Můj První Bitcoin
ČESKÁ REPUBLIKA

Bitcoinový diplom

Finanční vzdělání v Bitcoinové éře

Pracovní sešit

český překlad | 2024

Bitcoinový diplom

Finanční vzdělání v Bitcoinové éře

Pracovní sešit

český překlad | 2024

Můj První Bitcoin
EL SALVADOR

Podpořte nás

bc1q5es60qpa7gpkp0k32xl4zefkj43kd9zjkzd54sgmv3yzr34dw8dqm9pzsd

Příběh Bitcoinového Diplomu

Není nic mocnějšího než myšlenka, jejíž čas právě nadešel.

Příběh Bitcoinového Diplomu začal v Salvadoru, kde v červnu 2022 absolvovalo první pilotní projekt 38 studentů veřejných škol.

Je těžké uvěřit, že to bylo teprve před rokem a půl.

Růst v roce 2023 byl fenomenální, jelikož tisíce studentů z celé země absolvovalo náš kurz s názvem Bitcoinový Diplom. V září, pouhých 15 měsíců po této první promoci, započal mnohem větší pilotní program. Ministerstvo školství v Salvadoru vytvořilo svůj vlastní studijní program s naším pracovním sešitem jako primárním zdrojovým materiálem. Spolu s členy Bitcoin Beach vyškolili naši mentoři 150 učitelů veřejných škol. Tito učitelé se poté vrátili do svých škol a učili své vlastní žáky. V letošním roce (2024) plánujeme začít tím, že pomůžeme vyškolit dalších 700 učitelů veřejných škol rozprostřených po celé zemi, a doufáme, že do dvou let přineseme kvalitní bitcoinové vzdělávání do každé školy v Salvadoru.

Jedním z našich původních cílů bylo vzdělávat o Bitcoinu jako nástroji pro lepší budoucnost.
A ne jenom lokálně, ale v masovém měřítku. Tento sen je nyní na dobré cestě.

Salvador je středobodem zájmu, misí je celý svět.

Pracovní sešit, stejně jako řadu dalších vzdělávacích materiálů, jsme poskytli volně ke stažení a distribuci a mezinárodní zájem nás ohromil. V roce 2022, kdy výuka o Bitcoinu začala v Salvadoru, to bylo úplně poprvé, co se ve veřejném školském systému kdekoli na světě vyučovalo o Bitcoinu. Poté, v roce 2023, jsme materiál přeložili do 12 jazyků a nyní se vyučuje v Guatemale, Hondurasu, USA, Kanadě, na Kubě, v Dominikánské republice, Jižní Koreji, Kostarice, Brazílii, Uruguayi, Argentině, Indii, Itálii, Mexiku, Jihoafrické republice, Zambii, Keni, Portugalsku, Velké Británii & a Hongkongu. Stejně jako růst v roce 2023 překonal růst v roce předchozím, očekáváme, že v roce 2024 tomu bude stejně.

Jedná se totiž o globální, decentralizované hnutí.

Nezávislé, nestranné a komunitou vedené vzdělávání změní svět. Ono už se vlastně tak stalo.

V zájmu lepšího světa,

Tým Můj První Bitcoin - 2024

Obsah

Kapitola 5: Jak problémy vedou k řešení

Kapitola 6: Úvod do Bitcoinu

Kapitola 7: Jak používat Bitcoin

Kapitola 8: Síť Lightning network: Používání bitcoinu v každodenním životě

Kapitola 9: Úvod k technické stránce Bitcoinu

Kapitola 10: Proč Bitcoin?

Bitcoinový diplom

Desetitýdenní transformační cesta
k nezávislosti, nestrannosti a ke
kvalitnímu a svobodnému vzdělávání

Před studiem Bitcoinu je nezbytné mít základní znalosti o podstatě peněz, jejich historii a současném finančním systému. Pochopení těchto pojmů poskytuje pevný základ pro pochopení jedinečné a převratné povahy Bitcoinu. Když se seznámíte s vývojem peněz, budete moci lépe pochopit nedostatky a problémy současného finančního systému a to, jak se je Bitcoin snaží vyřešit. Bez tohoto základu může být obtížné plně pochopit význam a potenciální dopad Bitcoinu. Důvěřujte tedy sobě a své schopnosti se naučit novým věcem, protože odměna v podobě hlubšího pochopení a ocenění této revoluční oblasti bude stát za to.

Kapitola 1

Proč potřebujeme peníze?

Pracovní sešit

český překlad | 2024

Proč potřebujeme peníze?

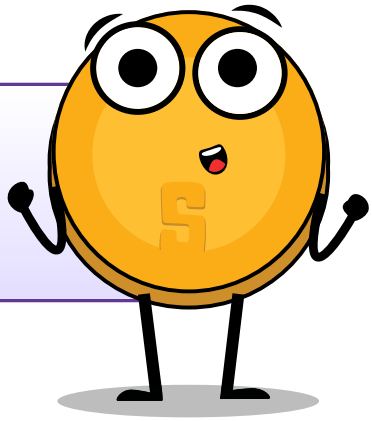
1.0 Úvod

> Peníze jsou jedním z největších nástrojů svobody, které kdy člověk vymyslel.
>
> **Friedrich Hayek**

Vítejte v Bitcoinovém Diplomu. V této kapitole se budeme zabývat základní otázkou, proč jsou peníze v našem životě nezbytné. Budeme se zabývat podstatou peněz, jejich různými formami a budeme usilovat o hlubší pochopení jejich významu. Peníze jsou něčím, co používáme téměř každý den. Ale rozumíme vlastně tomu, proč je potřebujeme a co skutečně jsou? Proč naši rodiče a další rodinní příslušníci vyměňují svůj čas za peníze? Proč jich někteří lidé mají více než jiní? Proč se peníze v jiných zemích liší? Proč si jich prostě nemůžeme vytvořit více, když je potřebujeme? Respektive kam to vede, když se nové peníze vytvářejí? Na všechny tyto a další otázky si postupně odpovíme.

1.1 Seznamte se se Satoshim

> ***Ahoj! Jsem Satoshi, interaktivní asistent, který vám bude pomáhat v průběhu Bitcoinového Diplomu. Budu vám poskytovat zdroje a užitečná doporučení, abyste se mohli lépe seznámit s klíčovými pojmy.***



Aktivita: Začněme kapitolu odpověďmi na pět níže uvedených otázek:

Zvažte praktické účely, jako je nákup základních potřeb, například potravin a vytoužených statků. Snažte se být ve svých příkladech konkrétní a vyvažujte kreativitu s realitou.

Proč potřebujeme peníze?

Co jsou to peníze?

Proč potřebujeme peníze?

Kdo ovládá peníze?

Co nebo kdo dává penězům jejich „hodnotu"?

Jakou otázku máte ohledně peněz? Napište ji sem a podělte se o ni ve své třídě.

Rozveďte diskusi pro celou třídu, sdílejte a porovnávejte své seznamy, abyste určili pět nejpodstatnějších důvodů, proč potřebujeme peníze. Poté určete společné myšlenky celé třídy. Dále se zamyslete nad svými individuálními jedinečnými nápady, které se do seznamu nedostaly, ale stojí za zvážení. Tyto postřehy si zaznamenejte.

1.2 Diskuse ve třídě: Proč potřebujeme peníze?

Třídu rozdělte do skupin a:

- Podělte se o odpovědi na první čtyři otázky a diskutujte o nich. Zapište si nejčastější odpovědi.
- Podělte se o své odpovědi na poslední otázku a hlasujte o nejoblíbenější variantě. Výsledek si zaznamenejte.
- Na konci Bitcoinového Diplomu se třída vrátí ke svým odpovědím a otázkám.

Nyní, byste měli mít jasnější představu o tom, proč jsou peníze nezbytné, a proto se v následujících kapitolách budeme zabývat tím, co to peníze jsou, jak se vyvíjely v průběhu času, kdo je ovlivňuje a jaká je jejich nejnovější podoba. V hodinách se průběžně vracejte ke svým zápisům z tohoto prvního dne, abyste si dokázali spojit své poznatky s tvorbou peněz, jejich definicí a používáním v průběhu času.

Kapitola 2

Co jsou to peníze?

Pracovní sešit

český překlad | 2024

Co jsou to peníze?

2.0 Úvod

> Peníze jsou zárukou, že v budoucnu můžeme mít to, co chceme. I když v tuto chvíli nic nepotřebujeme, zajišťují nám možnost uspokojit novou touhu, až se objeví.
>
> **Aristoteles**

V návaznosti na naše zkoumání potřeby peněz se v této kapitole budeme věnovat základní otázce: Co jsou to peníze? Začneme skupinovou diskusí a aktivitou.

Aktivita: Diskuse ve třídě "Co jsou to peníze?"

- Prosím, nejezte ještě sladkost, která je položena na vašem stole.
- Kdo by byl ochoten vyměnit svou sladkost za bankovku v hodnotě 1 USD?
- Nyní zvedněte ruce, pokud jste stále ochotni vyměnit svou sladkost za jedno dolarovou bankovku ze hry monopoly.
- Proč ano a proč ne?
- Proč je jedna bankovka tak žádoucí a druhá braná jako nežádoucí?
- Co dává penězům jejich "hodnotu"?
- Odkud se berou peníze a kdo rozhoduje o tom, kolik se jich vytiskne?
- Proč nenatisknout více peněz a nerozdělit je všem rovným dílem?

2.1 Definice peněz

Přemýšleli jste někdy o tom, co peníze skutečně jsou? Nebo o tom, co dělá peníze... no, penězmi? Většina z nás ví, jak s nimi zacházet, ale málokdo z nás chápe, odkud se berou a jak fungují. Peníze jsou v podstatě způsob směny zboží a služeb. Představují hodnotu těchto položek ve formě, se kterou lze snadno obchodovat. Mohou mít mnoho různých podob, například papírové bankovky, kovové mince a elektronické platby. Peníze obvykle vydávají a kontrolují vlády nebo jiné orgány, ale peníze jsou mnohem víc než jen fyzický nebo digitální prostředek směny; jsou jako univerzální jazyk, který nám umožňuje komunikovat s lidmi na celém světě, i když nemluvíme stejným jazykem nebo nemáme stejnou kulturu. Můžete být například na druhém konci světa a přesto "mluvit" penězi tím, že položíte výrobek na pult a vyměníte ho za místní měnu nebo tak, že použijete kreditní kartu.

Peníze jsou něco jako smlouva mezi lidmi, která nám umožňuje provádět směnu, aniž bychom se museli spoléhat na výměnný obchod nebo hledat někoho, kdo chce to, co zrovna nabízíme. Kdyby nějaká skupina lidí začala přijímat čokoládu jako platidlo za většinu zboží a služeb, čokoláda by se stala penězi (pokud však uvážíme to, že by se v některých částech světa roztekla, mohli bychom ji pak považovat za špatnou formu peněz).

Jak upozornil francouzský ekonom Jean-Baptiste Say: "Peníze plní ve směně pouze momentální funkci, a když je transakce nakonec uskutečněna, vždy se zjistí, že jedna komodita byla vyměněna za druhou."

Jinými slovy, peníze samy o sobě nemají moc uspokojit naše potřeby; jsou pouze nástrojem, který nám umožňuje směnit jedno zboží za jiné.

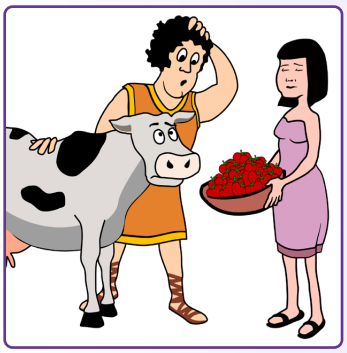
Transakce je směna nebo převod zboží a služeb. Je to způsob výměny hodnot mezi dvěma nebo více stranami.

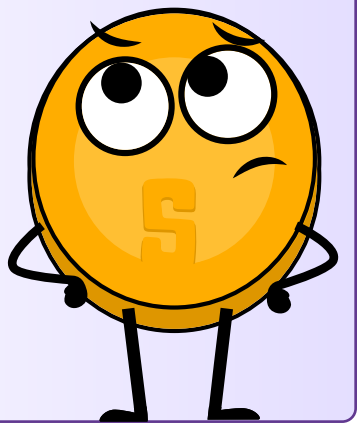
Existuje mnoho různých druhů transakcí, od jednoduchých směn (např. koupě sendviče v lahůdkářství) až po složitější finanční transakce (např. koupě domu nebo investice do akcií či dluhopisů). Transakce mohou být prováděny osobně, po telefonu, online nebo jinými prostředky a může se jich účastnit celá řada stran, včetně jednotlivců, podniků a finančních institucí.

Jak snadný nebo proveditelný by byl tento obchod bez peněz?

Vyměnili byste jednu krávu za 1 000 000 jahod?

Nebo je to 600 000 jahod? Co třeba 50 000?





Mrkněte na toto krátké video!

Peníze **JSOU** hodnotou, **PODLE** které se směňuje zboží.
Peníze **NEJSOU** hodnotou, **ZA** kterou se zboží směňuje.

Pokud to shrneme, tak peníze:

Usnadňují obchod, protože je každý přijímá jako finální platidlo. Umožňují také měřit hodnotu a porovnávat různé zboží a služby. Dále se podíváme na funkce peněz.

Co jsou to peníze?

2.2 Funkce peněz

Při nákupu či prodeji zboží a služeb hrají peníze klíčovou roli. Peníze by měly plnit ve světě několik důležitých funkcí, např:

1 Uchovatel hodnoty

Peníze by si měly udržet svou hodnotu v čase, díky čemuž jsou užitečné jako metoda spoření a investování hodnoty lidské energie. Lidé tak mohou peníze používat k plánování budoucnosti a k tomu aby mohli poskytovat půjčky nebo si sami půjčovali peníze. Až si tedy budete příště šetřit na něco mimořádného, vzpomeňte si, že peníze jsou víc než jen způsob, jak za něco zaplatit - jsou nástrojem, který vám pomůže plánovat a investovat do budoucnosti.

Jaký je váš uchovatel hodnoty?		BTC (USD)	Zlato (USD)	USD (EUR)
	Březen 14, 2019	$3,846	$1,293	€0.8817
	Březen 14, 2020	$5,258	$1,529	€0.90056
	Zisk/ztráta	+36.71%	+18.25%	+2.14%

2 Prostředek směny

S penězi nemusíte hledat někoho, kdo by chtěl přesně to, co chcete směnit vy. Místo toho můžete za peníze nakupovat a prodávat cokoliv, co potřebujete. Díky tomu je obchodování mnohem pohodlnější a efektivnější.

3 Účetní jednotka

Peníze představují univerzální měřítko hodnoty, které lidem nabízí možnost vyjádřit a porovnat cenu různého zboží a služeb. To umožňuje efektivnější a transparentnější trh, díky němuž mohou lidé dělat informovaná rozhodnutí o tom, co koupit a prodat.

Účetní jednotka

Spotřebitelé znají hodnotu věci, když jí přiřadíte cenu (peněžní hodnotu).

Představte si to takto: pokud byste si chtěli koupit nové auto, mohli byste porovnat ceny u různých prodejců a na základě ceny v korunách se informovaně rozhodnout, které si koupíte. Bez zúčtovací jednotky byste se museli pokusit porovnat hodnotu jednotlivých aut pomocí něčeho jiného, jako například počtem krav, nebo třeba doby, za kterou bylo vyrobeno auto.

Právě tyto tři funkce umožňují, aby se ekonomika stala komplexní a dynamickou. Bez peněz by bylo mnohem obtížnější nakupovat a prodávat zboží a služby a naše ekonomika by byla mnohem méně vyspělá.

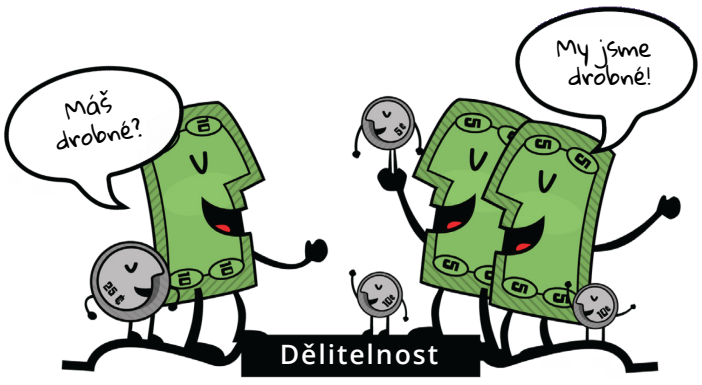
Třídní procvičování: Jaká funkce peněz je na tomto příkladu znázorněna?

- Evan se rozhodl ušetřit část své týdenní výplaty na koupi štěněte.
- Adam si v pizzerii koupí dva kousky pizzy za 80 Kč.
- Marek se nemůže rozhodnout, zda si koupí lístek na koncert za 1600 Kč, nebo si koupí lyžařský skipas za 2000 Kč.

2.3 Vlastnosti peněz

Postupem času si lidé nakonec uvědomili, že dobré peníze musí mít určité vlastnosti, aby mohly být účinným prostředkem směny. Mezi tyto vlastnosti patří trvanlivost (odolnost), dělitelnost, přenositelnost, akceptovatelnost, vzácnost a zaměnitelnost.

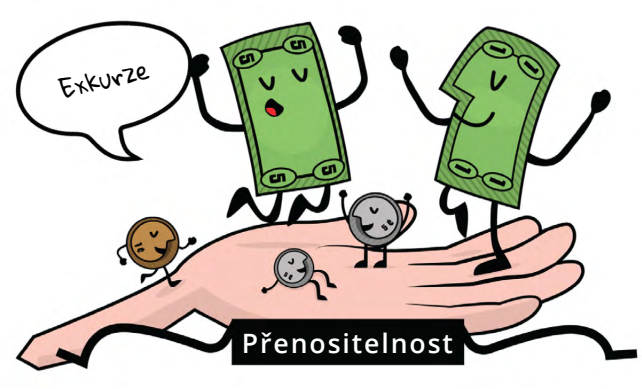
- **Odolnost** označuje schopnost peněz odolávat fyzickému poškození a vydržet po určitou dobu. To zajišťuje, že peníze mohou obíhat v ekonomice v přijatelném a rozpoznatelném stavu. Zlato je trvanlivý materiál, který odolává opotřebení, takže dobře reprezentuje charakteristiku trvanlivosti peněz.
- **Dělitelnost** označuje schopnost peněz rozdělit se na menší jednotky, aby je lidé mohli používat k nákupům v různých částkách. Papírové bankovky lze většinou snadno rozdělit na menší nominální hodnoty, ať už na jiné papírové bankovky či mince, což z nich činí vhodného zástupce vlastnosti dělitelnosti peněz.

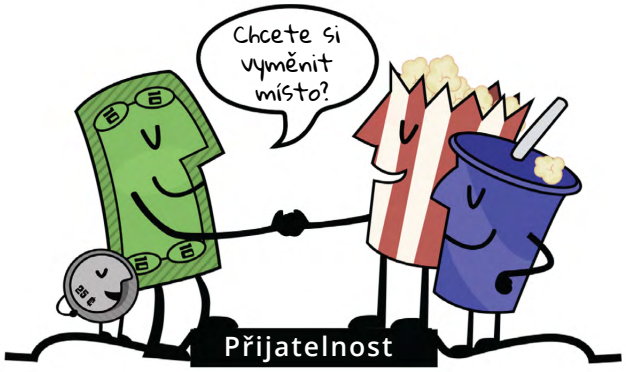


Co jsou to peníze?

Přenositelnost znamená jednoduchost, s jakou lze peníze přepravovat a přenášet. To umožňuje lidem bez problémů používat peníze k nákupu a prodeji zboží a služeb. Kreditní karty jsou přenosné, protože je lze snadno přenášet v peněžence nebo kabelce, což z nich dělá vhodného zástupce vlastnosti přenositelnosti peněz.

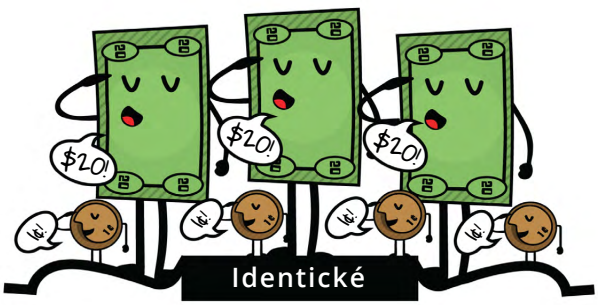
Akceptovatelnost se týká všeobecného přijetí peněz jako způsobu platby, aby je lidé mohli s důvěrou používat k nákupu a prodeji zboží a služeb. Americký dolar je široce přijímán jako platidlo, takže dobře reprezentuje charakteristiku přijatelnosti peněz.





Vzácnost se týká omezené nabídky peněz, která pomáhá udržet jejich hodnotu a zabraňuje tak tomu, abychom v budoucnu museli utrácet více peněz na nákup stejného množství zboží. Sběratelské známky, zejména vzácné a cenné, mohou být dobrou formou peněz, protože je jich málo a jejich hodnota se může v průběhu času zvyšovat. Sběratelé známek často používají své známky jako způsob, jak investovat své bohatství a diverzifikovat své portfolio. Zkrátka peníze musí být vzácné a zároveň musí být obtížné je získat. Například u zlata musíme vynaložit určité úsílí (práci) na jeho vytěžení a jeho celkové množství je omezené.

Zaměnitelnost znamená možnost výměny peněz tak, že jedna peněžní jednotka je ekvivalentní jiné jednotce stejné hodnoty. Peníze by měly být identické. Stejné mince mají jednotnou velikost a hmotnost, takže dobře reprezentují charakteristiku stejnorodosti peněz. Jedna koruna je vždy jedna koruna.



Celkově lze říci, že díky těmto vlastnostem jsou peníze užitečným a účinným nástrojem pro usnadnění obchodu a podnikání, a tak mají zásadní význam pro rozvoj a stabilitu ekonomiky.

Třídní cvičení

Různé druhy aktiv mají různé vlastnosti a plní tak odlišné funkce peněz. Společnost nakonec rozhoduje o tom, které aktivum se bude používat jako peníze, na základě faktorů, jako je jeho odolnost, vzácnost, dělitelnost, přenositelnost a přijetí jako prostředku směny.

Chcete-li zjistit, jak dobře jednotlivé položky splňují konkrétní charakteristiky peněz, můžete každou položku ohodnotit na stupnici od **1 do 5** pro každou charakteristiku. Sečtením bodového hodnocení jednotlivých položek můžete určit, která z nich se nejlépe hodí jako forma peněz.

[0 = Nedostečně, 3 = Dobře, 5 = Výborně]

*** Sloupec pro Bitcoin nevyplňujte, vrátíme se k němu později v průběhu kurzu.**

Následující otázky vám pomohou určit, jak dobře jednotlivé položky v tabulce splňují vlastnosti peněz.

- **Odolnost:** Odolávají peníze dlouhodobému opotřebení v čase a prostoru?
- **Přenositelnost:** Lze peníze snadno přepravovat a používat na různých místech?
- **Zaměnitelnost:** Jsou peníze zaměnitelné s jinými formami peněz?
- **Akceptovatelnost:** Jsou peníze široce přijímány jako platidlo?
- **Vzácnost:** Jsou peníze vzácné, tzn. je jich omezené množství?
- **Dělitelnost:** Lze peníze rozdělit na menší jednotky pro provádění transakcí?

Vlastnosti kvalitních peněz	Krávy	Cigarety	Diamanty	Eura	Bitcoin
Odolnost					
Přenositelnost					
Zaměnitelsnost					
Akceptovatelnost					
Vzácnost					
Dělitelnost					
Celkem					

Co jsou to peníze?

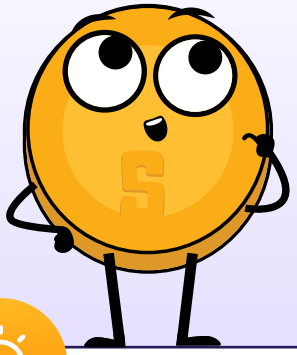
2.4 Druhy peněz

Peníze lze rozdělit do dvou hlavních kategorií: fyzické a digitální.

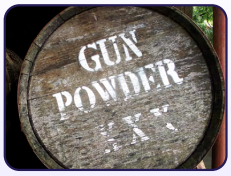
Fyzické peníze zahrnují:

- Fiat peníze, což jsou papírové bankovky a mince vydávané vládami, které jsou akceptovány jako prostředek směny.
- Reprezentativní peníze, které představují pohledávku na určitý fyzický statek.
- Komoditní peníze, což je fyzický předmět, který má vnitřní hodnotu a je široce přijímán jako prostředek směny. Například zlato a stříbro.

Ne všechny peníze jsou stejné!



Komoditní peníze



Vynález, jako byl střelný prach kdysi sloužil jako komoditní peníze.

Reprezentativní peníze

Reprezentativní peníze, jako tento stříbrný certifikát byl směnitelný za fyzické stříbro.

Fiat peníze

Dnes jsou bankovky federálních rezerv, známé jako Fiat peníze, dané zákonem a jsou to peníze s nuceným oběhem, pomocí kterých platíme daně.

Digitální měny mohou být na druhou stranu použity pro online transakce a patří sem elektronické měny, Stablecoiny a kryptoměny.

Elektronické měny jsou digitální verzí klasických peněz, jako je koruna, dolar, euro a mohou být používány na nákup a prodej věcí online pomocí digitálních **platebních bran.**

Platební brány jsou infrastrukturou, která umožňuje pohyb elektronických měn a jiných digitálních aktiv z jednoho místa na druhé. Nicméně v tradičním finančním systému vždy existuje prostředník, například banka nebo finanční instituce, která si účtuje poplatky a má pravomoc přijímat, blokovat, vracet nebo pozastavovat transakce.

Ve zprostředkovaném finančním systému patří mezi hlavní typy digitálních plateb síť debetních a kreditních karet, které usnadňují převod peněžních prostředků mezi finančními institucemi a obchodníky. Jsou to v podstatě online účty, které uživatelům umožňují uchovávat a spravovat jejich elektronické peníze a provádět platby převodem peněžních prostředků z jejich účtu na účet příjemce.

Digitální měny centrálních bank (CBDC):

jsou pouze digitální verzí fiat měny dané země, kterou vydává a zaštiťuje centrální banka prostřednictvím vlády. CBDC nejsou kryptoměny jelikož jsou řízeny centrální autoritou a nemají decentralizovanou platební síť.

Stablecoiny

jsou digitální měny, které jsou navrženy tak, aby udržovaly stabilní hodnotu ve vztahu k aktivu, kterým jsou podloženy. Například americký dolar.

Kryptoměny

jsou opět pouze digitální měny. Některé kryptoměny jsou decentralizované a řídí se určitými pravidly, zatímco jiné jsou centralizované a řídí je malá skupina lidí.

Měna, která funguje bez zprostředkovatelů, je v konečném důsledku efektivnější a pro společnost prospěšnější, protože zabraňuje několika jednotlivcům ovládat peněžní zásobu a možnost centralizovat svou moc. Ovšem vytvořit měnu, která by umožňovala bezpečné transakce, aniž by se spoléhala na důvěru mezi stranami, bylo vždy v historii obtížné. Aby toho bylo možné dosáhnout, je třeba vytvořit měnu, která bude fungovat podobně jako internet, a kde je kontrola rozložena mezi všechny a zároveň nikoho. To vyžaduje souhlas všech stran, včetně těch, které mají moc, vzdát se kontroly ve prospěch vyššího dobra.

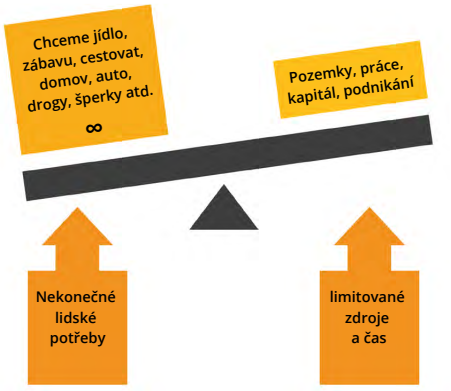
2.5 Psychologie peněz: vzácnost, časové preference a kompromisy

Představte si, že jste se ztratili v poušti a máte už jen jednu láhev vody. Máte žízeň a zoufale se chcete napít, ale zároveň víte, že vodu budete potřebovat k přežití, dokud nenajdete další. Toto je klasický příklad vzácnosti - máte k dispozici pouze omezené množství zdroje (vody) a musíte se rozhodnout, jak ho využijete. V této situaci se můžete rozhodnout tak, že ji budete dávkovat po malých doušcích po delší dobu, aby vám vydržela co nejdéle.

Co jsou to peníze?

Vzácnost nás nutí zvažovat výhody a nevýhody používání svých zdrojů a hledat tak kompromisy.

Případně se můžete rozhodnout, že vypijete co nejvíce vody najednou, a doufat, že vám příval hydratace dodá energii, kterou potřebujete k nalezení další vody. Ať už se rozhodnete jakkoli, stojíte před těžkým rozhodnutím. V takovém případě se rozhodujete mezi okamžitým ukojením žízně a uchováním vody na později. Tento koncept vzácnosti se vztahuje na všechny druhy zdrojů, nejen na vodu. Ať už se jedná o peníze, čas, nebo dokonce lásku a pozornost, neustále stojíme před volbou, jak rozdělit naše omezené zdroje.



Existují dva typy vzácnosti: Vytvořena člověkem a přírodní vzácnost.

- Lidmi vytvořená vzácnost, známá také jako centralizovaná vzácnost, zahrnuje například limitované edice značkových tašek, vzácné sportovní kartičky a očíslovaná umělecká díla. Ty lze snadno napodobit nebo padělat.
- Přírodní vzácnost, známá také jako decentralizovaná vzácnost, zahrnuje věci jako například sůl, mušle nebo drahé kovy jako zlato. Ty je obtížnější replikovat nebo padělat. Hlavním rozdílem mezi nimi je kontrola.

Centralizovaná vzácnost je pod kontrolou jednoho subjektu, například firmy nebo vlády, zatímco decentralizovaná vzácnost není pod kontrolou nikoho. Příkladem centralizované vzácnosti, která nepřiměřeně postihuje chudé, je kontrola základních zdrojů, jako je čistá voda. V některých regionech je přístup k čisté vodě řízen soukromými společnostmi nebo vládními subjekty, které mohou omezovat její distribuci, což vede k nedostatku tohoto životně důležitého zdroje. Tato centralizovaná kontrola může vést ke zvýšení cen nebo nerovnoprávnému přístupu k čisté vodě, přičemž chudé komunity často pociťují největší dopady. Omezený přístup k čisté vodě má vliv nejen na jejich zdraví a blahobyt, ale také udržuje chudobu, protože lidé mohou být nuceni platit vyšší ceny za vodu nebo musí cestovat na velké vzdálenosti, aby ji získali.

Vzácnost ovlivňuje naše rozhodnutí. Její pochopení tak nakonec může zlepšit naše rozhodování. Často musíme volit mezi okamžitým ziskem nebo dlouhodobým přínosem a tyto kompromisy určují naši cestu k dosažení cílů.

Vysoká Časová preference se týká myšlenky, kdy lidé obecně dávají přednost tomu, aby něco měli raději TEĎ než později.

Příklad časové preference:

Řekněme, že máte možnost získat 1000 Kč dnes nebo 1100 Kč za rok. Pokud máte vysoké časové preference, nejspíš se rozhodnete obdržet 1000 Kč dnes, protože si více ceníte toho, že máte peníze nyní, a nechcete čekat na dalších 100 Kč další rok. Na druhou stranu, pokud máte nízkou časovou preferenci, raději si počkáte na větší odměnu, protože se více zaměřujete na dlouhodobé plánování a méně vás zajímá okamžité uspokojení.

Aktivita: Časová preference

Vysoká časová preference vs. nízká časová preference

1. Poslechněte si učitelův výklad o výběru bonbónů.
2. Rozhodněte se, zda chcete dostat malý bonbón hned, nebo zda počkáte do konce hodiny a dostanete bonbóny dva. Nebo větší, žádanější bonbón.
3. Zavažte se ke svému rozhodnutí a oznamte učiteli svou volbu. Na základě svého rozhodnutí obdržíte bonbón buď ihned, nebo na konci hodiny.
4. Zapojte se do diskuse o této aktivitě ve třídě a zamyslete se nad svým rozhodovacím procesem a konceptem časové preference.

Závěr a diskuse:

- Jaké faktory ovlivnily vaše rozhodnutí vzít si sladkost teď, nebo počkat na větší odměnu později?
- Jak se cítíte ve svém rozhodnutí nyní, když je aktivita u konce?
- Napadají vás příklady z reálného života, kdy může být vysoká časová preference škodlivá a kdy může být nízká časová preference prospěšná?
- Jaké jsou možné důsledky volby vysoké časové preference před nízkou časovou preferencí?

V kontextu příkladu s pouští to znamená, že byste mohli mít větší tendenci vypít všechnu vodu hned, i když to znamená, že vám žádná nezbyde na později. Je to proto, že žízeň, kterou cítíte právě teď, je naléhavější než potenciální žízeň, kterou byste mohli pocítit v budoucnu.

Na druhou stranu, pokud se rozhodnete vodu dávkovat a pít ji pomalu v průběhu času, projevujete nižší časovou preferenci. To znamená, že jste ochotni počkat, abyste ukojili svou žízeň a zvýšili tak své šance na přežití. Koncept nákladů obětovaných příležitostí úzce souvisí s myšlenkou nedostatku a časové preference.

Co jsou to peníze?

Náklady obětovaných příležitostí označují hodnotu další nejlepší alternativy, které se při rozhodování vzdáte. **Každé rozhodnutí je spojeno s kompromisy.**

Dnešní volba	nyní	později
	  	  
Koupě jahodového smoothie za 100 Kč	Utratit 100 Kč jinak	těžit z výhod pravidelného spoření 100 Kč

V příkladu s pouští jsou náklady obětovaných příležitostí za okamžité vypití vody přínosem pro přežití oproti výhodám, které byste jinak získali, kdybyste vodu rozdělili na příděly a používali ji na delší dobu.

Řekněme, že se rozhodnete vodu dávkovat a užívat ji po malých doušcích po delší dobu. Výsledkem je, že máte energii a hydrataci, kterou potřebujete k hledání další vody. Při hledání narazíte na kaktus, který má v sobě malé množství vody. Není to mnoho, ale na zažehnání žízně to pro tuto chvíli stačí. Kdybyste se rozhodli vypít všechnu vodu najednou, možná byste neměli energii na hledání další vody a na kaktus byste nenarazili.

Tento příklad ilustruje, že náklady obětované příležitosti zahrnují nejen okamžitý kompromis mezi dvěma možnostmi, ale také potenciální budoucí příležitosti, které můžeme získat nebo ztratit v důsledku našich rozhodnutí.

Naše ochota vzdát se větší odměny v budoucnu výměnou za menší odměnu nyní je ovlivněna naší časovou preferencí neboli tím, nakolik si ceníme okamžitého uspokojení oproti dlouhodobému plánování.

V této kapitole jsme se zabývali základním konceptem peněz. Pokryli jsme definici peněz, jejich funkce, vlastnosti a různé formy peněz. Podstatným aspektem naší diskuse bylo pochopení psychologie peněz se zaměřením na pojmy jako vzácnost, časová preference a kompromisy. Toto zkoumání poskytlo základ pro pochopení složité povahy peněz a jejich role v našem životě. V další kapitole si povíme o historii peněz a o tom, jak se v průběhu času vyvíjely.

Kapitola 3

Historie peněz

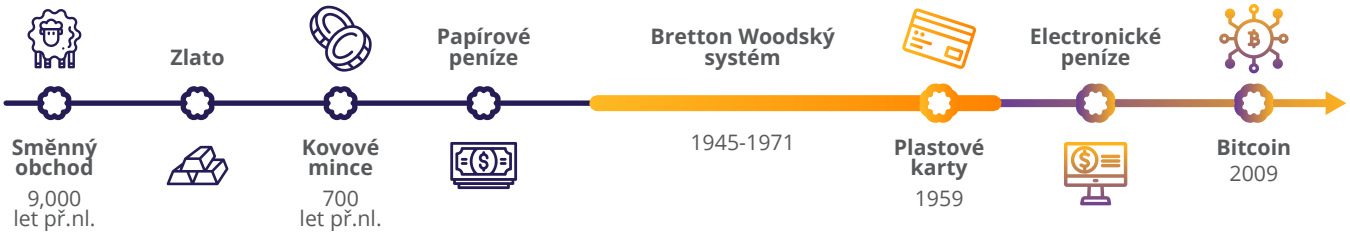
Pracovní sešit

český překlad | 2024

Historie peněz

3.0 Úvod

> Peníze se nevyvinuly náhodně, ale vznikly na základě tržního procesu. Nevytvořily je vlády. Vznikly v průběhu času jako spontánní řád.
>
> **Murray Rothbard**



Představte si dávnou minulost, kdy lidé neměli mince ani papírové bankovky, které používáme dnes. Tehdy však existoval takový způsob obchodování, kdy se jako platidlo používaly například mušle nebo drahé kovy (zlato). Může to znít divně, ale byly to tehdy varianty peněz, na kterých se vetšina obyvatel v komunitě shodla, že mají hodnotu. V této kapitole se vydáme na cestu časem a seznámíme se s vývojem peněz. Budeme sledovat jejich původ a také to, jak se v průběhu dějin měnily a přizpůsobovaly.

Aktivita: Třídní úloha - Hra na směnný obchod

Učitel vám dal kousek papíru. Vaším úkolem je vyměnit to, co "máte", za to, co "chcete". Na horní stranu papíru napište malým čitelným písmem své jméno.

Kolo #1: Barter

Píše se rok 6000 př. n. l. a netřeba dodávat, že peníze, jak je známe, ještě nebyly vynalezeny. Nacházíte se v Mezopotámii a vzájemně si s ostatními účastníky směňujete zboží a služby prostřednictvím **barteru**.

> Pro doplnění je třeba uvést, že mnoho podniků na světě stále přijímá za své zboží a služby nepeněžní platby a vlády tyto směnné transakce považují za stejné jako transakce v lokální měně.

List papíru rozstřihněte v místě přerušované čáry. Vaším úkolem je vyměnit co nejvíc toho co "mám", abyste nakonec získali své původní "chci". Své původní "chci" nemůžete změnit. Na splnění cíle tohoto cvičení budete mít 5 minut.

Až se váš nový papírek s tím co "máte", bude shodovat s vaším původním záměrem"chtěl jsem", vraťte se na své místo. Pokud jste po uplynutí této doby nenašli nikoho, kdo by vám papírek vyměnil, vraťte se na své místo.

Zvedněte ruku, pokud se vám podařilo získat to, co jste chtěli, po jedné výměně. Po dvou? Po třech?

Odpovězte stručně, ale zároveň smysluplně na následující otázky.

1. Proč se některým z vás podařilo vyměnit to, co jste chtěli a jiným ne?

2. Jaké jsou výhody směnného obchodu?

3. Jaké jsou nevýhody směnného obchodu na základě vašich zkušeností s tímto cvičením?

Kolo #2: Komoditní peníze

Přesuňme se na západní pobřeží Afriky někdy kolem 14. století před naším letopočtem. Směnný obchod se stal obtížným a neefektivním. Jako civilizace jsme se vyvinuli a nyní používáme **komoditní peníze.**

Od Kauri mušlí až po mince

1300 let př.n.l.

1000 let př.n.l.

687 let př.n.l.

Tento prototyp mincí měl oválný tvar, byl vyroben z "elektra" (slitina zlata a stříbra) a měly vzor pouze na jedné straně.

1300 let př.nl.
Mušle Kauri jsou převládajícím platidlem ve většině Asie, Afriky, Oceánie a některých částí Evropy.

1000 let př.nl.
Čínská dynastie Západní Čou začíná používat kovové mince.

687 let př.nl.
král Lýdie Alyattes (dnešní Turecko) nařizuje ražbu prvních kovových mincí v západním světě.

Zajímavý fakt
Mušle Kauri se dokonce používaly jako zákonné platidlo v některých částech Afriky až do 20. Století našeho letopočtu.

Historie peněz

Učitel vám dal jeden kus těstoviny (pro zjednodušení). Dejme tomu, že podle dohody je cena každého zboží právě jeden kus těstoviny.

Vaším cílem je opět získat to, co "chcete". Nyní však lidstvo mírně zmoudřelo a našlo způsob, jak určité problémy řešit.

- Proč považujeme těstoviny za komoditní peníze?
- Jak získáme věci, které nyní chceme?
- Bylo kolo s těstovinami jednodušší?
- Proč podle vás peníze nahradily komodity?
- V čem je používání komoditních peněz efektivnější než směnný obchod?
- Jaké jsou nevýhody používání těstovin jako peněz?
- Co myslíte, že se stalo, když Španělsko začalo do vaší komunity dovážet lodě plné těstovin (nebo zlato a stříbro z Ameriky zpět do Španělska)?

