

AKTUALIZOVÁNO

JAK NA BITCOIN

KROK ZA KROKEM



KAREL FILLNER

JAK NA BITCOIN

KROK ZA KROKEM

Ověřené postupy, tipy a triky jak ihned získat
a používat vaše nové digitální peníze - bitcoiny

KAREL FILLNER

Aktualizováno 2. 10. 2017
Vydáno 6. 4. 2014

1. A proč vlastně?.....	6
2. Co je to bitcoin a kryptoměna.....	8
Jak bitcoin vzniká	10
Jak funguje bitcoin - přenos.....	12
Konkrétní příklad transakce	14
3. Jak začít	16
Nainstalujte peněženku	16
Vytvořte bitcoinovou adresu	19
Zálohujte, heslujte, zálohujte	21
4. Jak získat bitcoiny	27
Burzy, směnárny	27
Localbitcoins - přímý nákup	32
Bankomat	33
Vlastní zboží, služby	34
Těžba, podíl na těžení.....	36
Bitcoiny zdarma	36
QR kód a weby, blogy	37
5. Užitečné odkazy	38
Pár slov na konec	39

To, že čtete tento e-book znamená, že jste už někde slyšeli o bitcoinu, virtuálních penězích, nebo kryptoměně a zajímají vás informace spojené s tímto fenoménem.

A to je skvělé! Bitcoin a technologie kryptoměn je revoluční myšlenka, která je – ne náhodou – přirovnávána k počátkům internetu v r. 1992. Před 25 lety existovalo pouhých 130 webových stránek a málokdo by si dokázal představit, jakým způsobem nám všem zasáhne internet do života. Kolik s sebou přinese možností, pokud jde o přenos informací, rychlost komunikace, sdílení zábavy a všechny další změny, které nám už dnes připadají jako samozřejmost.

Internet od základů změnil také svět byznysu a víc než kde jinde zde platilo a platí, že kdo má informace a umí s nimi pracovat, stojí nakonec na stupních vítězů. Nejde jen o úspěch Googlu, Facebooku, YouTube a dalších gigantů. Příležitost má prakticky každý.

Myslím si, že stejný vývoj může čekat i bitcoin a digitální „peníze“ – kryptoměnu. Již dnes se mu říká Internet 2.0, případně také digitální zlato – podle dosavadního vývoje, kterým si za pouhých 8 let existence prošel. Začínal na nule. Dnes má cenu několik tisíc dolarů, více než 120.000 míst na světě, kde si za něj můžete nakoupit zboží a služby a je stále více využíván pro rychlé, levné, částečně anonymní a přitom bezpečné platby po celém světě.

Bitcoin není jen platební prostředek. Přináší také nové příležitosti, ve světě i u nás vznikají start-up firmy, které vymýšlejí nové technologie a služby spojené s jedním z nejrychleji se rozvíjejících světových byznysů. A může to být i skvělá investice...

Budu rád, když vám tento e-book pomůže ve vašich začátcích s bitcoinem a získáte tak informace a zkušenosti, které vám přinesou užitek. Sledujte blog o bitcoinu a kryptoměnách – www.btctip.cz a budete tak vždy o krok napřed před ostatními.

Karel Fillner



Tato příručka slouží pro informační účely a jako informační produkt nezaručuje konkrétní výsledky. Zkušenosti, které jsem získal z praxe, fungují a ukazují konkrétní, vyzkoušené postupy. Negarantuji ale stejné výsledky všem a v různém prostředí mohou být odlišné. Každý je zodpovědný za své výsledky, které budou odpovídat jeho schopnostem a využití vlastních informačních zdrojů.

Stažením této příručky souhlasíte s tím, že informace v ní obsažené jsou pouze doporučením a vyjádřením mého názoru k problematice, kterou popisují. Jakékoliv šíření, nebo poskytování tohoto informačního materiálu třetím osobám bez souhlasu autora není dovoleno. Děkuji za pochopení a respektování tohoto sdělení.

1. A PROČ VLASTNĚ?

Můj příběh

O bitcoinu jsem poprvé slyšel někdy na sklonku r. 2012. V té době se rozhodně nedalo říct, že by kryptoměny byly v popředí zájmu médií a jeho uživatelé byli spíše „geekové“, tedy IT nadšenci, navíc s velkým zájmem o kryptografii. Mezi takové jsem se nikdy nepočítal a vlastně ani dnes moje znalosti nepřekračují úroveň průměrně poučeného uživatele počítačových technologií.

Cena bitcoinu se pohybovala kolem 15 USD/1BTC a mě zaujalo, že něco tak virtuálního má vůbec nějakou hodnotu a dokonce existují burzy, které s kryptoměnou obchodují. Zajímal jsem se o forexové trhy, obchodování s měnovými páry a kamarád, který na tom byl podobně, mě upozornil na poměrně velkou volatilitu bitcoinového trhu. To mě pochopitelně zajímalo, nicméně, potřeboval jsem si doplnit informace a znalosti o tom, co to vlastně kryptoměny jsou.

POPRAVDĚ, MYSLEL JSEM SI, ŽE BITCOIN JE NĚCO JAKO PLATIDLO V POČÍTAČOVÝCH HRÁCH, KDE SI MŮŽETE KOUPIT ZA VIRTUÁLNÍ PENÍZE NAPŘ. LEPŠÍ MEČ, NEBO BRNĚNÍ A ÚSPĚŠNĚ TAK POSTUPOVAT DO DALŠÍCH BOJOVÝCH LEVELŮ :-)

Nejvíce informací poskytovala [Wikipedie](#). Také většina webů, které se kryptoměny zabývaly, na tento zdroj odkazovala a i dnes zde najdete ucelený technický popis fungování bitcoinové sítě, vlastnosti bitcoinu a odkazy na další zdroje.

Není ale úplně jednoduché napoprvé pochopit všechny technické pojmy, se kterými se zde setkáte a je proto jen dobře, že v poslední době vzniká hodně webů, které se snaží o další osvětu a rozšíření bitcoinu mezi běžnou populaci.

Jedním z nich je i btctip.cz , na kterém najdete nejen obecné informace a návody, ale také blog s články a zajímavostmi ze světa virtuálních měn.

Jsem přesvědčený o tom, že bitcoin a další kryptoměny – altcoiny (alternativní coins) mají před sebou velkou budoucnost. O jeho výhodách a možnostech využití se dočtete dále. A pokud máte zájem dozvědět se vše, co budete potřebovat, abyste byli o krok napřed před ostatními, je tu pro vás tento e-book zdarma. Najdete v něm praktické postupy a návody – **vše na jednom místě, krok za krokem.**

2. CO JE TO BITCOIN A KRYPTOMĚNA

Jednotka	Číselný zápis	Poznámka
1 bitcoin	1 BTC	
1 cBTC	0.01 BTC	centi-bitcoin (BitCent)
1 mBTC	0.001 BTC	milibitcoin
1 μ BTC	0.000001 BTC	mikro-bitcoin
1 Satoshi	0.00000001 BTC	nejmenší možná jednotka pojmenovaná po svém zakladateli

Bitcoin vymyslel geniální programátor a kryptograf Satoshi Nakamoto. Není to jeho pravé jméno, jen pseudonym a není vlastně ani úplně jisté, jestli to byl jeden člověk, nebo více lidí... Princip digitální měny byl publikován již v r. 2008, poprvé však byla bitcoinová síť uvedena do ostrého provozu v lednu 2009, kdy také proběhla první bitcoinová transakce.

Satoshi Nakamoto dal dohromady první skupiny nadšenců, kteří postupně síť rozvíjeli, podíleli se na vylepšení platformy a také si mezi sebou bitcoiny platili. Komunikaci s ostatními však postupně omezoval a cca po dvou letech se odmlčel úplně. Před pár lety sice došlo k jeho „senzačnímu objevení“ reportéry Newsweeku, vše se ale ukázalo jako blamáž a dotyčný pán stejného jména potvrdil, že s bitcoiny nemá nic společného a vše je jen shoda jmen. Poprask to byl ale veliký. Není divu, pravý Satoshi by byl dnes celebritou No.1.

V BITCOINOVÉ SÍTI HRAJE ROLI TAKÉ ŠIFROVÁNÍ – KRYPTOGRAFIE, ODTUD TAKÉ NÁZEV KRYPTOMĚNA

Bitcoin je nejčastěji zmiňován jako digitální (virtuální) měna. Přesnější by však bylo spíše označení bitcoinová síť, případně protokol, kde rozlišujeme Bitcoin jako síť a bitcoin jako měnovou jednotku. Jedná se o síť počítačů, které navzájem komunikují

v režimu peer-to-peer (P2P) – tedy tzv. rovný s rovným. Je to pravý opak toho, kdy se počítač připojuje k nějakému centrálnímu zdroji (serveru). Právě tato decentralizace je jednou z hlavních výhod bitcoinu. Bitcoin vznikají miningem - těžením – vysvětlím samostatně.

