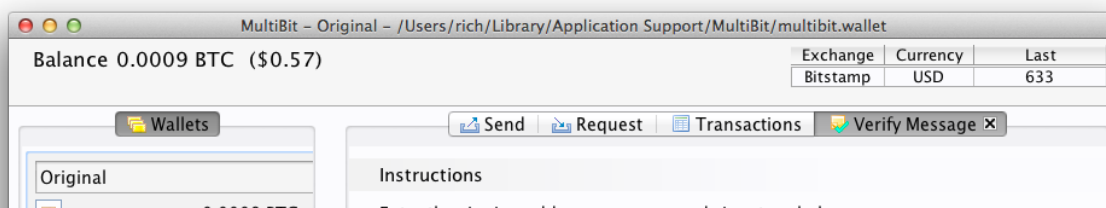
Kupující a prodávající postoupí případ před arbitra. Rozhodce požádá kupujícího, aby předložil zprávu podepsanou soukromým klíčem odesílající adresy v transakci block chain. Kupující tak učiní, arbitr zprávu

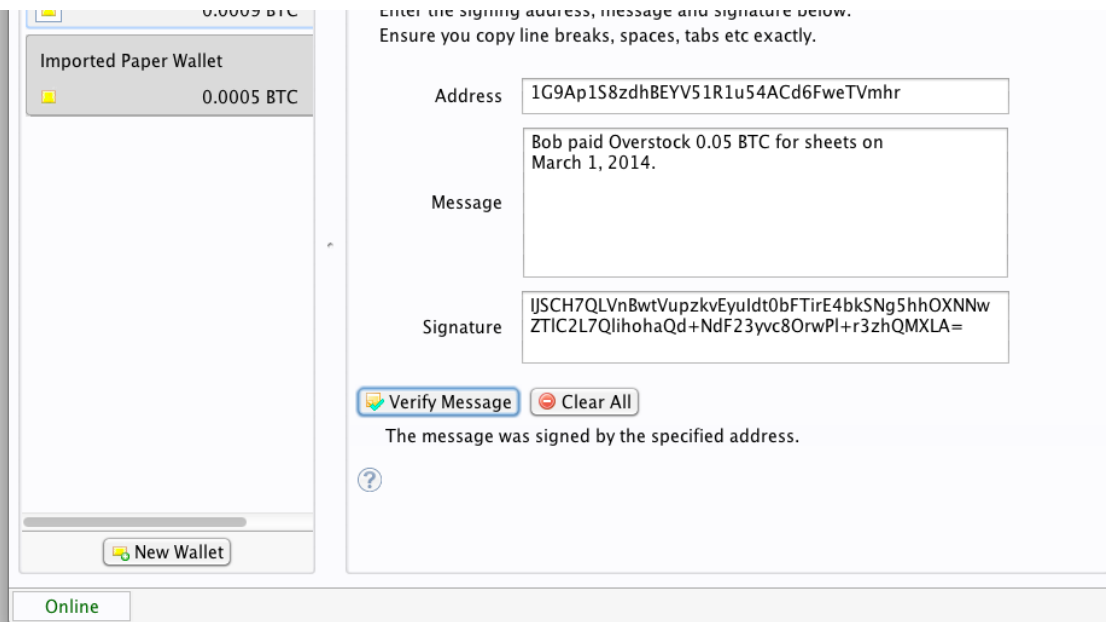
ověří a případ je rozhodnut ve prospěch kupujícího.

Podepisování zpráv se provádí přes volbu hlavní nabídky **Nástroje > Podepsat zprávu**. Zadejte adresu, ze které se chcete přihlásit, a zprávu. Stisknutím tlačítka „Podepsat zprávu“ se vytvoří podpis, který lze spolu se zprávou dát jako důkaz kontroly adresy.



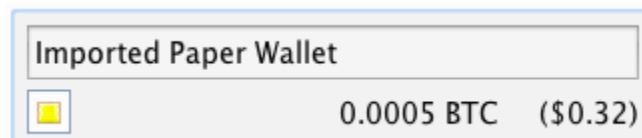
Ověřte podepsanou zprávu pomocí možnosti hlavní nabídky **Nástroje > Ověřit podepsanou zprávu**. Zadejte adresu, zprávu a podpis pro ověření. Poté klikněte na tlačítko „Ověřit zprávu“.