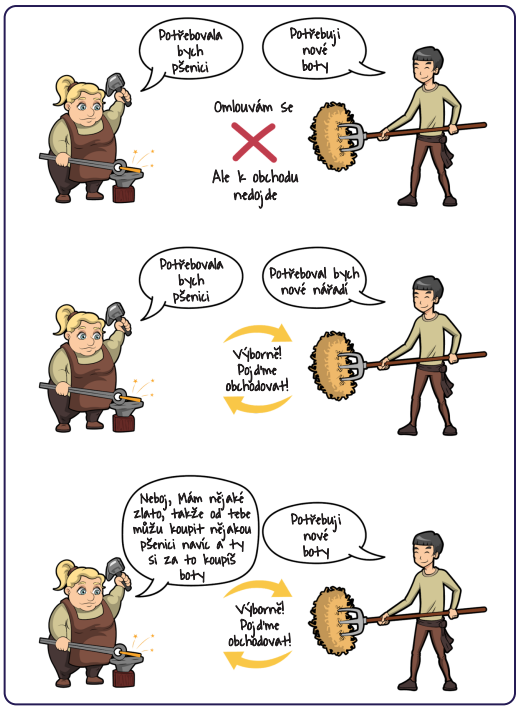
3.1 Vývoj od směnného obchodu k moderním penězům

3.1.1 Problémy s ranými formami peněz

Shlédněte toto krátké video a zjistěte více o počátcích směnného obchodu v sérii ,,Historie papírových peněz”

V barterové ekonomice mezi sebou lidé obchodují na základě relativní hodnoty zboží a služeb, které nabízejí. Barterová ekonomika je neefektivní a může být obtížné ji řídit, zejména ve složitých společnostech.

Situace, jako je **,,dvojí shoda potřeb”**, je nezbytná v každém směnném systému, protože lidé musí vždy najít někoho, kdo má to, co chtějí, ale také najít toho, kdo přijme jejich nabídku výměnou.



Dejme tomu, že:

- Josef chce vyměnit své banány za kokosový ořech od Jany.
- Jana však chce vyměnit svůj kokos pouze za Tomovo mango.
- A Tom chce vyměnit své mango pouze za Josefovy banány.
- Uvízli v nekonečném koloběhu výměny ovoce bez dvojí shody potřeb.
- Josef navrhne, že si svoje ovoce výmění za láhev coly, ale pak si uvědomí, že jsou na odlehlém ostrově a žádná cola zde není.
- Rozhodnou se tedy , že si prostě sednou na pláž a v tichosti si vychutnají každý své ovoce.

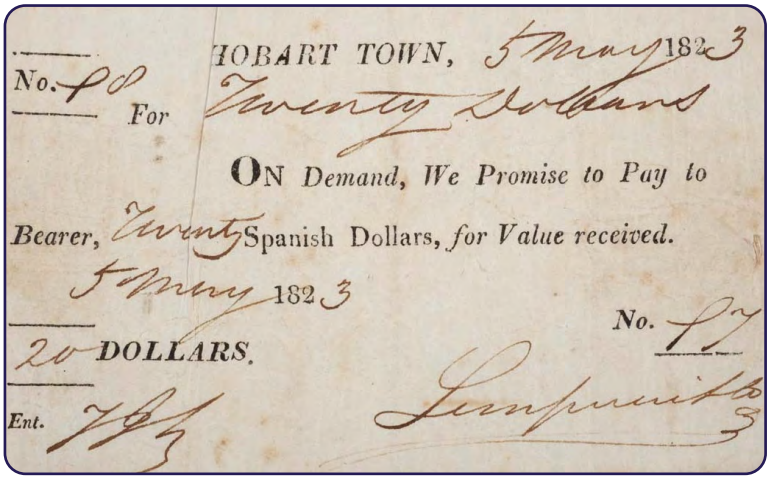
Toto je druhá epizoda s názvem „Nejenom nudle" ze série „Historie papírových peněz"

3.1.2 Vývoj mincí a papírových peněz

Jakmile se vy a vaše komunita více zapojujete do obchodování, uvědomíte si omezení v používání směnného obchodu a jiných nepeněžních forem. Proto se rozhodnete používat kovové mince jako formu peněz.

Komoditní peníze jsou takové peníze, které se vyrábějí z drahých kovů, jako je zlato a stříbro. Ty se historicky používaly jako uchovatel hodnoty, prostředek směny a v dávné minulosti i jako účetní jednotka.

Historie peněz



Nicméně jakmile začnete kovové mince používat častěji, narazíte na některé nevýhody. Mohou být těžké a nevhodné při velkých transakcích a navíc si všimnete, že někteří lidé (panovníci) zneužívají systém tím, že mince taví a vytvářejí nové mince tím, že je smíchají s levnějšími kovy. To způsobuje růst cen a narušuje důvěru v systém jako takový.

Ve snaze řešit tyto problémy začnete vy a vaše komunita používat papírové poukázky jako formu peněz. Tyto papírové stvrzenky, které mají svůj původ ve staré Číně, jsou pohodlnou a snadno směnitelnou formou peněz. Jsou kryté zlatem a dalšími cennými kovy a například v průběhu sedmnáctého až devatenáctého století je bylo možné plně za tyto kovy směnit. To umožnilo mít přenosnější a snadno převoditelnou formu peněz, přičemž hodnota a bezpečnost drahých kovů zůstala zachována.

3.1.3 Přechod od kvalitních k nekvalitním penězům

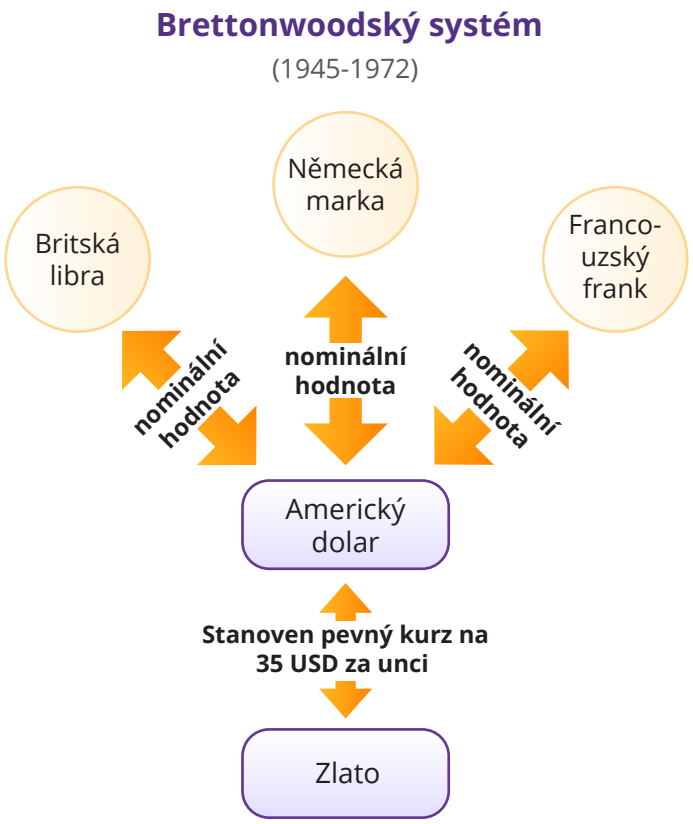
Přesuneme se do 17. století ve Švédsku. Nyní jste zcela závislí na bankách, které uchovávají váš cenný majetek. Začínáte si však všímat, že se děje něco podezřelého. Zdá se, že banky vydávají více papírových poukázek, než kolik mají ve skutečnosti zlata, což jim umožňuje vytvářet více peněz, než mají prostředků na jejich krytí. Tato záludná praktika umožňuje bankéřům vydělávat na rozdílu mezi hodnotou papírových stvrzenek a hodnotou zlata, které drží pro své klienty.

Co se stane, když se pokusíte aplikovat princip papírových peněz v praxi? To se dozvíte ve čtvrtém díle seriálu "Historie papírových peněz".

Uvědomujete si, že to znamená zásadní změnu ve fungování peněz. Přecházíte od systému "zdravých peněz" (tj. peněz krytých drahými kovy) k systému "nekvalitních peněz" (tj. fiat měny, které nejsou kryté žádnou fyzickou komoditou). K tomuto přechodu nedošlo ze dne na den, ale jednalo se o postupný proces ovlivněný několika faktory. Svou roli sehrála průmyslová revoluce s masovou výrobou a urbanizací, stejně jako růst vyspělých finančních systémů, jako jsou banky a akciové trhy. Vznik centrálních bank a dalších finančních institucí přispěl k centralizaci či kontrole peněz, což vedlo k tištění více fiat měn na podporu hospodářského růstu.

Zároveň se však začínají projevovat i **záporné stránky této centralizace**, jako je nezodpovědná spotřeba, **nárůst zadlužení** a manipulace prostřednictvím ekonomických incentiv (motivací) jednotlivců.

Až do první světové války jste mohli své papírové peníze vyměnit za předem stanovené množství zlata. Dvě světové války a hospodářská krize v roce 1929 tento systém ukončily. V roce 1944 byla podepsána Brettonwoodská dohoda, která ustanovila americký dolar jako světovou rezervní měnu a stanovila hodnotu amerického dolaru na cenu zlata ve výši 35 dolarů za unci. Měny ostatních zemí byly na dolar navázány, což pomáhá stabilizovat mezinárodní obchod a finanční trhy.



Bohužel koncem 60. let se tento systém začal hroutit, jelikož USA tiskla více dolarů, než ve skutečnosti měla zlata. Tento čin vedl k takzvanému "Nixonovu šoku" v roce 1971, kdy americká vláda pozastavila směnitelnost dolaru za zlato. To znamenalo konec zlatého standardu a začátek světa poháněného dluhem, který se neustále zvyšuje.

Při každodenním způsobu života si začnete všímat, že hodnota peněz už není zdaleka tak stabilní jako dřív. Stejně jako gumové pravítko, které se dá roztáhnout a smrštit, komplikuje přesné měření délky stolu, fungování ve společnosti s fiat měnou může také ztěžovat přesné měření hodnoty zboží a služeb. Panují obavy a nejistota do budoucna, jelikož se musíte přizpůsobit světu, kde hodnota peněz již není vázána na fyzickou komoditu, jako je například zlato.

Když vidíte dopady této změny na globální ekonomiku, začnete pochybovat o stabilitě a spolehlivosti fiat měn. Uvědomíte si, že v tomto moderním světě již dolar není pevně daný a konzistentní, jako tomu bylo v době, kdy byl vázán na zlato. Ba naopak, začíná podléhat neustálému poklesu kupní síly, a proto je obtížnější používat dolar jako účetní jednotku, protože jeho hodnotu ovlivňují různé faktory včetně inflace (růstu cen), úrokových sazeb, síly ekonomiky dané země, politických událostí, spekulací na trhu a poptávky v mezinárodním obchodě. Může to být matoucí a nepředvídatelné období, kdy se snažíte orientovat v neustále se měnící hodnotě dolaru a jeho dopadu na váš každodenní život.

Navzdory snahám o zlepšení kvality života prostřednictvím moderních peněžních systémů, zvýšení efektivity, lepšího přístupu k informacím a zlepšení komunikace, se životní úroveň většiny lidí začíná snižovat v důsledku:

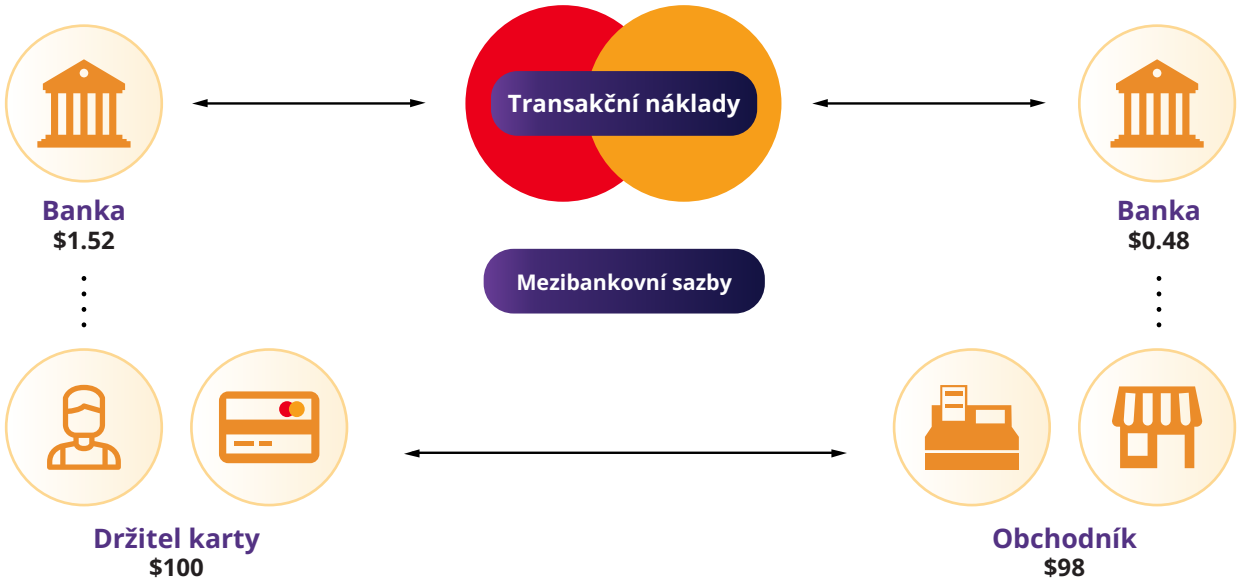
- zneužívání centralizace
- růst cen
- stagnace reálných mezd
- oslabování měn
- nezbytnost utrácet více peněz za méně věcí

To představuje problém pro osoby s nižšími příjmy, které mohou mít omezený přístup ke vzdělání, úvěrům, finančním prostředkům, sociálním sítím a politickému zastoupení. To může následně vést k jejich potenciálnímu znevýhodnění při dosahování úspěchů.

V důsledku toho se zdá, že bohatí stále bohatnou a chudí stále chudnou.

3.1.4 Od papíru k plastu

Od zavedení první kreditní karty v 50. letech minulého století jsme dnes ušli dlouhou cestu. Jednoduchým pohybem plastové karty si můžeme koupit cokoliv chceme, kdykoli chceme, a to bez jakýchkoli potíží. Je to jako kdyby se nám otevřel svět nekonečných možností a vše máme nyní na dosah ruky... nebo jsme si to alespoň mysleli. Netušili jsme, že naše závislost na úvěrech bude mít bolestivé následky - například zvýšení celkových cen zboží a podněcování určité ekonomiky, která je odsouzena ke krachu.



S rozvojem technologií se mění i způsob, jakým nakládáme s penězi. Internet se stává významným hráčem ve světě financí, protože internetové bankovnictví a webové stránky e-shopů umožňují spravovat a utrácet peníze výhradně online.

Nástup digitálních peněz představuje další významný skok v tomto vývoji, který nabízí nové možnosti a mění způsob, jakým provádíme finanční transakce.

3.2 Digitální měny

Digitální měny na rozdíl od těch tradičních existují výhradně v elektronické podobě. Jsou uloženy a směňovány pomocí počítačů a speciálního softwaru.

Digitální měna umožňuje jednotlivcům posílat své peníze prostřednictvím internetu. Podobně jako nám e-mail umožňuje posílat zprávy okamžitě a bez nákladů na poštovné, digitální měny nám umožňují posílat a přijímat prostředky okamžitě a většinou s velmi malými náklady.

Měny, které dnes používáme, jsou stále více digitální. Pouze malá část (pár procent) peněžní zásoby skutečně existuje ve formě mincí a papírových bankovek. Banky poskytují svým uživatelům aplikace pro snadnou výměnu peněz přes internet. Odkud se však peníze berou?

V této kapitole jsme byli svědky přechodu od kvalitních peněz, které představovalo zlato, k nekvalitním penězům v podobě papírových a nyní i digitálních fiat měn. V příští kapitole prozkoumáme, jak současný peněžní systém funguje a jak vůbec vznikl.

Kapitola 4

Co jsou to fiat měny a kdo je ovládá?

Pracovní sešit

český překlad | 2024

Co jsou to fiat měny a kdo je ovládá?

4.0 Úvod

> Dějiny lidstva jsou dějinami peněz, které ztrácejí hodnotu.
>
> **Milton Friedman**

V předchozí kapitole jsme si ukázali, jak se peníze v průběhu času vyvíjely a jak náš peněžní systém přešel od kvalitních peněz k nekvalitním, čímž se utvářel svět, ve kterém dnes žijeme. Tato kapitola se hlouběji věnuje tomu, jak tento vývoj vedl k dnešnímu fiat systému a jak tento systém funguje.

Jak tedy tento fiat systém funguje a proč vznikl?

Abychom mohli odpovědět na tuto otázku, musíme se nejprve zaměřit na americký dolar, který je v současnosti světovou rezervní měnou a hraje v dnešním světě dominantní roli. Každá země přímo či nepřímo zažívá dopady rozhodnutí, která se týkají amerického dolaru. Chcete-li skutečně pochopit, jak funguje politika fiat měn ve vaší zemi, je nezbytné odkrýt historické události, které ji spojují s místem zrodu fiat systému - se Spojenými státy americkými.

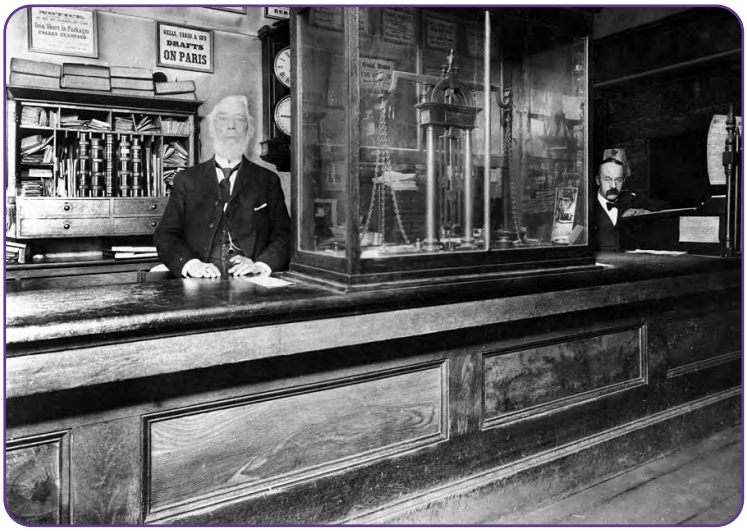
4.1 Stručná historie fiat měn

1815-1933	1913	1933	1934	1944	1971	1980
Zlatý standart	Vznik americké centrální banky zvané ,,FED”	Nařízení 6102. Každý občan byl povinen odevzdat své zlato v poměru 20,67 dolarů za jednu unci.	Zákon o zlatých rezervách. Lidé přišli o část svého bohatství tím, že vláda znehodnotila dolar o 40 % na 35 dolarů za unci zlata.	Brettonwoodská dohoda: Americký dolar se stal dominantní světovou rezervní měnou	,,Nixonův šok", který dal vzniknout fiat systému tím, že ,,dočastně"(do dnes) ukončil směnitelnost amerických dolarů za zlato.	Hodnota zlata vzrostla z 35 dolarů za unci v roce 1970 na 870 dolarů za unci v roce 1980, což způsobilo ztrátu hodnoty peněz lidí o 96 % za pouhých 10 let.

Časová osa

V 19. století se civilizace po celém světě opíraly o pevný peněžní standard a používaly drahé kovy, jako je zlato nebo stříbro a to na základě jejich vzácnosti, trvanlivosti a rozpoznatelnosti. S rozvojem celosvětového obchodu se přeprava velkého množství kovu stala náročnou, což vedlo ke vzniku velkoskladů zlata a stříbra. Tyto sklady bezpečně uchovávaly cenné kovy a poskytovaly papírové certifikáty, které bylo možné vyměnit za určité množství zlata nebo stříbra. Výměnou za uložení svých

peněz obdrželi jednotlivci papírové certifikáty přímo vázané na přesné množství zlata nebo stříbra, které uložili. Toto přímé spojení mezi papírovými certifikáty a hmatatelnými komoditními penězi znamenalo počátek toho, co dnes označujeme jako banky.

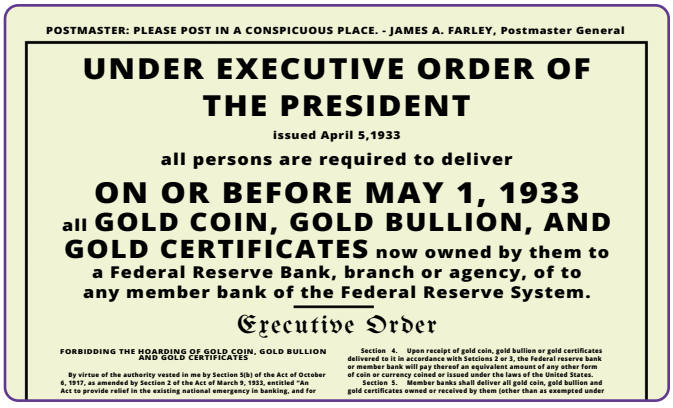


Zpočátku se banky snažily uchovávat peníze klientů, ale netrvalo to dlouho a později se zapojily do riskantních úvěrových praktik a vydávaly certifikáty na zlato, které neměly. Tato praxe představovala hrozbu v podobě aktu, který hovorově označujeme „run na banku". Jedná se o situaci, kdy se více klientů rozhodne vybrat si své prostředky a banka by je tak nebyla schopna všechny vyplatit. Aby banky toto riziko řešily,

začaly spolupracovat s vládami na vytvoření systému legalizujícího úvěrování v případě potřeb. V roce 1913 združení bank vytvořilo Federální rezervní systém, centrální banku odpovědnou za generování nových papírových certifikátů a případnou záchranu bank v problémech. Vlády na celém světě vždy uznávaly hodnotu zlata a stříbra, což vedlo ke konfliktům a válkám o získání nadvlády těchto kovů. V době před druhou světovou válkou se zlata pro strategické účely zmocnili vůdci jako Lenin, Stalin, Churchill, Roosevelt, Mussolini a Hitler.

Na počátku 30. let 20. století došlo ve Spojených státech k významné změně ve formě krytí státní měny. V té době měli lidé velkou část svého majetku právě ve zlatě. V roce 1933 však prezident Roosevelt vydal nařízení č. 6102, které požadovalo, aby se každý občan vzdal svého zlata. Nejednalo se o dobrovolnou výměnu - lidé museli své zlato odevzdat, a pokud odmítli, hrozily jim přísné sankce.

Vláda stanovila směnný kurz na 20,67 dolarů za unci zlata. To znamenalo, že za každou unci zlata, kterou člověk měl, obdržel v bance 20,67 dolarů. Lidé museli tyto papírové dolary přijímat v naději, že je jednoho dne budou moci vyměnit zpět za zlato.



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE. - JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

issued April 5,1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all **GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES** now owned by them to a Federal Reserve Bank, branch or agency, of to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES

By virtue of the authority vested in me by Section 5(b) of the Act of October 6, 1917, as amended by Section 2 of the Act of March 9, 1933, entitled "An Act to provide relief in the existing national emergency in banking, and for

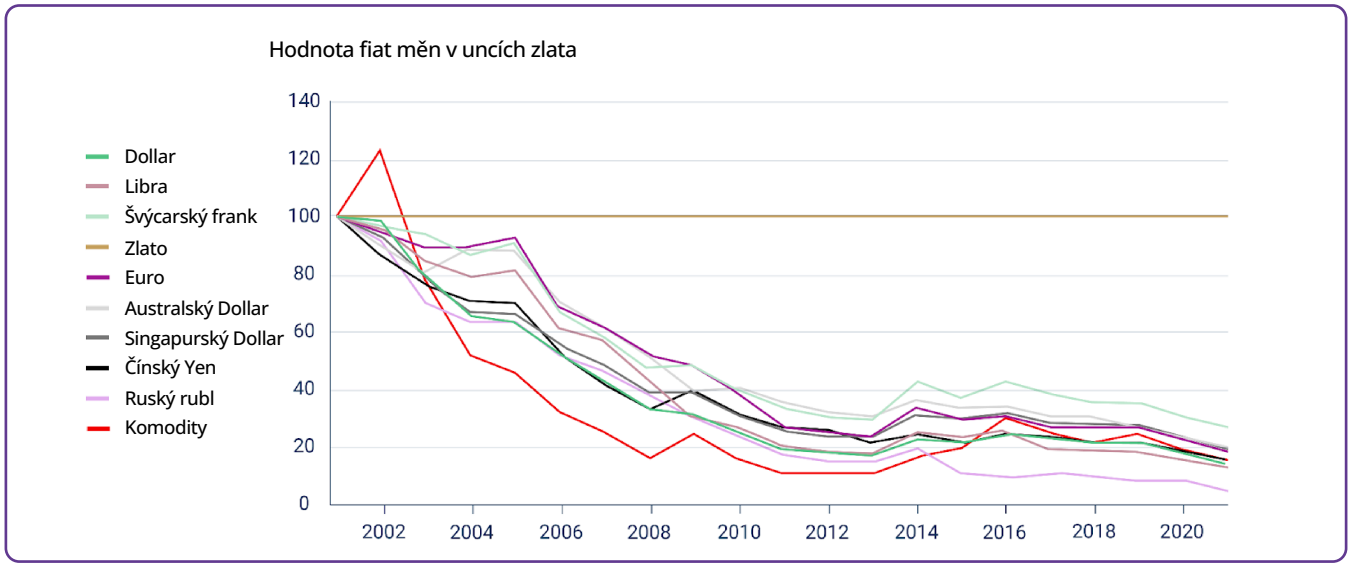
Section 4. Upon receipt of gold coin, gold bullion or gold certificates delivered to it in accordance with Sections 2 or 3, the Federal reserve bank or member bank will pay thereof an equivalent amount of any other form of coin or currency coined or issued under the laws of the United States.

Section 5. Member banks shall deliver all gold coin, gold bullion and gold certificates owned or received by them (other than as exempted under

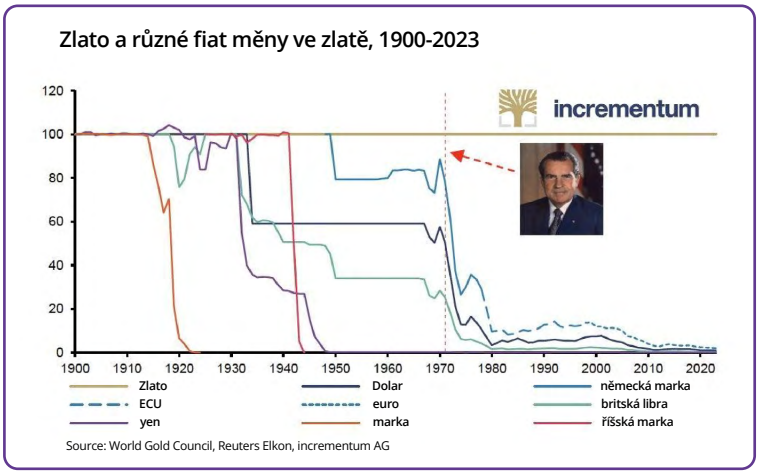
Co jsou to fiat měny a kdo je ovládá?

V roce 1934 umožnil zákon o zlatých rezervách lidem opět vyměnit dolary za zlato. Mělo to však jeden háček. Vláda záměrně znehodnotila dolary zvýšením směnného kurzu na 35 dolarů za unci zlata. Tato devalvace zasáhla těžce pracující jednotlivce z nižších a středních vrstev. Znamenalo to totiž, že jejich úspory, které měly kdysi větší hodnotu, nyní klesly přibližně o 40%.

Po druhé světové válce byl na základě Brettonwoodské dohody z roku 1944 stanoven americký dolar jako světová rezervní měna, kterou bylo možné směnit za zlato (pouze pro vlády jedlotlivých zemí). Tato vazba mezi americkým dolarem a zlatem však byla přerušena v roce 1971, kdy prezident Nixon ukončil směnitelnost amerického dolaru za zlato. To znamenalo významný zlom, který vedl k přijetí systému fiat měn, kde hodnota měny není kryta fyzickou komoditou, jako je zlato, ale spíše důvěrou lidí, kteří ji používají. Vzhledem k tomu, že vlády a centrální banky si ponechaly většinu zlata, které od lidí vybrali, hodnota zlata prudce vzrostla a v roce 1980 dosáhla 870 USD za unci.



Závěrem lze říci, že příběh o tom, jak lidská společnost přešla od kvalitního peněžního standardu k nekvalitnímu (fiat) standardu, je příběhem toho, jak se vlády a banky zmocnily cenných kovů svých občanů. Zatímco skutečné peníze skončily v kapsách vlád a bank, lidem zůstaly kusy papíru, jejichž jediná hodnota pochází z nařízení vlád o jejich používání.



4.2 Fiat systém

> Hlavním problémem konvenční měny je veškerá důvěra, která je nutná k jejímu fungování. Je třeba důvěřovat centrální bance, že měnu neznehodnotí, ale historie fiat měn je plná případů porušení této důvěry.
>
> **Satoshi Nakamoto**

Lidstvo přešlo od kvalitních peněz ovládaných většinou k nekvalitním penězům ovládaným menšinou. Jak přesně ale tento systém funguje?

4.2.1 Měnový systém stanovený ze zákona

Fiat systém je charakteristický svou povinností, která je lidem vnucena prostřednictvím předpisů o zákonném platidle. Výraz "fiat", pocházející z latiny, znamená "budiž" a představuje nařízení vydávané státními orgány.

Na rozdíl od peněz krytých hmotnými aktivy, jako je zlato, fiat peníze takovou oporu postrádají. Místo toho je jejich používání nařízeno zákonem. Do kategorie fiat peněz spadají běžná platidla, jako jsou koruny, dolary, eura, libry, jüany, pesa a další.

Právo zákonného platidla: Zákon, který ukládá všem občanům povinnost přijímat určitý druh měny.

Hodnota fiat měn je založena na víře, že je lze směnit za zboží a služby, a na iluzi, že si svou hodnotu udrží v čase. Fiat měny lze přirovnat ke vstupence na koncert; jejich hodnota nespočívá v samotné papírové vstupence, ale v ujištění, že kapela (vláda a její centrální banka) předvede skvělou show (zajistí ekonomickou stabilitu).

Výhody fiat měn

- **Snadné použití:** Fiat měny jsou vhodné pro každodenní transakce.
- **Nižší náklady a rizika:** Fiat měny nevyžadují přísné zabezpečení jako zlato, takže jsou levnější a bezpečnější.

Nevýhody fiat měn

- **Inflační rizika:** Inflace, neboli lidsky řečeno „tištění peněz" způsobuje zvýšení peněžní zásoby a následný růst cen v ekonomice. V některých případech dokáží i k hyperinflaci, což je inflace ve stovkách a více procentech za krátké období.
- **Centralizovaná kontrola a manipulace:** Malé skupiny vybraných lidí mohou systém ovlivňovat a manipulovat s ním, což může vést k cenzuře a konfiskaci.
- **Riziko protistrany:** Pokud vláda čelí určitým ekonomickým problémům, lokální měna může ztratit na hodnotě, jelikož si vláda kdykoliv další peníze může vytvořit z ničeho.
- **Možnost zneužívání:** Systém může být zneužíván, což může vést ke korupci a ztrátě důvěry.

Co jsou to fiat měny a kdo je ovládá?

Komodity vs. fiat měny: Najděte rozdíly

Vzpomeňte si, jak před vznikem fiat měn vlády razily mince z cenných, vzácných a těžko dostupných fyzických komodit, jako je zlato nebo stříbro. Také ale mohli tisknout papírové poukázky, které bylo možné vyměnit za určité množství fyzických komodit. To byl systém podložený komoditami.

Nyní, v systému fiat měn, je to spíše jako mít monopolní peníze. Peníze ve fiat systému tvoří kusy papíru vytištěné centrální bankou a politika vlády přímo ovlivňuje jejich hodnotu. Vláda a centrální banky jsou v podstatě "bankéři monopolní hry", kteří mají kontrolu nad tím, jak hra funguje, kdo kolik dostane a jakou mají peníze hodnotu. Jinými slovy, vláda slibuje, že bude dobře a efektivně spravovat měnový systém.

Závěrem lze říci, že fiat měny mají hodnotu pouze proto, že vláda nařizuje jejich používání; fiat peníze samy o sobě nemají žádnou užitnou hodnotu.

Stručně řečeno, fiat systém je hra na důvěru, v níž hodnota našich peněz závisí na slibech těch, kteří jsou v čele, a lidé mohou jen doufat, že jejich vláda jedná ve prospěch všech. Dále se podíváme, jak banky vytvářejí nové peníze, kdo se na tom podílí a jak tento proces ovlivňuje ekonomiku.

4.2.2 Bankovnictví frakčních rezerv: Systém poháněný dluhem

> Je dobře, že občané našeho národa nerozumějí bankovnímu a měnovému systému, protože kdyby mu rozuměli, věřím, že do zítřejšího rána by došlo k revoluci.
>
> **Henry Ford**

Bankovnictví částečných rezerv je jednou z hlavních součástí fiat systému, které bankám umožňuje půjčovat značnou část vkladů svých klientů. Přemýšleli jste někdy o tom, proč banky nabízejí svým klientům tolik služeb? I když se může zdát, že jsou velkorysé, je důležité si uvědomit, že banky jsou podnikatelské subjekty a jejich hlavním cílem je dosahovat zisku. Jak ale mohou dosahovat zisku, když rozdávají peníze tím, že je lidem půjčují?

Kromě úroků z vkladů banky generují příjmy i dalšími způsoby, jako jsou:

- Úročením úvěrů, které poskytují.
- Účtování poplatků za služby, jako je používání bankomatů, vedení účtu transakční poplatky atd.
- Vydělávání peněz prostřednictvím investic, jako je nákup a prodej cenných papírů nebo investice do nemovitostí a dalších aktiv.
- Ponechání určitého procenta úvěrů v rezervě a investování nebo půjčování zbytku.
- Úroky z vkladů klientů na spořicích účtech.

Když banka obdrží vklad, může si ponechat pouze jeho část (povinné minimální rezervy) a zbývající část může půjčit.

Například při vkladu 1 000 Kč s 10% povinnými rezervami může banka půjčit 900 Kč a ponechá si pouze 100 Kč jako rezervy. Dlužník uloží 900 Kč do jiné banky, čímž může cyklus pokračovat znovu. Navzdory počátečnímu vkladu 1 000 Kč vzroste celkový objem peněz v ekonomice na 2 710 Kč, které se zdánlivě objeví z ničeho nic – takový jev je známý jako multiplikační efekt.

Tento proces vede k měnovému systému založenému na dluhu, protože banky vytvářejí s každou půjčkou nové peníze, čímž zvyšují celkovou peněžní zásobu. S tím, jak bankovnictví s částečnými rezervami pokračuje, roste celkový dluh v ekonomice, což přispívá k inflaci.

Tento systém je založen na nepřetržitém cyklu tvorby peněz prostřednictvím půjček, což připomíná neustálý přísun drog pro drogově závislého člověka. Pokud však banky půjčí více peněz, než mají v rezervách, a vkladatelé se současně vrhnou na jejich výběr, může bankám hrozit zkrachování.

Centrální banka zde vystupuje jako věřitel poslední instance a poskytuje nově vytvořené peníze, aby případně zabránila krachu banky. Centrální banka tohoto cíle dosahuje buď odkupem aktiv banky nebo přímou podporou na účet banky. Banky jsou v podstatě zachráněny před krachem prostřednictvím neustálých „injekcí" nových peněz ze strany centrálních bank. Tento systém založený na dluhu, který je systematicky zachraňován centrální bankou, vede k cyklům od hospodářské prosperity k ekonomickému propadu.

Představte si, že máte přítele, který je shodou okolností také bankéř, říkejme mu Dalibor.

Dalibor miluje kola a chce si půjčit vaše kolo, protože má spoustu míst, kam by chtěl jet. Půjčíte mu své kolo a Dalibor obratem začne slibovat to samé kolo spoustě dalších kamarádů ve stejnou dobu. S vaším jediným skutečným kolem, které mu půjčíte, se Daliborovi podaří vytvořit další imaginární kola a začne je půjčovat kamarádům. Každý z jeho kamarádů si myslí, že si může užít pěknou jízdu, kdykoli se mu zachce. Ale zde nastává zlom - skutečné kolo je jen jedno! Všechna ostatní jsou vymyšlená a jen sliby.

Takže co se stane... Jakmile se v oběhu objeví více imaginárních kol, všichni jsou velmi spokojeni, alespoň zpočátku. A to proto, že na začátku nepoužívají kolo všichni v jeden okamžik. Vypadá to, že zde není žádný problém. Zdá se, že kol je pro všechny dostatek. A tak si všichni kamarádi začínají dělat další plány a přemýšlejí, kam všude se s kolem vydají.

Zde však kouzlo začíná ztrácet svůj šarm. Jednoho slunečného dne se všichni rozhodnou, že je ideální den na projížďku na kole. Všichni se objeví u Daliborových dveří a těší se, až se na svých imaginárních kolech projedou. Jenže realita je zaskočí - skutečné kolo je jen jedno. Následuje zklamání a hodnota slíbených vyjížděk najednou klesá.

Ve světě poskytování úvěrů s částečnými rezervami je to podobné. Banky půjčují více peněz, než kolik jich ve skutečnosti mají, a nějakou dobu si všichni užívají výhod. V oběhu je více peněz a zdá se, že jich je dost. Pokud se však příliš mnoho lidí snaží vybrat své peníze najednou, ukáže se skutečná hodnota: není jich dost na splnění všech závazků.

Tento scénář ovlivňuje obecné blaho a hodnotu všech zúčastněných. Příslib hojnosti se mění v podvod. Stejně jako imaginární kola ztrácejí svou pomyslnou hodnotu, když všichni chtějí skutečnou jízdu, může se snížit hodnota peněz v ekonomice, když se všichni vrhnou na to, aby si nárokovali svůj skutečný podíl. Když se tak stane, lidé zjistí, že peníze, které mají v bance, tam ve skutečnosti nejsou, což vede ke zmíněným „runům" na banky, a dokonce ke kolapsu celé ekonomiky státu. Ti, kdo na tyto kolapsy doplácejí, byli a budou vždy stejnou skupinou: nižší a střední třída.

Co jsou to fiat měny a kdo je ovládá?

Úvěrová expanze prostřednictvím bankovnictví s částečnými rezervami (komerční banky vytvářejí fiat měny a půjčují je klientům)

↓

Prosperita

↓

Expanze peněžní zásoby (nově vytvořené peníze vstupují do systému a navyšují peněžní zásobu)

↓

Nadměrné investice (zákazníci využívají úvěry k investicím na trzích, což vytváří prudký nárůst poptávky)

↓

Cenová inflace (růst cen v důsledku nové poptávky)

↓

Nedostatek nové poptávky

↓

Ekonomický úpadek

↓

Ceny klesají (investoři propadají panice a začínají prodávat své investice za nižší ceny, protože po nich není skutečná poptávka)

↓

Fyzické osoby a firmy nesplácejí své úvěry (protože hodnota jejich zástav klesá)

↓

Banky neplní své závazky (protože nyní vlastní aktiva, jejichž hodnota je nižší než hodnota poskytnutých úvěrů)

↓

Intervence centrální banky, záchrana bank komerčních/investičních

↓

Banky jsou zachráněny za pomoci nových peněz (centrální banka odkoupí aktiva, která banky drží, a to za vyšší cenu, než je aktuální tržní ocenění, aby je zachránila. A nebo vytvoří peníze nové a poskytne je bankám napřímo)

↓

Cyklus se opakuje (další úvěrová expanze, příprava na další fázi rozmachu)

Aktivita: Bankovnictví částečných rezerv

V následujícím cvičení prozkoumáme, jak může bankovnictví s frakčními rezervami vést ke znehodnocení měny, inflaci a poklesu kupní síly. Použijeme zjednodušený příklad zahrnující šest účastníků, z nichž jeden bude vystupovat jako banka, a povinné minimální rezervy, budou pro zjednodušení 10%.

- A právě vyhrál 1 000 000 Kč v loterii a uložil je do banky (B). Při 10% minimální rezervě musí B ponechat 100 000 Kč ve svém trezoru a zbývajících 900 000 Kč může půjčit.
- C si od B půjčí maximální částku (900 000 Kč) a použije ji na koupi mobilního domu od D.
- D uloží 900 000 Kč, které obdržel od C, do banky (B). Celková výše vkladů v bance nyní činí 1 900 000 Kč.
- E požádá B o půjčku a banka mu půjčí 90 % nového vkladu, což je 810 000 Kč.
- E použije půjčku ve výši 810 000 Kč na nákup uměleckého díla od F, který poté uloží peníze do banky (B). Celková výše evidovaných vkladů nyní činí 2 710 000 Kč.