Bitcoin není nic hmotného – je to jen digitální otisk informace o vlastnictví, spojený s konkrétní bitcoinovou adresou. Pokud tedy „vlastníte“ nějaké mince, jde v tomto případě o všemi sdílenou informaci, že jste nějaký počet BTC vytěžili, koupili, nebo vám je někdo poslal a nyní se nachází na bitcoinové adrese, ke které vlastníte tzv. privátní klíč (digitální podpis nutný k „utracení“ bitcoinu. Není to tedy ani soubor, který byste měli uložený v paměti počítače.

Systém je navržen tak, že do r. 2140 v síti vznikne cca 21 milionů BTC, 99% všech bitcoinů však bude vytěženo kolem r. 2033. V současné době je vytěženo více než 16.500.000 BTC

Toto množství je předem dané, konečné a navržený systém tím zaručuje, že nikdo nemůže vytvořit další peníze a devalvovat měnu, jako se to děje např. tisknutím peněz centrálními bankami. Potvrzování transakcí a zapsání v tzv. blockchainu také zaručuje, že můžete utratit jen ty bitcoiny, které skutečně vlastníte. Nemůže tak dojít ke znehodnocení vypouštěním „falešných“ mincí.

JAK BITCOIN VZNIKÁ

Klasické peníze, které označujeme také jako fiat měnu (zákonnou, nařízenou) tisknou centrální (národní) banky. Každou emisí nových peněz dochází k poklesu hodnoty peněz – inflaci. Jde o proces, který je založený na dluhu, vše mají v moci jednotlivé vlády a jejich banky. Hovoříme tedy o centralizovaném systému, kdy poměrně úzká část lidí svým vlivem a politikou ovlivňuje životy většiny těch ostatních, kteří mají jen velmi malou šanci na účinnou obranu proti tomu, co je tímto systémem vynuceno.

BITCOINY VŠAK NIKDO „NETISKNE“. VZNIKAJÍ TĚŽENÍM, ODTUD POJEM BITCOIN MINING

Pro fungování bitcoinové sítě je nezbytné, aby ji někdo udržoval v chodu a především potvrzoval transakce, které v ní probíhají. Této činnosti se věnují mineři – těžaři, kteří si za tím účelem pořizují specializovaný hardware.

Nechci zabíhat do úplných technických detailů. Dobrý popis fungování sítě najdete např. na [wikipedii – bitcoin](#).

Podstatné je, že těžaři poskytují špičkový počítačový výkon k vyřešení náročných výpočetních operací. Snaží se najít řešení matematického problému dříve než ostatní mineři a pokud se jim to podaří, získají právo k potvrzení všech transakcí, které jsou zahrnuty do tzv. bloku.

Nechci zabíhat do úplných technických detailů. Dobrý popis fungování sítě najdete např. na [wikipedii – bitcoin](#)

Podstatné je, že těžaři poskytují špičkový počítačový výkon k vyřešení náročných výpočetních operací. Snaží se najít řešení matematického problému dříve než ostatní mineři a pokud se jim to podaří, získají právo k potvrzení všech transakcí, které jsou zahrnuty do tzv. bloku.

Za to získají jednak předem nastavenou odměnu – v současnosti je to 12,5 BTC a také všechny poplatky z transakcí, které se v bloku nacházejí.

K NALEZENÍ BLOKU DOCHÁZÍ PRŮMĚRNĚ JEDNOU ZA 10 MINUT – DENNĚ TAK VZNIKÁ 1800 NOVÝCH BITCOINŮ

Jednotlivé bloky se následně zařazují do BLOCKCHAINU – sdíleného a veřejného registru, kde má každý možnost vidět všechny transakce – svoje i všech ostatních. A to jak probíhající, tak i všechny ostatní, zapsané od vzniku bitcoinové sítě.

Blockchain je také často označován za „účetní knihu“, do které má kdokoliv přístup a pro všechny se zde nacházejí ve stejném okamžiku stejné informace.

Nalezení kryptografické „nonce“ je výpočetně tak složité, že na něj dnes rozhodně nestačí běžné počítače. Dříve se používaly běžné procesory a grafické karty. V současnosti většina výpočtů probíhá na tzv. ASIC čipech a těžení představuje velké náklady jak na pořízení hardwaru, tak spotřebuje také obrovské množství elektrické energie.

Samostatné těžení je dnes spíše výjimkou. Těžaři se sdružují do „poolů“, kde se výkon jejich strojů sčítá a je daleko větší šance na vytvoření nového bloku. Odměna je pak rozdělována podle toho, jakým výkonem kdo přispěl...

Na rozdíl od samotného výpočtu matematického úkolu je pak jeho ověření zbytkem sítě otázkou několika desítek sekund. A právě toto ověření je nezbytné k tomu, aby nikdo nemohl jen tak „vypustit do světa“ nové bitcoiny – zaručuje tak jejich nefalšovatelnost.

JAK FUNGUJE BITCOIN – PŘENOS

Jednou ze základních vlastností bitcoinu je, že můžete **utratit jen ty peníze, které vlastníte**. Dá se to přirovnat ke standardní měně?

České koruny tiskne Česká národní banka (ve Státní tiskárně cenin). Ta garantuje, že si za své peníze budete moct koupit cokoliv v jejich nominální hodnotě. Zajišťuje, aby měly dostatek ochranných prvků a nešly snadno zfalšovat. Koruny jsou tedy obecně přijímaným platidlem a banka, nebo obchodník nezkoumá, kdo je přinesl. Jsou dostatečnou zárukou k tomu, aby byly přijaty.

Platíte-li něco bezhotovostně, banka vám peníze odečte z vašeho účtu a připíše na účet, který je uveden v platebním příkazu. Jinými slovy, není-li suma peněz odepsána z jednoho účtu, nemůže být na jiný ani připsána. Vše kontroluje a řídí centrální autorita.

Vše funguje na principu důvěry. Musíte věřit tomu, že ČNB má a používá nástroje, které korunu úplně neznehodnotí. Věříte bance, že jsou peníze dostatečně ochráněny proti zfalšování. Obchodník musí mít jistotu, že se stejná koruna nemůže ocitnout na dvou místech najednou.

A TADY SE DOSTÁVÁME K TOMU, PROČ DOSUD VŠECHNY POKUSY O VYTVOŘENÍ VIRTUÁLNÍ/ DIGITÁLNÍ MĚNY NEMĚLY ÚSPĚCH – AŽ DO PŘÍCHODU BITCOINU

Základním problémem je totiž vymyslet, jak to zařídit, **aby nikdo nemohl udělat kopii digitálních peněz**. Máte-li v počítači soubor s fotografií, můžete ho poslat komu chcete – a třeba stokrát. Stejně tak jakýkoliv jiný soubor – text, video, prezentaci...

Proč byste to tedy nemohli udělat i s digitálními penězi? Věřil by jim potom někdo? Určitě ne, takové peníze by neměly žádnou hodnotu. Každý by si jich mohl natisknout - nakopírovat, kolik se mu zachce.

JAK JE TEDY MOŽNÉ, ŽE JE BITCOIN NEZFALŠOVATELNÝ A NELZE JEDNY A TY SAMÉ PENÍZE UTRATIT DVAKRÁT?

Je to právě kvůli decentralizaci. Všechny transakce a jejich potvrzení jsou ověřeny celou sítí navzájem propojených počítačů. Pošlete-li někomu bitcoiny, nejdříve musí tuto transakci ověřit decentralizovaná síť tzv. nodů (uzlů), které díky sdíleným informacím v blockchainu zjistí, jestli je transakce tzv. validní. Tj., jestli se na adrese, ze které odesíláte např. 1 BTC, tento bitcoin skutečně nachází a vy ho tak můžete utratit. Následně tuto transakci spolu s ostatními zpracovávají těžaři – snaží se z nich vytvořit blok, který splňuje určitá kritéria, založená na řešení matematické úlohy (viz výše) – ten nejúspěšnější těžař sestaví blok, ve kterém jsou všechny transakce platné a ověřené.

A tento blok je přidán k celému řetězci všech ostatních bloků – tedy blockchainu.

