

Kapitola 7

Jak používat Bitcoin

7.0 Úvod

7.1 Jak získat nebo směnit bitcoin

7.1.1 P2P: Fyzicky

7.1.2 P2P: Online

7.1.3 Centralizované burzy/směnárný

7.2 Úvod do Bitcoinových peněženek

7.2.1 Vlastní vs. úschovné peněženky

7.2.2 Různé typy Bitcoinových peněženek

7.3.3 Otevřený vs. uzavřený zdrojový kód

Aktivita: Třídní hodnocení Bitcoinových peněženek

7.3 Nastavení mobilní Bitcoinové peněženky

Aktivita: Nastavení/obnovení Bitcoinové peněženky

7.4 Přijímání a odesílání transakcí

Aktivita: Bitcoinové transakce v praxi

7.5 Spoření v bitcoinu

7.6 DYOR - Důvěřuj, ale prověřuj

Jak používat Bitcoin

7.0 Úvod

Proč by měl někdo věřit penězům nerdů oproti penězům centrálních bank? Tito nerdi vám například vytvořili internet. Banky vám přinesly velkou ekonomickou krizi.

Andreas M. Antonopoulos

Nyní, když jsme lépe pochopili, co je Bitcoin a jaký je jeho účel, je čas naučit se ho používat prakticky. V této kapitole vás krok za krokem provedeme možnostmi, jak se k bitcoinu dostat, prozkoumáme různé typy dostupných peněženek, pomůžeme vám nastavit vlastní Bitcoinovou peněženku a dokonce si vyzkoušíme odeslání a monitorování bitcoinových transakcí v síti. Je čas přenést své znalosti do praxe!

7.1 Jak získat nebo směnit bitcoin

Existuje několik způsobů, jak přijít k bitcoinu, například:

- ✿ Vyměňte svou fiat měnu za bitcoin nebo naopak:
 - ✿ osobně (P2P)
 - ✿ online (na směnárnách, burzách)
- ✿ Nechat si za svou práci platit v bitcoinu a zároveň s ním platit za produkty a služby ostatním lidem. (více o tomto tématu v kapitole 8)
- ✿ Těžit bitcoiny (více o tomto tématu v kapitole 9).



Níže se budeme věnovat výměně fiat měn za bitcoin a naopak, a to jak prostřednictvím osobních transakcí s dalšími účastníky, nebo pomocí směnárny/burz, protože se stále jedná o nejrozšířenější způsob.

7.1.1 Peer-to-Peer: osobně

Provádění peer-to-peer (P2P) transakcí pro nákup a prodej bitcoinů zahrnuje přímou směnu vaší fiat měny (nebo jiného zboží či služby) za bitcoin s jinou osobou, čímž se eliminuje nutnost zapojení banky nebo jiné strany do této transakce.

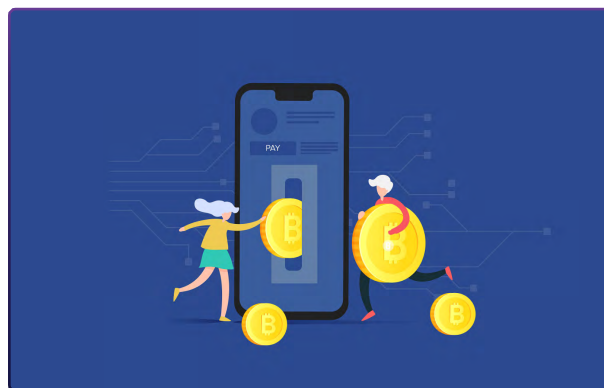
Obě strany si vzájemně určí směnnou částku a kurz. Kupující poskytne hotovost, prodávající převede bitcoiny a transakce je vypořádána. Ačkoli je jednodušší provádět P2P výměny fyzicky tak, že se s druhou osobou setkáte přímo v reálném světě, díky internetu tak můžete učinit také velice prakticky a to odkudkoli. Samozřejmě výměna bitcoinu za fiat měnu probíhá podobným postupem, akorát v opačném pořadí.



7.1.2 Peer-to-Peer: Online

Pokud využijete P2P platformy (webové stránky, aplikace), kde se v kyberprostoru setkávají kupující a prodávající bitcoinu, můžete nahradit fyzický (reálný) kontakt s druhou stranou a tato cesta tak může být pohodlnější.

Potom ale záleží na druhu platformy, kterou využíváte. Jedná-li se o směnu fiat měn za bitcoin, musíte nejdříve projít procesem zvaným KYC (doložit pas/občanku). Pokud směníte jinou kryptoměnu za bitcoin, najdete i platformy, kde doklady dávat nemusíte. Díky takovým platformám nemusíte nikomu svěřovat své informace, ale můžete zde najít protější stranu a obchodovat přímo s ní.