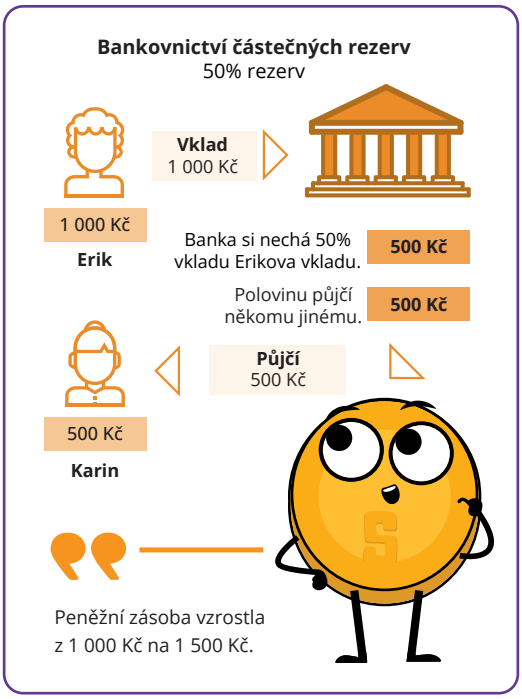
V tomto scénáři vyústil počáteční vklad ve výši 1 000 000 Kč na konečných 2 710 000 Kč. A to jen díky svému oběhu v ekonomice.

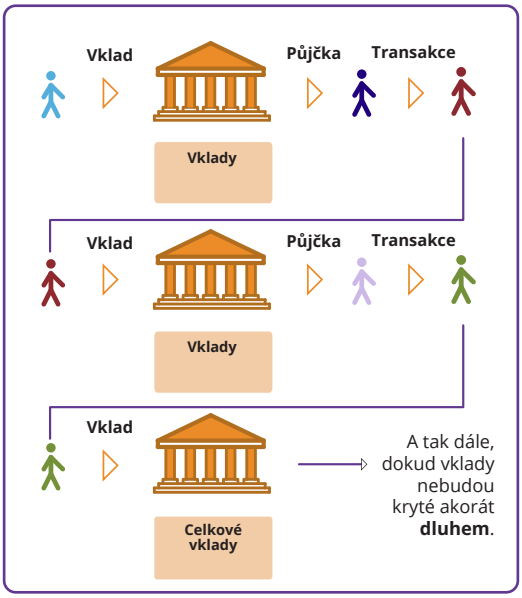
Pokud by se sazba minimálních rezerv snížila na 1 %, bylo by množství vytvořených peněz podstatně vyšší (1 000 000 Kč / 0,01 = 100 000 000 Kč). Kolik peněz by se v tomto případě skutečně vytvořilo se sumou 1 000 000 Kč, pokud by peníze obíhaly v ekonomice ještě déle?

Je také dobré zmínit, že Americký FED (centrální banka) v roce 2020 snížila minimální povinné rezervy bank na 0%. To z důvodu, aby stimulovala ekonomiku v době pandemie COVID-19.

Na tento úkol potřebujeme dobrovolníky:

A = Vkladatel (Výherce loterie) (Světle modrá)
B = Bankéř (Banka)
C = Dlužník č. 1 (tmavě modrý)
D = majitel nemovitosti/vkladatel (červená)
E = Dlužník č. 2 (světle fialová)
F = majitel/vkladatel umělecké galerie (zelená)



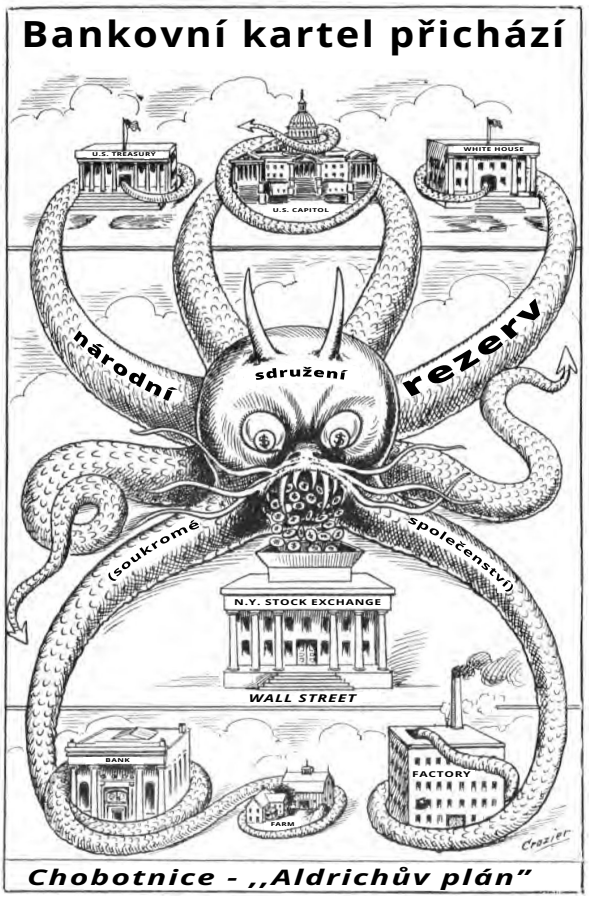


Co jsou to fiat měny a kdo je ovládá?

4.2.3 Kdo ovládá systém fiat měn a jaký z toho má prospěch?

Vystupují zde čtyři hlavní aktéři: vláda, bohatí jednotlivci, finanční sektor a centrální banka. Ti společně ovládají fiat systém.

- **Vláda:** Vláda je jako „režisér fiat show". Spolu s výběrem daní je financována prostřednictvím nových dluhopisů (obligací) vydávaných ministerstvem financí. Když po těchto dluhopisech není dostatečná poptávka, zbývající dluh odkoupí centrální banka. To znamená, že může nadále vykonávat svou činnost a prosazovat své zájmy, aniž by potřebovala souhlas lidu. Je to jako pořídit si kreditní kartu, aniž byste se museli starat o její okamžité splácení. Pro vládu se to může zdát výhodné, ale pro všechny ostatní to má následky.



- **Bohatí jednotlivci:** Bohatí jednotlivci benefitují hodně z fiat systému. Díky možnosti akumulovat více a více dluhu mohou investovat do aktiv, jako jsou komodity, nemovitosti a akcie, a téměř bez námahy vytvářet nové bohatství.

- **Finanční sektor (banky):** Banky a další finanční instituce neovládají fiat systém přímo, ale mají z něj také velký prospěch. Jsou téměř zbaveny zodpovědnosti a mohou pokračovat v tvorbě nových peněz prostřednictvím půjček. Zároveň díky systému frakčních rezerv profitují z vyšších výnosů. Banky jsou v podstatě zbaveny jakékoliv zodpovědnosti, protože jsou zachraňovány novými penězi, aby se celý systém nezhroutil.

- **Centrální banka:** Centrální banka je ta, která tahá za nitky a údajně kontroluje růst peněžní zásoby. Ale v tomto je právě ten trik - centrální banka také podléhá vládním zákonům a slouží vládním zájmům. Je to jako loutkář, kterého ovládá jiný loutkář. Může se zdát, že centrální banka je ta, která má vše pod kontrolou, ale nepřímo plní přání vlády, tudíž tiskne peníze ze vzduchu, když je vláda potřebuje.

Jak tedy tito aktéři benefitují: Tyto skupiny mají z aktuálního systému různý prospěch a vytvářejí složitou síť kontroly. Vláda získává finanční prostředky bez okamžitých následků, bohatí jednotlivci a banky bez námahy vydělávají peníze a centrální banka udržuje celou show v chodu. Zbytek obyvatelstva mezitím pociťuje dopady a čelí problémům, které systém přináší.

Ve finále loutkaři fiat systému hrají divadlo, z něhož má několik málo lidí velký prospěch, ale většina diváků pochybuje, zda je finanční scéna, na níž se ocitli, spravedlivá.

Role centrálních bank

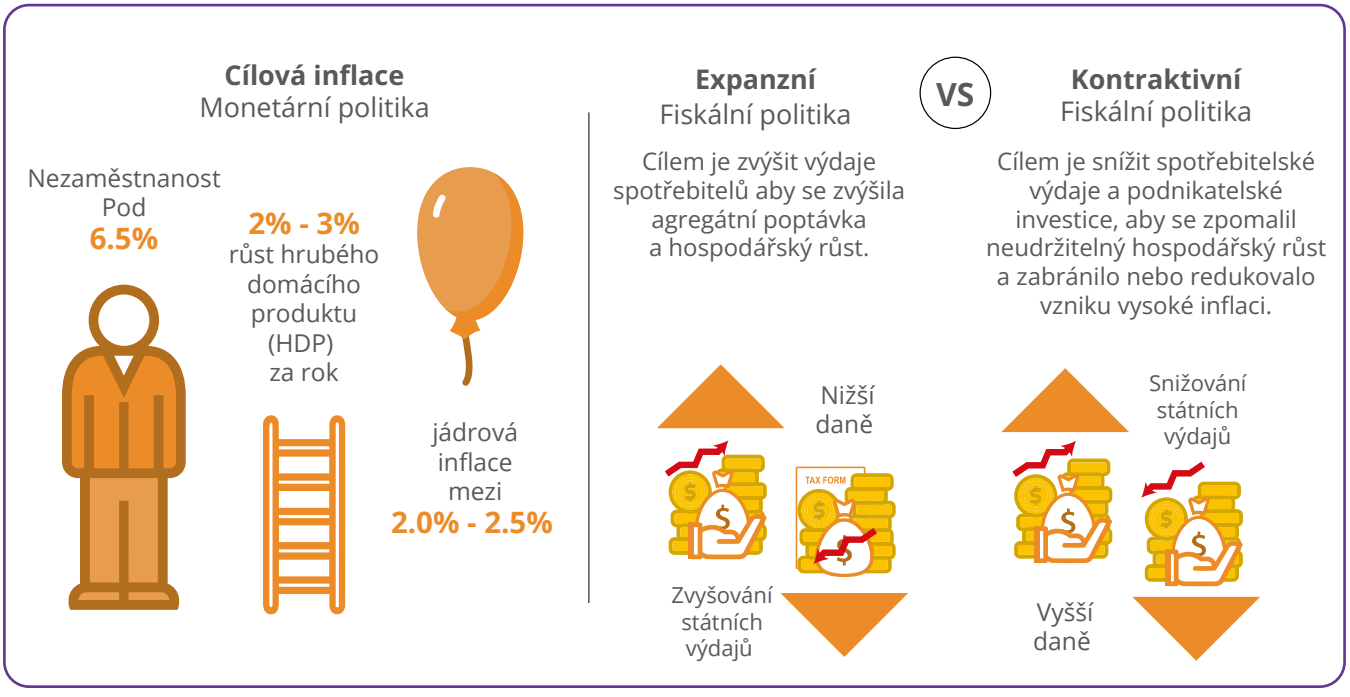
Centrální banky v tichosti určují způsob fungování ekonomiky. Jejich oficiálním úkolem je zajišťovat stabilitu, integritu a "udržovat vše ve stavu rovnováhy", ale jejich metody odhalují i tajuplnější stránku.

Centrální banky úzce spolupracují s vládami, tahají za nitky měnové politiky a pomocí nástrojů, jako jsou úrokové sazby, kontrolují peněžní zásobu. V době krize tisknou peníze ze vzduchu a prostřednictvím komerčních bank je pumpují do ekonomiky, aby se zdálo, že je vše v pořádku.

Nejenže na vše dohlížejí, ale centrální banky regulují komerční banky, určují pravidla hry a zasahují, aby pomohly, když se banky dostanou do potíží (fungují jako věřitelé poslední instance). Tato síť kontroly, která se tváří jako ochranářská, způsobuje, že ekonomika a banky jsou na nich ještě více závislé.

Pochopení toho, odkud se berou biliony dolarů na stimulaci a kdo rozhoduje o jejich přerozdělování, má zásadní význam pro pochopení širšího finančního systému. Vlády používají několik nástrojů k regulaci peněžní zásoby v určitých časových okamžicích.

Centrální banky a vlády mohou pomocí nástrojů měnové a fiskální politiky ovlivňovat množství peněz a ekonomiku. Například Federální rezervní systém Spojených států (FED) používá měnovou politiku k určování úrokových sazeb, čímž ovlivňuje množství peněz v oběhu. Fiskální politika naproti tomu zahrnuje použití výdajové a daňové politiky k ovlivnění hospodářské aktivity.



Kurzová politika, šoky v peněžní zásobě a cenová regulace slouží jako další nástroje kontroly peněžní zásoby a ovlivňují obchod a ekonomiku. Cílem těchto politik je stabilizovat ceny a kontrolovat inflaci, jejich zásahy však často vedou k opakovaným cyklům rozmachu a úpadku, což vytváří problémy pro všechny, kdo používají státní měnu.

Příklad: "Příliš velké na to, aby padly", označuje finanční instituce, které jsou tak velké a vzájemně propojené, že jejich selhání by mělo katastrofální dopady na celý finanční systém. Během finanční krize v roce 2008 bylo několik velkých bank považováno za "příliš velké na to, aby padly", což vedlo americkou vládu k zásahu a poskytnutí finanční pomoci, aby zabránila jejich krachu.

Jedním z nejznámějších příkladů instituce, která byla v době finanční krize "příliš velká na to, aby mohla padnout", byla investiční banka Lehman Brothers. Když Lehman Brothers v září 2008 vyhlásila bankrot, spustilo to dominový efekt událostí, včetně takřka úplného pádu pojišťovacího gigantu AIG a masivního poklesu akciového trhu. Americká vláda musela zasáhnout a poskytnout pomoc dalším významným finančním institucím, aby zabránila dalšímu chaosu a ochránila širší ekonomiku.

Pochopení fungování těchto procesů je zásadní pro pochopení omezení centralizovaných měnových systémů. Dokud nepochopíte problém, nepoznáte jeho řešení. Nyní, když jsme se zabývali tím, jak fiat systém fungoval v minulosti a v současnosti, probereme, jak v současnosti vypadá budoucnost fiat systému: Digitální měny centrálních bank neboli (CBDC).

4.3 Digitální měny centrálních bank: Budoucnost fiat měn

Digitální měny centrálních bank (CBDC) jsou dalším stupněm fiat měn. Na rozdíl od kombinace fyzických bankovek, mincí a digitálních plateb jsou CBDC pouze digitální verzí fiat měny vydávané vládami a kontrolované centrálními bankami.

Představte si měnu, kterou používáte každý den, ale bez jakékoliv fyzické přítomnosti - žádné mince, které by vám cinkaly v kapse, nebo bankovky, které byste museli dávat do peněženky. CBDC se liší především zvýšenou mírou kontroly a monitorování, kterou vládám a centrálním bankám nabízejí. Díky CBDC získávají úřady jedinečný přehled o finančních transakcích, což usnadňuje sledování a regulaci toku peněz.

Vlády a centrální banky mohou snadno upravovat formu a množství CBDC v oběhu, manipulovat s úrokovými sazbami a precizněji využívat nástroje měnové a fiskální politiky. CBDC v podstatě poskytují orgánům efektivnější prostředek k ovlivňování a řízení jejich fiat měny.

Zatímco CBDC se zdají být budoucností fiat měn, současný světový měnový systém již funguje na čistém fiat standardu. Fiat měny již nejsou vázány na zlato, což vede k výraznému rozšíření peněžní zásoby bez jakéhokoli reálného omezení.

Nyní, když už máte jasnější představu o fungování fiat systému, je čas prozkoumat jeho důsledky v kapitole 5.

Kapitola 5

Jak problémy vedou k řešení

Pracovní sešit

český překlad | 2024

Jak problémy vedou k řešení

5.0 Úvod do problému

> Ten, kdo ovládá většinu peněz v naší zemi, je absolutním pánem veškerého průmyslu a obchodu... když si uvědomíte, že celý systém je velmi snadno ovládán, už tak či onak, několika mocnými na vrcholu,nebude vám třeba vysvětlovat, jak dochází k obdobím inflace a deprese.
>
> **James A. Garfield, U.S. President**

V kapitole 4 jste se dozvěděli, že finanční svět se opírá o systém, který nemusí být tak stabilní, jak se zdá. Fiat systém, který je udržován neustálým tištěním nových peněz, se jeví jako výhodný spíše pro několik málo lidí než pro většinu. Tato kapitola odhaluje, co fiat systém představuje pro běžné lidi a společnost. Konečně prozkoumáme příběh několika jednotlivců, kteří si všimli zmíněných problémů a v tichosti se snažili najít řešení, které by mohlo změnit budoucnost celého lidstva.

5.1 Snižování kupní síly

5.1.1 Měnová inflace a její vliv na kupní sílu

Měnová inflace je zvýšení množství peněz v ekonomice, které má přímý dopad na průměrného člověka tím, že snižuje jeho kupní sílu. Cyklus cenové inflace začíná, když je v oběhu více peněz. To následně zvyšuje poptávku po zboží a službách, což v konečném důsledku způsobuje růst cen.

Představme si malou skupinu přátel - Alexe, Boba a Karla - každý z nich má v ruce dolar a na prodej je jedna láhev vody. Výchozí situace je jednoduchá: tři lidé s celkem třemi dolary a jednou lahví vody. Nyní předpokládejme, že se někdo, třeba místní vláda, rozhodne dát každému příteli dolar navíc. Nyní mají dohromady šest dolarů. Za tyto nově získané peníze mají všichni chuť koupit si námi zmíněnou láhev vody. Protože všichni tři kamarádi chtějí stejnou láhev, začnou mezi sebou dražit.

Zvýšená poptávka podpořená penězi navíc je přiměje nabídnout za láhev vody více, než byla původní cena. Nakonec se cena vody kvůli této zvýšené poptávce zvýší. Tato situace odráží pokles jejich kupní síly. Přestože mají více peněz, nemohou si koupit tolik lahví vody jako dříve, což ukazuje dopad inflace na hodnotu jejich peněz.

V tomto příkladu přátelé zaznamenali pokles své kupní síly, protože používali formu peněz, která byla ovlivněna vnějšími faktory, jako jsou dodatečné dolary vytvořené vládou. Nedostatečná kontrola nad peněžní zásobou v kombinaci se zvýšenou poptávkou vedla k růstu cen, takže pro přátele bylo obtížnější koupit si za dodatečné dolary stejné množství zboží.

To ukazuje, jak kupní sílu přátel ovlivnily faktory, které nemohli nikterak zvrátit, a zdůrazňuje důležitost pochopení a zpochybňování systémů, které ovlivňují hodnotu našich peněz.

Nyní prozkoumejme, jak se tato situace projevuje v reálném životě.

Aktivita: Působení inflace - dražební aktivita

Cíl: Pochopit pojem inflace a její vliv na ceny zboží a služeb v ekonomice.

Definice:

- Peněžní zásoba: celkové množství peněz v oběhu v ekonomice v určitém čase. Patří sem:
  - Fyzické peníze, jako jsou mince a bankovky
  - Prostředky na běžných účtech
  - Prostředky na spořících účtech
  - Fondy peněžního trhu
  - Krátkodobé termínované vklady
- Aukce: Veřejný prodej, při kterém se zboží nebo majetek prodává tomu, kdo nabídne nejvyšší cenu.

Třídní cvičení - Postupujte podle níže uvedených pokynů:

1. Od učitele obdržíte náhodný počet peněz ze hry monopoly. To představuje vaši peněžní zásobu ve společnosti.
2. Zapište celkovou peněžní zásobu do přiložené tabulky.
3. Učitel začne s dražbou tyčinky, kterou studentům nabídne. Abyste tyčinku vyhráli, musíte za své monopolní peníze přihodit nejvyšší částku. Vítěznou nabídku zapište vedle zásoby peněz.
4. Učitel poté přidá k celkové zásobě peněz značnou část dalších monopolních peněz. To představuje zvýšení peněžní zásoby v ekonomice. Později se dozvíte, jak se v ekonomice zvyšuje nebo snižuje peněžní zásoba.

Společnost může být často nepředvídatelsná a nejistá, jak ukazuje příklad učitele, který náhodně rozdává značné množství nových peněz pouze vybraným studentům. To znázorňuje reálné situace ve světě, kde jsou zdroje a nové příležitosti nerovnoměrně distrubuovány, a zároveň poukazuje na přirozenou nahodilost a nespravedlnost v mnoha situacích.

5. Učitel provede stejným postupem dražbu druhé tyčinky. Vítěznou nabídku zapíše do tabulky vedle zásoby peněz.
6. Učitel zopakuje dražbu potřetí.

Kolo	Peněžní zásoba	Nejvyšší nabídka
1		
2		
3		

Závěr:

1. Jak ovlivnilo zvýšení peněžní zásoby vítězné nabídky na tyčinky?
2. Jaký je vztah mezi zvyšováním peněžní zásoby a inflací?
3. Jaký význam má peněžní zásoba v reálném světě?
4. Když se do ekonomiky dostanou nové peníze, co se podle vás stane s cenami zboží a služeb? Myslíte si, že změna cen je dočasná nebo trvalá? A proč? Jak podle vás změny cen ovlivňují životy lidí ve společnosti z dlouhodobého hlediska?

5.2 Globální dluhová zátěž a sociální nerovnost

5.2.1 Dopad na jednotlivce - ztráta kupní síly

Jakub je vysokoškolský student, který žije v malém bytě. Pracuje na částečný úvazek v kavárně, aby pokryl své životní náklady a zaplatil školné. Jakmile začal žít samostatně, Jakub se naučil dobře vést svůj rozpočet.

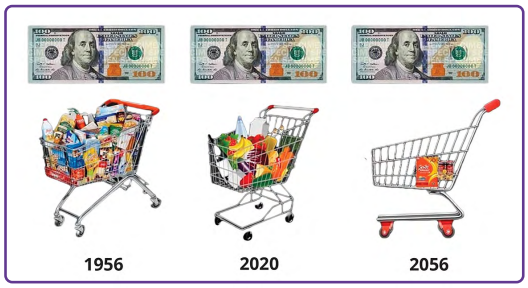
Účetní kniha je podrobný záznam všech vašich peněžních transakcí. Ať už jde o peníze, které vyděláváte, nebo utrácíte, účetní kniha vám pomůže mít o všem přehled.

Na začátku roku 2023 si na celý rok naplánoval 240 000 Kč jako jeho životní náklady, včetně nájmu, jídla a dalších nezbytných věcí. Toto byly jeho transakce na leden 2023:

Datum	Popis	Částka	Typ	Rozvaha
1.1.2023	Počáteční rozvaha			**20 000 Kč**
1.1.2023	Nájem za leden	**12 000 Kč**	**Výdaj**	**8 000 Kč**
5.1.2023	Potraviny	**4 000 Kč**	**Výdaj**	**4 000 Kč**
15.1.2023	Výplata	**10 000 Kč**	**Příjem**	**14 000 Kč**
20.1.2023	Palivo do auta	**2 000 Kč**	**Výdaj**	**12 000 Kč**
30.1.2023	Učebnice	**1 500 Kč**	**Výdaj**	**10 500 Kč**

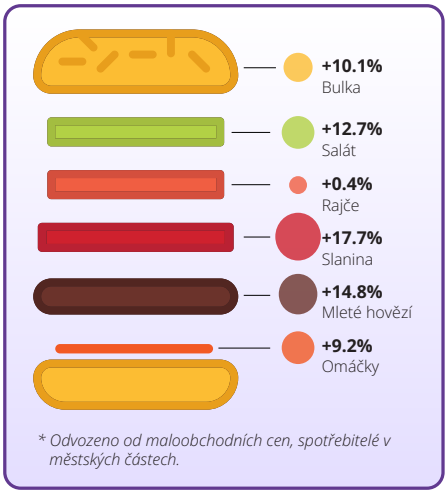
Z této účetní knihy vyplývá, že Jakubův počáteční zůstatek činil 20 000 Kč, z nichž vynaložil 12 000 Kč na zaplacení nájemného za daný měsíc. Poté utratil 4 000 Kč za potraviny a obdržel 10 000 Kč jako mzdu za práci na částečný úvazek, čímž se jeho zůstatek zvýšil na 16 000 Kč. Poté utratil peníze za benzín a učebnice, čímž se jeho zůstatek na konci měsíce snížil na 10 500 Kč.

O dvanáct měsíců později obědvá Jakub se svým dědečkem, kterému sděluje podrobnosti svého rozpočtu na rok 2024. Jakub si všimne, že jeho rozpočet už nedosahuje takové výše jako dříve a že jeho životní náklady za poslední rok výrazně vzrostly. Zatímco Jakub přemýšlí, jak je to možné, dědeček mu ukáže tento obrázek.



Jakub nevěří svým očím. V tu chvíli si uvědomí, že ceny zboží a služeb v průběhu času drasticky rostou, což vede ke snížení jeho kupní síly.

Jeho dědeček říká: *"V roce 1956 jsem byl mladý muž, který se právě vydal do světa. Vzpomínám si, že jsem jako dělník v továrně vydělával 1 200 korun měsíčně. Možná se to nezdá jako mnoho, ale v té době to byla slušná mzda. Vlastně jsem si dokázal našetřit dost peněz na to, abych si mohl koupit vlastní dům na předměstí."*



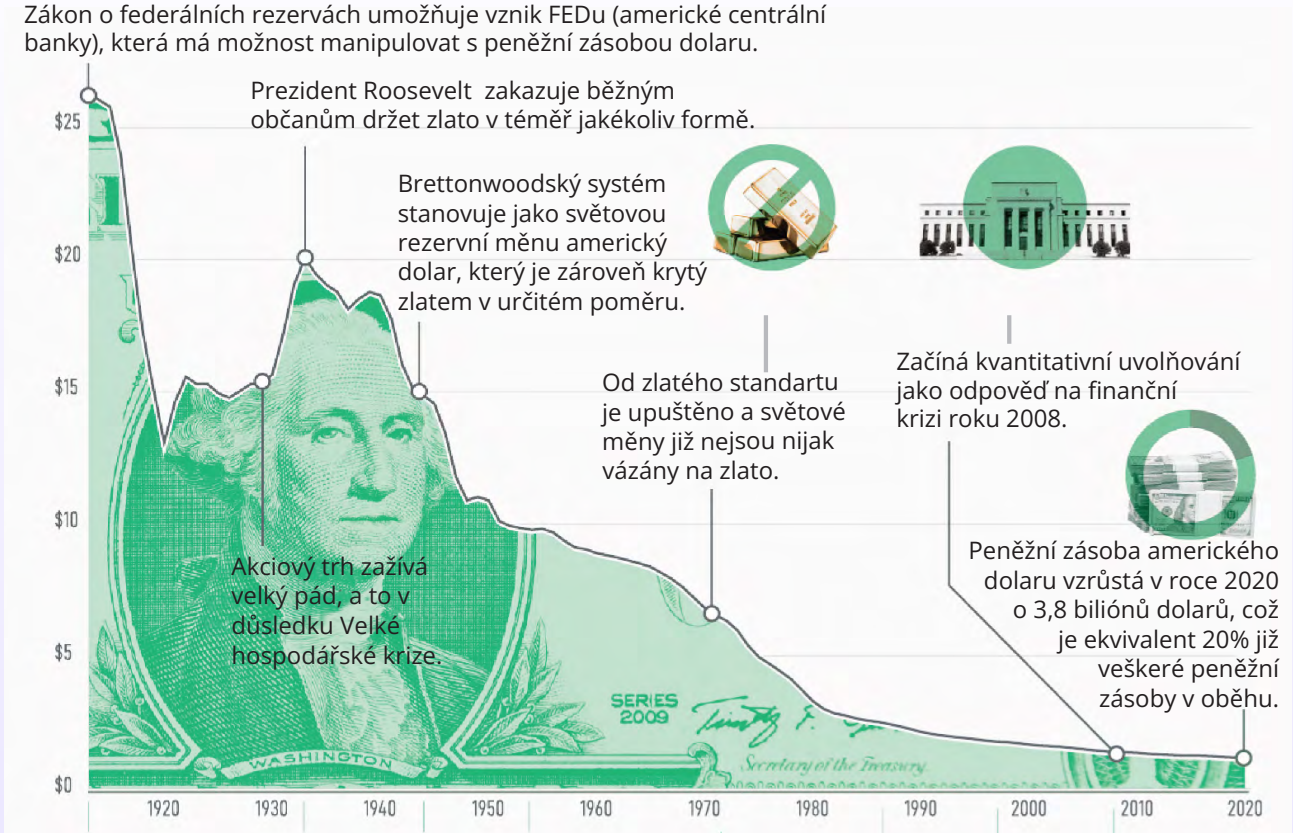
Dědeček pokračoval: *"V minulém století byly náklady na věci velmi odlišné. Například v roce 2020 by vás nákup čokolády Hershey's stál 23 Kč. Pokud se však vrátíme v čase do roku 1913, náklady na stejné množství tyčinek Hershey's Chocolate by činily pouze 0,88 Kč. Tedy 88 haléřů."*

Tento výrazný rozdíl v ceně poukazuje na změnu kupní síly v čase a ukazuje, jak se změna kupní síly v průběhu let vlivem inflace posunula.

Jak problémy vedou k řešení

Cena dolaru
Kupní síla amerického dolaru

Kupní síla dolaru za poslední století výrazně spadla, a to zejména kvůli inflaci a rostoucí měnové zásobě.



Kupní síla jednoho dolaru (DOLAR 2020)

$26.14	$15.14	$15.14	$14.71	$9.69	$6.39	$2.28	$1.61	$1.20	$1.00
30 tabulek čokolády	10 rolí toaletního papíru	10 lahví piva	20 lahví Coca-Coly	10 balíčků preclíků	17 pomerančů	2 krabice s tužkami	4 grepy	2 citróny	1 kafe z McDonaldu
1913	1929	1933	1944	1953	1971	1987	1997	2008	2020

Jakub: *„Cože? To je šílené. Nedokážu si představit, jak nízký nájem bych měl tehdy v porovnání s dneškem."*

Dědeček: *„No, ano, tehdy by byl tvůj nájem mnohem levnější. Mám pro ilustraci jiný příklad: za 10 korun by sis tehdy koupil asi 5 balení chipsů. V roce 2020 jsem za stejné množství zaplatil přes 100 Kč."(čili více než desetinásobek). Spočítej si, kolik by 5 balení stálo dnes."*

Jakub: *„Páni, to je opravdu zajímavé dědo. Jak jsi to prožíval tehdy, když jsi byl mladší?"*

Dědeček: *„Kubo, když jsem byl mladý, byly všechny věci mnohem levnější. Bochník chleba stál jen 2,5 Kč a litr benzínu stál také pár korun. Je neuvěřitelné, o kolik se zvýšily životní náklady."*

Po rozhovoru s dědečkem se Kuba vrátil domů, aby se znovu podíval do své účetní knihy. Rychle zjistil, že na rok 2024 musí do rozpočtu zařadit dalších 20 000 Kč, aby mohl nakoupit stejný koš zboží a služeb jako v předchozím roce. To znamená, že jeho kupní síla se snížila o zmíněných 20 000 Kč , protože nyní musí utratit více peněz, aby si mohl koupit stejné množství zboží. Zatímco Kubův plat se zvyšuje jen nepatrně, jeho životní náklady každoročně prudce rostou.

Následující tabulka ukazuje Kubovi náklady v prvním a druhém roce a také procentuální nárůst cen:

Aby si Jakob mohl dovolit žít na stejné životní úrovni, bude muset odpracovat více hodin každý týdně, aby získal dalších 20 000 Kč.

Na základě informací amerického Úřadu pro statistiku práce jsou dnes ceny přibližně třicetkrát vyšší než v roce 1913. To znamená, že za dolar si dnes lze koupit jen asi 3 % toho, co si za něj bylo možné koupit tehdy.

Položka	náklady za první rok	náklady za druhý rok	% nárůst o
Nájem	126 000 Kč	144 000 Kč	14,3 %
Potraviny	44 000 Kč	48 000 Kč	9 %
Další položky	100 000 Kč	105 000 Kč	5 %
Celkem	**270 000 Kč**	**297 000 Kč**	**10 %**

Pro ilustraci, pokud by někdo Kubovi nabídl možnost cestovat časem - buď si vzít 100 000 Kč v roce 1913, nebo počkat do roku 2023 a dostat jen 3 000 Kč - je to jako volit mezi velkým nákupem v minulosti a pořízením jen několika malých sladkostí dnes. Výrazný rozdíl v hodnotě ukazuje, jak moc se kupní síla peněz v průběhu let snížila.

1938 životní náklady

Bydlení

Nový dům	3 900 $
Průměrný příjem	1 731$ ročně
Nové auto	860 $
Průměrný nájem	27$ měsíčně
Školné na Harvardu	420$ ročně
Lístek do kina	25¢ jeden
Benzín	10¢ za 5 litrů
Poštovní známka	3¢ za jednu

Strava

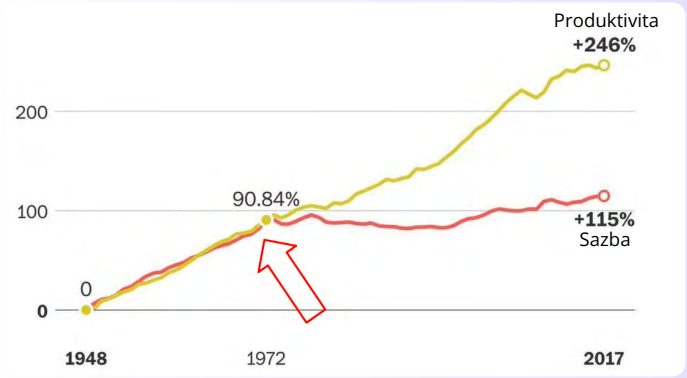
Cukr	59¢ za 4,5 kg
Mléko	50¢ za 5 l
Kafe	39¢ za 0,5 kg
Slanina	32¢ za 0,5 kg
Vajíčka	18¢ za 12 ks

(Na základě původního obrázku)

Jak problémy vedou k řešení

Když budeme uvažovat v číslech, Jakub sice vydělá za rok mnohem více korun než jeho dědeček, ale peníze, které měl Kubův dědeček, byly mnohem cennější a dalo se za ně koupit mnohem více věcí.

Růst produktivity v poměru s hodinovou sazbou (1948-2017)



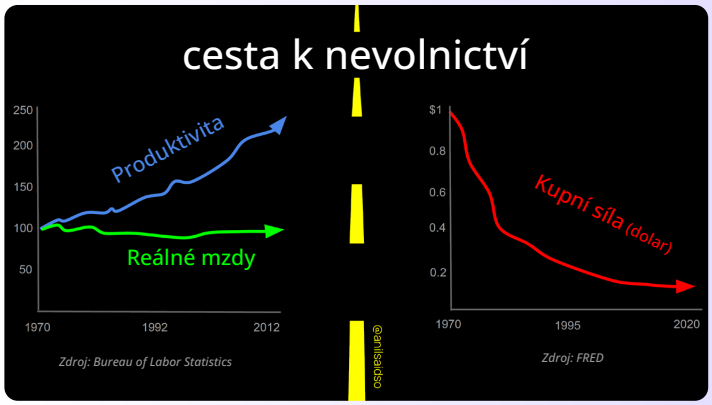
Poznámka: Hodinová sazba zahrnuje výplaty a benefity pro pracovníky střední třídy na pozicích,které nejsou manažerské.

V dnešním světě odrazuje lidi od spoření výrazný dopad inflace.

Místo toho se většina z nich rozhodne své peníze okamžitě utratit, protože jejich hodnota rychle klesá. Tento pesimistický pohled brání lidem plánovat do budoucna.

Jak je vidět z grafu, růst platu průměrného jednotlivce po očištění o inflaci stagnuje, což znamená, že se nezvyšuje plat stejným tempem, jakým klesá hodnota peněz, přestože zaměstnanec pracuje více.

Jakubův příklad je jen jedním z mnoha. Ve dnešním světě je zcela běžné, že vlády vytvářejí peníze ze vzduchu, aby podpořily své vlastní záměry, a následky pak nesou jednotlivci po celém světě. Ceny každodenních věcí, od chleba přes bydlení až po dovolenou, se každoročně zvyšují. Zatímco bohatí mají z inflace prospěch díky vlastnictví různých tříd aktiv, obyčejní lidé vidí, jak jejich těžce vydělané peníze ztrácejí hodnotu. Výsledek? Občané na celém světě se potýkají s problémy kvůli poklesu své kupní síly.



Lidé na celém světě pracují více a déle, jen aby si udrželi stejnou životní úroveň. Je to jako na běžícím pásu - I když běžíte stále rychleji, nikdy se nedostanete více dopředu. Fiat systém zanechává v jednotlivcích pocit, že jsou v nekonečném boji s rostoucími cenami.

Mnozí se ve snaze udržet krok s rostoucími náklady uchylují k zadlužování, což je jako použití malé náplasti na velmi hlubokou ránu. Lidé si berou půjčky nebo dělají impulzivní rozhodnutí, jen aby přežili. Rychlé peníze se stávají nutností a jednotlivci se ocitají v kruhu, kdy přežití dnes má přednost před plánováním zítřka.

Fiat systém s neustálým tiskem peněz ovlivňuje psychologii lidí. Vštěpuje nám potřebu vysokých časových preferencí – to znamená, že raději utratíme peníze dnes, než abychom je ušetřily do budoucna. Stejně jako rychlé řešení prášku pro okamžitou úlevu bolesti hlavy, mají dnes jednotlivci tendenci upřednostňovat krátkodobé výhody oproti dlouhodobým. Jde o pud sebezáchovy, který vytváří koloběh závislosti, kdy se jednotlivci snaží najít jakýkoli způsob, jak získat rychlé peníze, i když je to z dlouhodobého hlediska neudržitelné nebo nefunkční.

Dopad fiat systému v podstatě vykresluje problematický stav pro běžné občany na celém světě. Ve fiat systému ceny rostou, příjmy stagnují a boj o přežití se stává denním chlebem. Zatímco určité skupiny lidí bohatnou, většina jednotlivců na celém světě zůstává závislá na systému, který je činí chudšími a chudšími.

5.2.2 Dopad na společnost - zvyšující se majetková nerovnost

Ve společnosti založené na kvalitních penězích je finanční rozhodování vlády vázáno na schválení občanů. Ve fiat systému se však vlády mohou neomezeně zadlužovat na úkor všech ostatních.

Pravomoc tisknout peníze dle libosti často vede k politické centralizaci. Fiat systém umožňuje vládám hromadit obrovské dluhy a dělat rozhodnutí, která jsou výhodná spíše pro ně samotné. Velmoci, jako jsou Spojené státy, získávají díky tomuto jevu konkurenční výhodu. Mohou tisknout peníze v podstatě donekonečna, aby tak mohly financovat své plány, včetně válek. Tato schopnost umožňuje těmto dominantním státům kontrolovat, ovlivňovat a zapojovat se do geopolitických konfliktů, čímž vzniká globální nerovnováha moci. Války a rozsáhlé kroky k ovládání ostatních se pro velmoci stávají finančně schůdnými, zatímco ostatní státy, které nemají stejnou finanční flexibilitu, čelí omezením.

Ve fiat systému se bohatství nerozděluje rovnoměrně. Místo toho se soustřeďuje v rukou několika vyvolených. Tento jev se podobá hře Monopoly, kde hrstka hráčů vlastní téměř všechny hotely a nemovitosti, zatímco většina se snaží udržet nad vodou. Fiat systém se stal nástrojem určitých skupin ke koncentraci bohatství. Tisknutí peněz umožňuje vládám a centrálním bankám pumpovat do ekonomiky další peníze a příjemci těchto nově vytvořených peněz jsou ti, kteří mají stávající bohatství a postavení. Tyto skupiny mají z čerstvě natištěných peněz prospěch dříve, než se v ekonomice začnou projevovat jejich negativní účinky, například růst cen zboží a služeb.

Jak problémy vedou k řešení

Majetková nerovnost se netýká jen těch ,,kteří mají a těch, kteří nemají". Týká se I těch, kteří pocházejí z méně privilegovaného prostředí (země třetího světe, kde je bankovní účet vzácností). Pro takové lidi je stále obtížnější stoupat po ekonomickém žebříčku, což se podobá startu na závodech s těžkým batohem na zádech. Rostoucí propast mezi bohatými a chudými způsobuje problémy všem, přičemž bohatí utvářejí politiku ve svůj prospěch. To ztěžuje situaci obyčejným lidem, což vede k sociálním nepokojům, nedostatku důvěry v instituce a rozpadu komunit, které se podobají domečku z karet. Nestabilita fiat systému se projevuje hospodářskou nejistotou, politickými nepokoji a globálními krizemi, a to v situacích kdy západní svět čelí hospodářskému poklesu.

Jedná se o celosvětový fenomén, který postihuje společnosti v rozvinutých i rozvojových zemích. Bohatí, kteří často působí v nadnárodním měřítku, využívají globální finanční systém ve svůj prospěch a dále prohlubují propast mezi bohatými a chudými.

V rámci fiat systému se zadlužování stalo pro společnost běžnou záležitostí. Vlády, instituce, podniky i jednotlivci na celém světě se ocitli v záplavě dluhů.

Psychologický posun směrem k tomu, že dluh je považován za přijatelný, má své kořeny v konstrukci samotného fiat systému. Během posledních desetiletí bylo pro všechny stále snazší se výrazně zadlužit a pro obyčejné lidi se zadlužení často stává nutností vzhledem k rostoucím cenám a životním nákladům.

Konzumní způsob života, neboli neustálá touha nakupovat a spotřebovávat, vede lidi k tomu, že nakupují více, než potřebují, což má za následek nadměrné plýtvání všech zdrojů.