ZKUSTE SI TEĎ PŘEDSTAVIT BLOCKCHAIN JAKO OBROVSKOU, VEŘEJNOU ÚČETNÍ KNIHU A BLOK JAKO STRÁNKU V TÉTO KNIZE

- Každý blok musí být ověřen a „schválen“ celou sítí, aby se mohl stát součástí blockchainu
- Transakce se stává trvalou součástí - zápisem do účetní knihy
- Do blockchainu může vidět každý - účetní kniha je veřejná
- Každý počítač, který je součástí bitcoinové sítě, má od této účetní knihy neustále aktualizovanou kopii

KONKRÉTNÍ PŘÍKLAD TRANSAKCE

Karel má 2 bitcoiny. Koupil si je např. v bitcoinovém bankomatu. Pepa má kameru, kterou si cení na 1 bitcoin a dohodl se s Karlem, že mu ji prodá.

JAK TO PROBÍHÁ?

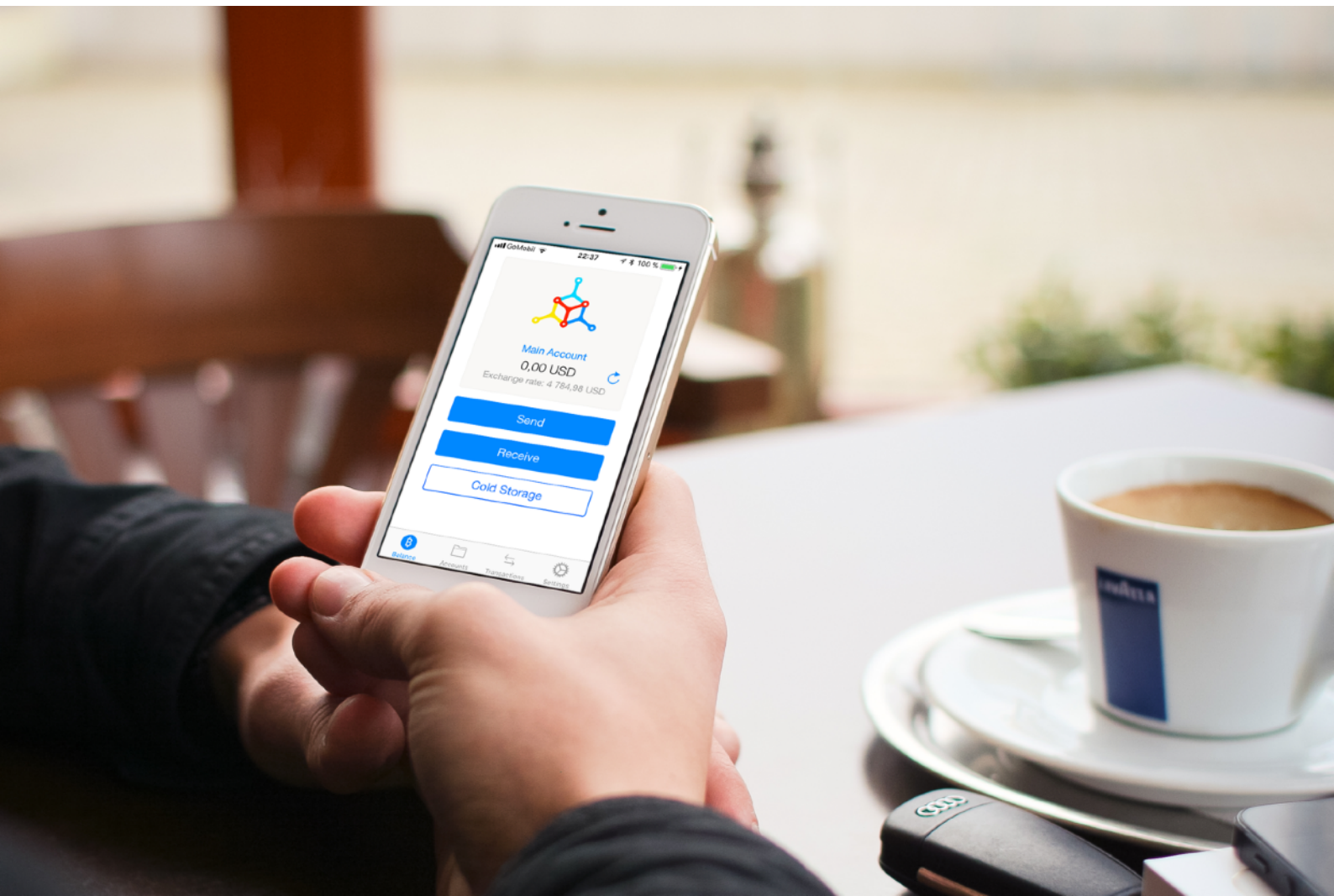
- Pepa sdělí Karlovi (mailem, SMS, ústně atd.) svoji BTC adresu. Např. [15au98CMDWzWqpKfm8iCfGsy7Kby1u6dG7](#)
- Karel ve své BTC peněžence dá tuto adresu do řádku pro odeslání a do dalšího řádku napíše částku - 1 BTC
- Transakci podepíše svým privátním klíčem (peněženka po Karlovi bude chtít heslo) a odešle
- Pepa ihned vidí, že mu bitcoin přišel do jeho peněženky. Síť však musí transakci potvrdit. Za bezpečné se dnes považují 3 až 6 potvrzení, jedno trvá cca 10 minut. Oproti běžným on-line převodům tak může se svými prostředky nakládat již za několik desítek minut - rychlost je v tomto případě neporovnatelná.
- Oba si mohou transakci on-line zkontrolovat - stačí zadat příslušnou adresu do vyhledávacího řádku na [blockchain.info](#)

A TEĎ TO NEJDŮLEŽITĚJŠÍ. KAREL MŮŽE POSLAT PEPOVI 1 BITCOIN JEN DÍKY TOMU, ŽE SI HO PŘEDTÍM KOUPILO A TEDY JEJ VLASTNÍ. V HISTORII SÍTĚ JE TATO TRANSAKCE ZAZNAMENÁNA. KDYBY TEDY CHTĚL UTRATIT VÍC, NEŽ MÁ, BITCOIN SÍŤ TO POZNÁ A TRANSAKCI ODMÍTNE

Co v podobném případě udělá vaše banka? Máte-li na účtě 1000 Kč, banka vám také neumožní odeslat na jiný účet 2 tisíce. Peníze z banky prostě neodejdou.

Rozdíl je jen v tom, že zatímco u banky vše kontroluje centrální orgán – instituce, které musíte důvěřovat, u bitcoinu je důvěra v prostředníka nahrazena matematickými zákony a kryptografií.

Bitcoinová mobilní peněženka Mycelium



3. JAK ZAČÍT

Základní kroky

Tak – teorii máme za sebou, alespoň tu část, díky které budete lépe chápat, co to bitcoin je a jak funguje. Pojdme teď bitcoiny vyzkoušet a začít používat!

NAINSTALUJTE PENĚŽENKU

Abyste mohli přijímat první bitcoiny, potřebujete program (aplikaci) – peněženku. Je to vlastně vaše osobní banka – účet, ke kterému máte přístup kdykoliv a na který si můžete nechat bitcoiny poslat, nebo z něj cokoliv zaplatit.

Rozlišujeme několik základních typů – podle toho, kde budete mít uložené své BTC a odkud k nim budete mít přístup.

- Základní softwarová peněženka - Bitcoin QT
- Odlehčená softwarová peněženka - např. Electrum
- Webová - online peněženka - např. Blockchain.info
- Mobilní aplikace - Mycelium, Blockchain.info
- Papírová peněženka - paper wallet
- Hardwarová peněženka - Trezor, Ledger a další

BITCOIN QT - TZV. TĚŽKÝ KLIENT

Oficiální bitcoinová peněženka, donedávna zřejmě nejpoužívanější software, k dispozici je také česká verze.

Charakteristické pro ni je, že uchovává celý blockchain. Je to nejbezpečnější řešení. To však může být pro mnoho lidí také velkou nevýhodou, protože už první synchronizace – stažení

blockchainu může trvat podle rychlosti připojení řádově i dny! Vyžaduje poměrně velký prostor na vašem pevném disku – stovky GB. Také při každé další otevření peněženky se stahují poslední části blockchainu od poslední synchronizace a to zabere několik minut, někdy i hodin, podle toho, kdy naposledy jste peněženku použili...

Práce s touto peněženkou je však poté již velmi jednoduchá a pokud vám nevadí její nároky na prostor na disku, může to být pro vás dobrá volba. Tím, že máte synchronizovaný celý blockchain, stáváte se také provozováním této peněženky součástí bitcoinové sítě jako tzv. full node – a to je pro infrastrukturu bitcoinu velmi užitečné.

Soubory pro stažení najdete zde: [Bitcoin.org](https://bitcoin.org)

ELECTRUM – TZV. LEHKÝ KLIENT

Electrum patří mezi bezpečné a nejpoužívanější peněženky. Hlavní výhodou je, že nestahuje kompletní blockchain, ale pracuje jen s jeho částí.