Na většině platform P2P musí uživatelé část prostředků uložit do úschovy, aby bylo zajištěno, že splní svou část dohody. Úschova znamená uložení peněz na bezpečném místě, které má platforma pod kontrolou, dokud obě strany nesplní, co slíbily. Je to jako důvěryhodný přítel, který drží vaše věci, dokud každý nedodrží své slovo.

7.1.3 Centralizované burzy/směnárnny

Používání centralizovaných burz je sice nejjednodušší způsob, ale také s sebou nese značné nevýhody. Centralizované burzy jsou společnosti, které umožňují klientům nakupovat a prodávat bitcoiny přímo jejich prostřednictvím. Toto pohodlí však přináší jistá rizika.



Centralizovaný

Centralizované burzy a jejich nevýhody

Je důležité si uvědomit, že při nákupu bitcoinu prostřednictvím centralizované burzy je často nutné poskytnout osobní údaje a ověřit vaši totožnost. Tím vzniká riziko krádeže identity a vaše osobní údaje jsou vystaveny potenciálním hrozbám. Centralizované burzy mají navíc vaše bitcoiny pod správou, což znamená, že nemáte své peníze pod kontrolou, dokud si je od nich nevyberete na svou peněženku.

K těmto obavám se přidává i fakt, že centralizované burzy mohou zpronevěřit finanční prostředky uživatelů nebo půjčit více bitcoinů, než mají v rezervách, a to do té doby, než se systém zhroutí. Ano, stejně jako banky! Ve světě Bitcoinu však neexistuje žádná centrální banka, která by podvodné banky zachraňovala tiskem dalších mincí, protože více bitcoinů vytisknout nelze!

Jak používat Bitcoin

7.2 Úvod do Bitcoinových peněženek

Na rozdíl od fyzických peněz se bitcoiny v bitcoinové peněženke ve skutečnosti nenacházejí. Žijí v distribuované účetní knize, kterou bitcoinová síť neustále ověřuje a zabezpečuje. Jak tedy můžete bitcoiny vlastnit?

Své bitcoiny vlastníte pouze tehdy, když vlastníte soukromé klíče, které vám umožňují podepisovat transakce a převádět vlastnictví bitcoinů od vás na někoho jiného.

S ohledem na to se podívejme na 2 pojmy, které popisujeme, když používáme termín **“peněženka”**:

- ✿ Soukromý klíč (což je něco jako heslo), ze kterého můžete generovat veřejné klíče (představte si jako e-mailové adresy, které můžete sdílet s ostatními a přijímat na ně bitcoin. Zároveň pomocí soukromého klíče můžete bitcoiny odesílat.
- ✿ Mobilní nebo počítačové rozhraní, z něhož můžete komunikovat s bitcoinovou sítí a načítat tak svůj zůstatek bitcoinů, odesílat a přijímat transakce a posílat je do sítě. Různé typy peněženek spolu s jejich výhodami a nevýhodami budou popsány v následující části.



7.2.1 Vlastní vs Úschovné peněženky

Než se pustíme do podrobností ohledně jednotlivých typů peněženek a jejich charakteristik, pojďme učinit důležité rozlišení mezi peněženkami pro vlastní úschovu a úschovnými peněženkami. Tato tabulka zahrnuje dva hlavní typy Bitcoinových peněženek, z originálu: self-custodial (vlastní) a custodial (úschovné). Budeme dále používat tyto anglické výrazy, a to kvůli nepřesnému překladu. Můžete zde vidět výhody a rizika používání jednotlivých typů peněženek a kdo má v jednotlivých případech bitcoiny pod kontrolou. Self-custodial znamená, že uživatel drží soukromé klíče, tudíž má své bitcoiny kompletně pod svou správou, zatímco u druhého typu drží jeho bitcoiny třetí strana.

Typ peněženky	Kdo má kontrolu nad mými bitcoiny?	Benefity	Rizika
Self-custodial peněženky	uživatel	Úplná kontrola nad finančními prostředky a transakcemi, žádný schvalovací proces nebo možnost zmrazení účtu. Žádná kontrola ze strany firem nebo vlády, ochrana proti libovolné konfiskaci, jako když máte peníze v peněženke nebo na bankovním účtu.	V případě ztráty privátních klíčů není možné obnovení prostředků, téměř žádná zákaznická podpora, zodpovědnost je zcela na straně uživatele.
Custodial peněženky	Třetí strana	Možné obnovení účtu v případě ztráty přístupu, lepší zákaznická podpora.	Peněžní prostředky jsou stále připojeny k internetu, a jsou tak náchylnější k hackerským útokům a prolomení bezpečnosti. Správci kontrolují účty a mohou je případně zmrazit.

V případě self - custody peněženek (nazývané také non - custodial) jsou privátní klíče pouze pod vaší správou a máte tak plnou kontrolu nad tím, co odesíláte a přijímáte. Na druhou stranu, v případě custodial peněženek, má klíč někdo jiný a může vaším jménem získat přístup k obsahu peněženky a spravovat jej.