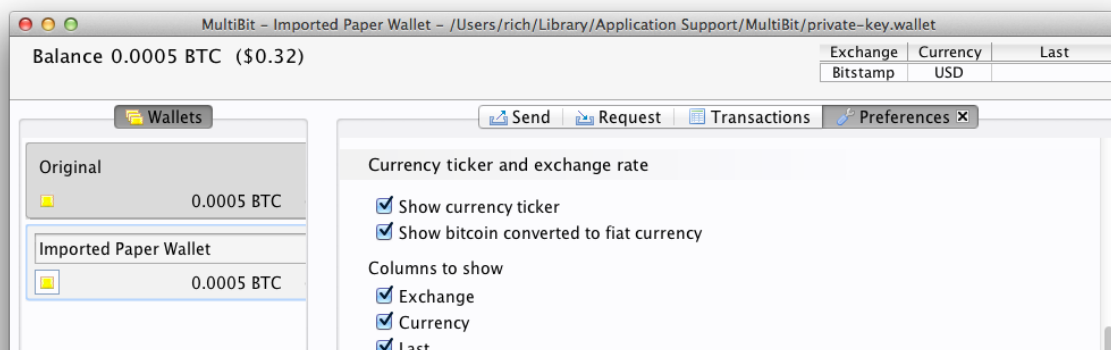


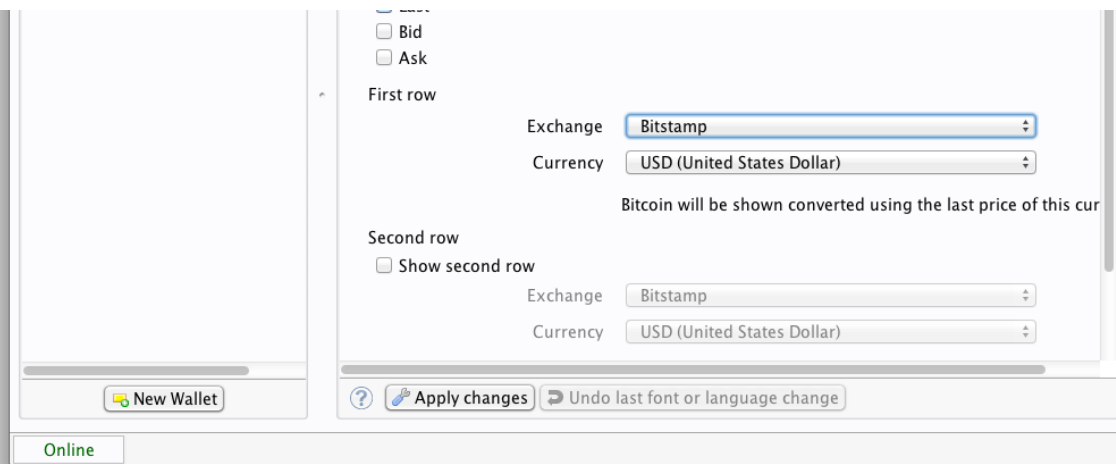
## převádění měny

MultiBit automaticky převádí bitcoiny na místní měnu. Výchozí směnný kurz je [Bitstamp](#), ale lze použít i jiné směnné kurzy.



Změny směny nebo měny používané pro tyto převody lze provést prostřednictvím obrazovky „Předvolby“. Kliknutím na název burzy ji otevřete. Po výběru možností klikněte na tlačítko „Použít změny“.





## Zabalit

Pro většinu použití funguje MultiBit dobře jako zjednodušená, rychle se načítající bitcoinová penženka. Tato příručka obsahuje základní informace, které by měl znát každý uživatel: příjem finančních prostředků; zasílání finančních prostředků; obnova zálohy; a import papírové penženky. Import papírové penženky a operace zálohování/obnovy vyžadují více než začátečnické počítačové dovednosti, což poněkud omezuje použitelnost MultiBitu. Přesto zůstává MultiBit oblíbenou jednoduchou peněženkou, kterou je třeba zvážit.

## Ano, pošlete mi další užitečné věci o bitcoinech, jako je tento

Jméno

me@example.com

**PŘIDEJ SE TEĎ**

Žádné hry, žádný spam. Když se zaregistrujete, budu vás informovat 1-2 e-maily týdně. Z odběru se můžete kdykoli odhlásit.



© 2014-2018 Richard L. Apodaca