Protože neobsahuje celou historii transakcí, je její instalace a synchronizace záležitost na pár minut. Výhodou také je, že umožňuje nejen vytvoření dalších adres, ale i vytváření dalších samostatných peněženek přímo v programu. Peněženku můžete stáhnout zde: [Electrum](https://electrum.org)

BLOCKCHAIN.INFO

Pro práci s bitcoiny – příjem, nebo odesílání, není vždy nutné, abyste měli nainstalovanou softwarovou peněženku. Na internetu existuje několik on-line řešení, které vám umožní zaplatit bitcoiny, aniž byste s sebou museli nosit notebook, tablet apod., tedy jakékoliv zařízení, kde potřebujete pracovat s pevným diskem.

Určitou nevýhodou může být to, že své bitcoiny nemáte 100% pod kontrolou. On-line řešení má přístup k vašemu privátnímu klíči a vy tak musíte důvěřovat tomu, že je provozovatel peněženky dostatečně chráněn proti bezpečnostním hrozbám.

Doporučuji proto, abyste webovou peněženku používali spíše pro uchování menších obnosů, kterými budete platit např. v restauraci, obchodě atd. – hlavní část bitcoinů si můžete ponechat ve svém počítači. Webovou peněženku si můžete kdykoliv „dobít“ a používat ji tak skutečně jen na placení na cestách apod.

Navíc, dnes už existuje dostatek výborných a bezpečných mobilních aplikací, kde na rozdíl od online peněženek máte vaše privátní klíče pod kontrolou – a i když se také nedoporučují pro uchovávání větších obnosů, stále je to lepší řešení, než skladovat bitcoiny v online prostoru.

Lidé si však hodně věcí snaží zjednodušit a pro úplnost zde tedy uvádím i jedno z nejpoužívanějších řešení – peněženku (nebo spíš účet) na serveru blockchain.info

Zde si vytvoříte účet, který ochráníte dostatečně silným heslem (alepoň 10 – 15 znaků, kombinace velkých a malých písmen, číslic a speciálních symbolů – lomítko, podržítka apod.). Zároveň zadáváte svůj e-mail.

Peněženka vám po zadání hesla vytvoří řadu náhodných anglických slov, ta si zapíšete – ideálně na papír, který dobře uschováte, určitě ne jako textový soubor ve svém počítači... Tento tzv. SEED slouží pro případ, že byste zapomněli své heslo. Na obrazovce ho uvidíte jako Wallet Recovery Mnemonic – viz obrázek.

System vám po přihlášení vytvoří vlastní adresu, na kterou budete přijímat bitcoiny. Můžete si ale samozřejmě vytvářet další nové adresy, jak budete potřebovat.

Peněženku BLOCKCHAIN si můžete nainstalovat také jako aplikaci do mobilního telefonu. Nemusíte se tak např. na cestách složitě přihlašovat přes webové rozhraní, práce s aplikací je rozhodně jednodušší. Aplikace jsou dostupné jak pro Android, tak pro iPhone.

KOMPLETNÍ PŘEHLED PENĚŽENEK PRO IPHONE A IPAD NAJDETE V [TOMTO ČLÁNKU NA BTCTIP.CZ](#)

MOBILNÍ PENĚŽENKA – APLIKACE MYCELIUM

Mezi nepoužívanější mobilní peněženky patří Mycelium. Aplikace do smartphonu, která nestahuje celý blockchain, ale přitom máte kontrolu nad svým privátním klíčem. Je to podobné řešení, jako když máte peněženku – softwarového klienta v PC, ale se všemi výhodami přenosného zařízení.

Peněženku můžete stáhnout např. na [této adrese](#), nebo standardně na trhu aplikací.

U jakékoliv mobilní peněženky je nejdůležitější, vytvořit si zálohu – vyexportovat privátní klíč, opsat na papír, nebo rovnou vytisknout v podobě QR kódu a dobře uschovat. V případě, že byste telefon ztratili, stačí stáhnout znovu mobilní peněženku a naskenovat kód – telefon si „přečte“ blockchain a bitcoiny se objeví v peněžence.

U peněženky Mycelium slouží jako záloha tzv. **seed** – soubor anglických slov, které fungují jako záloha – ztratíte-li např. telefon, nainstalujete na jiném stejnou aplikaci, po instalaci vložíte ve správném pořadí seed a disponujete znovu stejným množstvím bitcoinů, jako v minulém zařízení.

VYTVOŘTE BITCOINOVOU ADRESU

Bitcoinová adresa slouží k tomu, abyste na ni mohli přijímat platby. **Peněženka je vaše soukromá banka**, adresa číslo účtu.

V okamžiku, kdy si založíte bitcoinovou peněženku, získáváte svoji první btc adresu. Většina peněženek vám ji vytvoří automaticky po instalaci – případně zadáte pokyn k vytvoření. Adres můžete mít libovolné množství.

Nejdříve je vygenerován tzv. **PRIVÁTNÍ KLÍČ**. Už z názvu vyplývá, že je to něco, co byste rozhodně neměli s nikým sdílet.

Ihned po instalaci peněženky a získání první adresy nastavte silné heslo k privátnímu klíči a zálohujte. Jak na to, si popíšeme za chvíli.

Bitcoinová adresa vypadá např. takto:

1NRfJcNj7JFGD3ZucBSLuj52bHmqGJLcog

Podobně i privátní klíč je dlouhá řada písmen a čísel. Slouží k tomu, abyste transakci – platbu, kterou někam posíláte, mohli podepsat a potvrdit tak vlastnictví odesílaných bitcoinů. Podpis vypadá v praxi tak, že po zadání platby potvrdíte odeslání heslem, které patří k vašemu privátnímu klíči, peněženka potom vše ostatní zařídí sama. U mobilních aplikací většinou heslo vyžadováno není.

POZOR – KDOKOLIV, KDO BY ZÍSKAL VÁŠ PRIVÁTNÍ KLÍČ, MÁ MOŽNOST ODESLAT SI BTC NA SVOJI ADRESU – NEVRATNĚ!

Jak jsme si již řekli, informace o všech transakcích v síti se uchovávají ve velké „účetní knize“ – blockchainu. Tím, že podepíšete platbu svým privátním klíčem, potvrdíte, že jste to vy a vaše adresa, ke které příslušný počet BTC patří. Stejně tak, když někdo posílá BTC vám, jsou vždy přiřazeny prostřednictvím příjmové adresy právě k vašemu privátnímu klíči.

Kdokoliv, celý svět má možnost vidět, jak bitcoiny „putují“ v síti ke svému novému majiteli. Nebo, kolik a kam je jich posíláno. Zároveň však nikdo nevidí, kdo je skrytý za adresou, na kterou je připisována platba. Žádné IP adresy. Žádné skryté identifikátory, žádné cookies.

V tom je bitcoin anonymní. Přesto, že je systém veřejný a všichni vidí všechno, vlastníka adresy nikdo nezná. Samozřejmě – pokud např. posílám Pepovi BTC na adresu, kterou mi sdělí, tak vím, že tato konkrétní patří jemu. Protože má ale Pepa možnost vytvořit si neomezené množství adres, může mít třeba pro každého plátce jinou adresu.

Já tak sice uvidím, že Pepa přijal 1 BTC na adresu, kterou si můžu kdykoliv najít na blockchain.info a podívat se, kolik na ni v minulosti přišlo bitcoinů, nebo ještě přijde. Pokud ale Pepa používá tuto adresu jen ve styku se mnou a na další platby vytvoří jinou, nemám žádnou možnost, jak to zjistit.

A nejen to – stejně tak můžete mít i neomezené množství peněženek – na počítači, v mobilu, papírové zálohy.

ZÁLOHUJTE, HESLUJTE, ZÁLOHUJTE

A ještě jednou – ZÁLOHUJTE

Jedním z největších úskalí kryptoměn je bezpečnost. Bitcoin je nástroj, který se neobejde bez internetu a to je prostředí, které nemusí být vždy jen přátelské.

Transakce, které jednou odejdou z vaší peněženky, jsou nevratné. A protože ve většině případů nevíte, kdo se skrývá za btc adresu, můžete při velké neopatrnosti přijít o všechny bitcoiny, které máte. A nemáte si komu stěžovat.

DODRŽUJTE PROTO ZÁKLADNÍ PRAVIDLA:

- Pro práci s bitcoiny **používejte počítač, kterému věříte.** Pravidelné aktualizace, firewall a dobrý antivirus je základ, opatrní byste měli být i v tom, na jaké webové stránky se připojujete a jaké programy stahujete... To platí obecně, ale pokud chcete „skladovat“ bitcoiny v notebooku, který používá i váš syn na stahování filmů a on-line hry s kamarády, riskujete hodně.
- Po instalaci btc peněženky **vytvořte dostatečně silné heslo.** Ne heslo typu „beruška“, 12345 apod. Jde o peníze. Takže **M/4398tp7s%4L1o** bude určitě lepší (doslova ho neopisujte :-)) Kombinace velkých a malých písmen, znaků a čísel.