- Self-custody je jako být sám sobě vlastní bankou. Transakce nepodléhají kontrole ani pravomoci žádné vlády nebo společnosti, ale také to znamená, že nesete plnou odpovědnost za zabezpečení svých bitcoinů.
- Self-custody zajišťuje, že třetí strany nemohou zabavit vaše bitcoiny bez vašeho souhlasu.
- Self-custody poskytuje klid na duši v době nejistoty, protože víte, že vaše bitcoiny jsou v bezpečí.

Je důležité zvolit správný typ peněženky pro potřeby každého jednotlivce. Někdy je pro lidi těžké rozlišit, zda si instalují self-custodial nebo custodial peněženku. Tato tabulka ukazuje rozdíly v postupu instalace.

Typ peněženky	Krok 1: Vyberte si peněženku	Krok 2: Nainstalujte peněženku	Krok 3: Vytvořte novou peněženku	Krok 4: Zapište si obnovovací frázi	Krok 5: Začněte peněženku používat
Self-custodial peněženky	Vyberte si poskytovatele Self-custodial peněženky	Postupujte podle pokynů poskytovatele peněženky	Vygenerujte si frázi pro obnovení a alespoň jeden soukromý klíč	Zapište a uschovejte si fráze pro obnovení na bezpečném místě	Začněte používat peněženku k přijímání a odesílání bitcoinu
Custodial peněženky	Vyberte si poskytovatele custodial peněženky	Postupujte podle pokynů poskytovatele peněženky	Vytvořte si účet u poskytovatele peněženky	Není možné (soukromé klíče má poskytovatel peněženky)	Začněte používat peněženku k přijímání a odesílání bitcoinu



**NEJSOU TO
VAŠE KLÍČE,
NEJSOU TO
VAŠE MINCE**

"Mezi držiteli bitcoinu je oblíbené rčení "Nejsou to vaše klíče, nejsou to vaše mince". Odkazuje na myšlenku, že pokud nemáte přímou kontrolu nad soukromými klíči spojenými s vaší bitcoinovou peněženkou, nejste skutečným vlastníkem mincí.

Kdokoli získá přístup k vašim soukromým klíčům, získá vlastnictví vašich bitcoinů. Proto je nesmírně důležité je chránit tím, že je budete držet mimo dosah zvědavých očí! Později v učebnici si ukážeme několik způsobů, jak toho můžeme docílit.

V následujícím textu budeme hovořit pouze o peněženkách, které si uživatel spravuje sám a kde má nad svými bitcoiny plnou kontrolu.

Nebojte se, pokud to bude příliš složité nebo nebudete všemu rozumět. Jedná se zkrátka o běh na dlouhou trať a více pochopíte, až začnete Bitcoin častěji používat!

Jak používat Bitcoin

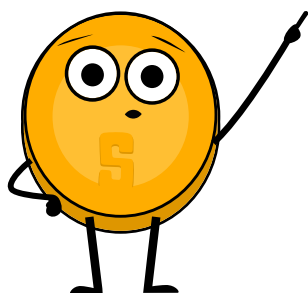
7.2.2 Různé typy Bitcoinových peněženek

V závislosti na tom, kde je váš soukromý klíč vytvořen a uložen, se pro popis peněženek běžně používají různé názvy. Pokud jsou klíče uloženy v chytrém telefonu, můžeme ji nazývat "mobilní peněženka". Pokud jsou bezpečně uloženy ve vyhrazeném zařízení, budeme ji nazývat "hardwarová peněženka". Pokud jsou klíče uloženy pouze na papíře, můžeme ji nazvat "papírová peněženka".

Zde je tabulka s různými názvy, které dáváme bitcoinovým peněženkám v závislosti na jejich struktuře:

Typ peněženky	Popis	Výhody	Nevýhody	Pro koho je určena
Online peněženka	Peněženka, do které se dostanete prostřednictvím webového prohlížeče.	Přístupná z jakéhokoli zařízení s připojením k internetu. Snadné použití.	Méně zabezpečená. Může být hacknuta nebo kompromitována.	Někdo, kdo potřebuje častěji přístup ke své peněžence a nemá mnoho finančních prostředků k uložení.
Mobilní peněženka	Peněženka nainstalovaná v mobilním zařízení.	Pohodlné. Lze k ní přistupovat odkudkoli.	Může dojít ke ztrátě prostředků, pokud je zařízení ztraceno, odcizeno nebo hacknuto.	Někdo, kdo potřebuje provádět transakce na cestách a nemá k dispozici mnoho finančních prostředků.
Peněženka na počítači	Peněženka nainstalovaná na stolním počítači.	Bezpečnější než online peněženky. Lze je používat offline.	Pokud je počítač infikován malwarem, může být peněženka hacknuta.	Někdo, kdo chce ukládat větší obnos peněz v bitcoinu a vyhovuje mu používání stolního počítače.
Hardwarová peněženka	Fyzické zařízení, které uchovává bitcoiny (soukromý klíč) offline.	Velmi bezpečné, pokud neexistuje digitální záznam privátních klíčů.	V případě ztráty nebo odcizení zařízení by mohlo dojít k tomu, že prostředky nebude možné získat zpět.	Někdo, kdo chce uložit větší množství finančních prostředků v bitcoinu a je ochoten zaplatit za vyšší bezpečnost hardwarové peněženky.
Papírová peněženka	Jde o fyzický záznam soukromých a veřejných klíčů Bitcoinové peněženky na papíru.	Bezpečné. Lze používat offline.	Prostředky mohou být nadobro ztraceny, pokud dojde ke ztrátě, odcizení nebo zničení fyzického záznamu.	Někdo, kdo chce uložit větší množství finančních prostředků v bitcoinu a je ochoten přijmout dodatečná opatření k zajištění jejich bezpečnosti.

Protože klíče lze přesouvat z jednoho zařízení na druhé, není „stav“ vaší peněženky Bitcoin definitivní. Pokud například vygeneruji klíče své bitcoinové peněženky na počítači a později je nahraji do svého telefonu, stane se pak z „počítačové peněženky“ identická „mobilní peněženka“.



Při úschově bitcoinu nejde jen o to, kdo nad ním má kontrolu - je třeba zvážit i mnoho dalších rizik. Proto je důležité najít takové řešení úschovy, které je zároveň bezpečné a pohodlné.

Při porovnání jednotlivých typů peněženek zjistíte, že neexistuje ideální peněženka, která by splňovala všechny potřeby.

Proto byste při výběru bitcoinové peněženky měli zvážit několik věcí:

- Zabezpečení:** Ujistěte se, že peněženka má zavedena silná bezpečnostní opatření, jako je dvoufaktorové ověřování a zásady bezpečného zadávání hesel.
- Ochrana soukromí:** Zvažte, zda peněženka umožňuje zůstat v anonymitě, nebo zda vyžaduje osobní údaje pro založení účtu.
- Jednoduché používání:** Vyberte si peněženku, která se snadno používá a ovládá, zejména pokud s Bitcoinem teprve začínáte.
- Kompatibilita:** Zkontrolujte, zda je peněženka kompatibilní s vaším zařízením a operačním systémem.
- Poplatky:** Porovnejte poplatky účtované různými peněženkami, abyste se ujistili, že dostáváte nejlepší nabídku.
- Pověst:** Prověřte si pověst peněženky a jejího týmu, abyste se ujistili, že je důvěryhodná.
- Kontrola:** Některé peněženky vám poskytují větší kontrolu nad vašimi soukromými klíči, což může být bezpečnostní výhoda.

Zvažte, zda chcete peněženku, která vám poskytne úplnou kontrolu, nebo peněženku, která je uživatelsky přívětivější, ale může mít menší rozsah kontroly.

7.2.3 Otevřený vs. uzavřený zdrojový kód

Dalším důležitým faktorem, který je třeba mít na paměti při výběru Bitcoinové peněženky, je vědět, zda je aplikace nebo software open-source, či nikoli.

Open-source kód (otevřený) je velmi důležitý, protože umožňuje komunitě přezkoumat kód a pokračovat ve vývoji projektu, pokud by na něm tým přestal pracovat.

Jak používat Bitcoin



Stejně jako je kód Bitcoinu zcela transparentní, aby si jej mohl každý prohlédnout, používat a upravovat, měl by být přístupný i kód peněženky, kterou používáte k ukládání svých bitcoinů.

Aktivita: Diskuse ve třídě a hodnocení Bitcoinových peněženek na bitcoin.org

Přejděte na následující webové stránky:

<https://bitcoin.org/en/choose-your-wallet> a využijte své nové znalosti o Bitcoinových peněženkách k výběru té nejlepší na základě kritérií, která jsme dnes probrali.

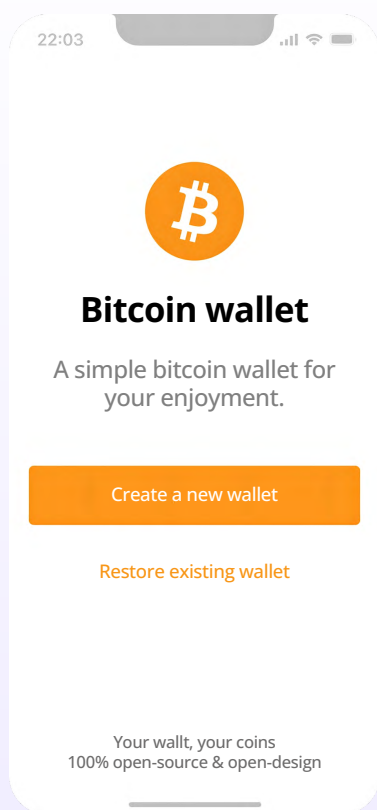


7.3 Nastavení mobilní Bitcoinové peněženky

Nyní, když už lépe rozumíme Bitcoinovým peněženkám a rozdílům mezi nimi, podíváme se, jak jednu z nich používat v praxi. Pro tento příklad vytvoříme mobilní peněženku přímo v našem chytrém telefonu.