Je zřejmé, že fiat systém není jen ekonomickým mechanismem. Je to spíše systém, který utváří lidskou společnost jako celek. Od koncentrace moci, přes rozdíly v bohatství až po společenské zvyky - fiat systém přímo ovlivňuje fungování národů a způsob, jak se běžní občané chovají ve společnosti.

Aktivita: Důsledky Fiat systému

1. Existují nějaké další důsledky, které jednotlivci a společnost jako celek pociťují v důsledku fiat systému?
2. Jaké jsou důsledky fiat systému v České republice? Co se stalo v průběhu historie a jaký to mělo dopad na společnost?
   - **a.** interaktivní sezení: praktické zkušenosti ze života nebo z vyprávění od rodičů a prarodičů.

5.2.3 Globální dluhová zátěž

V důsledku fiat systému se vlády po celém světě ocitly v obrovské dluhové síti, která se nazývá "globální dluhová spirála". Představte si scénář, kdy si půjčíte více peněz, než které kdy můžete splatit. To se děje v masovém měřítku po celém světě. Vlády, které se topí v dluzích, se ocitly v nebezpečné hře, kdy hromadí více dluhů, než jsou schopny kdy splatit. Je to příběh neuvážených výdajů, půjček a nedostatku předvídavosti, který nyní tlačí státy po celém světě na okraj finanční katastrofy.

K dnešnímu dni federální vláda USA od roku 2019 zvýšila svůj dluh o ohromujících deset bilionů dolarů. Celkový dluh prudce vzrostl z přibližně 23 bilionů dolarů během čtvrtého čtvrtletí roku 2019 na astronomických 35 bilionů dolarů v roce 2024 . Tempo, jakým vlády na celém světě chrlí nový dluh, se nezpomaluje, ve skutečnosti se zrychluje.

Stav zadlužení světových vlád

Poměr zadlužení vůči HDP 2021 (%)

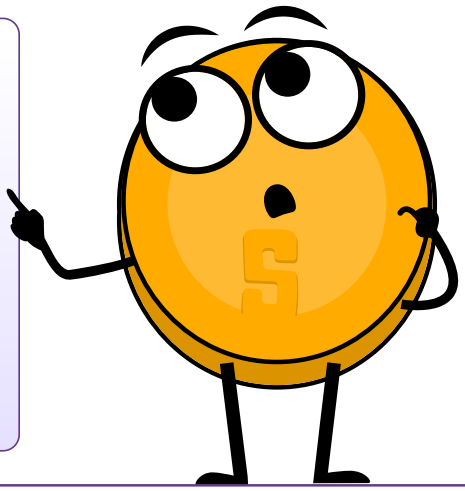
- 200 % a více
- 100 % - 199.9 %
- 50 % - 99.9 %
- 20 % - 49.9 %
- 10 % – 19.9 %
- Méně než 10 %

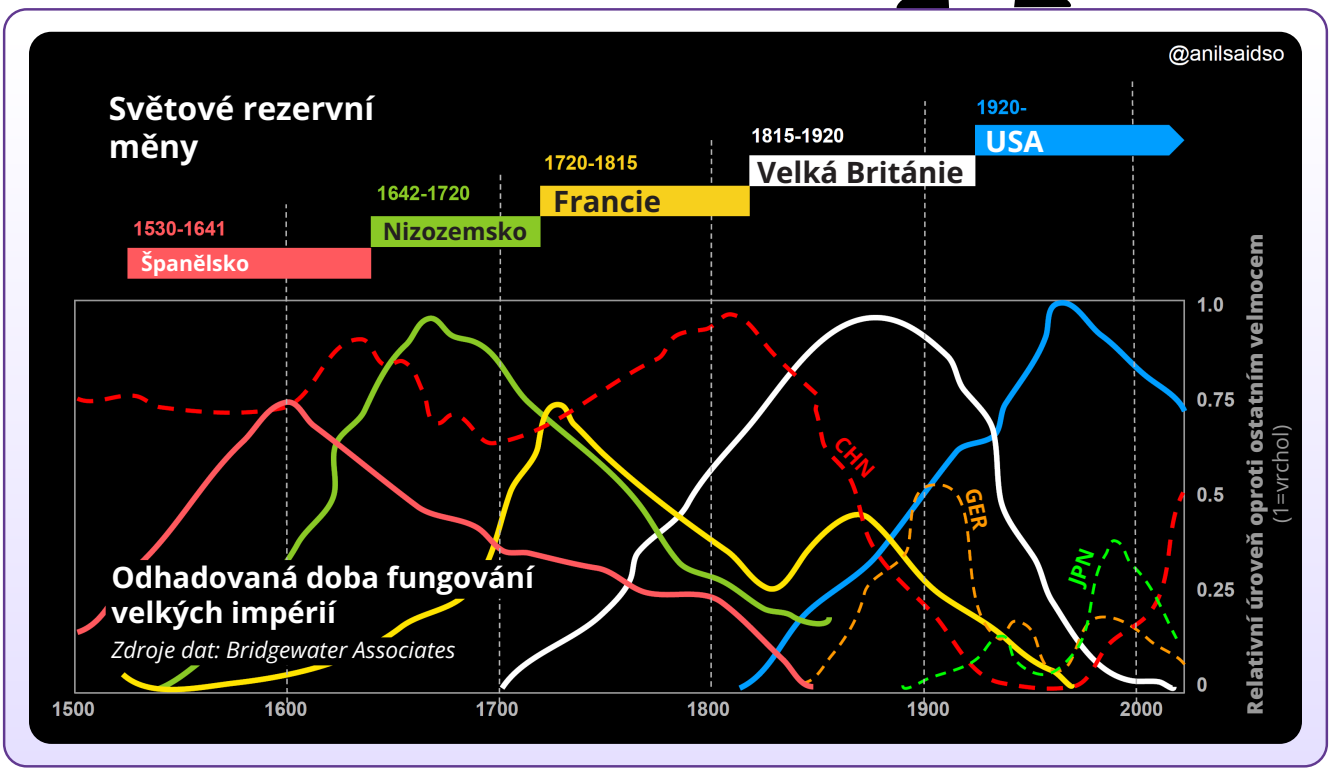
Co to tedy znamená pro jednotlivce a firmy, které se potýkají s důsledky tohoto systému? Dluhová spirála, v níž se ocitly, je jako sněhová koule valící se z kopce - stále se zvětšuje a my nevíme, jak ji zastavit.

Důsledky, o nichž jsme se zmínili dříve, od nerovnosti v bohatství až po společenské nepokoje, nezmizí. Naopak, globální dluhové zátěž dosáhla bodu, z něhož není návratu, což zajišťuje, že situace se bude dále zhoršovat.

Jak problémy vedou k řešení

> Nevěřím v návrat kvalitních peněz, dokud tato záležitost bude v rukou státu. Nemůžeme postupovat násilně. Můžeme jedině hledat nějakou chytrou okliku a přijít s něčím, co stát nebude moci zastavit.
>
> ***Friedrich Hayek***
> Nositel Nobelovy ceny za ekonomii





5.3 Cypherpunkeři a snaha o decentralizovanou měnu

V průběhu dějin jsme pozorovali postupné ovládnutí peněz bankami a vládami, které vedlo k dnešnímu fiat systému a jeho katastrofálním důsledkům pro společnost. Vzestup nových technologií, jako je šifrování a internet, však umožnil vznik nových myšlenek, jako jsou nezávislé digitální peníze bez možnosti vládních zásahů, otevřené a přístupné všem. Pojďme se podívat na příběh těch, kteří stojí v čele tohoto revolučního hnutí: cypherpunk.

5.3.1 Cypherpunkeři

> Počítač by se měl raději použít jako nástroj k osvobození a ochraně lidí než k jejich ovládání.
>
> **Hal Finney**

Ve druhé polovině 20. století se objevilo několik technologických objevů, jako je počítač a internet, které vytyčili cestu novému digitálnímu věku.

Skupina lidí zjistila, že tyto masivní inovace brzy změní fungování společnosti. Předvídali potenciál i nebezpečí osobního počítače, a to buď jako nástroje umožňujícího svobodu a podporující postavení jednotlivce, nebo jako nástroje pro úplnou kontrolu a dohled.

Tito lidé se nazývali Cypherpunkeři. Vznikli jako volně propojená skupina aktivistů, kryptografů, programátorů a zastánců soukromí, kteří sdíleli společnou vizi: snahu o soukromí, bezpečnost a decentralizovanou digitální budoucnost. Termín "cypherpunk" vznikl spojením slova "cypher", které označuje kybernetiku, a slova "punk", které představuje protestní étos rebelství.

Členové hnutí Cypherpunk věřili v sílu kryptografie, která chrání osobní svobody. Mezi jejich cíle patřil vývoj nástrojů pro zabezpečení online komunikace, anonymizaci internetových aktivit a zavedení digitálních měn, které by fungovaly mimo kontrolu centralizovaných orgánů.

Cypherpunkeři pochopili důsledky fiat systému a viděli hrozbu takzvané ,,orwellovské budoucnosti". Věřili, že musí zajistit, aby se osobní počítač a internet staly pro lidstvo přínosem, a ne nástroji, které by mohly prohloubit kontrolu státu nad lidmi.

DEFINICE ORWELLOVSKÉ BUDOUCNOSTI:

Orwellovská budoucnost označuje dystopickou vizi inspirovanou díly George Orwella. Tento termín je spojován s noční můrou a totalitní společností, která se vyznačuje utlačovatelskou vládní kontrolou, rozsáhlým dohledem, propagandou a manipulací s informacemi. Termín "Orwellovský" často popisuje scénář, v němž jsou svobody občanů a jejich individuální potřeby přísně omezeny, nesouhlas je potlačován a realita je překrucována tak, aby sloužila zájmům mocného a autoritářského režimu. Pojem je pojmenován podle George Orwella, který ve svých dílech varoval před potenciálním nebezpečím kontrolou ze strany vládny a omezování základních lidských práv.

Jak problémy vedou k řešení

Mezi klíčové osobnosti hnutí Cypherpunk patřili například Eric Hughes, Timothy C. May a John Gilmore. V roce 1992 napsal Eric Hughes "Cypherpunkový manifest", v němž nastínil zásady skupiny. Manifest zdůrazňoval význam soukromí, šifrování a potřebu, aby jednotlivci převzali kontrolu nad svou digitální identitou.

Shlédněte toto video a poznejte příběh hnutí Cypherpunk!

Jedním z nejvýznamnějších úkolů členů hnutí cypherpunk bylo vytvoření kryptografických nástrojů a protokolů. V roce 1991 představil Phil Zimmermanns protokolem PGP (Pretty Good Privacy), což byl software pro šifrování e-mailů. PGP umožňoval uživatelům posílat šifrované zprávy přes internet, aniž by je mohl dešifrovat kdokoli jiný než zamýšlený příjemce. Předtím mohla být jakákoli zpráva odeslaná přes internet zachycena a přečtena jinými osobami, například vládou.

Cypherpunkeři se domnívali, že průlom šifrování spolu s internetem a počítačem poskytl pevný základ pro vytvoření decentralizovaných sítí v digitálním prostoru, které umožňují jednotlivcům komunikovat a provádět transakce na internetu v soukromí a bez zásahu centrální autority.

Byli jsme tak na správné cestě k lepší budoucnosti pro lidstvo, kde by technologie byla nástrojem k maximalizaci svobody namísto kontroly. Jediným chybějícím prvkem byla decentralizovaná síť a decentralizovaná digitální měna.

5.3.2 Centralizované vs. decentralizované systémy

Centralizované vs. decentralizované systémy: Jedno pravidlo, mnoho problémů
V centralizovaném systému se vše točí kolem jednoho hlavního orgánu, jako například Sauronovo oko v trilogii Pána prstenů. Tento orgán řídí fungování celého systému. Představte si tedy tradiční banky, kde o všem rozhoduje malá skupina lidí.

Příklad z reálného světa: V roce 2022 během pokojných protestů v Kanadě banky zmrazily protestujícím účty a tím ukázaly, jak může centrální orgán zasáhnout a kontrolovat přístup k financím.

Problémy centralizovaných systémů:

- Centrální bod selhání: Pokud se něco pokazí v ústředním orgánu, může se celý systém zhroutit.
- Kontrola: Malá skupina na vrcholu má veškerou kontrolu a moc. Často přijímá rozhodnutí, která jsou pro ni výhodnější než pro všechny ostatní.
- Neefektivita a prostředníci: Podobně jako dopravní zácpy ve městě, mohou být centralizované systémy pomalé a drahé kvůli zbytečným prostředníkům.
- Nedostatek suverenity: Může se stát, že nemusíme mít možnost rozhodovat o svých financích sami, o všem rozhoduje nejvyšší orgán.
- Cenzura a omezení: Stejně jako mohou být některé části města zavřeny z důvodu oprav, mohou centralizované systémy blokovat nebo omezovat přístup k určitým finančním zdrojům.
- Problémy se škálováním: Když finanční služby potřebuje více lidí, centralizované systémy mohou mít problém s tím udržet krok.
- Bezpečnostní rizika: Problémy s centrálním orgánem mohou ohrozit celý systém kybernetickými útoky.
- Nedostatek transparentnosti a důvěry: Vnitřní fungování centralizovaných systémů může být obtížně pochopitelné, takže je pro lidi těžké jim důvěřovat.

Decentralizované systémy: Moc v rukou občanů

Představte si decentralizovaný systém jako velký les. Každý strom představuje samostatnou část a celý les představuje celý systém. Na rozdíl od města s jedním centrálním bodem se decentralizovaný systém podobá spíše odolnému lesu, který může pokračovat v činnosti, i když se některá jeho část potýká s problémy.

- Příklad: Prohlížeč Tor vytváří decentralizovaný systém, v němž mohou lidé zůstat na internetu anonymní a síť je obtížné zastavit nebo cenzurovat.

Výhody decentralizovaných systémů:

- Zvýšená odolnost a spolehlivost: Díky tomu, že neexistuje jediný bod selhání, je systém silný, i když se vyskytnou nějaké problémy.
- Zvýšená bezpečnost: S vhodným šifrováním decentralizovaný systém lépe odolává kontrole ze strany jediné autority.

Jak problémy vedou k řešení

- Větší suverenita: Lidé získávají větší kontrolu nad svými penězi, daty a rozhodnutími.
- Větší transparentnost: Všichni vidí stejné informace, takže systém je důvěryhodnější.
- Povaha bez nutnosti povolení a bez omezení: Každý se může připojit nebo se účastnit, což z něj činí otevřený systém.
- Stejné příležitosti: Každý má stejnou šanci přispět a vyjádřit se.
- Zvýšená ochrana soukromí: Data jsou distribuována mezi více účastníků a většinou jsou pseudonymní, takže decentralizované systémy jsou soukromější.

Zatímco mají decentralizované systémy spoustu výhod, rozhodovací procesy bývají celkem složité, jelikož vyžadují souhlas většiny účastníků sítě.

Změna způsobu, jakým se nakládá s mocí

Ve světě centralizovaných a decentralizovaných systémů záleží na tom, kdo má moc. Centralizované systémy dávají moc malé skupině, zatímco decentralizované systémy ji rozdělují a umožňují každému, aby se vyjádřil. Tento přenos moci znamená spravedlivější a demokratičtější budoucnost, kdy mnoho lidí ovlivňuje systém, který utváří jejich životy.

5.3.3 Stručná historie digitálních měn

Jedním z nejzásadnějších konceptů, o kterém Cypherpunkeři diskutovali, byla digitální hotovost. Členové hnutí si uvědomovali, že je třeba oddělit peníze od státu, aby byla budoucnost ku prospěchu všem. Průkopnická práce Davida Chauma na kryptografických protokolech pro bezpečné a soukromé transakce položila základy tomuto dění. Nevýhodou bylo, že tento protokol vyžadoval ke svému efektivnímu fungování centrální autoritu, což vyvolávalo obavy z jediného bodu selhání a možné cenzury.

V následujících letech se několik cypherpunkerů pokoušelo vzájemně zdokonalovat své nápady, aby vytvořili funkční řešení digitální měny bez vládní kontroly. Následující tabulka popisuje několik klíčových inovací, které Cypherpunkeři při své snaze o vytvoření digitální hotovosti vyvinuli:

Název a datum	Popis	Omezení
E-Cash (1982)	Projekt Davida Chauma E-Cash byl raným konceptem elektronických peněz, který se zaměřoval na ochranu soukromí pomocí kryptografických technik.	Projekt vyžadoval centrální orgán, což vyvolávalo obavy z jediného bodu selhání a možné cenzury.
DigiCash (1990)	Cílem projektu DigiCash, který vynalezl opět David Chaum, bylo vytvořit digitální měnu s důrazem na soukromí.	Centralizovaný model nakonec přispěl k jejímu bankrotu v roce 1998.

B-Money (1996)	B-Money, který navrhl Wei Dai, byl teoretický návrh anonymního distribuovaného systému elektronických peněz.	Nikdy nebyl realizován, zůstal jen koncepčním nápadem. Chyběla praktická implementace.
HashCash (1998)	HashCash, vyvinutý Adamem Backem, byl systém proof-of-work určený k zamezení šíření nevyžádané pošty a útokům typu denial-of-service.	Projekt přímo neřešil problém dvojí útraty spojený s digitálními měnami.
Bit Gold (1998	Bit Gold, který navrhl Nick Szabo, popisuje decentralizovaný systém digitální měny s prvky proof-of-work.	Nikdy nebyl realizován, zůstal teoretickým konceptem.
e-Gold (2004)	e-Gold byla centralizovaná digitální měna krytá fyzickým zlatem, která uživatelům umožňovala nakupovat a převádět jednotky e-Gold.	Právní problémy vedly k jejímu ukončení vládou v roce 2009 a poukázaly na problémy spojené s centralizovanými digitálními měnami.

Navzdory četným pokusům cypherpunkerů vytvořit digitální měnu, která by nebyla pod kontrolou žádné skupiny nebo vlády, se jejich snahy potýkaly s praktickými problémy a nemohly se plně uplatnit v reálném světě. Cypherpunkeři dospěli k závěru, že není tak snadné vytvořit digitální formu hotovosti, která by byla bezpečná, škálovatelná a měla potenciál stát se široce používanou.

Nicméně v příběhu dochází ke zvratu, když jednotlivec, který se poučil z lekcí členů Cypherpunku, povýší koncept decentralizované digitální měny na novou úroveň. V následujících kapitolách se budeme zabývat tím, jak příspěvek této osoby, navazující na 40 let předchozí práce, nakonec vedl k vytvoření funkčního systému.

Kapitola 6

Úvod do Bitcoinu

Pracovní sešit

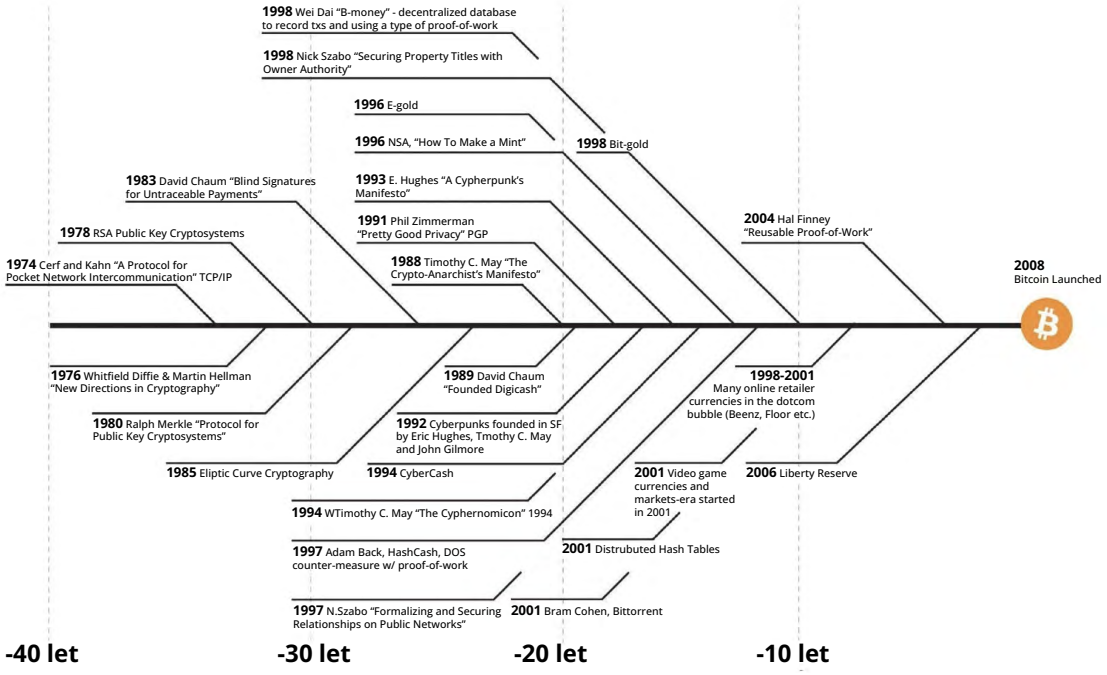
český překlad | 2024

Úvod do Bitcoinu

6.0 Satoshi Nakamoto a vznik Bitcoinu

> Mnoho lidí vzhledem ke všem projektům, které od 90. let zkrachovaly, automaticky odmítá jakoukoliv elektronickou měnu a považuje je za ztracené případy. Doufejme, že to bylo jen kvůli centrálně řízené povaze těchto systémů, která je odsoudila k zániku. Myslím si, že je to poprvé, co se pokoušíme o decentralizovaný systém, který není založen na důvěře.
>
> **Satoshi Nakamoto**

Události před vznikem Bitcoinu - výsledek 40ti let výzkumu, vývoje a poptávky



Jak jste se dočetli v předchozí kapitole, o vytvoření alternativního peněžního systému se pokusilo několik cypherpunkerů. V následující kapitole pokračuje příběh jednoho z nich: vizionáře jménem ,,Satoshi Nakamoto". Tato pseudonymní osoba (muž, žena nebo skupina osob) byla dlouho, ještě před Bitcoinem, součástí kryptografických nadšenců, jako jsou počítačoví vědci a hackeři, kteří se zapojovali do diskusí s cílem najít praktická řešení, jež by nahradila fiat systém.


« previous topic next topic »
print

Page: [1]

Author | Topic: Added some DoS limits, removed safe mode (0.3.19) (Read 25115 times)

satoshi (OP)
Founder
Sr. Member

Activity: 364
Merit: 6671

Ignore

Added some DoS limits, removed safe mode (0.3.19)
December 12, 2010, 06:22:33 PM

There's more work to do on DoS, but I'm doing a quick build of what I have so far in case it's needed, before venturing into more complex ideas. The build for this is version 0.3.19.

- Added some DoS controls
As Gavin and I have said clearly before, the software is not at all resistant to DoS attack. This is one improvement, but there are still more ways to attack than I can count.

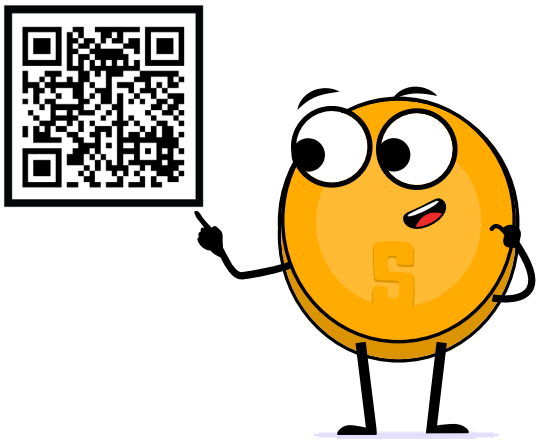
I'm leaving the -limitfreerelay part as a switch for now and it's there if you need it.

- Removed "safe mode" alerts
"safe mode" alerts was a temporary measure after the 0.3.9 overflow bug. We can say all we want that users can just run with "-disablesafemode", but it's better just not to have it for the sake of appearances. It was never intended as a long term feature. Safe mode can still be triggered by seeing a longer (greater total PoW) invalid block chain.

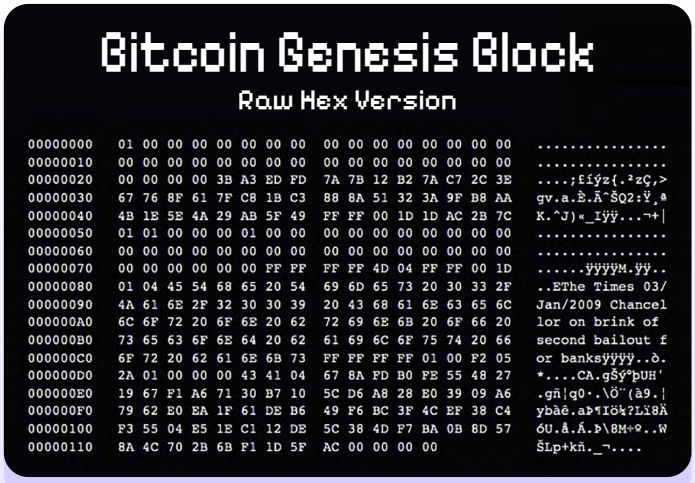
Builds:
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/

V říjnu 2008 Nakamoto představil na kryptografickém mailing listu přelomový dokument s názvem „Bitcoin: A Peer-to-Peer Electronic Cash System". Tento dokument položil základy decentralizovaného peer-to-peer (dále P2P) protokolu, který byl navržen tak, aby umožňoval bezpečné online transakce bez potřeby zprostředkovatelů.

Autorova vize byla jasná: vytvořit čistě P2P verzi elektronické hotovosti, která by se vymanila z kontroly mocných vlád a finančních institucí.



Přejděme k 3. lednu 2009, kdy Nakamoto vytěžil první blok Bitcoinu, známý jako "genesis blok". Tím byla oficiálně spuštěna Bitcoinová síť, nový peněžní systém postavený na bezpečnosti bez nutnosti důvěry prostřednictvím decentralizované účetní knihy. V následujících měsících a letech se k této myšlence začalo přidávat a přispívat stále více nadšenců.



Poté, co se v roce 2011 ukázalo, že Bitcoinová síť může úspěšně fungovat i bez svého tvůrce, poslal Nakamoto e-mail dalšímu vývojáři na Bitcoinu, ve kterém oznámil, že se stahuje ze scény a předává budoucnost Bitcoinu do „dobrých rukou". Čili lidem, kteří sdílejí jeho vizi.

Ačkoli Nakamotova identita zůstává dodnes záhadou, záměr vytvořit měnu jako Bitcoin nebyl nikdy tajemstvím. Nakamoto jej v podstatě vytvořil proto, aby odebral moc několika málo lidem a vrátil ji mnoha lidem vytvořením alternativy v podobě decentralizovaného, otevřeného a transparentního peněžního systému, který odděluje peníze od státu. Vznik Bitcoinu byl Nakamotovou reakcí na finanční krizi z roku 2008, která měla dopad na všechny občany po celém světě a zároveň opět obohatila elitní třídu. Bitcoin byl Nakamotovou odpovědí na korupci a křehkost fiat systému. Satoshi položil základy nové revoluce a odešel od ní, místo aby si nárokoval jakékoliv uznání.

Úvod do Bitcoinu

V následujících letech se Bitcoin začal rychle rozvíjet a stal se symbolem naděje, nezávislosti a odolnosti, který se postavil fiat systému a poskytl bezpečný přístav finančních transakcí odolných vůči cenzuře. Bitcoin je protokol s otevřeným zdrojovým kódem, což znamená, že nikdo nemá moc jej vlastnit nebo ovládat. Jeho zdrojový kód je veřejný a otevřený pro kohokoli, kdo se na něm chce podílet.

Nakamotův sen o transparentním a bezpečném finančním systému bez hranic žije dál a přispívá ke globální revoluci, které jsme dodnes svědky. Běžní lidé každý den dobrovolně opouští fiat systém a vstupují do světa Bitcoinu. Příznivci svobody po celém světě zakládají bitcoinová centra - takzvané bitcoinové cirkulární ekonomiky. Dokonce i celé země, které hledají alternativní cestu, jako například El Salvador, který v roce 2021 jako první stát oficiálně adoptoval Bitcoin jako zákonné platidlo.

6.1 Jak Bitcoin funguje?

6.1.1 Nakamotův mechanismus konsensu (shody)

Bitcoin má spoustu funkcí, vlastností a jeho pomyslná „králičí nora" sahá velmi hluboko. Naštěstí, pokud do světa Bitcoinu vstoupíte poprvé, nemusíte k jeho používání dokonale rozumět tomu, jak funguje. Totéž platí pro používání internetu.

Většina lidí neví, jak funguje protokol TCP/IP, a přesto denně posílají e-maily, zprávy a zveřejňují obsah na svém účtu na sociálních sítích. Totéž platí pro řízení auta. Většina lidí přesně neví, jak auto funguje mechanicky, přesto umí řídit. Bitcoin v tomto není vyjímkou.

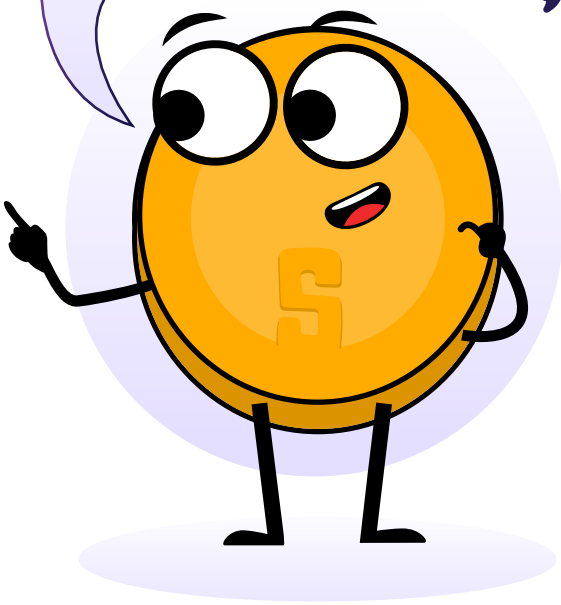
Nicméně Bitcoin zatím není široce rozšířený. Jedná se o poměrně novou technologii, podobně jako byl v 90. letech internet. Z tohoto důvodu může být výhodné pochopit základy Bitcoinu jednoduchým, méně technickým způsobem.

Klíčovou myšlenku Bitcoinu lze shrnout do jedné věty: Bitcoin je soubor pravidel, na kterých se shodli lidé na internetu. Můžete si to představit jako hraní stolní hry s přáteli. Když hrajete deskovou hru, jako jsou Monopoly, jste s ostatními hráči domluveni na konkrétních pravidlech. Jedním z pravidel hry Monopoly je, že se přijímají pouze speciální "monopolní bankovky". Pokud by Jan (jeden z hráčů) porušil pravidla tím, že by místo monopolních bankovek použil na koupi domu toaletní papír, ostatní hráči by Honzovi řekli, že je podvodník, a jednoduše by s ním přestali hrát. Zkrátka, abyste mohli hrát hru, musíte se mezi sebou dohodnout na souboru pravidel a od těchto pravidel se neodchylovat, jinak vás budou ostatní hráči ignorovat.

A takto v podstatě Bitcoin funguje. Bitcoin je síť lidí, kteří se shodují na stejném souboru pravidel. Tato pravidla jsou matematicky vázána, zapsána v počítačovém kódu a přijímána každým, kdo software bitcoinu používá. Pravidla platí pro všechny účastníky stejně, což znamená, že každý je buď dodržuje a je součásti ekosystému a pokud je nedodržuje, síť jej odmítne a nemůže se dál účastnit.

Například jedno z pravidel zní: „Nikdy nebude více než 21 milionů bitcoinů". Pokud si někteří lidé budou chtít vytvořit 1 milion bitcoinů navíc, nebude jim to nic platné, protože by byli automaticky identifikováni a odmítnuti všemi ostatními. Právě díky tomu je bitcoin tak robustní.

> Věděli jste, že od roku 2009 odolal Bitcoin více než desítkám tisíc pokusů o hacknutí, manipulaci nebo jakoukoliv změnu v protokolu? Bitcoin dokázal, že ho nikdo nedokáže zastavit, ovládnout ani zmanipulovat.



Nezáleží na tom, kdo jste nebo odkud pocházíte, pokud vstoupíte do ekosystému Bitcoinu, musíte hrát podle stejného souboru pravidel jako kdokoli jiný.

To platí i pro všechny lidi, kteří měli ve světě fiat obrovskou kontrolu a vliv. Ve světě Bitcoinu není žádný prostor pro podvádění nebo sabotáž. Se všemi se zachází stejně a nikdo s tím nemůže nic udělat.

Úvod do Bitcoinu

6.1.2 Uživatelé systémy

Abychom lépe pochopili decentralizaci Bitcoinu, musíme se hlouběji ponořit do různých rolí v síti. Ve světě Bitcoinu hrají různí účastníci odlišné, ale harmonické role, které přispívají k bezchybnému fungování sítě.

1. Těžaři: Architekti bezpečnosti

Těžaři jsou základním pilířem Bitcoinu. Jsou to lidé nebo skupiny lidí, kteří v zákulisí pracují na zabezpečení sítě prostřednictvím mechanismu zvaného Proof-of-Work (PoW). Tito účastníci disponují speciálními počítači, které obsahují velký výpočetní výkon. Tento výkon dodávají do celé sítě a snaží se vytěžit jednotlivé bloky (soutěží s ostatními těžaři). Dále ověřují transakce a přidávají nové bloky obsahující transakce do decentralizované účetní knihy (tzv. blockchainu). Jejich účast zajišťuje nezměnitelnou podobu účetní knihy a chrání ji před vnějšími útoky.

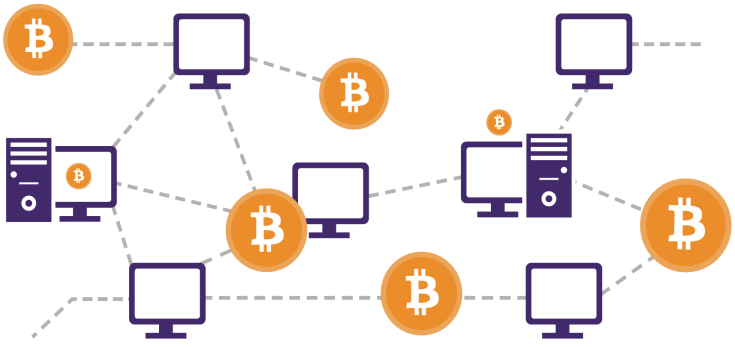
Těžaři, kteří vyřeší ,,hádanku" nejrychleji, jsou díky své ,,usilovné práci" odměněni v podobě nově vzniklých bitcoinů.

Těžaři bitcoinů jsou rozprostřeni po celém světě, čímž chrání síť před centralizací a zajišťují, aby bezpečnost sítě zůstala robustní a distribuovaná.

2. Uzly: Kontroloři pravosti

Bitcoinový uzel může provozovat téměř každý na této planetě. Uzly hrají svou roli v síti tím, že na svých osobních počítačích provozují bitcoinový software, v němž udržují kopii celé účetní knihy. Uzly ověřují transakce a zajišťují, aby všichni účastníci dodržovali pravidla konsensu (shody).

Díky rozdělení odpovědnosti za ověřování konsensu mezi síť uzlů zůstává Bitcoin odolný proti útokům a zachovává si svou důvěryhodnou povahu. Uzly hrají klíčovou roli při udržování neměnného stavu účetní knihy a přispívají k decentralizovanému charakteru Bitcoinu.



3. Uživatelé: Nezávislí účastníci

Jsou hybnou silou bitcoinové sítě, jelokož se podílejí na provádění transakcí. O uživatelích můžete uvažovat jako o běžných lidech, kteří prostě žijí své životy, ale kteří se také určitým způsobem podílejí na integraci Bitcoinu. Někteří uživatelé například spoří své finanční prostředky do bitcoinu. Jiní, jako například občané Salvadoru mohou používat bitcoin jako peníze na nákup potravin a také mohou dostávat bitcoin ve formě výplaty.

Bitcoin posiluje postavení uživatelů tím, že odstraňuje potřebu zprostředkovatelů, jako jsou banky a vlády, a umožňuje přímé P2P transakce. To také znamená, že uživatelé mají nad svými penězi plnou kontrolu, což jim poskytuje určitou suverenitu a nemožnost konfiskovat jejich majetku.

4. Vývojáři: Architekti inovací

Měnový systém budoucnosti se nevybuduje sám od sebe, ani se neujme celosvětově eticky správným způsobem bez vynaložení úsilí. Zde přicházejí ke slovu vývojáři Bitcoinu a projekty postavené na bitcoinové síti.

Vývojáři uplatňují své technické znalosti, aby vylepšili a inovovali bitcoinový protokol. Tito lidé přispívají do zdrojového kódu, navrhují vylepšení a řeší zranitelnosti, čímž zajišťují, aby se síť vyvíjela v reakci na všechny typy výzev. Open-source povaha Bitcoinu vybízí ke spolupráci, a proto umožňuje vývojářům z celého světa přispívat k jeho růstu.

Krása tohoto decentralizovaného přístupu zabraňuje tomu, aby si kontrolu nad protokolem uzurpoval jeden subjekt. To se děje prostřednictvím procesu založeném na konsensu. Vývojáři navrhují změny a pouze ti s nejlepšími nápady, které jsou v souladu s širokou vizí lepšího světa, získají podporu komunity. To umožňuje transparentní a demokratický vývoj Bitcoinu, dokud nebude připraven pro 8 miliard lidí.

Na bitcoinových projektech se podílejí různé skupiny, od neziskových organizací, přes korporace až po skupiny nadšenců či jednotlivce, kteří vytvářejí inovativní produkty. Jedná se o lidi, kteří společně pracují na konkrétním projektu nebo lidi, kteří se zaměřují na širší poslání Bitcoinu, které směřuje ke kolektivní svobodě.

Bitcoinové projekty hrají klíčovou roli při utváření a podporování adopce Bitcoinu a snaží se vytvořit budoucnost, která upřednostňuje posílení pravomocí a svobody všech obyvatel.

Symfonie

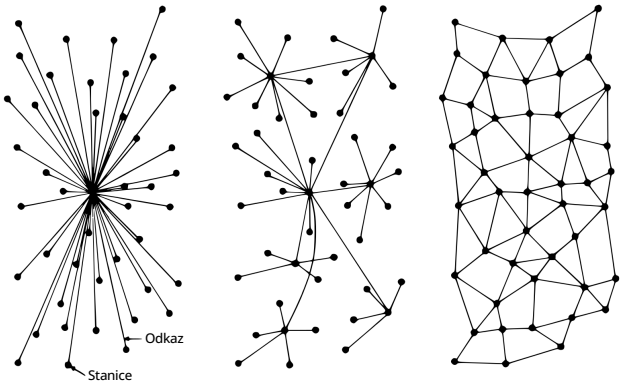
Decentralizaci bitcoinu si lze představit jako symfonický hudební orchestr, v němž všichni hráči hrají na různé nástroje a společně vytvářejí tu nejkrásnější hudbu. V bitcoinové síti není žádný šéf, namísto toho jsou těžaři, uzly, uživatelé, vývojáři a ti všichni plní své role autonomně a ve vzájemné spolupráci.

Decentralizovaná účetní kniha spravovaná uzly zaručuje transparentnost, zatímco mechanismus proof-of-work zajišťuje bezpečnost a brání centralizaci těžby. Uživatelé pociťují finanční suverenitu a nezávislost na kontrole fiat systému. Vývojáři, kteří se řídí metodou konsensu, zajišťují, aby se protokol přizpůsoboval měnícím se potřebám člověka. Bitcoinové projekty svým vlastním jedinečným způsobem přispívají k širšímu poslání kolektivní svobody.

Úvod do Bitcoinu

Jak vidíte, každý účastník hraje zásadní roli při formování adopce Bitcoinu a posilování lidských práv. Každý účastník tohoto decentralizovaného systému přispívá k vyšší odolnosti a životnosti bitcoinu, čímž vytváří ekosystém bez hranic a bez nutnosti důvěry.

Shrnuto a podtrženo, decentralizace v Bitcoinu rezonuje jako důkaz vize Satoshiho Nakamota a obrovského nadšení globální komunity, která usiluje o svobodu a posílení lidských práv.



Aktivita ve třídě - Vytváření konsensu v síti peer-to-peer

Cíl

Pochopit, jak se dosahuje konsensu ve skupině, seznámit se s kryptografií na Bitcoinu.

Materiály

Zpráva s šifrovanými a nezašifrovanými instrukcemi pro akce („zaútočit" nebo „neútočit").