POKUD NEMÁTE DOKONALOU PAMĚŤ, HESLO SI ZAPIŠTE NA PAPÍR NA BEZPEČNÉ MÍSTO. PAMATUJTE - NEMÁTE-LI HESLO, NEMÁTE PŘÍSTUP DO PENĚŽENKY, K PRIVÁTNÍMU KLÍČI - BEZ HESLA JSOU TEDY VAŠE BITCOINY NAVŽDY NEDOSTUPNÉ! TO SAMÉ PLATÍ PRO SEED

- **Vytvořte zálohu privátního klíče** – v desktopových peněženkách nejčastěji najdete volbu **Exportovat privátní klíč**. Vytvoříte tím soubor, který si nahrajete na flash USB, CD, externí disk apod. Pokud by se stalo, že vám např. někdo ukradne notebook, zničí se pevný disk, nebo jiným způsobem přijdete o počítač s peněženkou, je tu záloha. Na jiný počítač nainstalujete novou peněženkou, nahrajete soubor se zálohou a naimportujete privátní klíč do peněženky. Ta si načte historii transakcí v blockchainu a v peněžence budete mít znovu své bitcoiny.
- **Zapište si SEED** – výše uvedená možnost zálohy privátního klíče už dnes není tak častá, daleko častěji se setkáte se zálohou – backupem ve formě Seedu – tuto možnost používají tzv. HD peněženky (mobilní Mycelium, Copay, Coinomi, nebo hardwarová peněženka Trezor – o té píšu dále podrobněji. Seed má podobu buď 12, nebo 24 anglických slov, která je nutno zapsat v takovém pořadí, v jakém nám je peněženka při vlastní instalaci ukáže. Tato slova si ve správném pořadí pečlivě zapište na papír, nikdy si je neukládejte nikam online, ani je nefotěte! Tím by záloha a její bezpečnost ztratila smysl! Tento SEED si uložte nejlépe na více místech, ale zároveň tak, aby k nim nikdo jiný neměl přístup. Pomocí těchto 12 nebo 24 slov je totiž kdokoliv schopen zrekonstruovat kompletní peněženkou – což je vítané v případě, že např. ztratíte mobilní telefon, nebo hardwarovou peněženkou Trezor – ale v případě, že se k seedu dostane někdo cizí, máte smůlu a prázdnou peněženkou...

- V případě obnovy původní peněženky na jiný počítač, nebo mobilní telefon nainstalujete novou peněženku (aplikaci) a místo volby Nová peněženka zadáte volbu **RECOVERY** (Obnova peněženky). Obnova probíhá tak, že postupně zapisujete slova ze „seedu“ v pořadí, v jakém je po vás chce peněženka a po dokončení této operace získáváte úplnou kopii původní peněženky – se všemi adresami, privátními klíči a především se stejným stavem bitcoinů, jako na té původní.

Privátní klíč si můžete také vytisknout – některé peněženky umožňují zobrazit klíč jako QR soubor, který vytisknete v tiskárně a tuto zálohu uložíte opět na nějaké bezpečné místo. Více najdete v užitečných odkazech v 5. kapitole této příručky.

POKUD MÁTE V BITCOINECH ULOŽENÉ VĚTŠÍ PENÍZE, O KTERÉ BYSTE OPRAVDU NERADI PŘIŠLI, JSOU TU PRO VÁS DVĚ NEJBEZPEČNĚJŠÍ ŘEŠENÍ:

1) OFF-LINE VYTVOŘENÁ PAPIŘOVÁ PENĚŽENKA

Co není na internetu, to vám hacker neukradne. Na stránkách www.bitaddress.org najdete generátor, který vytvoří náhodným výběrem vaši veřejnou příjmovou adresu (public key) a privátní klíč (private key).

Takto vytvořený privátní klíč **vytiskněte** - ale v žádném případě neukládejte – ani do počítače, natož pak někam do veřejného prostoru. **Kdokoliv má přístup k soukromému klíči, může utratit všechny bitcoiny, které na něm budou.**

Na adresu, označenou jako Sdílejte (vaše příjmová adresa) si pošlete (necháte poslat) bitcoiny, které chcete mít v bezpečí. Pohyb BTC můžete zkontrolovat v blockchainu a jakmile budou na vaší off-line adrese, žádný hacker vám je nemůže vzít.

Pokud chcete mít ABSOLUTNÍ JISTOTU, zvolte i při vytváření privátního klíče off-line řešení – stránky bitaddress.org

zkopírujete, z bootovacího CD nebo flash disku spustíte bez připojení k internetu počítač a klíč vytvoříte off-line.

Budete-li v budoucnu potřebovat bitcoiny z této papírové off-line peněženky něco zaplatit, můžete privátní klíč jednoduše naimportovat do jakékoliv peněženky, která to umožňuje – načtením QR kódu.

Importováním privátního klíče se přiřazená veřejná adresa stane součástí softwarové peněženky. Znovu tedy platí vše už napsané o heslování.

POZOR – DŮLEŽITÉ UPOZORNĚNÍ! JAKMILE Z PAPIROVÉ PENĚŽENKY NAIMPORTUJETE PRIVÁTNÍ KLÍČ DO POČÍTAČE, NEBO MOBILU A ODEŠLETE JAKÉKOLIV MNOŽSTVÍ BTC NA JINOU ADRESU, NESPOTŘEBOVANÝ ZŮSTATEK SE VŽDY AUTOMATICKY ZAŠLE NA ADRESU, KTERÁ JE VYTVOŘENÁ V POČÍTAČOVÉ (MOBILNÍ) PENĚŽENCE!

Tedy – máte např. 2 BTC na adrese, uložené s privátním klíčem na papírové záloze. Po importu do standardní peněženky odešlete někomu např. 1 BTC. Ve skutečnosti ale každá peněženka odešla do blockchainu CELÉ MNOŽSTVÍ, kterým disponujete, v tomto případě tedy 2 BTC. 1 bitcoin dojde na vámi zadanou adresu jako platba a zbylý 1 bitcoin se vám vrátí do peněženky.

Ovšem – na adresu, která už byla předtím v peněženke vytvořena, nikoliv na tu vaši původní papírovou!

Je tedy nutné vytvořit novou zálohu a tu opět uschovat – export privátního klíče, jak je popsáno na začátku kapitoly. Samozřejmě, můžete si výše popsaným způsobem vygenerovat off-line novou papírovou peněženku s privátním klíčem a pokud nepotřebujete s bitcoiny operativně pracovat, pošlete si je do této zálohy.

Vím, vypadá to všechno složitě a zvláště pro začátečníky není jednoduché se ve všech postupech vyznat. **Chcete-li však mít vaše bitcoiny v bezpečí, je pochopení a dodržování těchto zásad klíčové.**

2) HARDWAROVÁ PENĚŽENKA - BITCOIN TREZOR

[Bitcoin Trezor](#) je hardwarová peněženka, která uchovává privátní klíč a slouží k podepisování transakcí.

Byla vyvinuta českou firmou Satoshi Labs a v prodeji je od června 2014, aktuálně za cenu 89 USD – na stránkách výrobce však můžete zaplatit pouze v bitcoinech, podle aktuálního kurzu.

Pokud máte větší množství bitcoinů a potřebujete bitcoiny uchovávat, ale také posílat zcela bezpečně a pohodlně, je to v současnosti nejlepší řešení. Na rozdíl od paper wallet s ní můžete fungovat kdykoliv a on-line.

Princip fungování Trezoru je v tom, jakým způsobem pracuje s privátními klíči. Podepisování transakcí probíhá zcela izolovaně od počítače, na kterém se zadávají příkazy k odeslání bitcoinů na konkrétní adresu.

Zařízení je kompatibilní zatím s dvěma klienty – peněženkami. [Electrum](#) a [Wallet.trezor](#) (vytvořená také Satoshi Labs).

V těchto peněženkách vytvoříte transakci a display Trezoru ukáže zadanou adresu. Zároveň nabídne možnost potvrzení transakce ANO/NE. Potvrzení se provádí stisknutím tlačítka přímo na Trezoru a uživatel tak má absolutní kontrolu nad činností peněženky.

Počítač, na kterém pracujete, může být kompromitován malwarem, programy, které mohou „odečíst“ heslo zadávané při podpisu transakce. Při dnešní složitosti procesů, které v počítači

probíhají, je prakticky nemožné zajistit 100% bezpečnost a ani nejdelší heslo ještě nezaručuje jeho neprolomitelnost.