Aktivita: nastavení/obnovení Bitcoinové peněženky

Pokud někteří studenti nemají telefon, spojí se s ostatními. Pro tuto aktivitu existují dvě možnosti:



Your Seed Phrase

Your Seed Phrase is used to generate and recover your account.

- | | | |
|-------------|-----------|-----------|
| 1. issue | 2. flame | 3. sample |
| 4. lyrics | 5. find | 6. vault |
| 7. announce | 8. banner | 9. cute |
| 10. damage | 11. civil | 12. goat |

Please save these 12 words on a piece of paper. The order is important. This seed will allow you to recover your account.

Třídní úloha: První možnost - Stáhněte si novou peněženku.

Jak vytvořit a používat Bitcoinovou peněženku:

- 1 Vyhledejte aplikaci v obchodě App Store (iOS) nebo Google Play (Android).
- 2 Otevřete aplikaci a opište si na papír 12- nebo 24slovnou frázi pro obnovení (někdy nazývanou jako seed). **Nezapomeňte si ji uschovat na bezpečném místě!** Tato fráze pro obnovení vám v případě potřeby umožní obnovit plný přístup k vašim finančním prostředkům.

Nezapomeňte, že pokud tuto řadu slov ztratíte nebo zapomenete, nebudete mít v případě ztráty přístup ke svým bitcoinům.

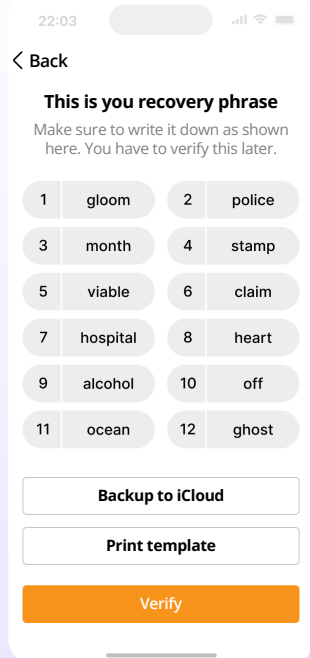
- 3 Poté musíte potvrdit, že jste skutečně uložili svou frázi pro obnovení neboli seed frázi. K tomu musíte ve stejném pořadí této fráze slova zadat (záleží ale na typu peněženky).
- 4 Jako dodatečné bezpečnostní opatření umožňují některé peněženky zvolit si bezpečné heslo. Váš soukromý klíč a první bitcoinovou adresu pro vás peněženka vytvoří automaticky.

Představte si svou veřejnou adresu jako e-mailovou adresu – tu můžete sdílet s ostatními, aby vám mohli poslat bitcoin, nebo v případě e-mailové adresy, e-mail.

Svou soukromou adresu si představte jako heslo k vašemu e-mailu. Nechcete ji s nikým sdílet, protože byste mu tím umožnili přístup k vašemu e-mailu.

- 5 Pro příjem bitcoinů použijte svou adresu "přijmout". Vygenerujte fakturu a nyní můžete bitcoin přijmout. Učitel vám malou část bitcoinu na zkoušku pošle.

Jak používat Bitcoin



Třídí úloha: Druhá možnost - Obnovení peněženky (hra na rychlost).

Učitel vytvoří novou bitcoinovou peněženku a pošle na ni pár satoshi pro každého studenta.

Každému studentovi dejte list s obnovovací frází pro získání přístupu do peněženky.

Provázejte studenty krok za krokem:

- 1 Při prvním spuštění peněženky se zobrazí několik způsobů vytvoření peněženky, klepněte na „**Importovat existující peněženku**“. Zobrazí se úvodní obrazovka, klepněte na „**Obnovit pomocí fráze pro obnovení**“.
- 2 Zadejte postupně 12/18/24 slov fráze pro obnovení ve správném pořadí.
- 3 Po dokončení stiskněte tlačítko „**Obnovit**“.
- 4 Po úspěšném provedení obnovení se zobrazí "Import úspěšný".
- 5 Vyberte dané množství satů na jinou peněženku. Ne na všechny ale vyjde, takže rychle!

7.4 Přijímání a odesílání transakcí

Bitcoinové transakce jsou převodem vlastnictví stávajících bitcoinů na nového vlastníka. Namísto převodu skutečných mincí však všechny uzly v síti aktualizují svou místní kopii veřejné účetní knihy tak, aby odrážela změnu vlastnictví.