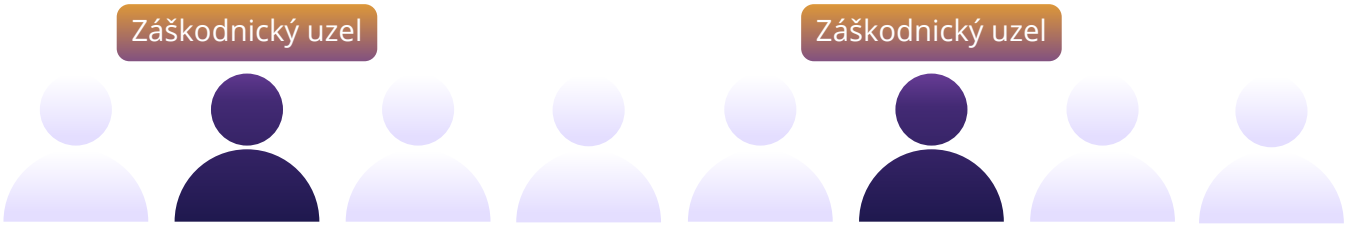
Příprava na aktivitu

Učitel před hodinou vybere skupinu 3 nebo 4 studentů, kteří budou v následující aktivitě „záškodnickými uzly". Těmto záškodnickým uzlům zadá učitel jako domácí úkol v předchozí hodině kryptografickou hádanku.

Postup cvičení:

1. Učitel vybere "iniciátora", který obdrží zprávu na papírku s nápisem "ÚTOK" a sérii čísel, které jsou následující "4-16-14-21-1-21-21-1-3-11-", a to jednomu studentovi ze skupiny.

2. Studenti vytvoří kruh ve vymezeném prostoru a zajistí, aby vybraní studenti, kteří budou škodlivými uzly, nestáli vedle sebe, čímž se zvýší efektivita celé lekce.



3. Jakmile skupina vytvoří kruh, iniciátor předá poznámku jednotlivci na pravé straně kruhu.

4. Poté, co si všichni zprávu přečtou, dá iniciátor skupině pokyn slovem "Teď" a skupina na zprávu současně zareaguje. Pokud zpráva zní "ÚTOK", všichni účastníci udělají krok vpřed.

5. Po počáteční reakci zůstanou někteří studenti (ti, kteří obdrželi zašifrovanou zprávu a správně ji interpretovali) v klidu, zatímco ostatní se budou řídit původním pokynem, což odhalí absenci shody.

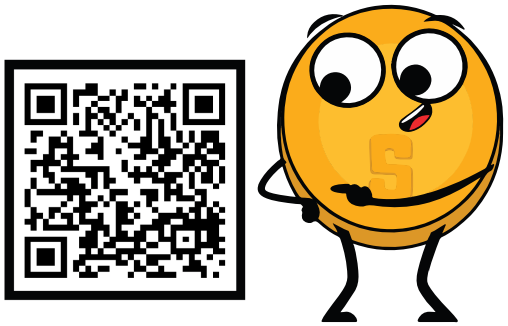
Závěr:

Pobavte se o tom, proč nebylo dosaženo shody, a přibližte si koncept ,,problému byzantských generálů", jak souvisí s nutností dosáhnout společného cíle, a později diskutujte o tom, jak Bitcoin nabízí řešení tohoto problému.

6.2 Bitcoin jako kvalitní digitální peníze

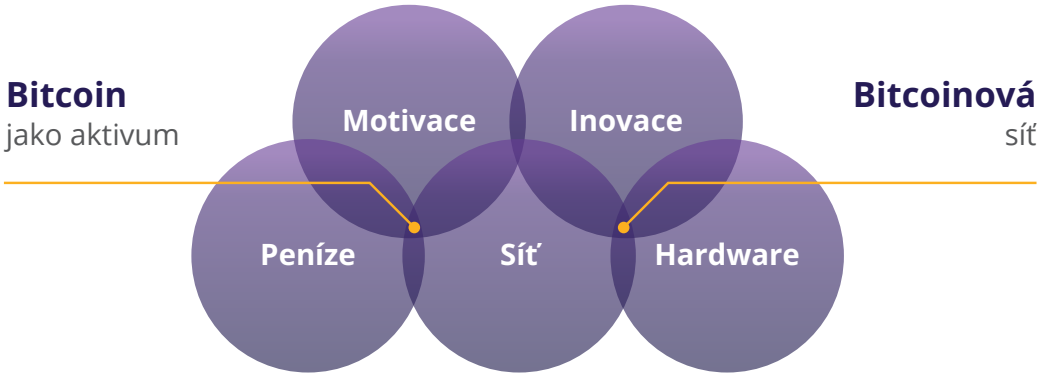
6.2.1 Úvod

Aktivita:
Podívejte se na krátké video „Co je Bitcoin?"



Bitcoin jsou stručně řečeno peníze. Nejedná se o investici, ale spíše o bezpečný a účinný způsob, kam si dlouhodobě uložit své těžce vydělané peníze.

To, že máte bitcoin, neznamená, že z vás bodou boháči, protože vám nepřinese výnos v podobě dalších bitcoinů. Jeho hodnota měřená vůči fiat měně sice dlouhodobě stoupá, ale to jen díky jeho vzrůstající adopci a devalvaci fiat měn.



Bitcoin je nová forma peněz. Je to "internet peněz", což znamená, že se k němu může připojit kdokoli a okamžitě si s ostatními může předávat hodnotu. I ty nejizolovanější a nejchudší komunity na světě mají konečně přístup k peněžnímu systému. Podobně jako může každý, kdo má telefon a připojení k internetu, používat vyhledávač, umožňuje Bitcoin každému, kdo má telefon (lze i bez internetu), přístup k novému globálnímu peněžnímu systému.

Rychlejší a levnější platby

Posílejte peníze po celém světě během několika minut a to s velmi nízkými poplatky.

Zapojení do finančního systému

2,5 miliardy lidí bez bankovního účtu může mít nyní přístup k digitálním transakcím pomocí svého telefonu nebo počítače.

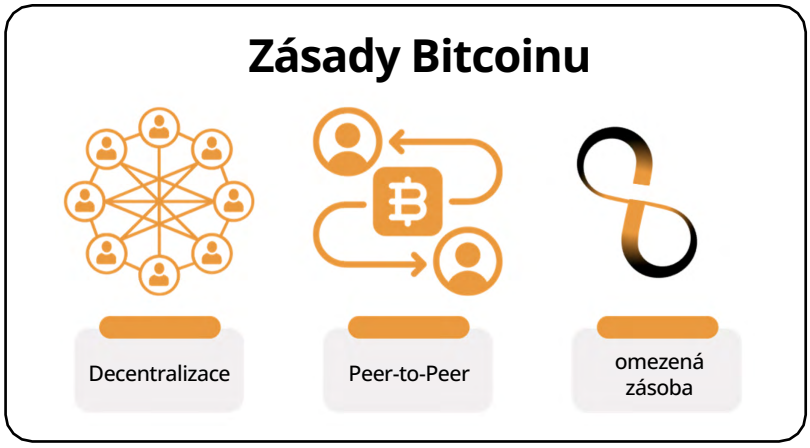
Zvýšená ochrana soukromí

Bitcoinové transakce jsou veřejné, ale vaše identita nikoli.

Bitcoin je kompletně digitální a zároveň bez hranic. Nezáleží na tom, kde se nacházíte, protože se nachází v počítačích a chytrých telefonech lidí po celém světě. Spousta uživatelů po celém světě provozuje software bitcoinu a vlastní kopii jeho účetní knihy.

Tento software a záznam všech transakcí má velmi malou šanci, že zmizí, protože existuje nespočet jeho kopií. K jeho vypnutí by bylo nutné vypnout internet po celém světě, a to navždy. Tento scénář je velmi nepravděpodobný.

A nakonec, bitcoin je vzácný, což znamená, že množství bitcoinových mincí, které mohou existovat, je absolutně omezené. Nikdo nemůže bitcoin padělat. Dokonce ani nejmocnější vlády a finanční instituce.



6.2.2 Vlastnosti Bitcoinu

Evoluce zdravých peněz

Jak jste se dozvěděli v kapitole 2, životní cyklus kvalitních peněz prochází třemi fázemi, než dojde k jejich obecnému přijetí ve společnosti: A to od uchovatele hodnoty přes prostředek směny až po účetní jednotku.

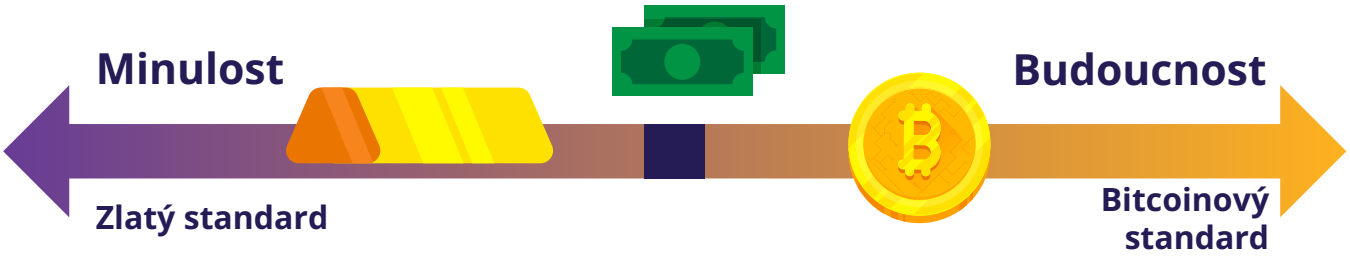
První stádium peněz, které je uchovatel hodnoty, nastává, když si platidlo začne získávat důvěru jako stabilní (nebo zhodnocující se) aktivum v čase. Lidé, kteří tuto skutečnost včas rozpoznají, se snaží chránit své bohatství uložením peněz v této podobě, a to zejména v době geopolitické a makroekonomické nejistoty.

Některé mediálně známé subjekty označují bitcoin za formu "digitálního zlata". Je to proto, že Bitcoin se v uplynulém desetiletí prosadil jako bezpečný uchovatel hodnoty. Každým dnem začíná stále více lidí vnímat bitcoin jako pojistku proti inflaci, podobně jako to v historii dokázalo zlato.

Další fází je posílení důvěry ohledně stability měny. To je okamžik, kdy měna začíná být prostředkem směny a usnadňuje transakce v každodenním životě lidí. V této fázi začíná být široce přijímána pro směnu zboží a služeb.

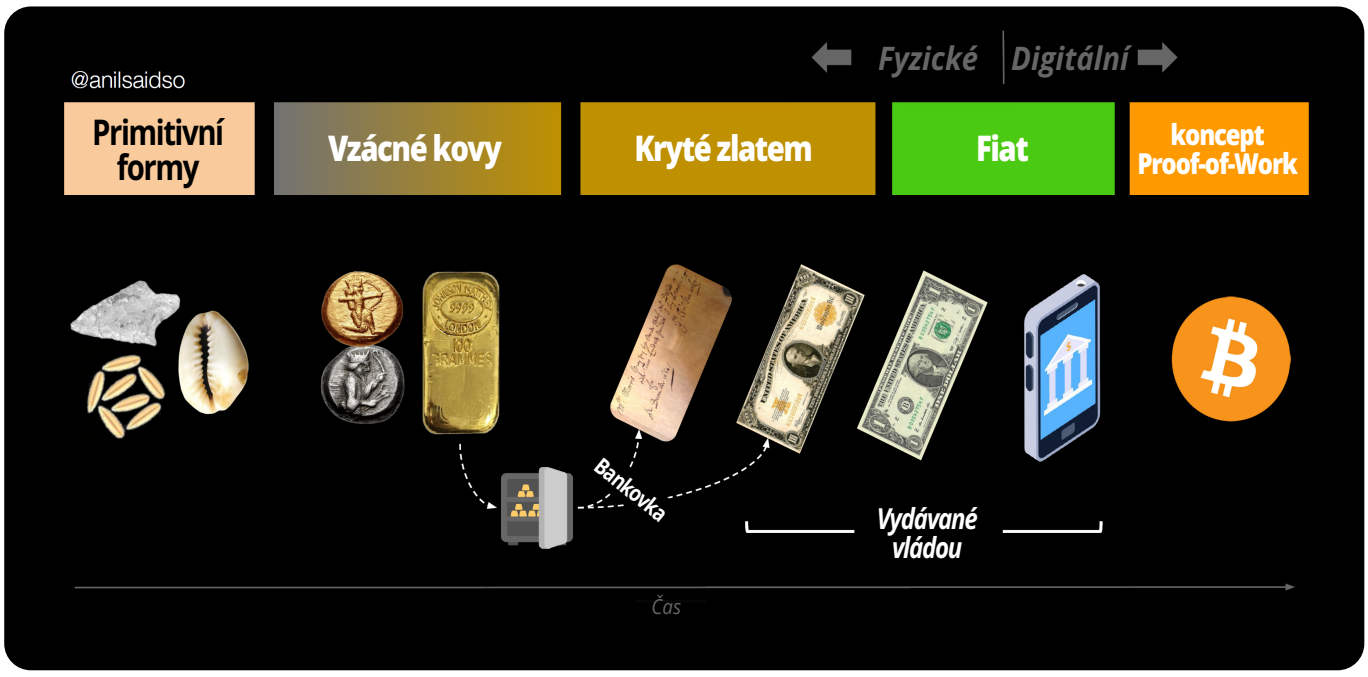
Bitcoin pomalu směřuje k tomu, aby se stal prostředkem směny. S rostoucí mírou přijetí ze strany obchodníků a vývojem protokolu se transakce s bitcoinem stávají efektivnějšími a běžnějšími v každodenním obchodování. Jedním z příkladů je Salvador, kde je bitcoin oficiálně uznán jako zákonné platidlo. Každým dnem začíná stále více běžných občanů a podniků používat bitcoin jako prostředek směny.

Úvod do Bitcoinu



V závěrečné fázi získává platidlo status účetní jednotky, která slouží jako společné měřítko pro oceňování zboží a služeb. V této fázi se stává základním měřítkem, podle kterého se poměřují všechny ostatní hodnoty.

Cesta k tomu, aby se Bitcoin stal účetní jednotkou, je dlouhý proces. Svět v současnosti měří zboží a služby pouze ve fiat měnách, a proto Bitcoin potřebuje širší přijetí a integraci do různých finančních systémů. Nicméně tento předpoklad je již na dobré cestě, protože podniky i jednotlivci začínají uvažovat o denominaci zboží a služeb přímo v bitcoinu.



Jak je vidět, Bitcoin je v tomto evolučním cyklu zdravých peněz na dobré cestě. Až se Bitcoin plně začlení do globálního finančního systému, mohl by se stát standardní zúčtovací jednotkou a změnit tak celý globální monetární systém.

Vlastnosti peněz

Jak jste se dozvěděli v kapitole 2, lidstvo postupem času přišlo na to, že skutečné kvalitní peníze musí mít určité vlastnosti, aby byly efektivní. Těmito vlastnostmi jsou odolnost, dělitelnost, přenositelnost, přijatelnost, vzácnost a zaměnitelnost.

Podívejme se, zda Bitcoin v tomto testu obstojí.

Odolnost: Bitcoin je čistě v digitální podobě, a proto je zcela odolný.

Dělitelnost: Pro srovnání: fiat měnu jako je dolar lze dělit na centy (100 centů = 1 dolar). Bitcoin lze rozdělit na tzv. satoshi neboli sat (100 000 000 sats = 1 bitcoin). A vzhledem k digitálnímu charakteru bitcoinu jej lze v budoucnu dělit ještě více, bude-li to lidstvo potřebovat. Bitcoin je v současné době nejvíce dělitelným peněžním aktivem na světě.

Přenositelnost: V dubnu 2020 bylo převedeno 1,1 miliardy dolarů za pár minut, a to za pouhých 68 centů. Žádný jiný způsob placení nedokáže přesunout tolik peněz s tak nízkými náklady, tak rychle a to pouze v rámci sítě samostatné. Právě to dělá z bitcoinu nejsnáze přenositelnou formu peněz na světě.

Přijatelnost: Bitcoin je stále v počátečním stádiu své existence jako prostředek směny, a proto je v porovnání s fiat měnami jeho akceptovatelnost v současné době nízká.

Vzácnost: Bitcoinů bude vždy existovat pouze 21 milionů. Podle pravidel konsenzu je nemožné, aby se toto množství někdy zvýšilo, což znamená, že počet mincí je nejen vzácný, ale je zároveň nejvzácnějším peněžním aktivem na světě.

Zaměnitelnost: Každá jednotka bitcoinu je stejná jako jakákoli jiná jednotka a lze ji směňovat a obchodovat s ní prostřednictvím protokolu na základě stejného druhu. To z nich činí stoprocentně zastupitelnou měnu.

Bitcoin vs Zlato vs Dolar

Vlastnosti peněz	Zlato	Fiat	Bitcoin
Odolnost	Vysoká	Střední	Vysoká
Přenositelnost	Střední	Vysoká	Vysoká
Dělitelnost	Střední	Střední	Vysoká
Zaměnitelnost	Vysoká	Vysoká	Vysoká
Vzácnost	Střední	Nízká	Vysoká
Ověřitelnost	Střední	Střední	Vysoká
Prověřenost v čase	Vysoká	Střední	Nízká
Odolnost vůči cenzuře	Střední	Střední	Vysoká
Programovatelnost	Nízká	Střední	Vysoká

"Bitcoin vs Zlato vs Dolar" Bitcoin Magazine, https://bitcoinmagazine.com

Bitcoin je druh ,,chytrých" peněz, které jsou programovatelné, nelze je odcizit a mají všechny vlastnosti, díky nimž jsou skvělé pro spoření a snadno použitelné pro obchodníky, kteří chtějí rychlé transakce.

Protože se jedná o transparentní digitální účetní knihu, může být Bitcoin mimořádně efektivní v takových věcech, jako je odhalování podvodných praktik a zjišťování rizik v určitých online službách. Bitcoin má všechny dobré vlastnosti zlata, jako je jeho omezené množství, ale má také výhody oproti fiat měnám, protože jej můžete jednoduše rozdělit a přenášet. Stručně řečeno, od obou aktiv si bere ty jejich nejlepší vlastnosti a to bez jejich omezení a nevýhod.

Co myslíte? Bitcoin sice zatím není široce rozšířen a adoptován, ale mohl být zdravými penězi?

Aktivita: Diskuse ve třídě - Jsou Bitcoin kvalitní peníze?

Nyní, když jsme se Bitcoinem zabývali podrobněji, podívejme se znovu na naši srovnávací tabulku peněz z kapitoly 2 a zhodnoťme, jak si Bitcoin stojí v porovnání s ostatními formami peněz:

Vlastnosti kvalitních peněz	Krávy	Cigarety	Diamanty	Eura	Bitcoin
Odolnost					
Přenositelnost					
Zaměnitelsnost					
Akceptovatelnost					
Vzácnost					
Dělitelnost					
Celkem					

6.2.3 Přijetí osobní odpovědnosti

> Výsledkem je distribuovaný systém bez jediného centrálního bodu selhání. Uživatelé drží kryptografické klíče ke svým vlastním penězům a provádějí transakce přímo mezi sebou formou P2P v síti, která kontroluje, zda nedochází k dvojímu utrácení stejných mincí.
>
> **Satoshi Nakamoto**

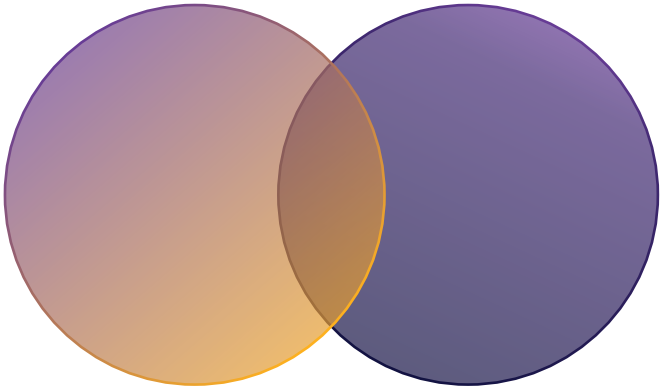
Úvod do Bitcoinu

V systému fiat měn se lidé spoléhají na vlády, banky a zavedené platební instituce. Šéfové těchto institucí určují pravidla sítě a účastníci (většinou běžní občané) se musí těmito pravidly řídit. Nezáleží na tom, kde žijete, vždy existuje soubor standardních postupů, které vás vedou k tomu, co a jak máte dělat.

Díky tomuto systému jsou lidé zvyklí svěřovat odpovědnost za své finance do rukou jiných. Většina lidí například spoléhá na to, že jim někdo jiný pomůže, a to zejména tehdy, když se něco pokazí (například když ztratí přístup ke svému bankovnímu účtu).

„Bitcoin bude zastaven"

Pochopení monetární historie



„Bitcoin se stane zastaralým"

Pochopení Digitálních sítí

„Bitcoin už dávno vyhrál"

Monetární systém Bitcoinu je, jak víte, velmi odlišný. Bitcoin funguje specifickým způsobem a vládci byli nahrazeni autonomním systémem pravidel. Neexistuje žádný diktátor nebo vůdce, což také znamená, že vám nikdo nebude diktovat, co máte dělat. Pokud chcete nově objevenou svobodu a suverenitu v podobě Bitcoinu, budete se muset naučit, jak funguje, a začlenit do svého života tuto technologii způsobem, který vám osobně vyhovuje.

	Jednotka	Vypořádání	Emise
$	1 cent		
₿	Sat 0.00000001		

S Bitcoinem máte nad svými prostředky plnou kontrolu, ale s touto dodatečnou kontrolou přichází i zvýšená zodpovědnost. Například ztráta přístupu k bitcoinům ztrátou privátních klíčů k digitální peněžence znamená, že jste o své úspory přišli natrvalo. Neexistuje žádná zákaznická linka, na kterou byste mohli zavolat, nebo někdo jiný, na koho byste se mohli obrátit v případě problému. Musíte se o své soukromé klíče starat sami.

Naštěstí se to nestane jedincům, kteří se rozhodnou převzít plnou zodpovědnost za svůj život. Používat Bitcoin není ze své podstaty složité, je to jen nový koncept. Případné nepříjemnosti vznikají proto, že jde o něco neznámého. Pokud jste však ochotni naučit se Bitcoin používat a plně přijmout odpovědnost za ochranu svého bohatství, stává se Bitcoin mocným nástrojem, protože jej máte pod kontrolou a nikdo nemůže vaše bohatství zkonfiskovat.

Klíčem k úspěchu je pochopení fungování Bitcoinu a jeho implementace v souladu s vašimi jedinečnými potřebami a životní filozofií. V další kapitole začneme používat bitcoin tím způsobem, že si založíme libovolnou bitcoinovou peněženku, odešleme a přijmeme první transakce a projdeme si osvědčené bezpečnostní postupy.

Kapitola 7

Jak používat Bitcoin

Pracovní sešit

český překlad | 2024

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).

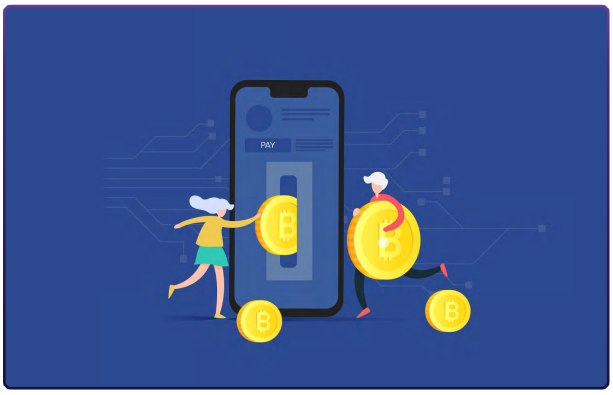
Níže se budeme věnovat výměně fiat měn za bitcoin a naopak, a to jak prostřednictvím osobních transakcí s dalšími účastníky, nebo pomocí směnáren/burz, protože se stále jedná o nejrozšířenější způsob.

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 platforem 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/směnárny

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!

7.2 Úvod do Bitcoinových peněženek

Na rozdíl od fyzických peněz se bitcoiny v bitcoinové peněžence 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 jedlitlivých 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 zmražení účtu. Žádná kontrola ze strany firem nebo vlády, ochrana proti libovolné konfiskaci, jako když máte peníze v peněžence 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**	Zapiště 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!

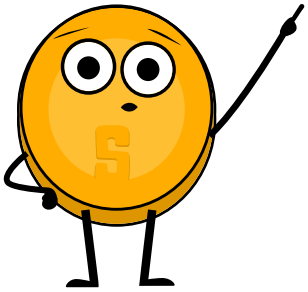
7.2.2 Různé typy Bitcoinových peněženek

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 nim 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.

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

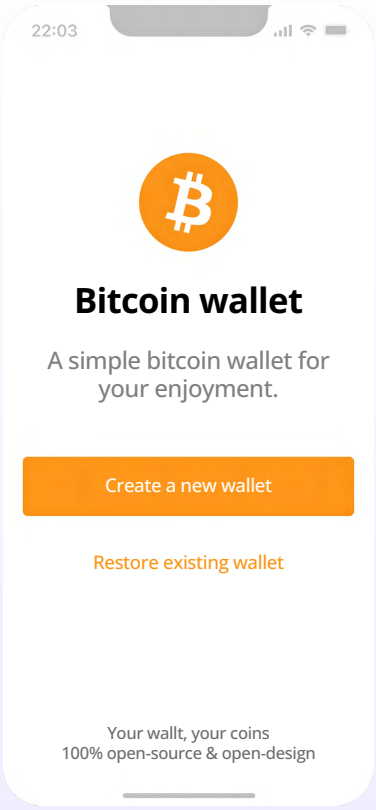
Přejděte na následující webové stránky: **https://bitcoin.org/en/choose-your-wallet** a využijte své nové znalosti o Bitcoinových peněženkách k výběru té nejlepší na základě kritérií, která jsme dnes probrali.

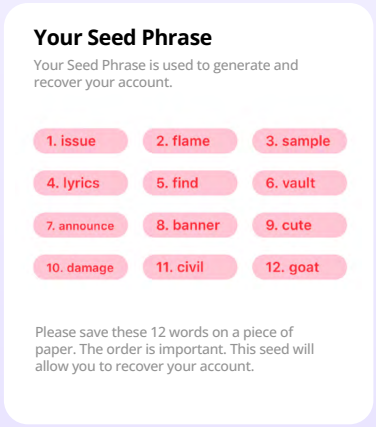
7.3 Nastavení mobilní Bitcoinové peněženky

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:





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 24 slovnou 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.

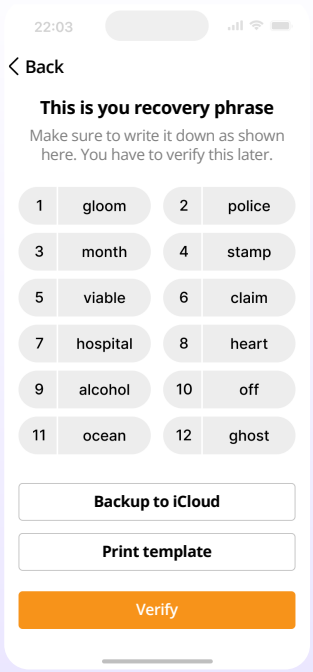
Nezapomeňte, že pokud tuto řadu slov ztratíte nebo zapomenete, nebudete mít v případě ztráty přístup ke svým bitcoinům.

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 "přjmout". Vygenerujte faktru a nyní můžete bitcoin přijmout. Učitel vám malou část bitcoinu na zkoušku pošle.



Třídní 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 možství 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

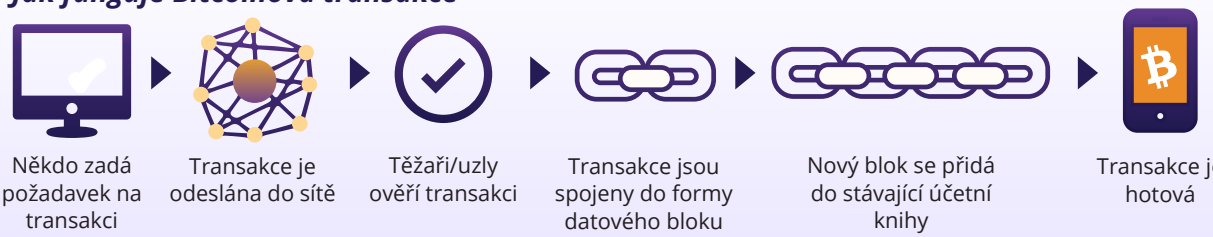
Nové bitcoinové transakce jsou zadávány z peněženek po celém světě, ale neexistuje žádný ústřední zpracovatel plateb. Místo toho těžaři po celém světě soutěží o zápis transakcí do účetní knihy.

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 peněžence 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 peněžence.

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.

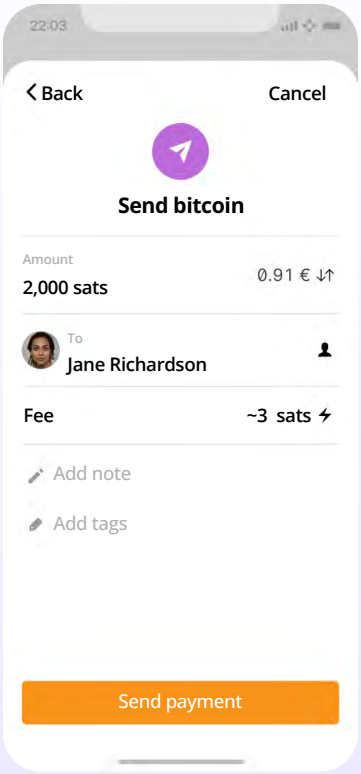
Svou bitcoinovou adresu pak můžete s odesílatelem sdílet několika způsoby:

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 peněžence 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. Bitcoiny 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 vložením 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 překontrolovat 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 sítě. Transakce "on-chain" jsou nejbezpečnějším způsobem, jak provádět transakce s bitcoiny; 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 Bitcoiné síti.

Než začneme, připomeneme si klíčové hráče při bitcoinových transakcích:

- Odesílatelé a příjemci jsou strany, které si vzájemně směňují bitcoiny.
- Uzly ověřují transakce a ukládají kompletní kopii 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

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.
   - Hoďte 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 peněžence.

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 příležitosti" 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.

Kapitola 8

Síť Lightning network: Používání bitcoinu v každodenním životě

Pracovní sešit

český překlad | 2024

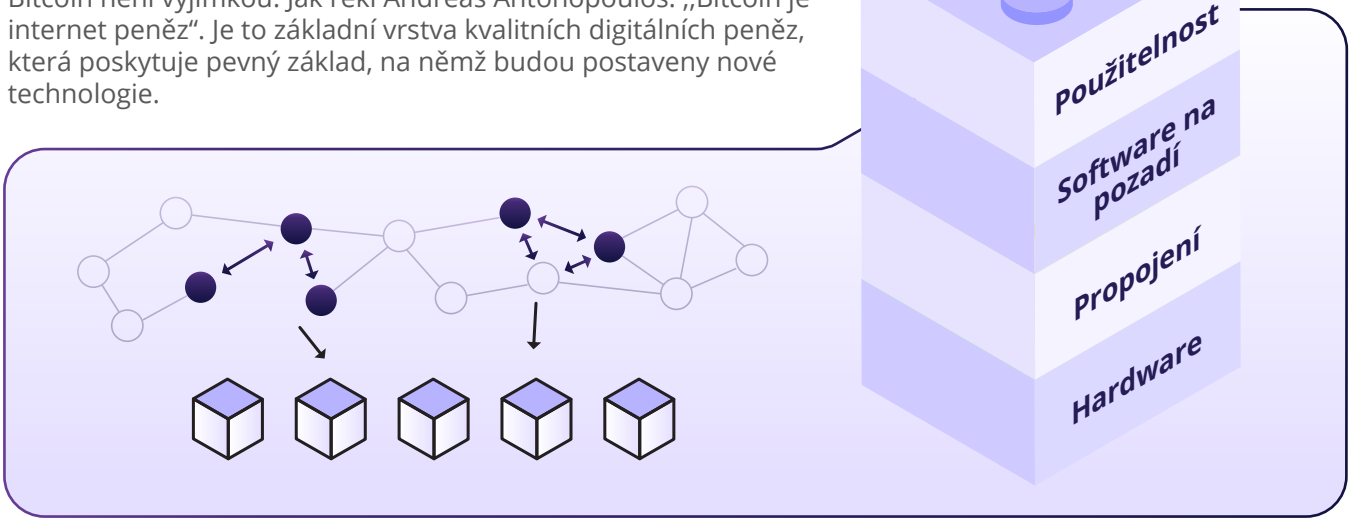
Síť Lightning network: Používání bitcoinu v každodenním životě

8.0 Úvod

> Vytváříme síť Visa , akorát že pro Bitcoin. Co si ale myslím, že je silné narozdíl od Visy je, že každý může stavět na bitcoinových základech.
>
> **Elizabeth Stark**

Technologie obvykle rostou a rozvíjejí se ve vrstvách, podobně jako komín. Vzpomeňte si na svou oblíbenou webovou stránku, e-mail nebo sociální média: byly postaveny na internetovém protokolu, který byl postaven na počítačích, které byly postaveny na elektřině atd. Tyto technologie začínaly s velmi jednoduchou koncepcí a postupem času se dále zdokonalovaly.

Bitcoin není výjimkou. Jak řekl Andreas Antonopoulos: ,,Bitcoin je internet peněz“. Je to základní vrstva kvalitních digitálních peněz, která poskytuje pevný základ, na němž budou postaveny nové technologie.

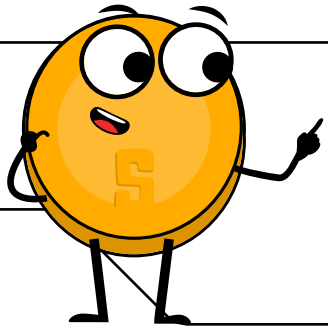


Jedna z těchto vrstev se nazývá Lightning Network. Lightning Network je jako superrychlá dálnice pro Bitcoin. Pomáhá lidem posílat a přijímat bitcoiny opravdu rychle a s velmi nízkými poplatky. Umožňuje uživatelům provádět okamžité a malé transakce nad běžnou Bitcoinovou sítí. Díky tomu si můžete jednoduše a rychle koupit kávu nebo zaplatit kamarádovi.

Nezapomeňte: Satoshi je nejmenší část bitcoinu. Stejně jako lze dolar rozdělit na centy, lze jeden bitcoin rozdělit na menší jednotky zvané satoshi. Jeden bitcoin se pak rovná 100 milionům satoshi. Pokud budeme v této kapitole mluvit o posílání bitcoinu prostřednictvím sítě Lightning Network, budeme tomu říkat "posílání satoshi".

Satoshi	Bitcoin
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

Aktivita: Zhlédněte ,,Vysvětlení sítě Lightning network: Jak to vlastně funguje"



8.1 Lightning Network

Jak jsme právě viděli, Lightning Network slouží jako platební systém, který usnadňuje rychlé a nákladově výhodnější transakce s bitcoiny. Funguje to tak, že si každý účastník vytvoří peněženku (otevře si ,,kanál" s druhou stranou) a na ní bude držet určité množství bitcoinů. Jednotlivci pak mezi sebou mohou provádět nespočet transakcí, aniž by bylo nutné každou z nich zaznamenávat do hlavní účetní knihy (Blockchain). Konečný zůstatek je pak zaznamenán do hlavní knihy po dokončení transakcí.

Funguje to tak, že si každý účastník vytvoří peněženku (otevře si ,,kanál" s druhou stranou) a na ní bude držet určité množství bitcoinů. Jednotlivci pak mezi sebou mohou provádět nespočet transakcí, aniž by bylo nutné každou z nich zaznamenávat do hlavní účetní knihy (Blockchain). Konečný zůstatek je pak zaznamenán do hlavní knihy po dokončení transakcí.

Představte si den strávený prací v kavárně. V očekávání celodenního pobytu si otevřete účet a zaplatíte předem, místo abyste platili pokaždé, když si něco objednáte. Když jste na konci dne připraveni odejít, zkontrolujete s majitelem účet a vyrovnáte konečný dluh. Pokud jste zaplatili více, než byla vaše skutečná spotřeba, dostanete část peněz zpět.

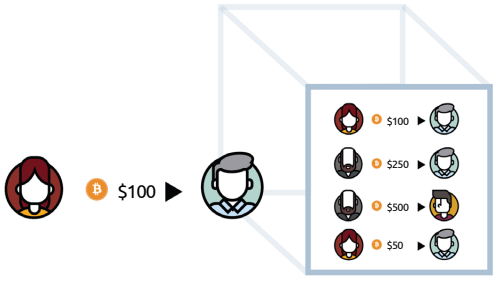
A teď si představte, že tisíce lidí dělají totéž a současně umožňují ostatním používat jejich otevřené účty ke spojení s více lidmi. To je Lightning Network!

Pomocí Lightning network můžete provádět platby komukoli v síti, nejen osobě, se kterou sdílíte platební kanál napřímo. Vaše platba může procházet sítí, dokud nedorazí do cíle, i když nemáte s příjemcem otevřený kanál napřímo.

Podívejme se na rozdíl mezi ,,On-Chain" transakcemi (typ, který jsme probírali v kapitole 7) a Off-Chain transakcemi (síť Lightning):

On-chain transakce:

Jedná se o transakce, které se zapisují přímo do blockchainu Bitcoinu. Jejich potvrzení může trvat přibližně 10 minut (nebo déle) a poplatky závisí na velikosti transakce v bajtech a prioritě, kterou zvolí odesílatel. Tyto transakce jsou bezpečnější, ale pomalejší.

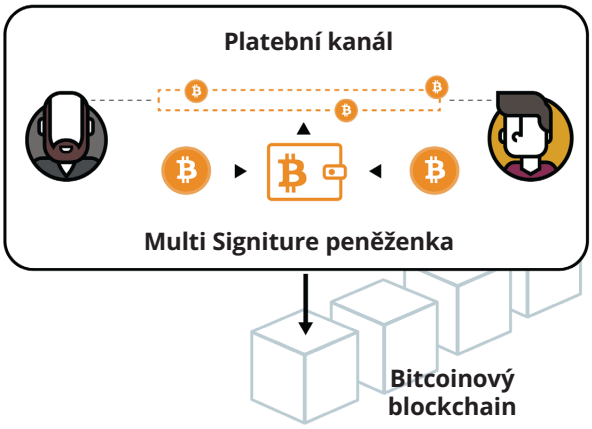


Síť Lightning network: Používání bitcoinu v každodenním životě

Off-chain transakce (Lightning Network):

Probíhají v samostatné síti postavené nad blockchainem Bitcoinu. Jsou vypořádány rychleji a s nižšími poplatky. Ve srovnání s on-chain transakcemi jsou méně bezpečné.

Celkově lze říci, že síť Lightning umožňuje téměř okamžité transakce s velmi nízkými poplatky, zatímco transakce na základní vrstvě Bitcoinu jsou velmi bezpečné, ale pomalejší a dražší.



Platební síť	Bitcoinová síť	síť Lightning
Definice	Decentralizovaná digitální síť, která k zabezpečení finančních transakcí používá kryptografii.	Platební protokol na druhé vrstvě, který funguje nad blockchainem Bitcoinu a umožňuje rychlejší a levnější transakce.
Výhody	Decentralizovaná a bezpečná. Žádné zpětné poplatky ani podvody. Lze používat anonymně (resp. pseudonymně). Globální akceptovatelnost.	Rychlejší a levnější transakce. Větší škálovatelnost. Transakce probíhající off-chain a nezahlcují blockchain.
Nevýhody	Pomalé provádění transakcí. Možné vysoké poplatky. Složitější pro začátečníky.	Vyžaduje důvěru v provozovatele kanálů. Stále se vyvíjí a málo rozšířená. Vyžaduje on-chain transakce pro otevírání a zavírání kanálů.

8.2 Různé typy Lightning peněženek

Lightning peněženka je trochu jiná než Bitcoinová peněženka, i když plní stejnou funkci. Přijímá a odesílá bitcoiny. Rozdíl je v tom, že Lightning peněženka umožňuje posílat bitcoiny v síti Lightning, která je sama o sobě druhou vrstvou nad sítí Bitcoin.

Stejně jako jsme viděli v předchozí kapitole u Bitcoinových peněženek, i Lightning peněženky mají různé vlastnosti, které je třeba zvážit před výběrem jedné z nich.

8.2.1 Vlastní vs. Úschovné peněženky

Lightning peněženky lze rozdělit do velmi specifických kategorií, ale pro zjednodušení je rozdělíme na dvě, stejně jako v předchozí kapitole: vlastní (self-custodial) a úschovné peněženky (custodial).

Tak jako u klasických bitcoinových peněženek je self-custodial Lightning peněženka taková, kde klíče k peněžence kontrolujete vy, zatímco custodial peněženka je taková, kde klíče kontroluje někdo jiný.

Při používání custodial peněženky máte sice přístup k peněžence, ale jste závislí na povolení někoho jiného používat vaše peníze. Vzdáváte se vlastnictví svých peněz ve prospěch pohodlí.

Pro malé částky to může být vyhovující, ačkoli se doporučuje používat self-custodial peněženku, jakmile se s touto technologií lépe seznámíte.

V následujícím textu budeme hovořit pouze o self-custodial peněženkách.

8.2.2 Otevřený vs. uzavřený zdrojový kód

Stejně jako klasické bitcoinové peněženky, které jsme viděli v předchozí kapitole, mohou být Lightning peněženky open-source nebo closed-source. Vždy používejte peněženky s otevřeným zdrojovým kódem, protože jsou zcela transparentní a prověřené komunitou.