V tom je právě [Bitcoin Trezor](#) unikátní – jednoduše řečeno umožňuje přesun dat pouze jedním směrem – z Trezoru do počítače. Bezpečnost je tak zaručena i v případě, že je peněženka

nainstalovaná na potenciálně zavirovaném počítači. Trezor funguje jako samostatná počítačová jednotka a posledním stupněm kontroly je „mechanické“ stisknutí tlačítka – to zatím nedokáže žádný hacker...

Bitcoinová HW peněženka TREZOR



4. JAK ZÍSKAT BITCOINY

Je vám teď jasnější, co to bitcoin je, jak vzniká a jaké pro vás může mít výhody? Máte založenou peněženku a svoji první bitcoinovou adresu? Zaheslovali jste privátní klíč a vytvořili zálohu?

Výborně! Pojdme tedy zjistit, kde a jak získáme svoje první digitální peníze...

BURZY, SMĚNÁRNY

Jednou z hlavních myšlenek tvůrce bitcoinu bylo, že má kryptoměna umožnit rychlé a levné placení po internetu. Bitcoin má být směnný prostředek, který nebude závislý na žádné centrální autoritě. Rychlý, levný, neinflační, bezpečný.

Jak si ale jeho uživatelé začali uvědomovat jeho výhody, začal být bitcoin žádaným zbožím a jeho hodnota rostla. Jakmile jeho cena začala dosahovat parity s dolarem, začaly vznikat první směnárny, kde je možné získat za digitální měnu hotovost.

Princip je stejný, jako na běžné burze. Zájemce o koupi bitcoinu zadá požadovaný počet a nabídne cenu, jakou je ochoten zaplatit. Jakmile se najde prodávající, který nabízí dostatečné množství BTC v této ceně, obchod se automaticky „spáruje“, směna je provedena. Burza si za tuto službu vezme poplatek, obvykle ve výši 0,1 – 0,5% za nákup, nebo prodej.

Základním předpokladem však je, že chcete-li na burze/směnárně obchodovat, musíte tam nejdříve své bitcoiny, nebo peníze převést. To vyžaduje důvěru v konkrétní instituci a zvláště v poslední době se ukazuje, že byste měli dobře vybírat...

Legendární [krach burzy MtGox](#), kde zůstaly mnoha lidem velké peníze a oči pro pláč, je toho učebnicovým příkladem.

Je pravda, že tato neslavná událost donutila ostatní velké i malé burzy k přijetí sofistikovanějších bezpečnostních řešení a také k pravidelným účetním a bezpečnostním auditům, takže další případy (Bitfinex, Bitstamp atd.) neměly už tak fatální následky.

Bitstamp po bezpečnostním incidentu pokračoval dál a peníze klientů zůstaly netknuty, Bitfinex vykradení tzv. hot wallet řešil „socializací ztrát“ a burza jede dál. Stále však platí, že pouze máte-li pod kontrolou své privátní klíče, patří vám také bitcoiny...

BURZA/SMĚNÁRNA NEMÁ V ŽÁDNÉM PŘÍPADĚ SLOUŽIT JAKO NÁHRADA VAŠÍ PENĚŽENKY. **VELKÁ ČÁST POSTIŽENÝCH KLIENTŮ MĚLA V MTGOX SVÉ BITCOINY ULOŽENY DLOUHODOBĚ – A TO JE CHYBA**

Bitcoin a decentralizovaný systém, na jehož základě funguje, je bezpečný. Jakmile ho ale nemáte ve svých rukách a svěřujete jej např. burze, je vše závislé na tom, jak je burza důvěryhodná, jaké má zabezpečení atd.

Při nákupu, nebo prodeji bitcoinů na těchto obchodních místech je proto důležité nevybírat neznámé a malé směnárny jen proto, že zrovna nabízí lepší kurz. Případů, kdy taková směnárna skončila svoji činnost ze dne na den – ať už proto, že měla slabé zabezpečení a byla vykradena, nebo se z jiných důvodů dostala do insolvence, je stále dost.

BITSTAMP

Velká, tradiční a stále spolehlivá směnárna. Firma založena v Anglii, fyzicky sídlí ve Slovinsku. Po pádu MtGox patřila mezi několik burz, které se od MtGox a jejich praktik distancovaly. Pro zvýšení své důvěryhodnosti podstoupila finanční a bezpečnostní audit, který prokázal její důvěryhodnost (více zde v článku).

Pro založení účtu na bitstamp.net je nutná e-mailová registrace a následná verifikace – pro ověření budete potřebovat naskenované doklady – OP nebo cestovní pas. Dalším vyžadovaným dokladem je jakýkoliv dokument, který prokazuje trvalé bydliště – naskenovaný účet za elektřinu, nebo plyn, případně výpis z bankovního účtu s vaší adresou, nebo výpis z katastru nemovitostí. Účet za telefon mezi uznávané doklady nepatří.

V nastavení účtu potom zadáte bankovní účet, ze kterého budete do Bitstampu posílat peníze pro nákup BTC.

Dalším krokem je vklad na účet v eurech – nejrychlejší je tzv. SEPA platba, tedy bankovní příkaz evropského standardu, kde jsou také nejmenší poplatky. Bitstamp vám připraví údaje pro zadání bankovního příkazu, **důležité je uvést do poznámky přihlašovací ID vašeho BITSTAMP účtu – slouží k identifikaci platby!**

Vaše peníze budete mít připsány na burze cca 2-3 dny po odeslání a Bitstamp je automaticky převede na dolary, za které potom budete nakupovat BTC. Stejný postup platí pro výběry z burzy.

Nákup bitcoinů probíhá tak, že v položce Nákup/prodej zvolíte jednu ze dvou možností:

- Okamžitý příkaz - zde zadáte počet BTC, které kupujete a nákup proběhne za aktuální cenu.
- Limitní příkaz - můžete zde zadat nákup za nižší cenu, než je současná, nákup se provede automaticky v případě, že se BTC na tuto cenu dostanou. Vyžaduje to ale už jisté zkušenosti s tím, jak se vyvíjí cena v čase a pokud je trend stoupající, nákup neproběhne.

Budete-li chtít na Bitstampu naopak BTC prodat, získáte od směnárny adresu, na kterou odešlete bitcoiny ze své peněženky (cca do hodiny je budete mít potvrzené v bilanci účtu) a dále už postupujete stejně, jak uvádím výše – buď prodáte BTC za aktuální cenu, nebo nastavíte v Limitním příkazu cenu vyšší, než je ta současná.

COINMATE

Ověřená burza se sídlem v Anglii, s českým zázemím.

Na [Coinmate](#) je kladen velký důraz na bezpečnost uložení prostředků uživatelů, je považována za jednu z nejbezpečnějších burz. Velkou výhodou burzy Coinmate je pro české uživatele fakt, že lze vložit finanční prostředky pro nákup bitcoinů rovnou v českých korunách – pokud máte účet u FIO banky, probíhá vklad

prakticky instantně. Burza obchoduje přímo v obchodním páru BTC/CZK.

Tak jako u jiných burz, které pracují s vklady a výběry ve FIAT měně (EUR, USD, CZK atd.) je i zde potřeba projít verifikačním procesem a podle úrovně ověření také dostáváte limity, v jejichž rámci se budete při převodu peněz pohybovat. Další informace o burze Coinmate najdete také v [tomto článku](#).

COINBASE

Americká směnárna [Coinbase](#) je často využívána pro přímý nákup bitcoinů a altcoinů, jako je například Litecoin, jednou z výhod je, že zde můžete zaplatit také platební kartou, přestože spíše v menších objemech.

Coinbase patří mezi dlouholeté a spolehlivé zahraniční směnárny. Pokud se navíc zaregistrujete přes tento odkaz, získáte hned na začátek do své peněženky 10 USD ve formě milibitcoinů.

DALŠÍ BURZY

Mezi spolehlivé zahraniční burzy se v současné době řadí např. [Bitfinex.com](#), nebo [Kraken.com](#). Přihlašovací, ověřovací a další postupy jsou podobné. Rozdíl je ale v tom, že např. Bitfinex nemá možnost vkladů a výběrů v běžných penězích (fiat měně) a lze tedy pracovat pouze s kryptoměnami.

V České republice byla v minulosti využívána směnárna Bitcash.cz, ta však byla v r. 2014 napadena hackery a vykradena...

Od té doby zde bylo několik pokusů o založení důvěryhodné směnárny, nebo burzy – jedním z nich je [Bitstock.cz](#), kde se hodně dbá na bezpečnost a pokud např. prodáváte bitcoiny, nezůstávají na účtu směnárny, ale u vás. Kupující posílá české koruny do Bitstocku a ten funguje jako „escrow“ služba. Je tedy jakýmsi garantem, že vám při prodeji bitcoinů dojdou v pořádku koruny na účet a stejně tak obráceně.