Při odesílání Bitcoinové transakce odesílatel podepíše zprávu, kterou může podepsat pouze svým soukromým klíčem, čímž signalizuje síti, že se vlastnictví bitcoinu mění na adresu příjemce.

Bitcoin bude nyní vázán na adresu, ze které může odesílat pouze nový vlastník, čímž získá vlastnictví bitcoinu.

Účetní kniha

Majitel účtu	Hodnota
Sam	2,5
Adam	3,0
Michal	6,0
Jan	1,5
Robert	2,0
Ivana	1,75
Daniel	5,25

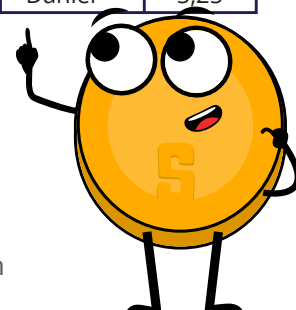
Požadavek na bitcoinovou transakci
Jan odesílá 0,50 BTC na adresu Ivany
Jan ▶ Ivana 0,5 BTC

Účetní kniha

Majitel účtu	Hodnota
Sam	2,5
Adam	3,0
Michal	6,0
Jan	1,0
Robert	2,0
Ivana	2,25
Daniel	5,25

Nové bitcoinové transakce jsou zadávány z peněženek po celém světě, ale neexistuje žádný ústřední zpracovatel plateb. Místo toho těžaři po celém světě soutěží o zápis transakcí do účetní knihy.

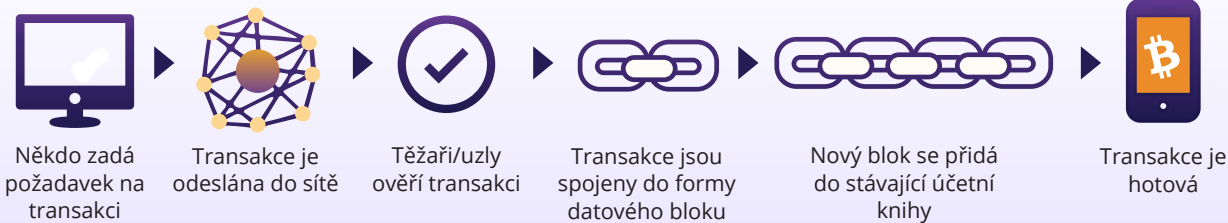
Řekněme, že Jan dluží Ivaně 0,5 BTC a je připraven ji peníze vrátit. Oba mají digitální peněženky.



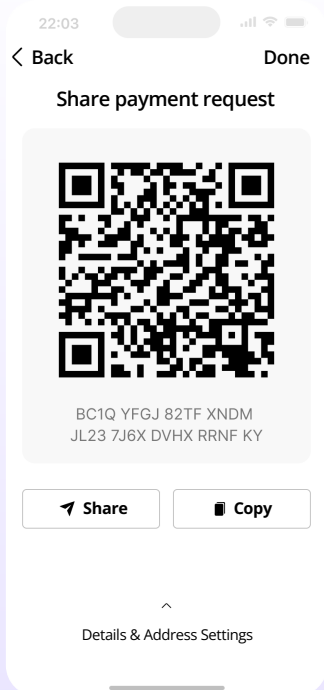
- 1 Iva se s Honzou podělí o svou veřejnou adresu.
- 2 Honza pomocí svého softwaru v peněženke vytvoří transakci, která obsahuje Ivaninu adresu, částku, která má být převedena (0,5 BTC), a poplatek pro těžaře.
- 3 Po podepsání je transakce odeslána do sítě, kde je ověřována uzly. Uzly zkontrolují validitu transakce a ujistí se, že Jan má dostatek prostředků. Pokud je nemá, transakci okamžitě odmítnou.
- 4 Jakmile je transakce ověřena, těžaři ji přidají do účetní knihy (blockchainu) a finanční prostředky jsou převedeny na adresu Ivany.
- 5 Ivana pak může použít svůj soukromý klíč aby získala přístup k převedeným prostředkům ve své peněženke.

Je důležité si uvědomit, že jakmile je transakce dokončena, nelze ji vzít zpět.

Jak funguje Bitcoinová transakce



Přijímání Bitcoinových transakcí:



Chcete-li přijímat bitcoiny, musíte odesílateli poskytnout adresu své bitcoinové peněženky. Jedná se o jedinečný řetězec písmen a čísel, který představuje vaši peněženku a slouží k její identifikaci v Bitcoinové síti. Adresu své peněženky najdete tak, že se přihlásíte do své bitcoinové peněženky a vyhledáte možnost "Přijmout" nebo "Vložit" bitcoiny.