Peněženka s open source kódem také znamená, že kdokoli může přispívat ke zdokonalování softwaru, což z ní dělá lepší volbu pro uživatele.

8.3 Nastavení Bitcoinové Lightning peněženky

Nastavení self-custodial Lightning peněženky je stejné jako nastavení self-custodial on-chain peněženky.

Síť Lightning network: Používání bitcoinu v každodenním životě

Třídní cvičení - První možnost: Stáhněte si novou self-custody Lightning peněženku

Jak vytvořit a používat Lightning peněženku.

1. Vyhledejte aplikaci v obchodě App Store (iOS) nebo Google Play (Android).

2. Otevřete aplikaci a napište si 12- nebo 24 slovnou frázi pro obnovení (seed fráze). **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 frázi pro obnovení neboli seed. Za tímto účelem musíte ve stejném pořadí zadat slova svého seedu.

4. Některé peněženky umožňují jako dodatečné bezpečnostní opatření zvolit heslo. Váš soukromý klíč a první bitcoinovou adresu pro vás peněženka vytvoří automaticky.

5. Vygenerujte lightning fakturu, adresu nebo QR kód pro příjem bitcoinů. Převeďte bitcoiny do své peněženky. Co se týče těchto peněženek, ve většině případů si v nichž nemůžete nakoupit bitcoin na přímo, a proto si ho nejdříve musíte sehnat jiným způsobem a následně poslat do této peněženky.

Vaše seed fráze

Vaše seed fráze je použita k vygenerování a obnově vašeho účtu.

1 Issue	2 Flame	3 Sample	4 Lyrics	5 Find
6 Vault	7 Scissors	8 Banner	9 Cute	10 Damage
11 Civil	12 Goat			

Prosím pečlivě si tato slova zaznamenejte ve správném pořadí na kus papíru. Později vám mohou sloužit k obnově vašich prostředků.

*Poznámka: pokud používáte custodial peněženku, nemusíte provádět některé kroky uvedené v části 8.3. Používání custodial peněženky s sebou nese riziko, protože nebudete mít kontrolu nad svým soukromým klíčem, což znamená, že nebudete mít úplnou kontrolu nad penězi, které v peněžence uchováváte.

Nyní, když jsme si nastavili Lightning peněženku, se podíváme na přijímání a odesílání lightning transakcí a taky na to, jak se liší od transakcí on-chain, které jsme odesílali v kapitole 7.

8.4 Odesílání a přijímání Lightning transakcí

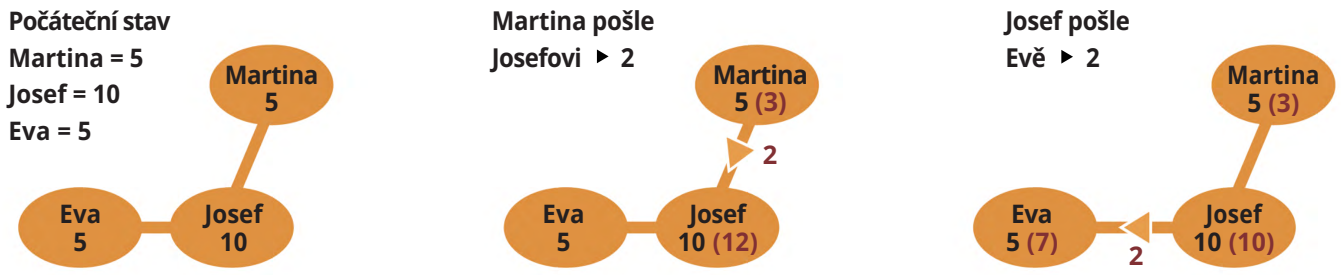
S Lightning peněženkou je používání bitcoinu rychlé, levné a téměř anonymní, takže transakce mezi dvěma účastníky jsou snadné. Bitcoiny můžete rychle posílat a přijímat za věci každodenní potřeby, jako je nákup kávy nebo placení v obchodech.

Podívejme se na několik příkladů Lightning Network v akci:

Příklad 1:

Níže je vidět, že Martina má 5 jednotek nějaké měny a Eva má také 5 jednotek. Martina chce poslat 2 své jednotky Evě, a proto pošle 2 jednotky Josefovi. Ten pak předá tyto 2 jednotky Evě, která má nyní 7 jednotek. Martina má nyní 3 jednotky. A to je vše! Transakce je dokončena.

Klíčové je, že Martina a Eva nemusí pro uskutečnění transakce využívat banku nebo jiného prostředníka.



Josef v tomto scénáři, kdy si Martina a Eva přímo nedůvěřují, vystupuje jako prostředník neboli "důvěryhodná třetí strana". Josef obdrží od Martiny 2 jednotky a poté je předá Evě, čímž je transakce dokončena. Díky využití Josefa jako prostředníka mohou Martina a Eva dokončit transakci bez nutnosti použití banky nebo jiné centralizované instituce, což může transakci urychlit, zlevnit a zabezpečit. Josef je klíčovým prvkem v tomto procesu peer-to-peer transakce.

Josef, jako provozovatel uzlu při transakcích v síti Lightning Network z toho benefituje několika způsoby:

1

Transakční poplatky

Josef získává malý poplatek za každou transakci, která projde jeho uzlem (počítačem), což mu kompenzuje čas a úsilí, které vynakládá na údržbu a provoz svého uzlu.

2

Zapojení do sítě

Provozem Lightning uzlu se Josef zapojuje do sítě a pomáhá zvyšovat její decentralizaci, bezpečnost a stabilitu. To může zvýšit Josefovu pověst a důvěryhodnost jako spolehlivého provozovatele uzlu, čímž se stane atraktivnějším zprostředkovatelem pro budoucí transakce.

Síť Lightning network: Používání bitcoinu v každodenním životě

3 Růst sítě

S růstem sítě Lightning Network a jejím používáním více lidmi se pravděpodobně zvýší počet transakcí procházejících Josefovým uzlem, což může vést ke zvýšení příjmů z transakčních poplatků.

4 Zvýšená bezpečnost sítě

Josefova role prostředníka pomáhá zvýšit bezpečnost sítě tím, že přidává další vrstvu ochrany mezi Martinou a Evou. To může zvýšit důvěru uživatelů v síť, čímž se stane atraktivnější pro nové uživatele a pomůže to podpořit růst. Celkově vzato, být provozovatelem uzlu v síti Lightning Network může Josefovi poskytnout stálý zdroj příjmů a také možnost přispět k růstu a rozvoji sítě.

Shrnuto, **on-chain transakce jsou pomalejší, ale bezpečnější, zatímco off-chain (Lightning Network) jsou rychlejší, ale méně bezpečné.** V závislosti na svých potřebách byste měli zvážit kompromis mezi bezpečností a rychlostí.

Příklad 2:

Nina má oblíbenou jednu restauraci, kam chodí téměř každý den na snídani, oběd i večeři! Je k dispozici několik možností placení a Nina si není jistá, která z nich je nejlepší volbou. Naštěstí se něco málo dozvěděla o Bitcoinu a síti Lightning Network. Po porovnání níže uvedených tabulek Nina nemá nejmenší pochybnosti o tom, že použití metody Lightning je tou správnou cestou.

Lightning network vs tradiční bankovní systém

Výhody	Lightning	Tradiční bankovní systém
Rychlost	Rychlý	Pomalý
Transparentnost	Zcela transparentní	Neprůhledný
Bezpečnost	Velice bezpečný	Zranitelný
Poplatky	Nízká	Vysoká
Možnost začlenění do finančního systému	Vysoká	Omezená

Výhody	Lightning	Tradiční bankovní systém
Škálovatelnost	Vysoká	Nízká
Soukromí	Vysoká	Střední
Interoperabilita	Vysoká	Nízká
Soulad s pravidly zdrojového kódu	Střední	Vysoká
Efektivita nákladů pro používání	Vysoká	Střední

Visa, Inc.

v průměru zpracovává 1 700 transakcí za sekundu.

Maximální kapacita je 65 000 transakcí za sekundu.

Bitcoin On-chain

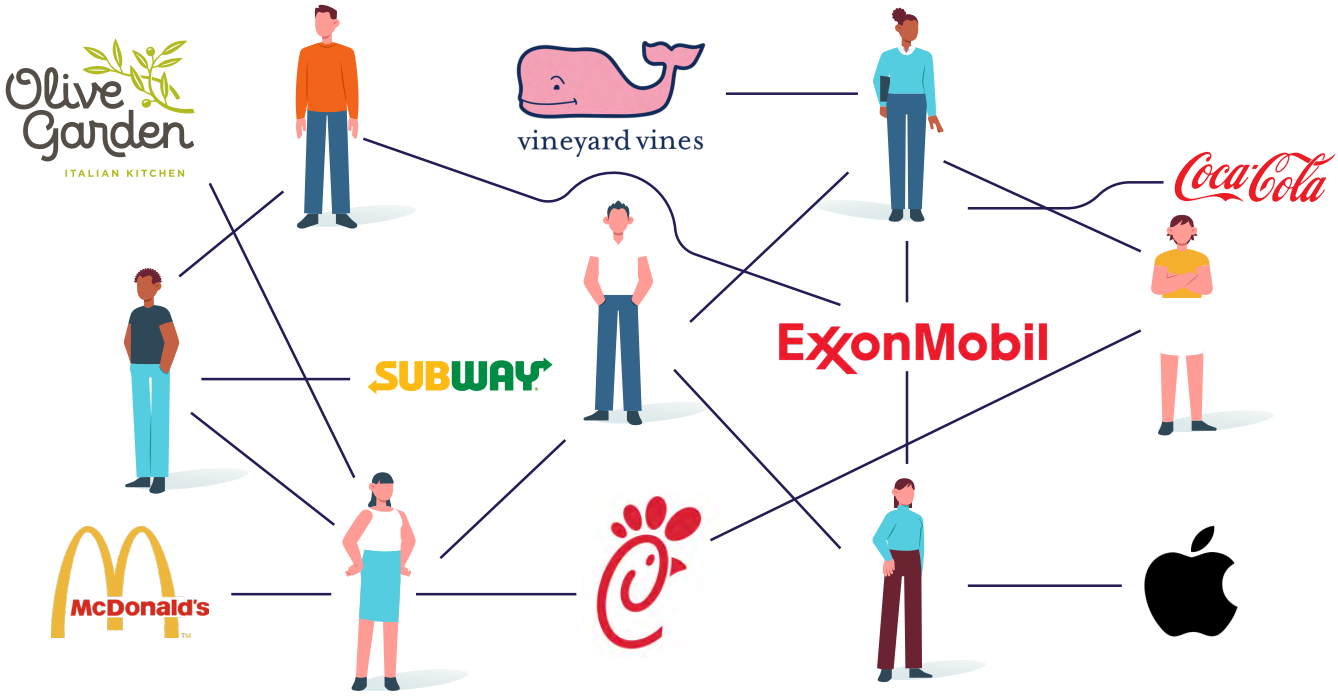
Kapacita je 7 transakcí za sekundu.

Bitcoin Lightning síť

Miliony transakcí za sekundu.

Nina je také příznivcem rychlých, bezpečných a nákladově efektivních transakcí, a proto se rozhodla používat Lightning pro své nákupy v McDonald's. Díky Lightningu si může jídlo vychutnat ještě více, protože ví, že její platby jsou zpracovány okamžitě, bezpečně a s nízkými poplatky.

Pokud to zjednodušíme, tak aby mohla Nina začít používat Lightning, stáhne si nejprve do telefonu aplikaci libovolné Lightning peněženky. Poté svou Lightning peněženku „nabije“ tím, že pošle nějaké bitcoiny ze své běžné bitcoinové peněženky do své nové Lightning peněženky. Tento proces se nazývá „nabití peněženky" nebo „otevření platebního kanálu". Nina může na svou peněženku poslat libovolné množství bitcoinů, které jí vyhovuje, ale je důležité si uvědomit, že množství bitcoinů, které uzamkne ve své Lightning peněžence, nemůže použít při svých on-chain transakcích.



Jakmile je její Lightning peněženka nabitá, může s ní platit ve své oblíbené restauraci, která má svůj lightningový uzel, takže Nina s ním může otevřít platební kanál tak, že pošle část svých bitcoinů ze své Lightningové peněženky na konkrétní adresu, kterou jí restaurace poskytne. Tím se její bitcoiny přesunou z její Lightningové peněženky přímo do jejich peněženky.

Díky otevřenému platebnímu kanálu může nyní Nina utrácet bitcoin, aniž by musela otevírat nový kanál nebo pokaždé platit vysoké poplatky. Kanál zůstane otevřený tak dlouho, dokud ho bude chtít používat jak Nina, tak zmíněná restaurace. Pokud si například Nina nabije peněženku jedním bitcoinem a následně koupí hamburger za 0,0005 bitcoinu (50 tisíc sats), kanál zaznamená, že Nina má nyní 0,9995 bitcoinu. A pokud si následující den koupí mléčný koktejl za 0,0003 bitcoinu, kanál zaznamená, že Nina má nyní 0,9992 bitcoinu.

Síť Lightning network: Používání bitcoinu v každodenním životě

Když se Nina rozhodne, že chce svůj zůstatek použít na něco jiného, uzavře kanál tím, že vyšle signál o transakci do sítě. To se provede tak, že iniciuje uzavírací transakci ve své Lightning peněžence a tato transakce bude obsahovat konečný zůstatek kanálu, na kterém se obě strany dohodly. Transakce je poté odeslána do bitcoinového blockchainu a potvrzena těžaři/uzly. Jakmile je transakce potvrzena, kanál se uzavře a zbývající bitcoiny v kanálu se vrátí zpět Nině a na účet její oblíbené restaurace.

Je důležité si uvědomit, že uzavření kanálu může nějakou dobu trvat, než se vůbec potvrdí v blockchainu. Během této čekací doby jsou prostředky stále uzamčeny v kanálu a nelze je použít pro transakce on-chain. Nina obdrží oznámení, jakmile bude uzavření transakce potvrzeno.

Nyní, když jsme si nastavili lightning peněženku a přečetli si o tom, jak síť Lightning funguje, zahrajeme si hru, ve které budeme posílat satoshi ostatním studentům ve třídě.

Toto je mapa celého světa. Díky síti Lightning Network můžete posílat satoshi jakémukoli uživateli v síti s Lightning peněženkou. Platba dorazí během několika sekund a bude stát jen několik haléřů/korun.

Přesvědčte se sami!

Aktivita: Třídní cvičení - závod Lightning peněženek

1. Nejprve si stáhněte Lightning peněženku do svého telefonu nebo počítače.
2. Postupujte podle pokynů pro instalaci peněženky dle části 8.3 této kapitoly.
3. Jakmile je peněženka nainstalována, otevřete ji a podle pokynů ji nastavte. To může zahrnovat vytvoření nové peněženky nebo obnovení stávající a následně zabezpečení heslem nebo jinou formou ověření.
4. Vygenerujte fakturu, adresu nebo QR kód pro příjem bitcoinu.
5. Jakmile je vaše peněženka nastavena a jste připraveni přijímat satoshi, učitel vám poskytne počáteční množství satoshi tak, že je pošle přímo do vaší peněženky.

A. Úkolem vaší skupiny je přeposílat satoshi z peněženky jedné osoby do peněženky druhé, a to pomocí sítě Lightning Network, dokud se nedostanou k poslední osobě ve skupině.

B. Chcete-li poslat satoshi jiné osobě, otevřete svou peněženku a postupujte podle pokynů pro provedení platby. Budete muset zadat lightning fakturu příjemce nebo naskenovat QR kód a zadat částku v satoshi nebo fiat měně, kterou chcete poslat.

C. Pokud vaše skupina jako první úspěšně pošle satoshi poslední osobě, vyhráváte! (A satoshi si ponecháte).

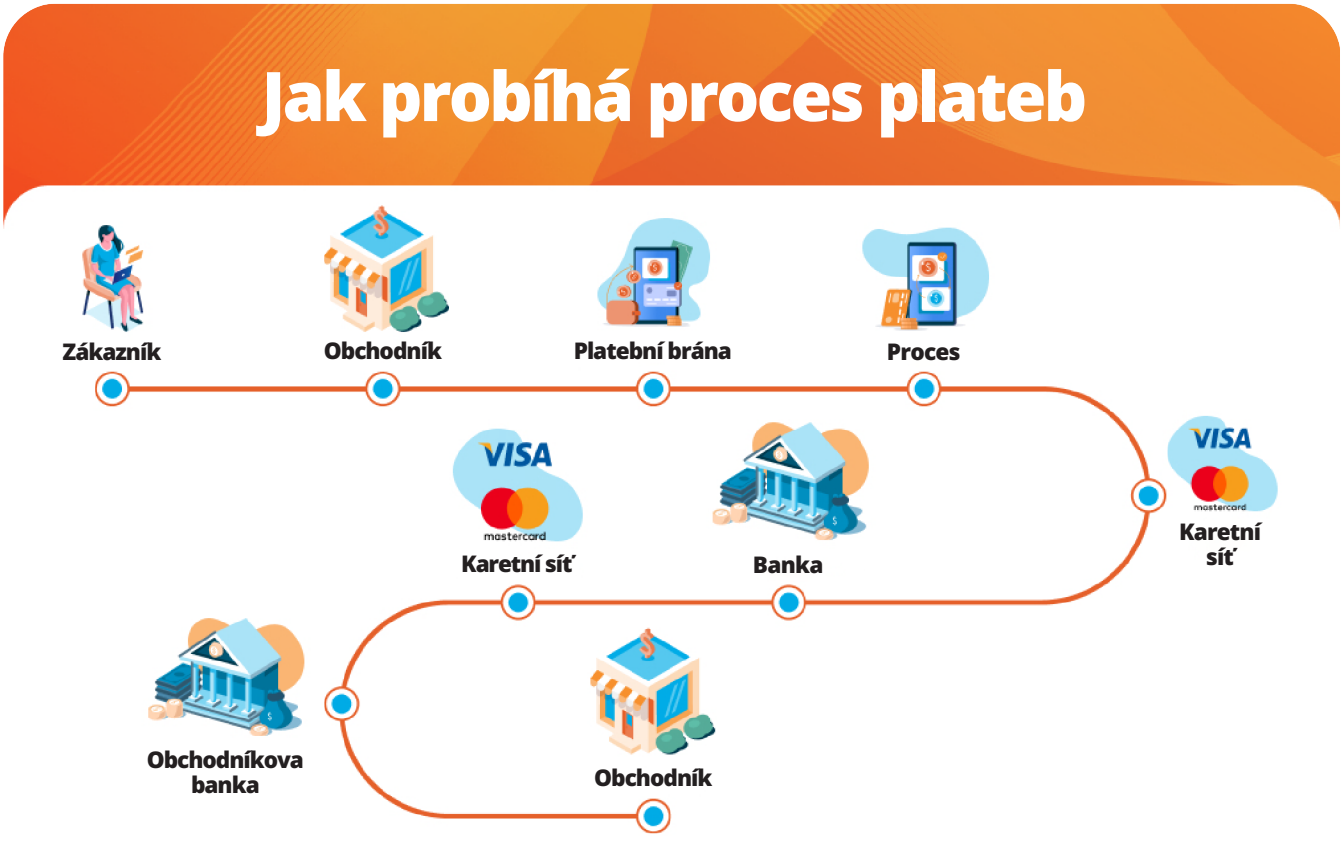
Prodiskutujte případné potíže, které vaše skupina při této aktivitě měla. Bylo odeslání transakce snadné, rychlé a levné? Myslíte si, že je síť Lightning snadná na používání a pochopení?

Síť Lightning network: Používání bitcoinu v každodenním životě

8.5 Nákup kávy a potravin za bitcoin

Přemýšleli jste někdy o tom, že byste si za bitcoin mohli koupit šálek kávy nebo nakoupit potraviny? Ano, je to možné. Existuje mnoho způsobů, které vám umožňují platit bitcoinem. Prozkoumáme některé z těchto možností a také nástroje, které vám pomohou najít místní obchody, abyste mohli bitcoin utrácet.

I když se platba kreditní kartou nebo aplikací může zdát pro platící osobu snadno pochopitelná, zpracování platby je ve skutečnosti velmi složité a zahrnuje mnoho různých stran.



Když nakupujete v obchodě, je do tohoto procesu zapojeno mnoho stran a každá z nich si účtuje poplatek. Pro majitele obchodů mohou být tyto poplatky vysoké, více než 3 % z ceny, což nemusí být zanedbatelná částka.

A to ani nemluvíme o poplatcích za směnu jednotlivých fiat měn!

Poplatky za zprostředkování platby kartou

$100	-$1.75	-$0.14	-$0.30	-$97.81
Zákazník zaplatí	Vypořádající banka	Proces v karetní síti	Platební proces	platba přijde obchodníkovi

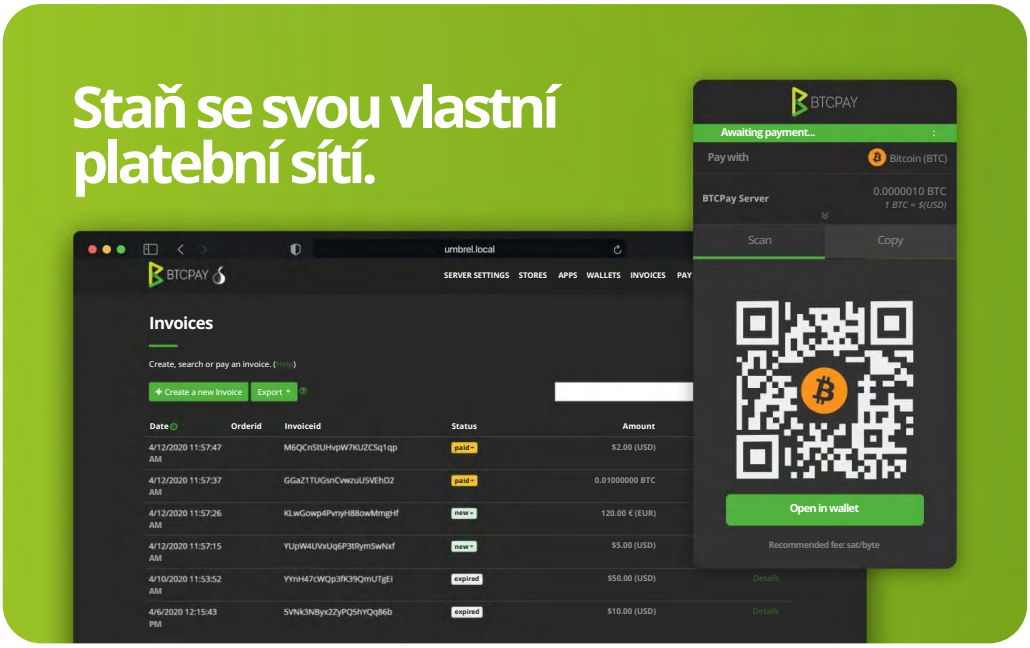
Díky Bitcoinu a síti Lightning mohou podniky přijímat okamžité platby z celého světa prostřednictvím bezpečného internetového systému bez hranic, který je odolný vůči cenzuře a případné konfiskaci.

Dále se podíváme na několik způsobů, jak mohou obchodníci snadno přijímat platby v bitcoinu.

8.5.1 Online: Platební nástroje – E-commerce

BTCPay Server je open-source platební procesor, který umožňuje obchodníkům přijímat platby v bitcoinu bez větších technických znalostí. Je zcela zdarma a neúčtuje si žádnou provizi.

Internetové podniky mohou BTCPay Server bezproblémově integrovat přidáním pluginu BTCPay na své webové stránky.



Síť Lightning network: Používání bitcoinu v každodenním životě

Protože BTCPay Server je open-source projekt, nikoli společnost, můžete se do projektu zapojit, jakmile se o něm a počítačovém programování dozvíte více.

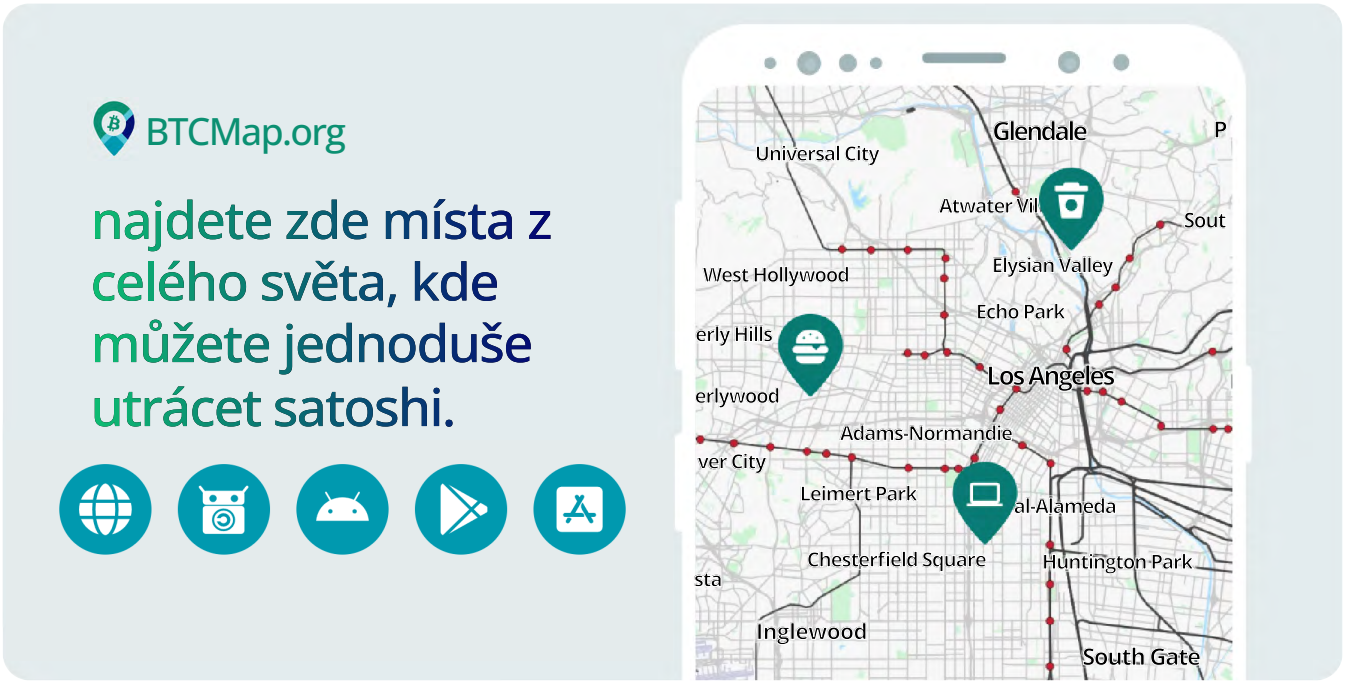
Mrkněte na BTCPayServer https://btcpayserver.org/ pro více informací o tom, jak tento platební systém používat.

8.5.2 Osobně: Najděte obchodníka ve svém okolí

Fyzické obchody mohou k přijímání plateb používat také BTCPayServer nebo si mohou jednoduše stáhnout jakoukoliv bitcoinovou peněženku a přijímat platby přímo prostřednictvím svého telefonu nebo počítače.

Chcete-li najít obchodníka, který přijímá bitcoiny ve vašem okolí, přejděte na stránku BTCMap.org a vyhledejte svůj region.

BTCMap.org je mapa s otevřeným zdrojovým kódem, kde mohou obchodníci, kteří přijímají bitcoin, uvést své podniky. Jedná se o užitečný nástroj pro lidi, kteří chtějí utrácet své bitcoiny po celém světě.



8.5.3 Přechodové nástroje: Poukázky, dárkové karty a platební karty

Chcete-li nakupovat produkty z obchodů, které ještě nepřijímají bitcoiny, můžete k tomu použít prostředníka: Dárkové karty.

Některé podniky se zaměřují na nákup a prodej dárkových karet výměnou za bitcoin. To znamená, že si můžete výměnou za bitcoin pořídit dárkovou kartu obchodu, do kterého chcete jít, a pak jít dárkovou kartu utratit přímo do obchodu.

Letenky, hotely, hry, eSIM, poukazky do obchodů - dárkové karty zkrátka můžete koupit téměř na cokoliv! Jedním z příkladů je služba Bitrefill, která je velice rozšířená a populární díky své široké nabídce služeb.

8.5.4 Cirkulární ekonomiky a bitcoin jako prostředek směny

Koncept cirkulární ekonomiky vychází z myšlenky úplně jiného zaměření, a to minimalizace odpadu v ekonomice prostřednictvím opětovného použití a recyklace co největšího počtu výrobků a vedlejších produktů.

Z tohoto konceptu vychází i bitcoinová cirkulární ekonomika, kde se transakce provádějí v bitcoinu a kde peníze zůstávají a rostou v rámci jedné ekonomiky.

Síť Lightning network: Používání bitcoinu v každodenním životě

Lightning Network umožňuje rozvoj cirkulární ekonomiky téměř po celém světě a to díky téměř okamžitým transakcím s nízkými poplatky.

Historicky první Bitcoinová cirkulární ekonomika se nachází v nizozemském Arnhemu. Vznikla dávno předtím, než se objevila síť Lightning Network, ale tehdy byly on-chain poplatky opravdu nízké!

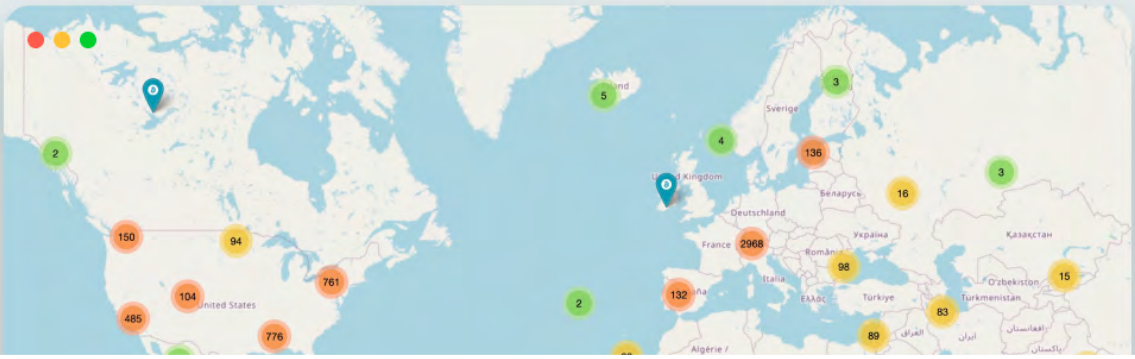
Druhým místem byla Bitcoinová pláž, která se nachází v El Zonte, ve státu Salvador. Ta využila potenciál sítě Lightning Network a poskytla lidem, kteří většinou neměli ani bankovní účet, okamžité digitální platby pomocí jejich chytrých telefonů!

V současné době vznikají po celém světě stovky cirkulárních ekonomik, které jsou postaveny na Bitcoinu a jeho ekosystému.

Na stránkách BTCmap.org nebo jednadvacet.org můžete vyhledat bitcoinové komunity, kde se setkáte s dalšími uživateli bitcoinu a najdete podniky, které bitcoin přijímají. Jakmile budete připraveni a například uvidíte, že ve vašem městě ještě bitcoinová komunita není, můžete jednu založit vy!

BTCMap.org

najdete zde místa z celého světa, kde můžete jednoduše utrácet satoshi.



zdroj: btcmap.org/communities ; https://jednadvacet.org/

V kapitole 8 jste získali informace o používání Bitcoinu v každodenním životě prostřednictvím sítě Lightning Network. Lightning Network usnadňuje rychlejší a dostupnější transakce a nabízí náhled na to, jak se bude Bitcoin v dalších vrstvách měnit a vyvíjet.

V kapitole 9 prozkoumáme technickou stránku Bitcoinu. Připravte se na bližší seznámení s tím, jak Bitcoin skutečně funguje, a to od kryptografie přes uzly až po těžaře a další.

Kapitola 9

Úvod k technické stránce Bitcoinu

Pracovní sešit

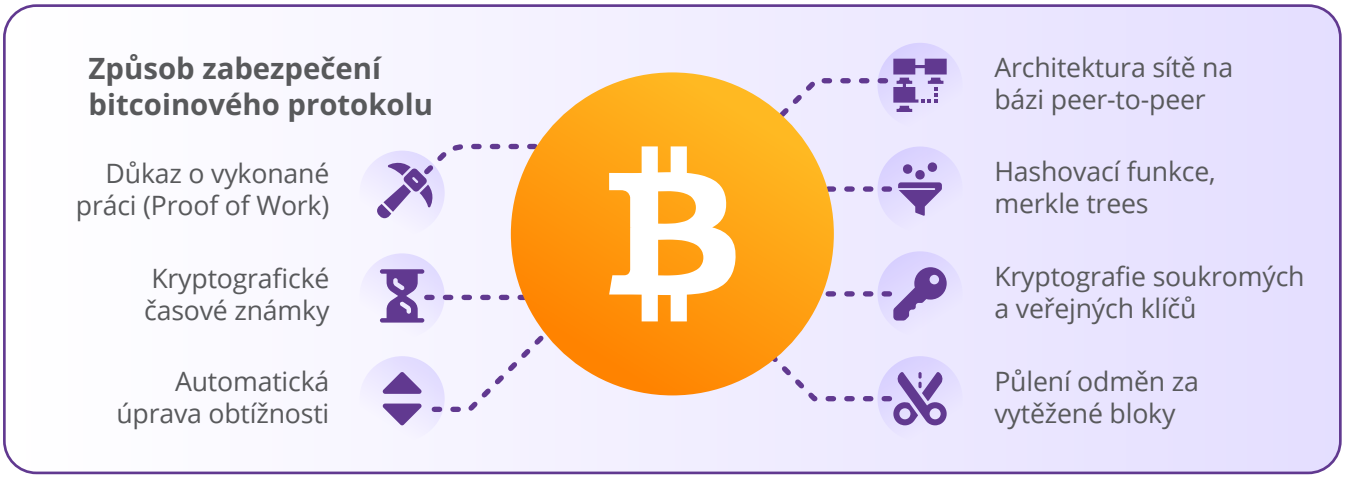
český překlad | 2024

Úvod k technické stránce Bitcoinu

9.0 Úvod

> Bitcoin není neregulovaný. Místo toho, aby byl regulován vládní byrokracií, je regulován algoritmem. Je tedy nezkorumpovatelný.
>
> **Andreas M. Antonopoulos**

V této kapitole se blíže podíváme na technologii, která umožňuje zcela decentralizované fungování Bitcoinové sítě. Zjednodušeně si vysvětlíme, co se děje při odesílání transakcí, jak se tyto transakce zpracovávají a co dělají těžaři a uzly v síti. V této kapitole se budeme zabývat některými náročnějšími a technickými koncepty. Důležité je si uvědomit, že mnoho lidí například nerozumí ani tomu, jak dnes funguje internet, a přesto ho denně používají k posílání e-mailů, kontaktování přátel na sociálních sítích a dokonce i k placení účtů. Naučit se technickou stránku fungování Bitcoinu je dlouhá cesta, kterou nemusí chtít podniknout každý, i když se rozhodne používat ho jako peníze. I když vám doporučujeme, abyste se o technických aspektech Bitcoinu učili dál, v této kapitole se zaměříme na základní klíčové pojmy.



Chcete-li se hlouběji seznámit s technickými aspekty fungování Bitcoinu, v zadní části této učebnice naleznete zdroje. Na našich webových stránkách se také můžete zaregistrovat do kurzu Bitcoin Diploma - Technical Edition, abychom vás kontaktovali, jakmile bude tento odbornější kurz dostupný.

Pojďme se podívat na video, které ukazuje, jak Bitcoinová síť funguje.

Aktivita: Zhlédněte „Jak Bitcoin funguje pod pokličkou"

Jak jste viděli ve videu, Bitcoinová síť je zjednodušeně řečeno účetní kniha nebo záznam transakcí, který je uložen na mnoha počítačích, které nazýváme uzly. Bitcoinová účetní kniha je pseudonymní, což znamená, že neobsahuje osobní údaje, pouze informace o transakcích a adresách. V účetní knize jsou uvedeny všechny bitcoiny a jejich pohyby od spuštění sítě 3. ledna 2009.

Dále se podrobněji podíváme na technologii, která umožňuje, aby byl tento systém funkční.

9.1 Veřejné a soukromé klíče: Zabezpečení skrze kryptografii

> Bitcoin nám nabízí závazný slib: tento program bude vykonávat přesně to, co bylo stanoveno ve zdrojovém kódu.
>
> **Andreas M. Antonopoulos**

9.1.1 Kryptografické veřejné/ soukromé klíče

Kryptografie je způsob utajení informací jejich zašifrováním v kódu.

- Šifrování je proces, při kterém se informace převezme a převede do speciálního kódu, tak aby ji nikdo, kdo nemá správnou dešifrovací metodu, nemohl přečíst. Je to podobné jako při zamykání trezoru, který může otevřít pouze osoba se správným klíčem nebo kombinací.

- Dešifrování je oproti tomu proces, kdy se zašifrované informace vezmou a znovu se stanou čitelnými, podobně jako když odemknete trezor a můžete si informace uvnitř přečíst.

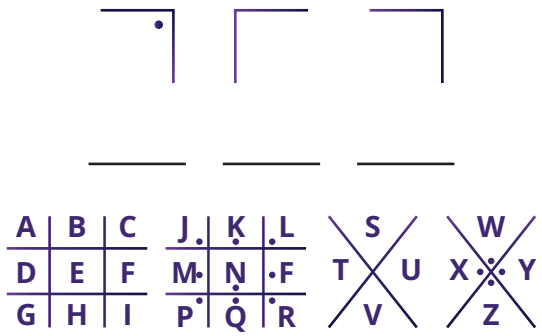
Řekněme například, že Jan chce poslat Adamovi tajnou zprávu, kterou nemá nikdo jiný číst. Dohodnou se, že před odesláním zprávy použijí k jejímu zamaskování Pigpen šifrovací metodu. Zprávu mohou dešifrovat pouze ti, kteří šifru znají, takže pro kohokoliv jiného je nečitelná. Ačkoli tato metoda není dnes považována za bezpečnou, ilustruje princip šifrování pomocí soukromého klíče pro odesílání zpráv.

Jak vyřešit

Pigpen šifru

Při řešení Pigpen šifry dostane hráč zašifrovanou zprávu a šifru. Aby hráč dešifroval zprávu, musí najít symbol ze zašifrované zprávy na šifře a najít tak dešifrované písmeno.

- Příklad zašifrované zprávy:



Jak tedy funguje kryptografie při Bitcoinových transakcích?

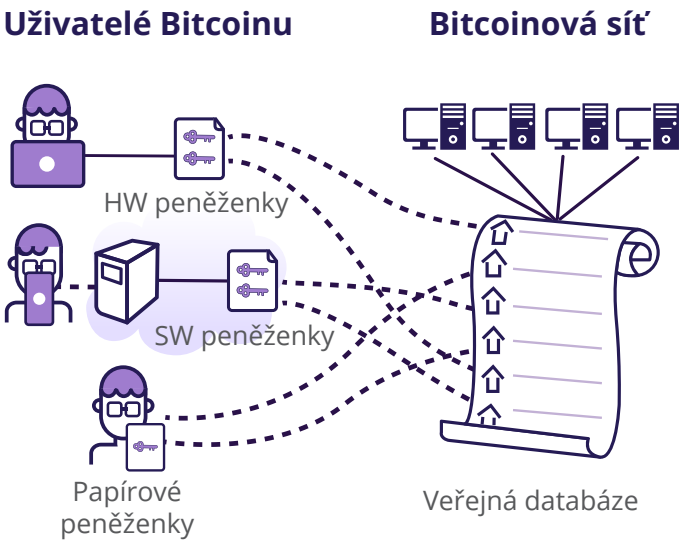
V tradiční kryptografii soukromých klíčů by Jan a Adam museli nejprve vzájemně nasdílet tajný klíč, například heslo nebo Pigpenovu šifru. Jan by pak tento klíč použil k zašifrování své zprávy před odesláním Adamovi. Adam, který také zná tajný klíč, by pak použil stejný klíč k dešifrování zprávy a jejímu přečtení.

Pokud by však klíč vlastnil někdo jiný a zprávu zachytil, mohl by ji taky zašifrovat a přečíst.

Úvod k technické stránce Bitcoinu

Kryptografie s veřejnými klíči, která se používá v Bitcoinových transakcích, tento problém řeší. Díky kryptografii s veřejným klíčem si Jan a Adam nemusí navzájem sdělovat heslo ani způsob šifrování. Místo toho má každý z nich dva různé klíče: **veřejný klíč** (který může bezpečně sdílet s kýmkoli) a **soukromý klíč** (musí zůstat soukromý).

V tomto případě, když chce Jan poslat zprávu Adamovi, může před odesláním zprávy použít Adamův **veřejný klíč** k zašifrování své vlastní zprávy. Když Adam zprávu obdrží, může ji dešifrovat pouze on pomocí svého **soukromého klíče**. Kdokoli jiný, i kdyby zprávu zachytil, by ji nemohl přečíst. Šance na krádež klíče je také mnohem menší, protože ani Jan ani Adam si nemusí tento klíč navzájem sdělovat.