Na Bitstocku ovšem nehledejte obchody za nějaké větší objemy, pro spekulanty to není zřejmě ta nejpoužívanější platforma...

Podobně si svoje místo v ČR nachází i služby směnárny [Simplecoin](#), nebo [EasyCoin](#), kde navíc máte možnost nákupu a prodeje za hotové prostřednictvím sítě trafik Geco, nebo můžete využít služby Bitcoin Banking.

O burze [Coinmate](#) jsem se již zmiňoval, ta má sice sídlo v zahraničí, ale stojí za ní také Češi.

Hlavním rozdílem mezi směnárnou a burzou je ten, že **směnárna** určuje a nabízí vlastní kurzy a zpravidla má i vyšší spread (rozdíl mezi nákupní a prodejní cenou pro klienta), zatímco **burza** slouží jako platforma, na které se soustřeďují nabídky uživatelů, kteří chtějí bitcoiny koupit a těch, kteří chtějí naopak prodat. Burza tedy žádné bitcoiny sama nenabízí, jen páruje nabídky a poptávky.

Burza si účtuje poplatky za poskytnutí své platformy, zpravidla jsou však o dost nižší, než u směnárny. Na druhou stranu je většinou nutné se na burze nějakým způsobem registrovat a také verifikovat, což bývá někdy poměrně komplikované a zdlouhavé.

Ve všech případech, kdy budete chtít využít služeb zahraničních, nebo českých burz a směnáren vždy platí:

- Zajímejte se o reputaci služby, dosavadní reference zákazníků.
- Doba, po kterou je firma na trhu a další skutečnosti vám napoví, nakolik můžete konkrétní směnárně, burze důvěřovat.
- Na rozdíl od své peněženky zde svěřujete své prostředky soukromému subjektu a jako takový pro vás musí být důvěryhodný.

Nákup a prodej bitcoinů a dalších kryptoměn může být vysoce lukrativní záležitost, ale stejně tak s sebou nese rizika. Vysoká volatilita (výkyvy kurzů) může v nezkušeném investorovi vyvolat paniku a rozhodnutí, která mohou vést ke ztrátám. Stejně tak neopatrnost a nedodržení bezpečnostních opatření, ztráta hesla k peněženke apod. může vést ke ztrátě bitcoinů.

VŽDY PROTO PAMATUJTE, U BITCOINU TO PLATÍ DVOJNÁSOB – INVESTUJTE JEN TOLIK, KOLIK SI MŮŽETE DOVOLIT ZTRATIT.

LOCALBITCOINS – PŘÍMÝ NÁKUP

Zajímavou možností, jak získat bitcoiny, je přímý nákup od lokálních obchodníků.

Celosvětová služba localbitcoins.com propojuje zájemce o nákup a prodej bitcoinů.

Vyhledá pro vás nejbližšího obchodníka, který je ochoten prodat bitcoiny (případně koupit), stačí buď přímo zadat lokalitu, ve které se nacházíte, nebo povolit notebooku, mobilu apod. lokalizaci přes GPS. Do služby je plný vstup po registraci.

V Praze a dalších větších městech je možné takto vyhledat soukromníka, se kterým se přímo domluvíte jak na ceně, tak na způsobu platby. Možná je platba v hotovosti – s obchodníkem se sejdete (nejlépe na veřejném místě), on vám převede BTC do peněženky, vy si zkontrolujete, aby platba dostala několik potvrzení a platba může proběhnout...

Stejně tak se lze domluvit i na bankovním převodu, nebo vklady přes různé internetové peněženky (OK PAY apod.)

Více než kdy jindy je i tady však na místě opatrnost – u jednotlivých prodejců je možné v záložkách najít reference zákazníků, přesto je lepší začít spíše s menším množstvím a dále postupovat podle osobní zkušenosti.

Také ceny jsou většinou o něco vyšší, než ve směnárnách. Výhodou je rychlost a minimum byrokracie...

BANKOMAT

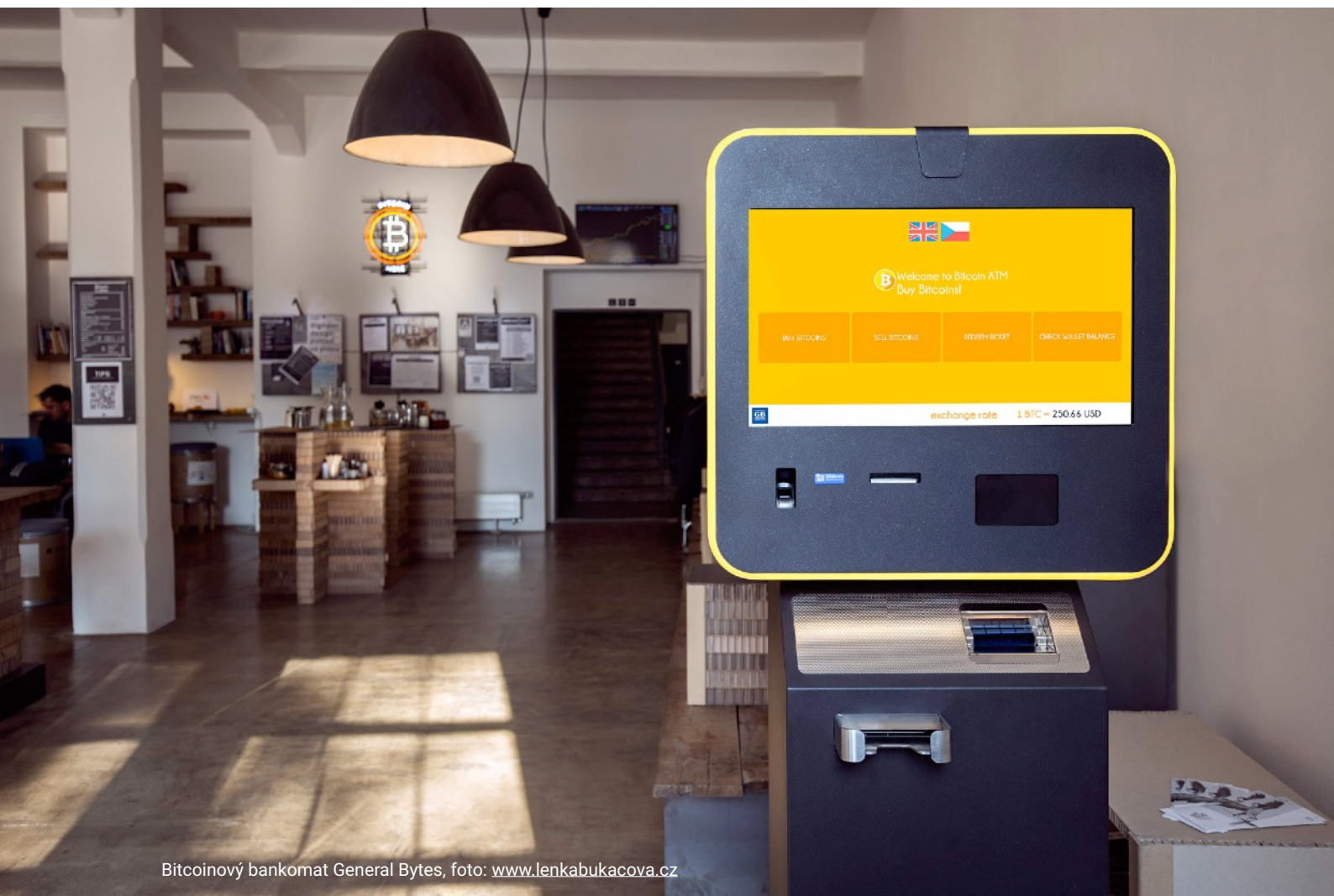
Bitcoin můžete už dnes koupit v bankomatu.

V této chvíli je v České republice k dispozici dokonce 20 bitcoinmatů. V Praze jich je 10, další najdete v Plzni, Karlových Varech, v Pardubicích, Liberci, v Brně a v Ostravě.

Kurzy vycházejí z aktuálních cen na burzách, většinou podle Bitstamp, nebo Kraken + poplatky bankomatu.

Po zadání množství BTC, které chcete nakoupit a po výpočtu ceny je výstupem z bankomatu buď vytištěný privátní klíč – v podobě QR kódu, nebo bitcoinmatu ukážete QR kód své peněženky v mobilu a bitcoiny jsou zaslány přímo.

Privátní klíč si bezpečně uschováte – do té doby, než budete potřebovat bitcoiny zaplatit, poslat je dál.