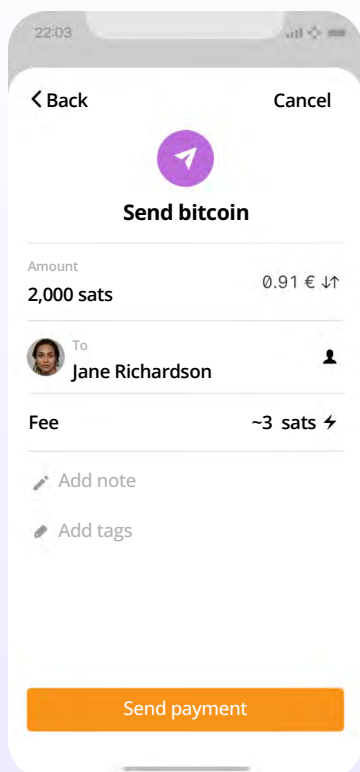
Svou bitcoinovou adresu pak můžete s odesílatelem sdílet několika způsoby:

- 1 Zkopírujte a vložte adresu: Adresu můžete zkopírovat tak, že ji zvýrazníte a na klávesnici stisknete tlačítko "Kopírovat" a poté ji vložíte do e-mailu nebo zprávy odesílateli.
- 2 Sdílejte odkaz na svou peněženku: Některé bitcoinové peněženky umožňují vytvořit odkaz na vaši peněženku, který můžete sdílet s odesílatelem. Ten pak může kliknutím na odkaz získat přístup k vaší peněženke a odeslat bitcoiny.
- 3 Sdílejte QR kód (jednorázový nebo trvalý): Pokud má odesílatel chytrý telefon s aplikací bitcoinové peněženky, může naskenovat QR kód a získat vaši bitcoinovou adresu.

Jak používat Bitcoin

Jakmile má odesílatel vaši bitcoinovou adresu, může vám poslat bitcoin zadáním vaší adresy a částky, kterou vám chce poslat. Bitcoinů pak budou odeslány do vaší peněženky a budou viditelné, jakmile bude transakce potvrzena v Bitcoinové síti. To obvykle trvá několik minut (v případě on-chain).

Dále se podíváme na odesílání bitcoinových transakcí.



Odesílání bitcoinových transakcí:

K odeslání bitcoinu potřebujete několik věcí: bitcoinovou peněženku, bitcoinovou adresu příjemce a částku, kterou chcete odeslat.

- 1 Otevřete si Bitcoinovou peněženku. Na vaše telefonní číslo bude zaslán SMS kód, který musíte zadat do příslušného okýnka. Pokud máte aktivovanou funkci Google 2FA, budete muset zadat šestimístný kód z aplikace Google Authenticator.
- 2 Přejděte na funkci "Odeslat" nebo "Vybrat" a zkopírujte adresu příjemce.
- 3 Zadejte bitcoinovou adresu příjemce vložení do volné kolonky.
- 4 Do pole "Částka" zadejte množství bitcoinu nebo hodnotu ve fiat měnách, kterou chcete odeslat.
- 5 Dvakrát zkontrolujte adresu příjemce a částku, která má být zaslána.
- 6 Před kliknutím na tlačítko Potvrdit a odeslat doporučujeme ještě jednou přezkontrolovat údaje o transakci, abyste se ujistili, že odesíláte příslušnou částku bitcoinů na správnou adresu peněženky.
- 7 Potvrďte transakci a počkejte, až síť transakci potvrdí.

Nyní víte, jak vyhodnotit, vybrat a nastavit si vlastní Bitcoinovou peněženku. Posílání bitcoinů z jedné peněženky do druhé v síti se nazývá posílání transakcí "on-chain". Je to proto, že transakce probíhá v hlavním blockchainu síť. Transakce "on-chain" jsou nejbezpečnějším způsobem, jak provádět transakce s bitcoinem; transakce jsou však dražší a pomalejší než jiné možnosti, které probereme v kapitole 8.





Aktivita: Bitcoinové transakce v praxi

Cíl: Pochopit základní koncepty a mechanismy peer-to-peer transakcí v Bitcoinové síti.

Než začneme, připomeneme si klíčové hráče při bitcoinových transakcích:

- Odesílatelé a příjemci jsou strany, které si vzájemně směřují bitcoiny.
- Uzly ověřují transakce a ukládají kompletní kopie blockchainu.
- Těžaři jsou zodpovědní za zabezpečení sítě a přidávání nových transakcí do blockchainu.

Nejdříve pochopte svou roli. Byla vám přidělena jedna z následujících rolí: odesílatel, příjemce, uzel nebo těžař.




-  Odesílatelé budou zodpovědní za vytváření a odesílání transakcí.
-  Příjemci budou zodpovědní za příjem a ověřování transakcí.
-  Uzly budou zodpovědné za ověřování transakcí tím, že budou kontrolovat, zda je transakce platná.
-  Těžaři budou zodpovědní za přidávání transakcí do blockchainu.