Hlavní výhodou kryptografie s veřejnými klíči oproti kryptografii se soukromými klíči je tedy to, že umožňuje bezpečnou komunikaci, aniž by odesílatel a příjemce museli nejprve sdílet tajný klíč (nebo jinou šifrovací metodu), který by mohla zachytit třetí strana.

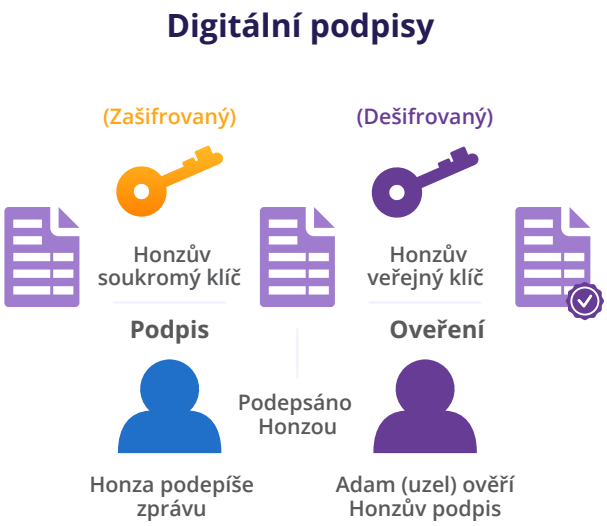
V Bitcoinu se k odesílání šifrovaných zpráv nepoužívá kryptografie s veřejným klíčem. Místo toho se používá k vytváření jedinečných **digitálních podpisů**, díky nimž jsou bitcoinové transakce neměnné. **Digitální podpis** je způsob, jak prokázat pravost bitcoinové transakce, v jistém smyslu podobný tomu, když napíšete svůj podpis na fyzický dokument.

Kryptografie veřejných klíčů (pro transakce mezi dvěma uživateli):

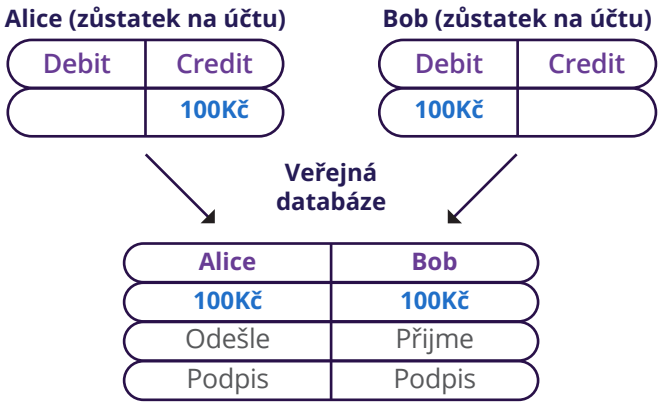
Každý uživatel má dva klíče, **soukromý klíč**, který je **uchováván v tajnosti**, a **veřejný klíč** který může **sdílet s ostatními.**

Soukromý klíč slouží jako forma identifikace a důkaz vlastnictví, který potvrzuje, že **„tato adresa patří mně a mám nad ní úplnou kontrolu“.**

Digitální podpisy se vytvářejí za účelem identifikace jedinečných transakcí.



- Bitcoinové transakce zahrnují převod určitého množství bitcoinů přímo na adresu jiné osoby.
- Šifrování se používá k zajištění toho, aby pouze skutečný držitel bitcoinu měl kontrolu nad tím, zda může své peníze poslat někomu jinému. Zajišťuje, aby byl majetek střežen před zneužitím jinými aktéry.
- Jako dodatečné ochranné opatření má každá transakce, kterou odešlete v bitcoinu, automaticky **UNIKÁTNÍ podpis**. Tento **jedinečný podpis** je vybaven technologií prokazující neoprávněnou manipulaci, která pomáhá síti ověřit, že bitcoin odeslal skutečný vlastník, a ne někdo jiný.



Jak to jednoduše funguje při odesílání bitcoinových transakcích:

1. **Vytvoření transakce:**
   Uživatel zadá údaje, jako je adresa příjemce a částka v bitcoinech, která má být odeslána.
2. **Generování digitálního podpisu:**
   Odesílatel vygeneruje jedinečný **digitální podpis** pomocí svého **soukromého klíče**. Tento podpis je jedinečný kryptografický kód, který ověřuje platnost transakce.
3. **Vysílání transakce:**
   Podepsaná transakce se vyšle do bitcoinové sítě, čímž se vyjádří záměr převést vlastnictví bitcoinu z odesílatele na příjemce.
4. **Ověření v síti:**
   Uzly v Bitcoinové síti přijmou transakci a použijí **veřejný klíč** příjemce k dešifrování a ověření úplnosti transakce. Současně použijí **veřejný klíč** odesílatele k ověření **digitálního podpisu**.
5. **Potvrzení v Bitcoinové síti:**
   Pokud je ověření úspěšné, transakce se přidá do účetní knihy, která slouží jako bezpečný a transparentní záznam všech transakcí. Po potvrzení je vlastnictví bitcoinu oficiálně převedeno z odesílatele na příjemce.

Když to shrneme, digitální podpis vytvořený pomocí soukromého klíče odesílatele slouží jako kryptografický důkaz pravosti a vlastnictví. Zároveň tak umožňuje v decentralizované síti potvrdit a zaznamenat transakce do účetní knihy.

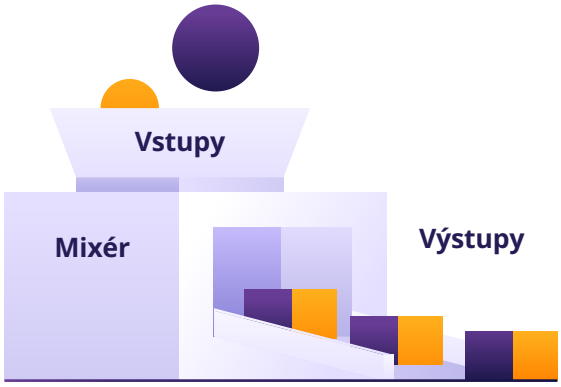
Úvod k technické stránce Bitcoinu

9.1.2 Vysvětlení hashovací funkce

Nenechte se prosím zastrašit technickými termíny a matematickými pojmy. Chápeme, že ne každý je blázen do matematiky, ale možná sami sebe překvapíte a zjistíte, že i ty nejsložitější myšlenky lze s trochou snahy pochopit celkem jednoduše.

Co to je funkce?

Funkce je jako stroj, který vezme nějakou informaci a přemění ji na něco nového. Informace, které funkci předáte, se nazývají **vstup.** Nová informace, kterou funkce vytvoří, se nazývá **výstup.** Funkce pomáhají počítačům plnit úkoly a řešit problémy.



Představte si to jako recept na přípravu salátu. Recept (nebo funkce) vám říká, jaké ingredience použít a jak je smíchat dohromady, abyste salát připravili. Můžete do něj vložit různé přísady, ale výsledkem receptu bude vždy salát. Funkce lze použít k usnadnění a zefektivnění práce.

Tento recept je tedy funkcí, která na **vstupu** apřijme ingredience a na **výstupu** vytvoří míchaný salát.

V Bitcoinu se funkce používají k provádění transakcí. Už víme, že Bitcoinové transakce jsou v podstatě převody hodnoty (peněz) z jedné adresy na druhou. K provedení transakce se používá řada kryptografických funkcí, které transakci ověřují a aktualizují stav Bitcoinové účetní knihy.

Mezi funkce používané při bitcoinových transakcích patří ověřování pravosti vstupů transakce, kontrola, zda má odesílatel dostatek finančních prostředků, a aktualizace zůstatků na příslušných adresách. Jakmile je transakce ověřena a přidána do bloku v účetní knize, stává se součástí trvalého záznamu všech transakcí v síti.

Co to je jednosměrná funkce?

Jednosměrná funkce používá sadu instrukcí ke zpracování informací a mění je v něco nového, podobně jako recept na smoothie mění ingredience v nápoj. Ale stejně jako nemůžete rozmixovat smoothie a získat zpět původní ingredience, nemůžete ani obrátit jednosměrnou funkci a získat zpět původní informace.

Kryptografie s veřejnými klíči, je založena na použití jednosměrných funkcí, které znesnadňují určení **soukromého klíče** z **veřejného klíče**. Teoreticky není úplně „nemožné“ zjistit **soukromý klíč** z **veřejného klíče**, ale je to nesmírně obtížné a splnění tohoto úkolu by vyžadovalo nesmírné množství času a výpočetního výkonu.

Najít **soukromý klíč** z **veřejného klíče** v Bitcoinu je jako hledat jehlu v kupce sena o velikosti fotbalového hřiště. Jehla představuje **soukromý klíč** a kupka sena všechny možné **soukromé klíče**.

Stejně tak jsou jednosměrné funkce navrženy způsobem, aby byly nevratné a nebylo možné je dešifrovat.

Co je to hashovací funkce?

Hashování je jako otisk prstu pro digitální data. Je to proces, při kterém se digitální zpráva převede na kód pevné délky, který slouží jako jedinečný identifikátor.

Stejně jako otisk prstu umožňuje identifikovat osobu, hash může identifikovat digitální zprávu. Hashe se používají v mnoha aplikacích, včetně bitcoinových transakcí.

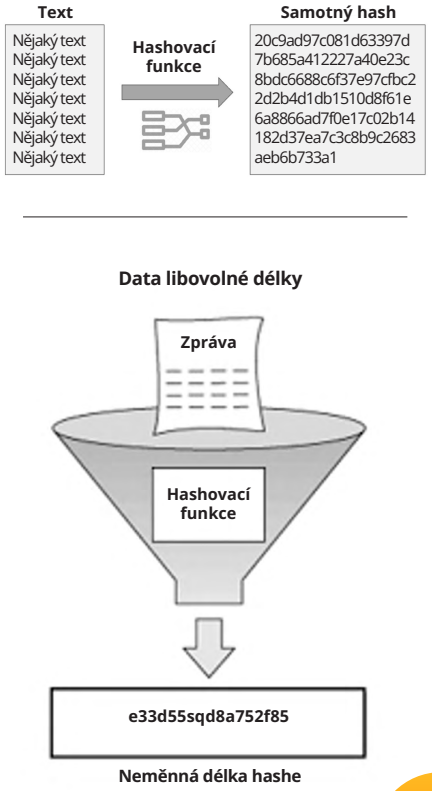
Jak se hashování používá v Bitcoinových transakcích?

V Bitcoinu je každá transakce před přidáním do bloku v účetní knize hashována. Hash slouží jako podpis transakce a ověřuje, že transakce je platná a nebylo s ní manipulováno. Pokud se někdo pokusí změnit byť jen jediné písmeno v transakci, hash bude úplně jiný a upozorní na změnu ostatní.

Úloha hashování při zajišťování bezpečnosti

Hashování je pro bezpečnost Bitcoinové sítě zásadní. Pomocí hashů k identifikaci transakcí může síť odhalit jakýkoli pokus o změnu nebo manipulaci s transakcemi. To pomáhá předcházet podvodům a zajišťuje, že všechny transakce jsou v účetní knize zaznamenány přesně a neměnným způsobem.

Hashovací funkce je typ jednosměrné funkce, která přijímá vstup (označovaný jako „zpráva“ nebo „data“) a převádí jej na číselnou reprezentaci označovanou jako „hash“. **Výstupní** hash je jedinečný pro vstupní data, takže i malá změna **vstupních** dat vede k úplně jinému výsledku.



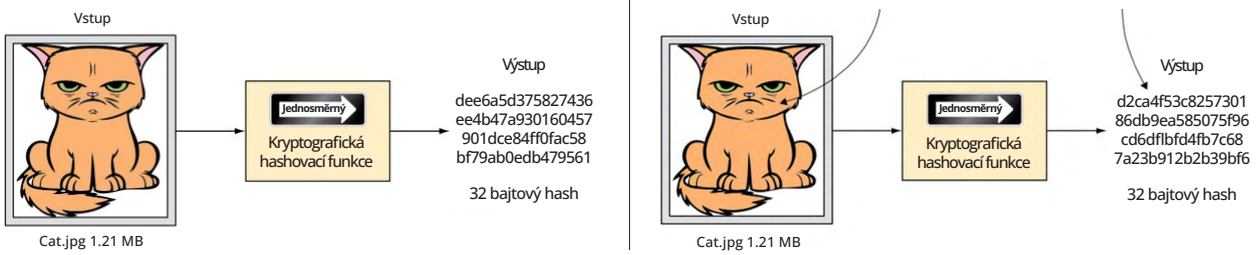
Hashovací funkce je jako stroj na vytváření tajných kódů. Přijme **zprávu** a přemění ji na kód.

Úvod k technické stránce Bitcoinu

Kód vypadá pro jednu a tutéž zprávu vždy stejně. Pokud zprávu jen trochu změníte, kód bude zcela jiný. To pomáhá počítačům zapamatovat si věci a kontrolovat, zda se něco nezměnilo.

Vygenerujte si hash SHA256 libovolného řetězce nebo vstupní hodnoty. Hashovací funkce se používají jako jednosměrné metody.

Aktivita - vygenerujte si funkci SHA256



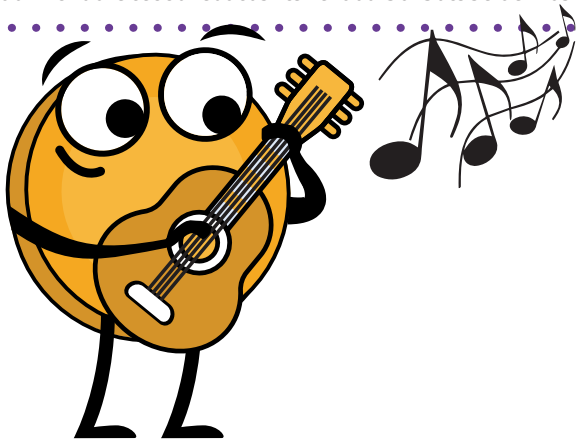
Výstup neboli hash má vždy stejnou délku bez ohledu na to, jak dlouhá byla původní informace.

Bitcoin používá několik specifických typů hashovacích funkcí nazvaných **SHA-256** a **RIPEMD160.** Níže uvádíme několik příkladů:

- Všimněte si, že malá změna (kurzíva) druhého vstupu zcela změní výstup ve srovnání s prvním vstupem.
- Třetí vstup je obrovský soubor, přesto má výstup stále stejnou pevnou délku jako ostatní dva.

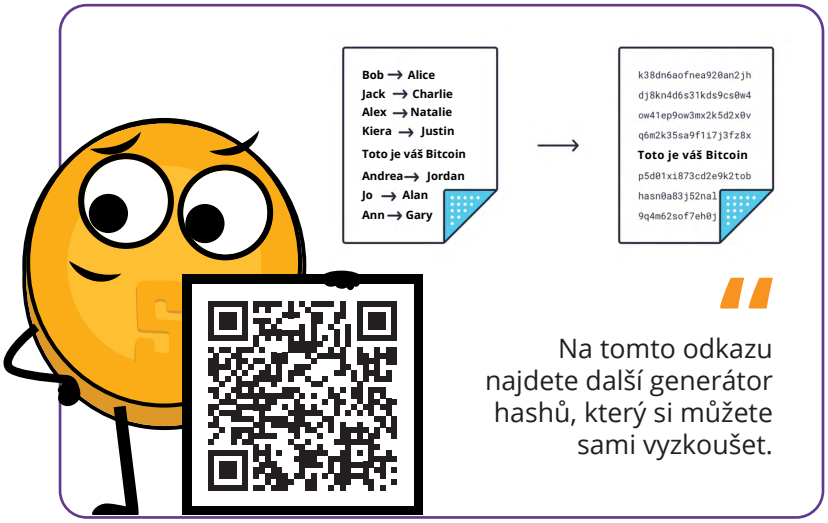
- SHA256 hash anglických slov ***hello world***
  B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9
- SHA256 hash anglických slov **hello world.**
  7ddb227315f423250fc67f3be69c544628dffe41752af91c50ae0a9c49faeb87
- SHA256 hash stahovatelného ISO souboru **Ubuntu 18.10**
  7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

Hashování si lze také představit jako hudební noty, které zachycují refrém hudební skladby. Stejně jako jsou noty jedinečnou reprezentací melodie, je hodnota hashe jedinečnou reprezentací kusu dat. Porovnáním notového zápisu hudební skladby se skutečným provedením může hudebník určit, zda je představení přesné. Podobně lze porovnáním hodnoty hashe přijatých dat s původní hodnotou hashe určit, zda byla data během přenosu změněna.



Stejně jako nepatrná odchylka v hudebním výkonu může způsobit, že melodie bude znít jinak, i sebemenší změna původních dat povede k jiné hodnotě hashe. Díky tomu je hashování mocným nástrojem pro zajištění integrity a pravosti Bitcoinové transakce.

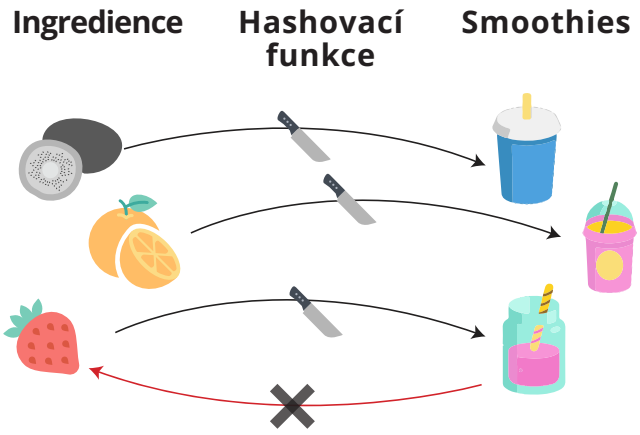
Proces kódování **veřejného klíče** pomocí hashování se používá ke zvýšení bezpečnosti informací tím, že se převedou do nečitelného formátu s pevnou délkou. Bitcoin používá k vytváření veřejných adres algoritmy SHA-256 a Ripemd-160. Výsledný výstup slouží jako jedinečný identifikátor **veřejného klíče** a pomáhá zajistit integritu a bezpečnost transakcí uložených v účetní knize. Tímto způsobem šifrování informací je pro neoprávněné osoby obtížnější získat přístup k datům a manipulovat s nimi.



Na tomto odkazu najdete další generátor hashů, který si můžete sami vyzkoušet.

Hashovací funkce

Vezme jakkoliv dlouhý vstup a vytvoří z něj výstup o jednotné délce.



- **Deterministický.**
  Ze stejných ingrediencí bude vždy stejné smoothie.
- **Odoslnost vůči defaultní hodnotě.**
  Nelze získat zpátky jahody, které rozmixujete do smoothie.
- **Odolnost vůcí korelaci.**
  malou změnou ingrediencí získáte úplně jiný koktejl.
- **Odolnost vůči kolizi.**
  Je těžké najít různé ingredience pro smoothie, ze kterých by vzniklo přesně to samé.
- **Rychlost a ověřitelnost.**
  Vhoďte ovoce do mixéru. Je to rychlé a výsledek bude určitě smoothie.

9.2 UTXO Model

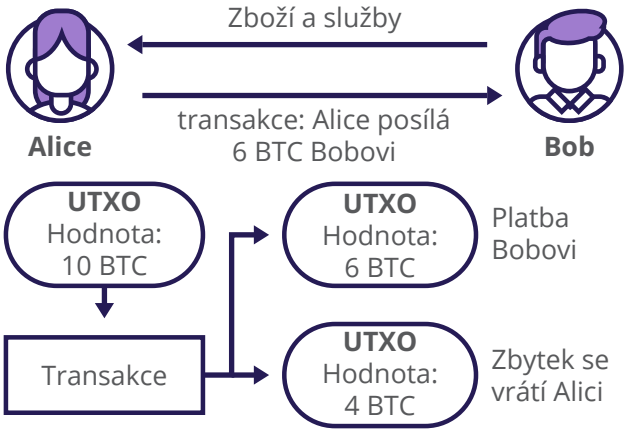
UTXO znamená Unspent Transaction Output (Neutracený výstup z transakce)

Úvod k technické stránce Bitcoinu

Co to jsou UTXO?

V Bitcoinu fungují transakce tak, že větší „kus" bitcoinu rozdělíte na menší kousky a tyto menší kousky pošlete ostatním i sobě.

UTXO si můžete představit jako různé velikosti a kousky bitcoinu nebo různě denominované bankovky ve vaší peněžence. Když utratíte UTXO, přetvoří se na nové UTXO pro příjemce a to, co zbyde, se vám pošle zpět v podobě nového UTXO. Je to podobné, jako když si za 10-ti dolarovou bankovku koupíte dva šálky kávy za 6 dolarů. 6 dolarů si kavárna ponechá a 4 dolary vám vrátí v drobných.

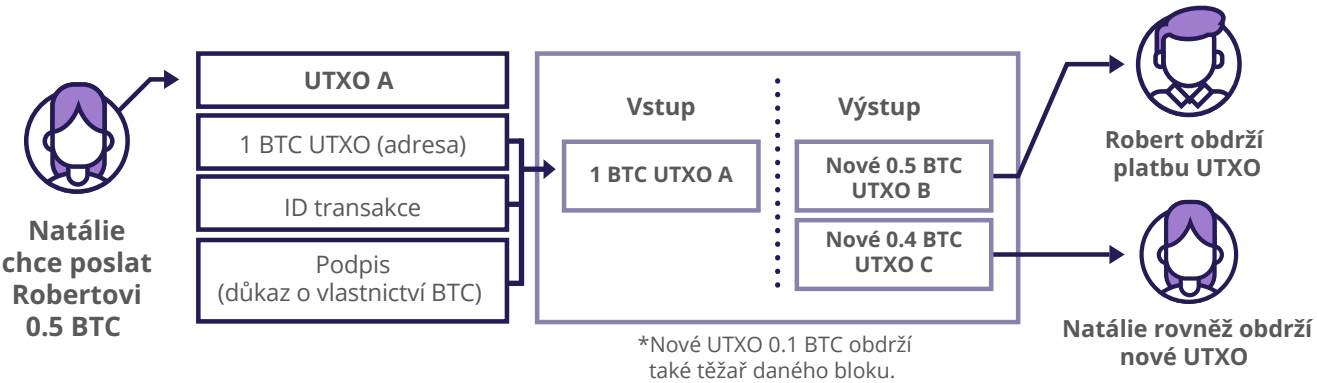


Při odesílání bitcoinů posíláte vždy celou částku jednoho (nebo více) UTXO v Bitcoinové peněžence. Co se stane? Část pošlete příjemci a zbývající částku obdržíte zpět jako drobné na jednu ze svých nových bitcoinových adres. Drobné, které obdržíte zpět, se nazývají neutracený výstup transakce neboli UTXO a lze je použít jako vstup pro novou budoucí transakci.

Zůstatek vaší Bitcoinové peněženky je součtem všech vašich různých UTXO. Součet vašich UTXO je tedy součtem množství bitcoinů, které vlastníte.

Je důležité si uvědomit, že byste neměli dávat ostatním vědět o svých UTXO, protože když někdo zná vaše UTXO, může sledovat vaše bitcoinové transakce v síti a nakonec zjistí, kolik peněz vlastníte.

Závěrem lze říci, že pokaždé, když provedete transakci, použijete jedno nebo více svých stávajících UTXO k utrácení bitcoinů a vytvoří se nová UTXO (pro vás i pro příjemce).



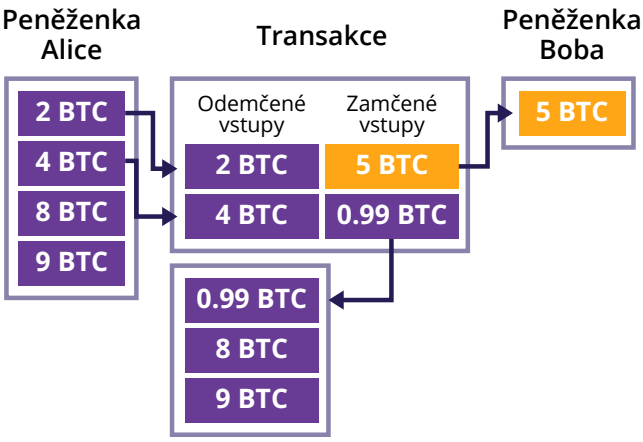
Při transakci se odeslaná částka bitcoinů rozdělí na více výstupů, z nichž každý je spojen s novou bitcoinovou adresou (novým UTXO).

Když někomu posíláte bitcoiny, použijete jednu nebo více UTXO jako zdroj finančních prostředků (vstup). Tyto UTXO se v případě potřeby zkombinují a vytvoří nové výstupy, které patří jak příjemci transakce, tak vám. Tyto nové výstupy neboli UTXO se pak stanou majetkem příjemce i vaším majetkem. Tyto UTXO pak můžete použít jako zdroj prostředků v dalších budoucích transakcích. Tento řetězec UTXO vytváří transparentní a dohledatelnou historii všech bitcoinových transakcí v účetní knize, počínaje úplně prvním blokem (3. ledna 2009).

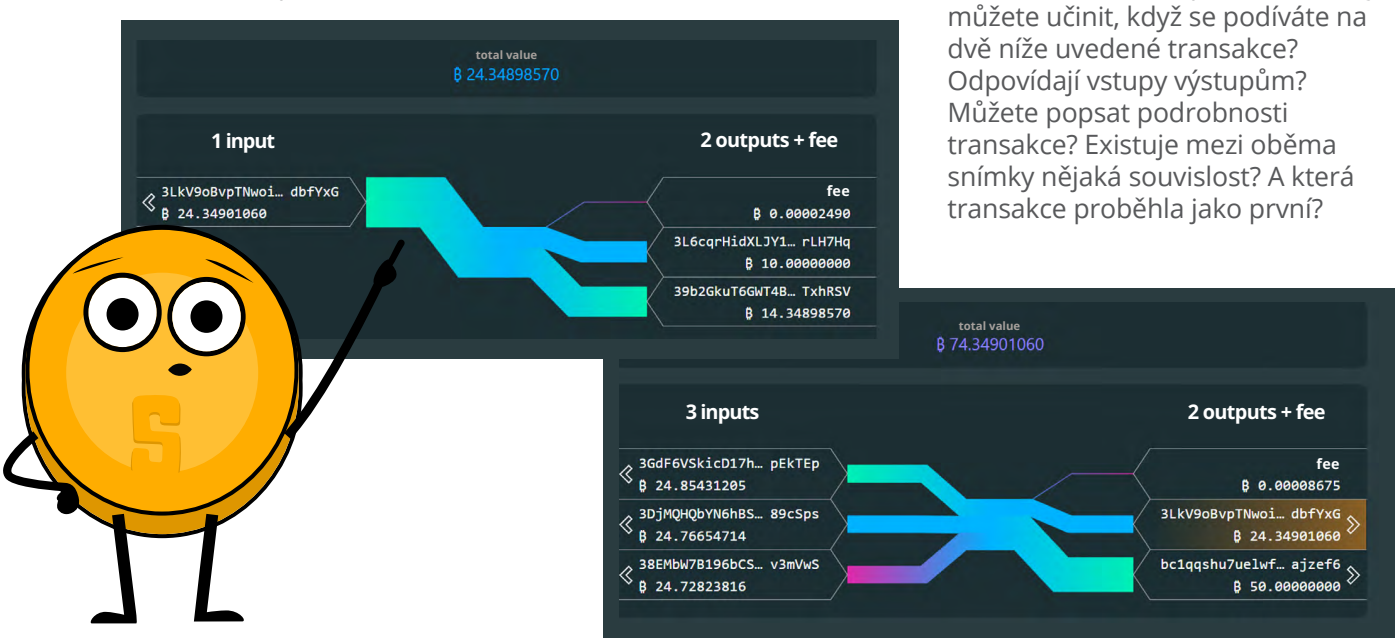
Ilustrační příklad: pokud chcete poslat 2 bitcoiny, ale máte pouze UTXO v hodnotě 5 bitcoinů, rozdíl 3 bitcoinů vám bude zaslán zpět jako "drobné". Tato změna pro vás představuje nové UTXO a toto nové UTXO můžete utratit v budoucí transakci.

Další příklad:

1. Alice chce poslat Bobovi 5 bitcoinů.
2. Spojí 6 bitcoinů ze dvou svých UTXO.
3. Z těchto UTXO pošle Bobovi 5 bitcoinů, zpět k sobě dostane 0,99 bitcoinu jako drobné a musí zaplatit poplatek za transakci ve výši 0,01 bitcoinu.
4. Po potvrzení je transakce přidána do účetní knihy a aktualizují se všechny uzly, které mají kopii této knihy.



Řekněme, že se Alice pokusí použít jeden ze svých již utracených výstupů k provedení další transakce. Uzly ji automaticky odmítnou, protože si udržují kopii účetní knihy (a všech jeho transakcí), a tak mohou snadno zkontrolovat zůstatek Aliciných UTXO a ověřit, že transakce není platná.



Níže je reálný snímek obrazovky skutečné transakce, kde je pouze jeden vstup. Počáteční zůstatek však může být v jiném případě součtem více UTXO (více vstupů). Jaké závěry můžete učinit, když se podíváte na dvě níže uvedené transakce? Odpovídají vstupy výstupům? Můžete popsat podrobnosti transakce? Existuje mezi oběma snímky nějaká souvislost? A která transakce proběhla jako první?

Úvod k technické stránce Bitcoinu

9.3 Bližší pohled na Bitcoinové uzly a těžaře

V této části se podrobněji podíváme na dvě velmi důležité účastníky Bitcoinové sítě, kteří byli poprvé představeny v kapitole 6. Podíváme se na:

1. **Bitcoinové uzly:**

   Jejich hlavním úkolem je uchovávat kopii Bitcoinové účetní knihy, dohlížet na platnost všech transakcí a na to, aby se všichni řídili stejnými pravidly.

   Tím, že je tato práce rozdělena mezi mnoho lidí po celém světě, zůstává Bitcoin odolný proti potenciálním útokům. Tyto uzly pomáhají udržovat systém důvěryhodný a věrný jeho decentralizované myšlence, kdy žádná osoba ani skupina nemá příliš velkou moc.

2. **Těžaři bitcoinů:**

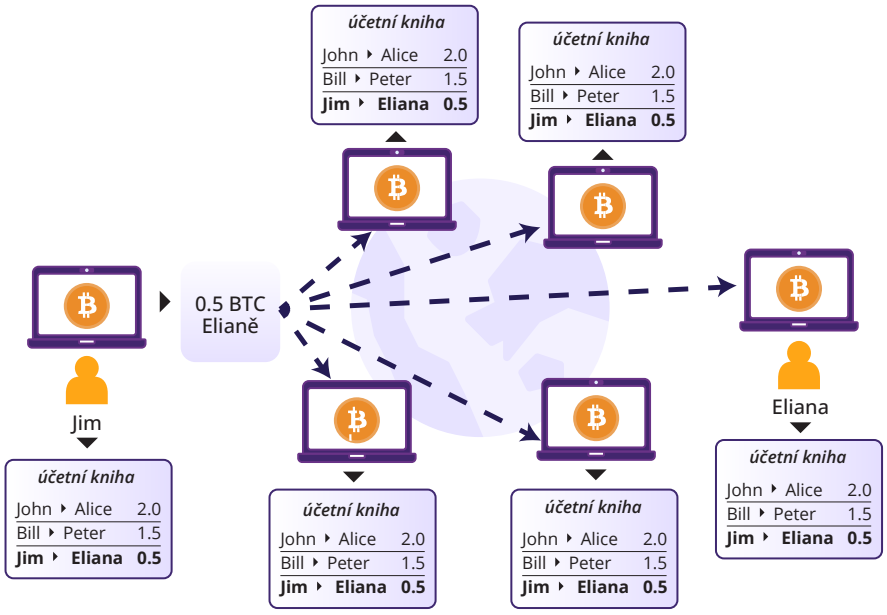
   architekti bezpečnosti, kteří pomocí výkonných počítačů a elektřiny kontrolují/potvrzují transakce a zároveň zajišťují, aby vše bylo bezpečné. Díky této práci je účetní kniha neboli blockchain odolný vůči všem subjektům, které by se snažily síť napadnout.

Společně pracují uzly a těžaři bitcoinu jako tým, aby udržovali decentralizovaný, bezpečný a odolný systém - nový způsob nakládání s penězi, na který se mohou spolehnout lidé na celém světě. Prozkoumejme tyto role podrobněji, abychom pochopili, jak přispívají k tomuto inovativnímu systému.

9.3.1 Co to je Bitcoinový uzel a jak si ho nastavit doma?

Bitcoinový uzel může znít jako příliš technická záležitost, ale je to jen kus softwaru, který provozuje kopii bitcoinové účetní knihy. Když spustíte svůj vlastní bitcoinový uzel, získáte možnost podílet se na tvorbě pravidel bitcoinové sítě.

Představte si to: pokud se skupina lidí pokusí změnit fungování Bitcoinu, například změnou celkového množství bitcoinů, máte možnost se k tomu vyjádřit. Můžete se rozhodnout, že svůj uzel na nový systém nezměníte, což je jako hlasovat o prosazení pravidel sítě, která podporujete.



Představme si Bitcoinový uzel jako digitálního dopravního policistu s několika nezbytnými úkoly:

1. **Strážci platnosti:**
   Bitcoinový uzel uchovává digitální kopii blockchainu, což je něco jako sdílená účetní kniha všech bitcoinových transakcí. Stejný záznam uchovává tisíce uzlů po celém světě.
2. **Komunikační uzel:**
   Uzly se vzájemně propojují a vytvářejí rozsáhlou komunikační síť. Sdílejí informace, zejména transakce čekající na přidání do blockchainu, uložené v digitální databázi zvané „mempool“.
3. **Kontrolor kvality:**
   Každý přidaný údaj do blockchainu prochází kontrolou. Uzly zajišťují platnost transakcí a odmítají všechny, kteří nesplňují pravidla Bitcoinové sítě.
4. **Informátor blockchainu:**
   Ostatní aplikace, jako jsou například peněženky, mohou požádat uzel o informace v blockchainu, například o bitcoinových zůstatcích. Uzly slouží jako informační uzly.
5. **Přijetí nových uzlů:**
   Když se chce připojit nový uzel, stávající uzly mu velkoryse poskytnou kopii blockchainu. Nový uzel nezávisle kontroluje platnost každé transakce, což klade důraz na systém bez důvěry.

Aktivita:
Zhlédněte video o Bitcoinových uzlech

Jednou z možností, jak spustit vlastní uzel, je stáhnout si software Bitcoin Core a dát mu nějaký čas na stažení celého blockchainu. Jakmile je připraven, můžete jej nechat zapnutý a přibližně každých 10 minut přibudou nové bloky s transakcemi. Váš uzel zkontroluje jejich platnost a přidá je do vaší lokální kopie blockchainu.

Zdroj:
Bitcoin Core Software

Provozování uzlu poskytuje suverenitu a nezávislost. Nespoléháte se na ostatní, je to váš vlastní dopravní policista. Na rozdíl od vaší bitcoinové peněženky, která postrádá kopii blockchainu, uzel zajišťuje soběstačnost. Namísto toho, abyste důvěřovali ostatním ohledně svých bitcoinů (a stavu bitcoinové sítě), vaše peněženka komunikuje s vaším osobním uzlem, díky čemuž je vaše digitální působnost bezpečnější a důvěryhodnější.

9.3.2. Co to je těžební stroj a jak těžba funguje?

> Účelem těžby není vytváření nových bitcoinů. To je motivační systém.
> Těžba je mechanismus, díky němuž je bezpečnost Bitcoinu decentralizovaná.
>
> **Andreas M. Antonopoulos**

Úvod k technické stránce Bitcoinu

Těžaři shromažďují nepotvrzené transakce, vytvářejí bloky a vynakládají elektrickou energii na hledání předem daného čísla, **které doplní a zajistí tak místo bloku v blockchainu.**

Těžaři se předhánějí v přidávání dalších bloků do blockchainu. Vytouženou cenou je „platný hash bloku“, který je důmyslně ukrytý mezi miliardami dalších a odemknout ho může pouze specifický klíč přidělený sítí.

Představte si obrovskou kupku sena plnou milionů klíčů, z nichž každý představuje jedinečný hash bloku. Síť vybrala jeden konkrétní klíč, který odemkne cennou odměnu. Těžaři se prohrabávají kupkou sena, testují každý klíč v zámku, ale pouze jeden šťastlivec objeví dokonalou shodu.

Jakmile těžař najde správný hash bloku, sdílí jej se sítí spolu s vytvořeným blokem nových transakcí. Ostatní těžaři toto řešení ověří, aby se ujistili, že je správné. Pokud vše souhlasí, je blok přidán do blockchainu, čímž se vytváří bezpečná a veřejná účetní kniha.

Těžaři získávají odměny za své úsilí dvěma způsoby:

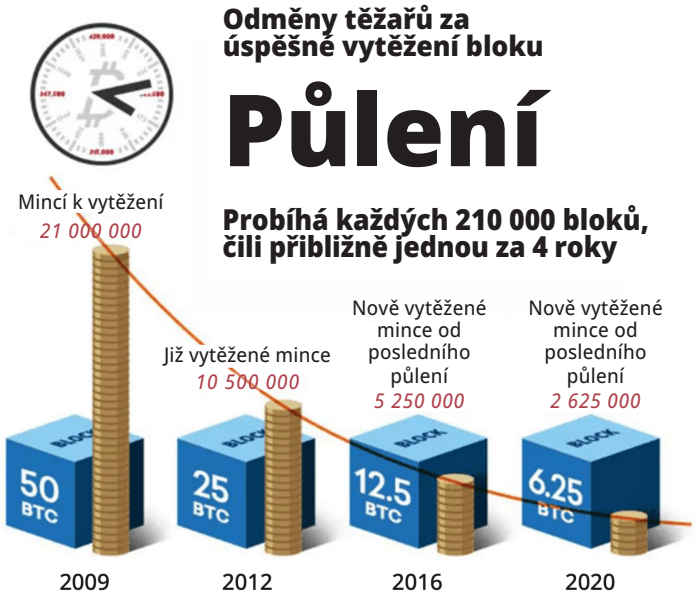
1. Odměna v bloku
2. Transakční oplatky

Odměny za bloky jsou nové bitcoiny uvolněné do oběhu s každým blokem přidaným do blockchainu. Transakční poplatky jsou malé částky, které uživatelé bitcoinů platí za to, že jejich transakce jsou zpracovávány rychleji a těžař je upřednostňuje. Těžaři si mohou vybrat, které transakce zahrnou do těženého bloku, přičemž obvykle upřednostňují transakce s vyššími transakčními poplatky.

Halving Bitcoinu

Je nezbytnou součástí bitcoinového světa, která pomáhá udržet jeho vzácnost a hodnotu v čase. Jak víte, existuje pevná nabídka celkem 21 000 000 bitcoinů. Tato zásoba není plně k dispozici ode dne spuštění Bitcoinu. Místo toho se tato zásoba v ekosystému uvolňuje postupně.

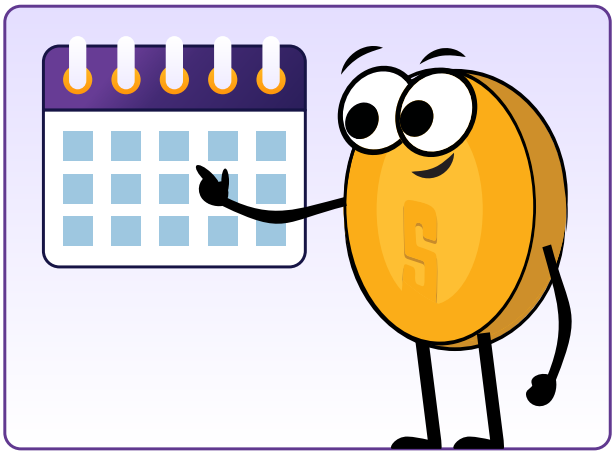
Satoshi Nakamoto chytře navrhl systém blokových odměn, který umožňuje distribuci nových bitcoinů bez centrální autority. V počáteční fázi dostávali těžaři za každý vytěžený blok sladkou odměnu 50 bitcoinů, což je motivovalo k investicím do výkonného vybavení a elektřiny pro těžební operace.



Aby byla síť stabilní a bylo možné řídit přírůstek nových bitcoinů, snižuje se odměna za blok každých 210 000 bloků na polovinu (cca každé 4 roky). Tato událost, česky nazývaná „půlení“, snižuje počet nových bitcoinů vstupujících do oběhu a nadále motivuje těžaře k ochraně sítě a udržování její decentralizace. Historicky vedly události halvingu k výraznému nárůstu cen na trhu, a to v důsledku snížené nabídky nových bitcoinů, které se dostávají do oběhu.