Postup je stejný, jako ve 3. kapitole tohoto e-booku – doklad o nákupu je vaše papírová peněženka, kterou můžete kdykoliv naimportovat do té mobilní, softwarové v počítači, případně do webové on-line služby.

PŘEHLED BITCOINOVÝCH BANKOMATŮ V ČR I VE SVĚTĚ NAJDETE NA TÉTO MAPĚ

VLASTNÍ ZBOŽÍ, SLUŽBY

Provozujete e-shop, kamennou prodejnu, poskytujete nějakou službu? Nechte si zaplatit v bitcoinech!

Celosvětově je nyní více než 120.000 akceptačních míst, tedy prodejen, podniků a služeb, kde je bitcoin přijímán jako platební metoda. U nás jsme zatím přibližně na počtu 150, čísla však neustále rostou...

HLAVNÍ DŮVODY, PROČ PŘIJÍMAT PLATBU BITCOINY:

- Získáte konkurenční výhodu, budete něčím jedineční
- Marketing a reklama - dáte o sobě vědět
- Ušetříte na poplatcích (žádná procenta jako u platebních karet)
- Podpoříte technologii budoucnosti a budete o krok před ostatními

Detailně si o všem můžete přečíst v článku 7 důvodů pro obchodníky, proč zavést platbu bitcoiny

Platba není složitá a v menší kamenné prodejně pro ni stačí jednoduchá aplikace v mobilu. Zákazník načte QR kód, který se vygeneruje po zadání požadované částky – dá se to přirovnat k čárovému kódu, nebo bezkontaktní platební kartě...

Větším prodejnám, nebo e-shopům se vyplatí spíš implementace řešení platební brány – například Bitcoinpay, jejíž služby využívá i největší e-shop s elektronikou - Alza. Platby, které se načtou od zákazníka, jsou instantně převedeny do lokální měny a odpadá tak obava z vysoké volatility a kurzových rozdílů.

U menších on-line prodeju postačí příjmová btc adresa, na kterou zákazník pošle platbu a po ověření v blockchainu odesíláte zboží, nebo poskytnete službu. Daňové otázky můžete probrat se svým účetním, prodej zboží a služeb tak jako tak vykazujete v korunách.

Bitcoin si buď necháte – se spekulací na další růst, nebo je vyměníte na burze, prodáte v bankomatu apod.

Denně aktualizovanou mapu obchodů, které přijímají bitcoinové platby, najdete na těchto stránkách – [bitcoin obchody a služby](#).

Nově je zde zařazen také katalog zboží a služeb, které můžete pořídit za bitcoiny v České republice.



TĚŽBA, PODÍL NA TĚŽENÍ

Tady už první nebudete – bohužel. Od doby, kdy se v r. 2009 s touto činností začalo, se vše zásadně změnilo...

Sám nejsem klasický „geek“ a žádné kryptoměny netěžu. Mám ale několik kamarádů, kteří jsou zapojeni v poolech a těží buď bitcoiny, nebo na speciálních sestavách (GPU rigy) jiné měny – Ethereum, Monero, Zcash, Litecoin apod. Láká mě to, asi to ještě také zkusím.

I dnes se dá při správné konfiguraci nastavit výkon speciálně sestaveného „železa“ tak, aby se vám investice do hardwaru, elektrické energie a někdy také vhodného prostoru (i nároky na chlazení jsou opravdu veliké) nejen vrátila, ale i slušně vydělávala.

Jednotlivec nemá šanci a základem je najít slušný a výkonný pool k připojení a také experimenty s různými „altcoiny“ – jejich cena je hodně proměnlivá. Altcoiny se po vytěžení převádí na specializovaných směnárnách na bitcoiny, které mají přece jen větší likviditu.

Možným řešením je také nákup těžebního výkonu, podílu – investujete tak peníze (většinou BTC) přímo do poolu, který těží za vás. Nekupujete tedy hardware, elektřinu atd. – většinou se jedná o víceleté kontrakty typu podílových listů. Na internetu se dá najít více podobných nabídek, nedá se ale dobře odhadnout, jak se bude „těžba“ vyplácet s neustále rostoucí obtížností a výkonem sítě.

BITCOINY ZDARMA

Pokud si chcete především vyzkoušet, jak funguje vaše nová peněženka, jsou stránky s bitcoiny zdarma nejjednodušší řešení.

Na internetu bylo už dříve velké množství tzv. „klickaček“, kde je možné za kliknutí na reklamní stránku dostat odměnu v řádu desetin centů dolaru a i dnes je hodně lidí, kteří se takové činnosti věnují a mají pocit, že je to pro ně ta pravá „práce z domu“. S tím, jak přišel na scénu bitcoin, dostal tento průmysl nový impuls. „Výdělky“ jsou rychlé a bez poplatků, firem, které potřebují propagovat své stránky a výrobky je také dost.

Já vám určitě zbohatnutí, ani solidní výdělků slibovat nebudu. Ale pro ten pocit, kdy vám přijdou do peněženky první zlomky bitcoinů, jsou „klikací“ stránky s mincemi zdarma ideálním řešením – zvláště pro začátečníky.

Vyzkoušené a relativně štědré jsou stránky [freebitcoin](#) , [btcclicks](#) nebo [moonbitcoin](#).

Kompletní návod a postupy najdete na stránkách [btctip.cz](#) pod tímto odkazem - [Bitcoin zdarma](#)

QR KÓD A WEBY, BLOGY

Jak můžete ještě získat bitcoiny? Vlastně docela jednoduše...

Pokud provozujete např. e-shop, vytváříte webové stránky, píšete články, blogujete, nebo cokoliv publikujete, použijte svoji bitcoinovou adresu, nebo přímo QR kód veřejného klíče a zveřejněte ho.

U mnoha článků a blogů najdete v posledních několika měsících btc adresu jejich autora. Na webech vidíte QR kódy se slušnou žádostí o podporu, především u nekomerčních stránek. A pokud se ještě navíc zajímáte o problematiku bitcoinu a kryptoměn, je tato forma propagace častá a využívaná.

Existuje poměrně velká skupina lidí, kterým se mohou vaše webové stránky, blog, články apod. líbit a přispět na jejich činnost drobným obnosem v BTC je pro ně pohodlné a také „in“.

Stejně tak pro různé neziskové organizace, charitativní spolky, nebo zájmová sdružení může být tato forma podpory zajímavá. Založit si k tomu účelu btc peněženku je záležitostí pár minut a výsledky vás možná překvapí...

5. UŽITEČNÉ ODKAZY

Na závěr uvádím několik zajímavých odkazů, které vám mohou poskytnout další informace, nebo inspiraci

www.btctip.cz - tím musím samozřejmě začít :-).

Čtete blog s novými články, sledujte novinky

www.bitperia.cz - mobilní appka, která obsahuje snad všechny informace o bitcoinu a kryptoměnách pro nováčky i pokročilé

www.bitcoin-info.cz , www.bitcoinman.cz - další webové stránky, věnující se bitcoinu a kryptoměnám

<https://bitcoinwisdom.com> - online grafy s vývojem ceny bitcoinu, litecoinu - na hlavních burzách

Youtube a Marek Palatinus - nejen tento, ale i další rozhovory a přednášky. Marek „Slush“ Palatinus je průkopníkem v české bitcoinové komunitě, vynálezcem těžebních poolů a bezpečné peněženky **Bitcoin Trezor**. Vyplatí se sledovat.

Fiatleak.com - info grafika s pohybem bitcoinů - nákup, prodej a všechny přesuny BTC v reálném čase

PÁR SLOV NA KONEC

Děkuji, že jste stažením (a snad i přečtením) tohoto e-booku projevíli zájem o bitcoin a kryptoměny. Doufám, že jsem vám poskytl informace, které pro vás budou užitečné.

Možná už jste slyšeli, nebo ještě uslyšíte názory mnoha lidí, kteří o smyslu a budoucnosti bitcoinu pochybují. Nechci se přít, kdo má pravdu, i když jsem přesvědčený, že během krátké doby, několika let budeme svědky obrovského rozmachu kryptoměn a jejich využívání.

Pokud si potom vzpomenete, že jste někdy četli tento e-book, je to přesně důvod, proč jsem ho napsal. Abyste byli o krok napřed a věděli jste, kam si můžete přijít pro další informace.

Budete-li potřebovat vysvětlení pojmů, kterým nerozumíte, nebo mi třeba dát vědět, jestli se vám tato příručka líbila a pomohla vám, kdykoliv mi napište na e-mail karel.fillner@btctip.cz. Bude-li to v mých silách, rád vám poradím a samozřejmě uvítám i váš názor.



Karel Fillner
Bitcoinový evangelista

A handwritten signature in grey ink, appearing to be 'K. Fillner', written in a cursive style.