Uzly i příjemce musí transakci ověřit

1 Jako odesílatel: Vytvořte transakci.



Chcete-li vytvořit transakci, postupujte podle následujících kroků: Vezměte si potvrzení o transakci (kus papíru) a napište počet mincí, které chcete poslat, a jméno nebo iniciály příjemce. Podepište poznámku svým jménem nebo iniciálami čímž simulujete soukromý klíč. Předejte příjemci poznámku o transakci a příslušný počet mincí.

2 Jako příjemce: Jste zodpovědní za ověření transakcí. Postupujte podle následujících kroků:

-  Zkontrolujte, zda je v poznámce k transakci uveden správný počet mincí a jméno nebo iniciály příjemce.
-  Spočítejte přijaté mince a porovnejte je s počtem mincí zapsaným na poznámce.
-  Pokud se mince shodují, zaškrtněte políčko schválení. Pokud mince nesouhlasí nebo máte pochybnosti, transakci zamítněte.

Posláno mincí	Odesílatel	Podpis odesílatele	Příjemce	Datum a čas	Potvrzení příjemce

3 Jako uzel: Zkontrolujte a ověřte transakci. Jste zodpovědní za kontrolu platnosti transakce.

-  Ověřte, že adresa odesílatele je platná a že adresa příjemce je platná.
-  Zkontrolujte, zda má odesílatel dostatek prostředků k dokončení transakce a zda transakce nevede k dvojité útratě stejných mincí.

Posláno mincí	Odesílatel	Podpis odesílatele	Příjemce	Datum a čas	Schválení uzlu

Jak používat Bitcoin

4 Jako těžař: přidávejte transakce do blockchainu. Jste zodpovědní za přidávání transakcí do blockchainu. Postupujte podle následujících kroků:

- ✿ Zkontrolujte transakce, které byly schváleny příjemci a potvrzeny uzly.
- ✿ Hodte kostkou a porovnejte čísla s ostatními těžaři. Těžař s menším číslem přidá transakci do blockchainu.
- ✿ Za svůj čas, energii a úsilí získáte bod. Na konci aktivity vyhrává těžař s největším počtem bodů.

**Jakmile je transakce přidána do blockchainu, nelze ji změnit ani zvrátit.

5 Sledujte svůj zůstatek mincí: V průběhu aktivity sledujte zůstatek svých mincí počítáním ve své digitální peněženke.

Posláno mincí	Odesílatel	Podpis odesílatele	Příjemce	Datum a čas	Schválení

6 Proberte ve třídě získané poznatky.

7.5 Spoření v bitcoinu

Bitcoin je způsob, jak ochránit své peníze před inflací a před tím, aby je ovládal někdo jiný. Pokud to tedy děláte správně. Spoření v Bitcoinu představuje prostředek k ukládání, akumulaci a budování bohatství v průběhu času. Jak jste již pochopili, typ peněz, které si vyberete ke spoření, je jedním z nejdůležitějších rozhodnutí, které můžete učinit. Moudrá volba vám umožní vybudovat lepší budoucnost pro sebe a svou rodinu.



Klid na duši: Při správném uchování je Bitcoin jedinou formou majetku, který vám nikdo nemůže vzít.



7.6 Důvěřuj, ale prověřuj

Ať už s Bitcoinem děláte cokoli, pamatujte si toto: „Důvěřuj, ale prověřuj“. V Bitcoinu neexistují žádní představitelé. Nikdy byste neměli slepě následovat něčí tvrzení. Spíše byste měli vždy zpochybňovat to, co vám někdo říká, a sami si to ověřit. Dodržováním této mantry se ochráníte před ztrátou svých bitcoinů. To platí pokud vám někdo tvrdí věci jako „příští Bitcoin“, stejně jako když jde o „jedinečnou investiční příležitost“ nebo sliby „rychlého a snadného zisku“.

V kapitole 7 jste se dozvěděli, jak používat Bitcoin v každodenním životě. Dozvěděli jste se, jak bitcoiny různými způsoby získávat a směňovat a jak je udržovat v bezpečí pomocí různých peněženek.

Díky nastavení mobilní peněženky a provádění transakcí s ostatními máte nyní praktické zkušenosti, abyste mohli Bitcoin s jistotou používat každý den. Pochopením Bitcoinu jako způsobu ukládání peněz a dodržováním myšlenky „DYOR (Do your own research) - Důvěřuj, ale prověřuj“ nyní máte své peníze pod kontrolou.

V nadcházející kapitole se budeme zabývat sítí Lightning network. Podíváme se, jak tato inovativní technologie mění způsob, jakým lidé na celém světě mají přístup k penězům a jak je používají. Dozvíte se, jak Lightning Network poskytuje jednotlivcům, komunitám a podnikům přístup k finančním službám - od každodenních transakcí až po pokročilejší aplikace.