Nabídka kolující v oběhu označuje celkové množství dostupných jednotek. U Bitcoinu je celková nabídka v oběhu počet mincí, které byly vytěženy a jsou v daném okamžiku v oběhu, bez mincí, které jsou navždy ztraceny.

Během každé události půlení dostávají těžaři menší odměnu v bitcoinu, což snižuje míru emise nových mincí. V důsledku toho a s nárůstem celkového výpočetního výkonu, se obtížnost těžby zvyšuje, aby se udržel čas vytěžení bloku stále jednou za 10 minut v průměru. To nám zajišťuje, že nové bloky jsou do blockchainu přidávány stabilním tempem. Snížení odměn za těžbu nemusí nutně znamenat, že těžaři mají menší zisk, protože cena bitcoinu v čase může růst a těžaři také získávají transakční poplatky za ověřování transakcí a jejich přidávání do blockchainu. To může kompenzovat snížení odměn za těžbu v průběhu let.



Události půlení jsou předem naprogramovány v protokolu Bitcoinu, takže je jejich distribuce předvídatelná a transparentní.

Distribuce bitcoinů je předem stanovený a veřejný plán uvolňování nových mincí do oběhu, jehož cílem je udržet vzácnost bitcoinu v čase.

V následující tabulce jsou uvedeny podrobnosti o nadcházejících událostech půlení bitcoinů, včetně očekávaného data příští události půlení, čísla bloku, ve kterém k události půlení dojde, odměny za vytěžený blok během této události půlení a procenta celkové nabídky, které bude vytěženo.

Událost	Rok	Blok	Odměna za blok	Vytěženo v procentech
Čtvrté půlení	2024	840,000	3.125	96.875 %
Páté půlení	2028	1,050,000	1.5625	98.4375 %
Šesté půlení	2032	1,260,000	0.78125	99.21875 %

Úvod k technické stránce Bitcoinu

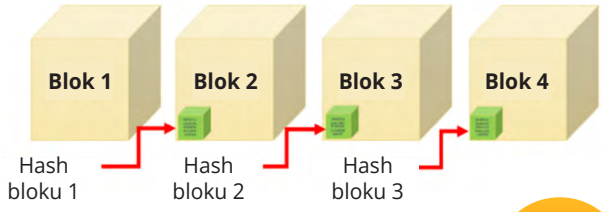
V průběhu let se bude zvyšovat nabídka bitcoinů v oběhu a také procento celkové nabídky, které bylo vytěženo. A to do té doby, dokud nebude dosaženo celkové nabídky 21 000 000 bitcoinů. Snížená nabídka v kombinaci s rostoucí poptávkou tak může zvýšit cenu bitcoinu (měřeno v dolarech). To přináší výhody prvním uživatelům a také motivuje těžaře, aby pokračovali v zabezpečování sítě a přispívali svým výpočetním výkonem a finančními prostředky.

Bitcoin: Vytěženo z celkové zásoby 21 miliónů BTC

Co to je platný hash v bitcoinovém bloku?

Platný hash je v něco jako speciální kód, který se těžaři snaží najít. Je to jedinečné číslo, které pomáhá sledovat každý blok v blockchainu, v němž jsou uloženy informace o transakcích. Bloky na sebe navazují v řetězci od prvního („genesis block“) po nejnovější, čímž vzniká veřejný záznam všech transakcí. Tento hash bloku je klíčový, protože spojuje každý blok s tím předchozím, což komukoli usnadňuje kontrolu historie transakcí. Je to něco jako otisk prstu každého bloku, který zajišťuje správnost a bezpečnost informací. Hash bloku slouží jako způsob, jak potvrdit, že data v bloku nebyla změněna.

Jednotlivé bloky jsou navzájem propojeny a navazují na sebe. Každý nový blok obsahuje „otisk“, což je hodnota hashe bloku předchozího. Hashovací funkce dokáže vzít veškeré informace v bloku a vytvořit z nich nevratný hash o stejné délce znaků.

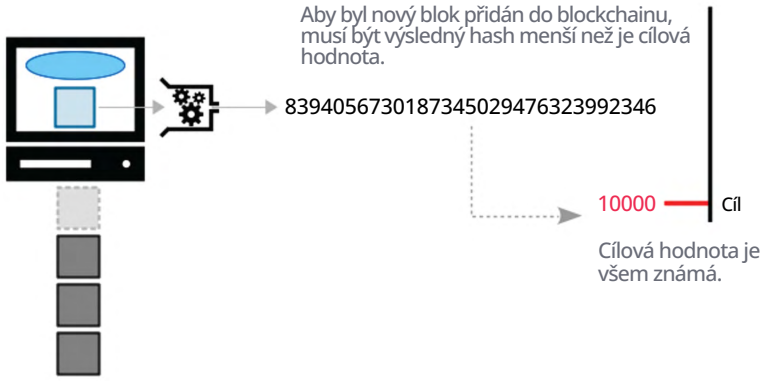


Satoshi Nakamoto, tvůrce bitcoinu, vytěžil úplně první blok, který obsahoval celkem 50 bitcoinů.

Závod o vytěžení bloku

Těžaři soutěží o to, kdo odhalí hash bloku, který se shoduje s cílem (speciálním číslem) stanoveným sítí. Těžař, který jako první úspěšně odhalí správný hash bloku, získá možnost přidat tento blok do blockchainu a přiřadit mu odpovídající hash ID. Toto řešení slouží jako ověření pravosti bloku.

Těžbu lze přirovnat k závodu, jehož cílem je co nejrychleji dorazit do cíle. To, jak obtížné je najít hash bloku, se pravidelně upravuje a zajišťuje, aby byl každý blok vytěžen jednou za cca 10 minut (podle toho, jak těžaři připojují a odpojují své stroje). Tento mechanismus se nazývá „automatická úprava obtížnosti".



Řekněme, že cílové číslo stanovené sítí je 1000. Těžaři by museli využít svůj výpočetní výkon a energii k hledání hashe bloku (konkrétního čísla), který je nižší než 1000. Těžař, který jako první najde hash bloku nižší než 1000, přidá nový blok do blockchainu a je odměněn bitcoiny.

Úroveň obtížnosti při těžbě bitcoinů je měřítkem toho, jak obtížné je najít platný hash bloku, který splňuje cíl stanovený sítí. Upravuje se každých 2016 bloků (zhruba každé dva týdny), aby se zajistilo, že bloky budou do blockchainu přidávány konzistentní rychlostí. Úroveň obtížnosti je vyjádřena číslem a čím vyšší je, tím obtížnější je najít platný hash bloku.

Vezměme si například dva různé hashe:

- **Hash 1:** 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK
  Úroveň obtížnosti: 1
- **Hash 2:** 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK
  Úroveň obtížnosti: 2

V tomto příkladu má hash 2 vyšší úroveň obtížnosti než hash 1, protože je delší a má na začátku více nul. Pro těžaře by bylo těžší najít Hash 2, protože jejich počítače by musely vynaložit více práce.

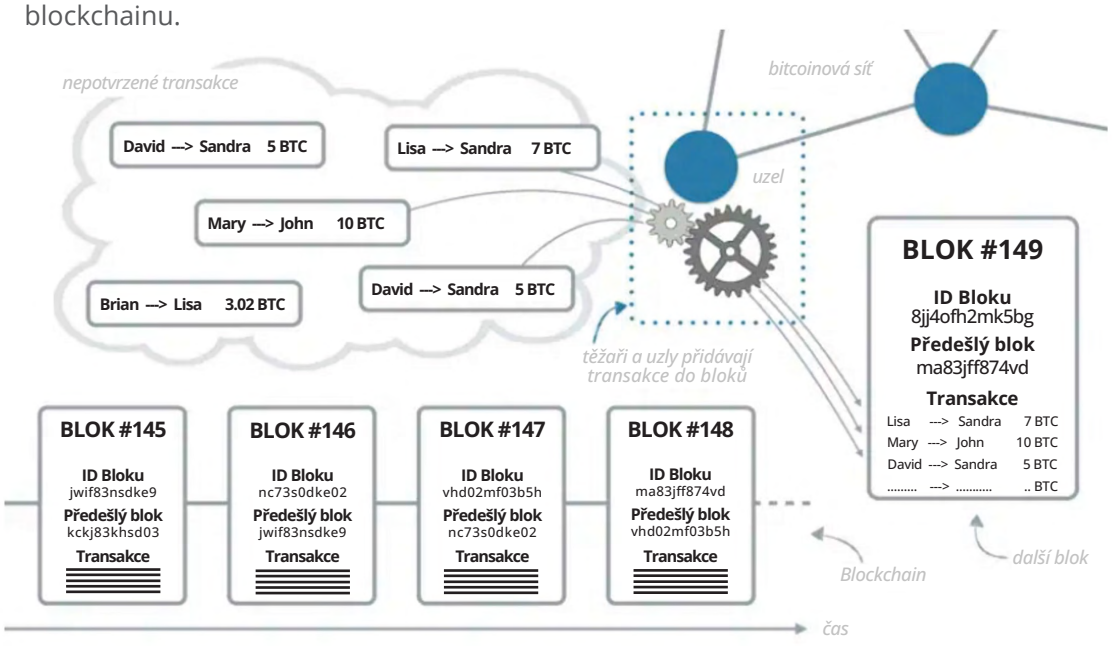
Nalezením platného hashe bloku těžař prokáže, že vykonal práci potřebnou k přidání nového bloku do blockchainu, a za své úsilí dostane odměnu v bitcoinech plus transakční poplatky. Důkaz o vykonané práci (Proof of Work - PoW) je metoda, kterou bitcoinová síť používá k ověřování transakcí a přidávání nových bloků do blockchainu.

Úvod k technické stránce Bitcoinu

PoW udržuje Bitcoin v bezpečí tím, že znesnadňuje převzetí kontroly nad sítí někým, kdo má nekalé úmysly.

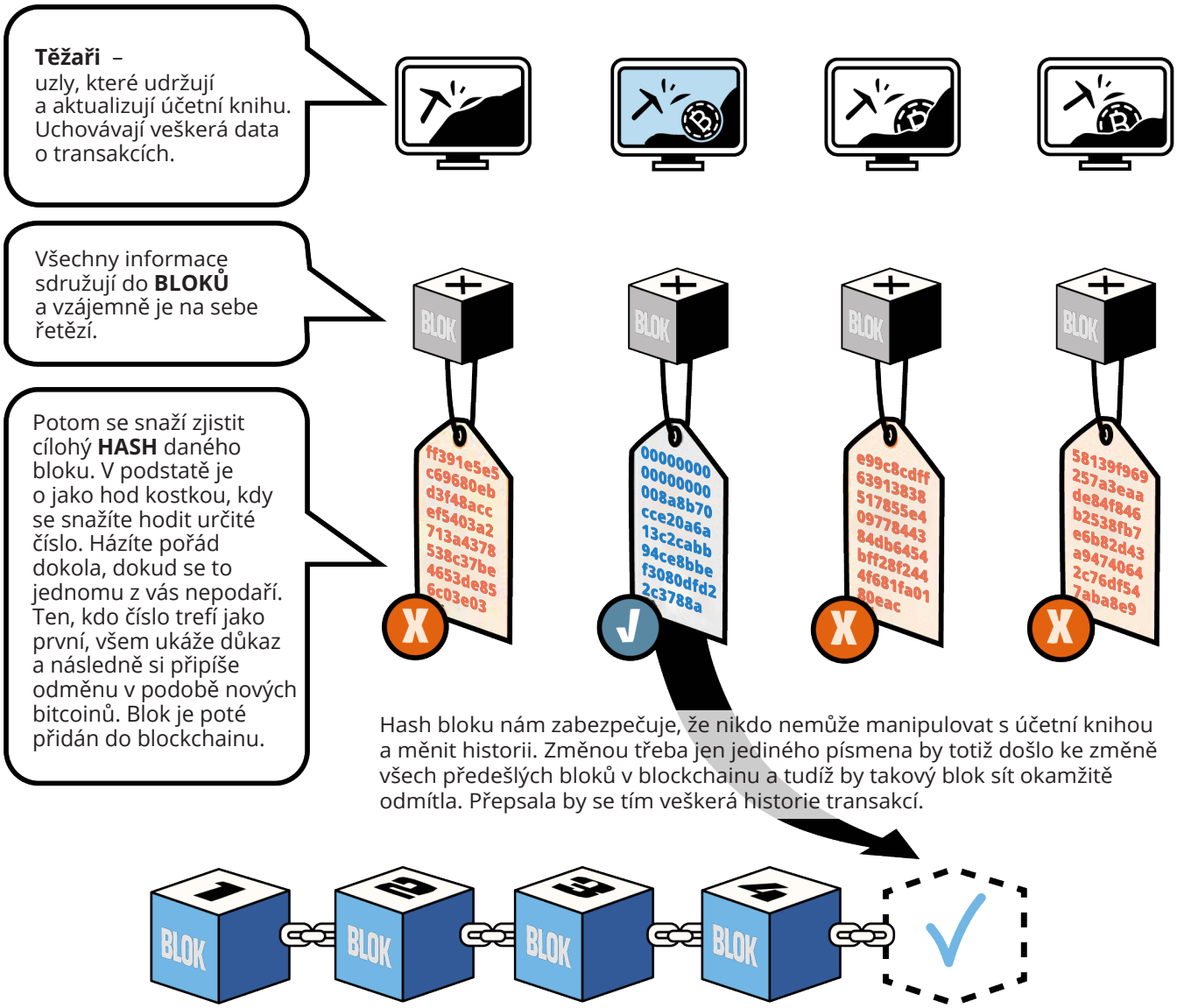
Stručně řečeno, úkoly těžařů spočívají v:

1. **Spojování transakcí do bloků:**
   Zatímco uzly ověřují nově vytvořené transakce, které čekají v „mempoolu“, těžaři z nich vyberou podmnožinu, kterou zahrnou do svého kandidátského bloku.
2. **Proof of Work (důkaz o vykonané práce):**
   Těžaři mezi sebou závodí v hledání platného hashe bloku.
3. **Vysílání platných bloků:**
   Po nalezení platného hashe bloku se nový blok zveřejní a aktualizuje v síti.
4. **Získávaní odměny:**
   Nakonec vítěz obdrží nově vytvořené bitcoiny a transakční poplatky za úspěšné přidání bloku do blockchainu.



Na vytváření nových bloků může pracovat více těžařů současně. Těžař, který jako první objeví hash bloku splňující cíl stanovený sítí, jej oznámí síti a ostatní těžaři pak zkontrolují transakce v kandidátském bloku tohoto těžaře, aby se ujistili, že jsou platné. Pokud jsou transakce skutečně platné, je blok přidán do blockchainu. Ostatní bloky vytvořené ostatními těžaři v té době přidány nejsou a jsou vyřazeny. Tento proces pomáhá udržovat konsensus v síti a zabraňuje dvojímu utrácení stejných mincí.

Kandidátský blok je soubor transakcí, o jejichž přidání do blockchainu se uvažuje, ale dosud nebyly přidány.



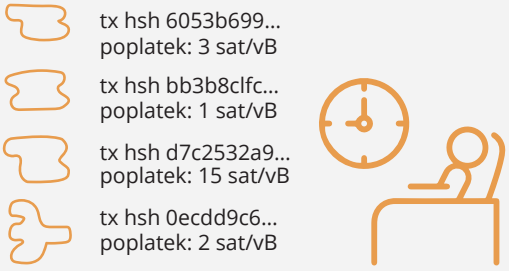
9.4 Co je to Mempool?

„Mempool“ neboli Memory Pool je něco jako ,,čekárna pro transakce v bitcoinové síti”. Když provedete transakci, je nejprve vysílána do Mempoolu, než je ověřena, vybrána a přidána do blockchainu.

Představte si, že čekáte ve frontě v restauraci. Vaše jméno je přidáno na seznam lidí čekajících na stůl. Když se stůl uvolní, hostitel zavolá vaše jméno a usadí vás. Podobně je bitcoinová transakce přidána do Mempoolu a následně je potvrzena a přidána do blockchainu v momentě, kdy ji těžař zahrne do bloku.

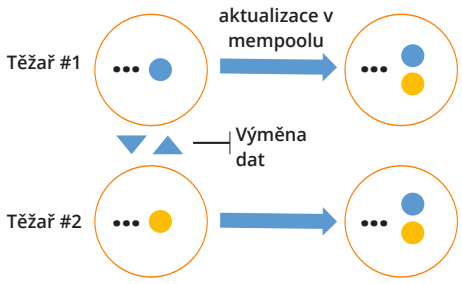
Úvod k technické stránce Bitcoinu

Mempool je místo, kde transakce čakají na potvrzení.



Jakmile provozovatel uzlu obdrží nějakou transakci, musí ověřit její pravost. Nikdo totiž nechce falešné/podvodné transakce. V bitcoinové síti zkrátka nelze podvádět.

Synchronizace v mempoolu tak umožňuje jenotlivým uzlům sdílet jejich informace o transakcích s ostatními a tím tak dosáhnout shody.



Hlavním účelem **mempoolu** je:

1. Ověřit nepotvrzené transakce.

2. Poskytovat těžařům transakce k těžbě.

Aby transakce byla zahrnuta do mempoolu, tak se musí zkontrolovat následující:

- Už mám transakci zahrnutou v bloku?
- Není transakce v kolizi s jinou transakcí?
- Je to, co skutečně jedna strana posílá, ***bitcoin***?
- Je digitální podpis validní k odeslání těchto bitcoinů?
- Je na účtě dostatek prostředků na zaplacení poplatků?

Jak se transakce ověřují a přidávají do Mempoolu?

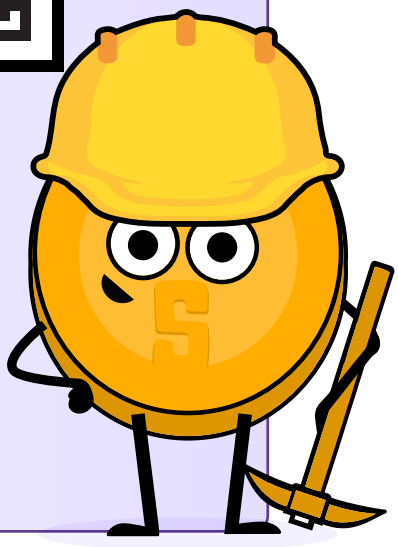
Když jsou do bitcoinové sítě vysílány nové transakce, uzly je ověřují, aby se ujistily, že jsou platné a že prostředky nebyly již dříve utraceny. Jakmile jsou tyto transakce ověřeny, uzly je přidají do svého Mempoolu. Poté uzly sdílejí transakce s ostatními uzly, aby je mohly překontrolovat. Nakonec, pokud většina uzlů souhlasí, budou transakce zpřístupněny těžařům, aby je vybrali a zařadili do bloku. Existuje však několik důvodů, proč transakce nemusí být po 72 hodinách potvrzena:

1. **Nízké transakční poplatky:**
   Transakce s nízkým poplatkem nemusí být zpracovány dostatečně rychle, protože těžaři si do svých bloků vybírají transakce s vyššími poplatky.
2. **Přetížení sítě:**
   Pokud je síť přetížená, může dojít ke zpoždění při potvrzování transakcí, i když mají vysoký poplatek.
3. **Pokus o dvojí útratu:**
   Pokud se záškodník pokusí o dvojí útratu, bude jeho transakce sítí odmítnuta.
4. **Nesprávné nebo neúplné údaje:**
   Pokud transakce obsahuje nesprávné nebo neúplné údaje, může ji síť odmítnout.
5. **Špatně vytvořená transakce:**
   Pokud je transakce nesprávně formulovaná, může ji síť odmítnout.

Abyste se vyhnuli odmítnutí transakce, doporučujeme uvést dostatečně vysoký poplatek, který zajistí včasné zpracování transakce, a před odesláním transakce dvakrát zkontrolovat, zda jsou všechny údaje v transakci správné.

Aktivita: Mempool

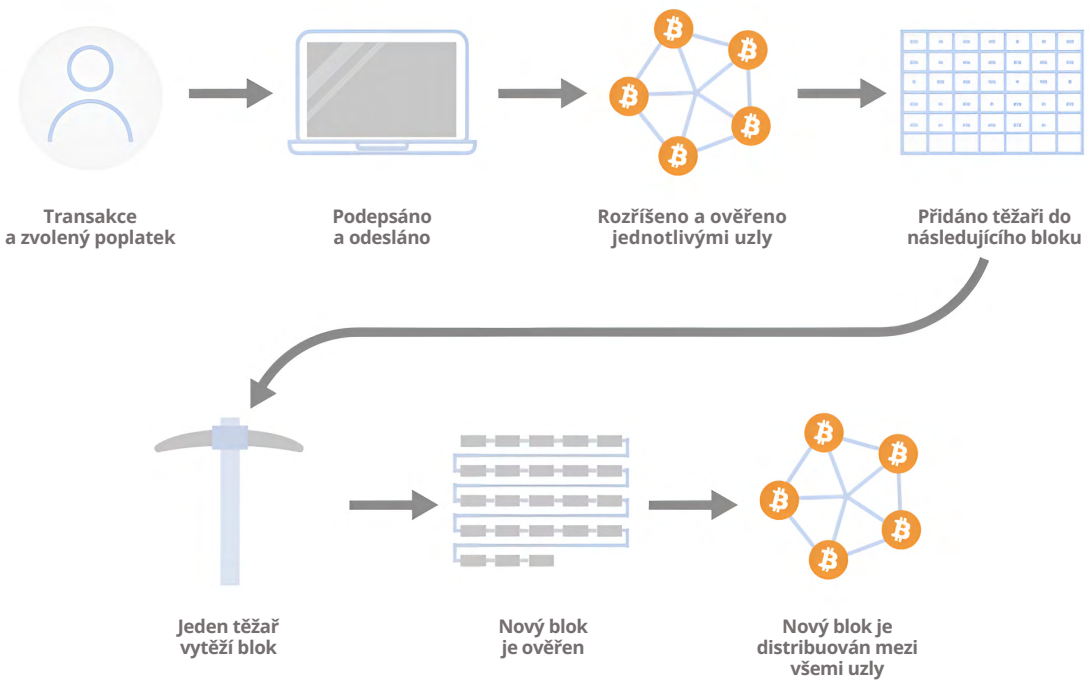
1. Naskenujte následující **QR code:**
2. Prohlédněte si jednotlivé údaje zobrazené na stránce, včetně nejnovějších bloků, potvrzených transakcí, počtu transakcí, využití paměti a přibližné hodnoty celého bloku. Odpovězte na otázky:
   - Jaký byl poslední vytěžený blok?
   - Kolik transakcí bylo v tomto bloku zahrnuto?
   - Jaká je celková hodnota zobchodovaných bitcoinů?
   - Jaká byla velikost bloku v megabajtech?
   - Kolika nulami začíná „nonce" bloku?
   - Kolik bitcoinů těžař celkem vydělal?
   - Jaká byla celková hodnota poplatků, které těžař obdržel za přidání transakcí do sítě?
   - Vyberte jednu z transakcí s nejvyšší hodnotou v bloku. Na kolik bitcoinových adres se tato částka rozdělila?



Úvod k technické stránce Bitcoinu

9.5 Jak fungují Bitcoinové transakce od začátku až do konce

1. Adam chce poslat bitcoin Petrovi. Vybere si jedno ze svých UTXO, vytvoří transakci a přidá všechny potřebné údaje, včetně částky bitcoinů, kterou chce poslat, Petrovu adresu a nadprůměrnou výši transakčních poplatků.
2. Poté, co provede závěrečnou kontrolu, zda jsou všechny údaje správné, Adam podepíše transakci svým soukromým klíčem.
3. Adam vyšle transakci do bitcoinové sítě.



Od: Stevenot, Ted, "Co je to Bitcoinový uzel a jak funguje?". Unchained Capital, 17. Ledna 2023, https://unchained.com/blog/what-is-a-bitcoin-node/

4. Uzly v síti přijmou transakci a ověří její platnost podle pravidel konsensu (například zkontrolují, zda je Adamův podpis platný a zda má dostatek prostředků na provedení transakce).
5. Transakce je označena za platnou a uzly ji rozšíří mezi ostatní uzly v síti a přidají ji do Mempoolu.
6. Protože si Adam vybral dostatečně vysoký poplatek za transakci, téměř všichni těžaři jeho transakci zařadí do svých bloků.

7. Důkaz o vykonané práci: Těžaři závodí a snaží se vytěžit svůj blok nalezením platného hashe bloku. Jeden z těžařů najde hash a pošle svůj blok do sítě.

8. Uzly obdrží nově vytěžený blok a ověří jeho platnost. To zahrnuje ověření všech transakcí v rámci bloku a zajištění splnění požadavku na PoW.

9. Většina uzlů se shodne na tom, že blok je platný, a přidá jej do blockchainu. Petr obdrží potvrzené bitcoiny na svou přijímací adresu.

10. Jak jsou v následující hodině do blockchainu přidávány další bloky, počet potvrzení této dané transakce roste. S rostoucím počtem potvrzení transakce získává Petr větší důvěru v její správnost a nezvratnost.

Stručně řečeno, odesílatel podepíše transakci svým soukromým klíčem, uzly ověří transakci UTXO a těžaři přidají ověřenou transakci do blockchainu. Příjemce pak má k bitcoinu přístup pomocí svého soukromého klíče. Jakmile je blok vytěžen, jsou všechny transakce v něm obsažené považovány za potvrzené a UTXO použité jako vstupy v těchto transakcích jsou považovány za spotřebované a nemohou být znovu použity.

Na závěr této kapitoly jste získali cenné informace o základních principech fungování Bitcoinu. Probrali jsme základní aspekty, od základů peněz až po technickou stránku Bitcoinu. Nyní si všechny tyto koncepty v další kapitole propojíme. Čeká nás kapitola 10, kde se ponoříme do významné otázky: „Proč Bitcoin?“

Kapitola 10

Proč Bitcoin?

Pracovní sešit

český překlad | 2024

Proč Bitcoin?

10.0 Úvod

> Bitcoin je víc než jen měna, je to revoluce, která navrací lidem moc, a nabízí nám mír a svobodu ve světě, který touží po posílení lidských práv.
>
> **Můj První Bitcoin**

V této závěrečné kapitole shrneme poznatky získané během naší cesty, zároveň si položíme několik důležitých otázek a prozkoumáme budoucnost Bitcoinu.

Bitcoin není jen technologie, je to typ sítě, která pohání novou formu peněz, jejichž nabídku nemůže změnit žádná jednotlivá skupina. Lidstvo ještě nikdy v historii nemělo formu peněz s fixní zásobou a bez centralizované kontroly. Pokud bude Bitcoin široce přijat, je to nástroj, který odemkne zámek k pozitivní změně pro společnost, jelikož může změnit životy lidí na celém světě. Zároveň představuje nenásilnou revoluci směrem ke kolektivní svobodě a rovnosti, která lidstvu otevře nové příležitosti vytvořením sdíleného globálního peněžního systému.

Bitcoin jako decentralizovaný globální systém umožňuje větší finanční svobodu a přesouvá moc od několika lidí k mnoha. Poskytuje bezpečné útočiště odolné vůči cenzuře a pro ukládání a převod hodnoty, která jednotlivcům umožňuje převzít kontrolu nad svým majetkem. To je obzvláště důležité v dnešní nejisté době a v situaci, kdy tradiční finanční systém čelí bezprecedentním výzvám.

Aktivita: Shlédněte video

Pravděpodobnost pozitivní změny je veliká, a proto vás vyzýváme k tomu, abyste shlédli toto video a zjistili tak více informací.

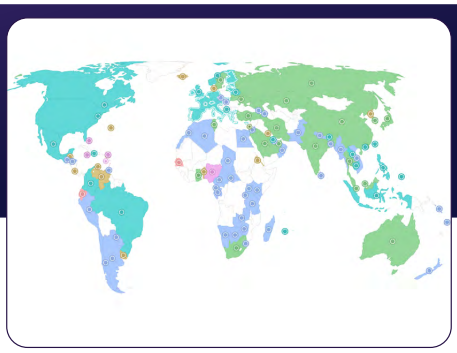
Dále se podíváme na novou formu digitálních měn, která se nazývá CBDC (Central Bank Digital Currency), a zhodnotíme, v čem je podobná a v čem se naopak liší od Bitcoinu.

10.1 Co jsou to digitální měny centrálních bank (CBDC), a kdo je řídí?

Digitální měny centrální banky (CBDC) jsou digitální verze běžných fiat měn. CBDC se řídí stejnými pravidly jako běžné fiat peníze, kdy centrální orgán, jako je vláda, může vytvářet větší nabídku, a tím je schopna snížit kupní sílu lidí. CBDC však také poskytuje vládám a centrálním bankám nové a silné nástroje ke kontrole toho, jak lidé na celém světě tyto peníze používají.

Podle průzkumu Nadace pro lidská práva (Human Rights Foundation, HRF) 119 ze 193 vlád na světě zkoumá, testuje nebo již CBDC používá.

Na stránkách Nadace pro lidská práva (Human Rights Foundation) si můžete ověřit, zda a jak se ve vaší zemi provádí výzkum CBDC.
https://cbdctracker.hrf.org/home nebo
https://cbdctracker.org/

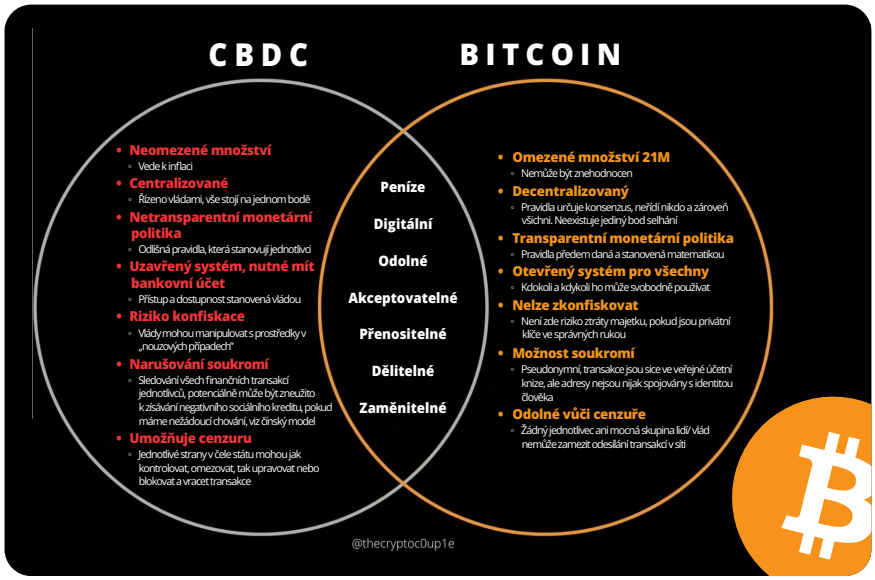


Čím se tedy CBDC liší od běžných fiat měn kromě toho, že jsou digitální? Klíčové je pochopit, že na rozdíl od běžných fiat měn v podobě papíru nebo mincí umožňují CBDC vládě digitálně sledovat a kontrolovat každou transakci po celém světě. To znamená, že vláda může pozastavit určité transakce nebo dokonce zmrazit celý váš účet, pokud se jí nelíbíte vy nebo způsob, jakým své peníze používáte.

Představte si například, že chcete poslat peníze rodinnému příslušníkovi do země, která potřebuje pomoc, ale místní vláda vaši transakci odmítne, protože nesouhlasí s vedením této země. Nebo si představte, že jdete do obchodu koupit si něco, co se vám líbí, ale nemůžete, protože jste vyjádřili svůj názor na sociálních sítích.

CBDC dávají vládám neomezenou moc kontrolovat, jak jsou peníze používány po celém světě, a omezují tak možnost jednotlivců utrácet peníze na základě jejich vlastního rozhodnutí. Někteří dokonce tvrdí, že CBDC by umožnily mocným vládám centrálně prosazovat tyranskou politiku v celosvětovém měřítku - pouhým stisknutím vypínače - bez potřeby lidských zástupců.

CBDC i Bitcoin jsou digitální, ale kromě této společné vlastnosti představují velmi odlišné formy peněz s odlišnou filozofií, což vede k různým výsledkům pro lidstvo.



10.2 Filozofie Bitcoinu

V kapitolách 6 a 9 jsme zjistili, že jednotlivci, kteří provozují bitcoinový uzel, pomáhají udržovat pravidla sítě v bezpečí. To je velká věc, protože poprvé v historii mohou být lidé jako my součástí týmu, který zajišťuje ochranu pravidel našeho peněžního systému. Mezi tato pravidla patří i to, že existuje pouze omezené množství peněz a žádná jednotlivá strana nemůže tato pravidla změnit. Je to mimořádná šance pro obyčejné lidi, aby pomohli udržet naše peníze bezpečné a spolehlivé.

Filozofie Bitcoinu spočívá v posílení pravomocí, svobodě, finanční nezávislosti, kritickém myšlení a konceptu, že bychom všichni měli mít možnost ovlivnit pravidla systému, který si sami zvolíme. Na rozdíl od fiat systému ovládaného mocnými centrálními stranami funguje Bitcoin na síti, kde žádná strana nemá veškerou kontrolu. To znamená, že na rozdíl od jiných typů peněz, jako jsou CBDC, vám nikdo nemůže vzít váš majetek ani vám zabránit v tom, abyste své peníze utratili tak, jak chcete.

V tradičním finančním světě se větší bohatství přímo promítá do většího vlivu a kontroly. Bitcoin naopak funguje tak, že jde o moc ve prospěch lidí. Je to jako týmová práce, kde každý, bez ohledu na to, kolik má peněz, hraje v systému klíčovou a stejnou roli. Představte si to jako kolektivní sílu, kde vaše finanční velikost automaticky neznamená, že vše ovládáte. Bitcoin je postaven na neměnných pravidlech a v této harmonii jako by systém ovládalo samo lidstvo. Není to několik velkých hráčů, kteří rozhodují; je to spolupráce nás všech, podobně jako u odolné komunity, která řídí chod Bitcoinu, aniž by mu nějaká jednotlivá autorita říkala, co má dělat.

Zatímco ve fiat systému diktují pravidla mocní, v ekosystému Bitcoinu je to kolektivní síla jednotlivců, která udržuje síť. Žádný jednotlivý subjekt, bez ohledu na své bohatství, nemůže diktovat, jakým směrem se Bitcoin vydá. Je to naprosto odlišný přístup než ten, který známe v dnešním světě, jelikož robustnost systému leží v rukou ne několika jednotlivců, ale v rukou každého uživatele sítě.

Hlavní myšlenkou je vytvořit bezpečný, přehledný a spravedlivý systém, v němž budou mít všichni stejný přístup ke globálním penězům.

Aktivita: Diskuse ve třídě - Máte právo mít kontrolu nad svými vlastními penězi?

1. Jsou peníze lidskou potřebou a lidským právem? A proč?
2. Pokud nemůžete své peníze utratit, jak chcete, poslat je, komu chcete, nebo si je vzít s sebou do nové země, jsou skutečně vaše? A proč?
3. Proč se přestal používat barterový obchod? Jaký je problém s dvojí shodou potřeb?
4. Která historická událost na vás měla největší dopad? Proč je důležité pochopit „Nixonův šok" a jeho význam pro každého člověka v dnešní době?
5. Jak se liší peníze s pevnou zásobou od tradičních fiat měn?

6. Kdy byl Bitcoin vytvořen, kým, za jakým účelem a jak tento účel definuje koncept decentralizovaného systému?
7. Jaký je rozdíl mezi úschovnou a vlastní peněženkou? Jaká byla vaše oblíbená peněženka?
8. Čemu rozumíte v souvislosti se sítí Lightning Network? Pro jaký typ transakcí byste ji použili?
9. Proč provozování vlastního uzlu podporuje síť?
10. Jak vám kontrola nad vlastními penězi pomáhá v každodenním životě a při plánování budoucnosti?
11. Jakým způsobem může finanční svoboda zvýšit vaši schopnost pozitivně přispívat komunitě nebo společnosti?

10.3 Výhody používání Bitcoinu

„Hyperbitcoinizace" je teoretická budoucnost, kdy se Bitcoin stane dominantním globálním peněžním systémem. To by znamenalo, že Bitcoin by používali všichni, všude a na všechno. Od nákupu kávy přes placení účtů až po koupi domu.

Rostoucí zájem o Bitcoin ze strany jednotlivců, podniků, zemí a vlád poukazuje na potenciální dopad jeho širokého přijetí na ekonomiku a společnost. Zde jsou některé z výhod hyperbitcoinizovaného světa:

1. **Budoucnost suverénního člověka:**
   je taková, kdy jednotlivci na celém světě mají plnou kontrolu nad svou vlastní digitální identitou a majetkem. To by mohlo vést k větší finanční inkluzi (začlenění), svobodě, soukromí a bezpečnosti, a tím přispět k většímu rozkvětu, hojnosti a celkovému štěstí lidí.

2. **Spolehlivý uchovatel hodnoty:**
   bitcoin je díky své digitální vzácnosti spolehlivým dlouhodobým uchovatelem hodnoty, což by mohlo přimět více lidí, aby jej používali jako prostředek spoření do budoucna.

3. **Změny v měnové politice:**
   pokud by se Bitcoin rozšířil, mohl by zrušit schopnost vlád kontrolovat nabídku peněz prostřednictvím tradičních nástrojů měnové politiky. Masové přijetí Bitcoinu by potenciálně zvýšilo kupní sílu lidí a povzbudilo společnost k přechodu k činnostem s nízkou časovou preferencí.

4. **Zvýšená transparentnost a sledovatelnost:**
   neporušitelný a nezměnitelný záznam všech transakcí v blockchainu by mohl zvýšit transparentnost a odpovědnost v různých odvětvích a sektorech. V současné době mají mocné subjekty možnost přesouvat biliony dolarů po celém světě bez jasného přehledu o tom, kam tyto prostředky putují a jak jsou využívány. Poskytnutím otevřeného a ověřitelného záznamu finančních transakcí by Bitcoin mohl zajistit, aby se pohyb kapitálu stal odpovědnějším a přístupnějším veřejnosti.

5 **Revoluce na trhu s peněžními převody:**

trh s remitencemi zahrnuje převod finančních prostředků z jedné země do druhé. Navzdory klesajícím nákladům zůstávají remitence ve srovnání s domácími bankovními převody relativně drahé, zejména u menších částek. Síť Lightning Network nabízí rychlé a nízkonákladové transakce, díky čemuž se dobře hodí pro tento trh a řeší vysoké náklady a další problémy spojené s remitencemi, jako je pomalá doba vypořádání a omezení pracovní doby.

6 **Nadbytek energie:**

když je k dispozici dostatek cenově dostupné energie, společnosti se daří dobře a mnoho průmyslových odvětví a komunit může uspokojit rostoucí potřebu energie v domácnostech, podnicích a nových technologiích. Těžba bitcoinu motivuje těžaře k využívání přebytečné energie, která by obvykle přišla nazmar, a to především z udržitelných zdrojů, jako jsou solární, větrné a vodní elektrárny. Těžaři bitcoinu tuto přebytečnou energii využívají k vytváření nových bitcoinů prostřednictvím těžby, zabezpečují síť a přebytečnou energii, kterou vytvoří, nabízejí zpět do energetické sítě, kterou společnost využívá v případě potřeby.

10.4 Zářná budoucnost

Bitcoin jsou peníze.

Peníze pomáhají lidem sdělovat, které činnosti, zboží a služby jsou ve společnosti nejdůležitější. Jak jsme viděli v této učebnici, pokud jsou peníze pod kontrolou centralizovaných orgánů, dochází k manipulaci s nimi.

Jednou z chyb, které lidstvo v historii neustále opakuje, je manipulace s penězi, která pak negativně ovlivňuje jednotlivce, rodiny, podniky, vlády a nakonec i globální prosperitu lidstva.

Tím, že převezmeme kontrolu nad penězi z rukou centralizovaných stran a místo toho budeme používat peníze s pevnou nabídkou, kterou žádná strana nemůže měnit, vytvoříme jiný svět. Takový, ve kterém nemusíme věřit, že člověk udělá správnou věc, ale naopak takový, ve kterém člověk není schopen udělat špatnou věc.

Tento svět je zásadně odlišný.

A vy, milí studenti, se můžete podílet na vytváření tohoto světa. Používáním Bitcoinu, provozováním vlastního uzlu a pomáháním svým blízkým dozvědět se více o budoucnosti peněz, hlasujete pro jiný svět.

Aktivita: Závěrečná diskuse ve třídě - Jak se změnil váš pohled na věc?

Odpovězte na 5 níže uvedených otázek:

Proč potřebujeme peníze?

Co jsou to peníze?

Proč Bitcoin?

Kdo ovládá peníze?

Co nebo kdo dává penězům jejich „hodnotu"?

Jakou otázku máte ohledně peněz? Napište ji sem a podělte se o ni ve své třídě.

1. **Vraťte se k první aktivitě v kapitole 1 a porovnejte své nové odpovědi se starými.**
2. **Porovnejte a prodiskutujte původní odpovědi a otázky. Změnilo se něco?**
3. **Položte si tuto závěrečnou otázku: Jaký je můj další krok? A jak mohu tyto nové znalosti využít k posílení svých schopností?**

„Pokud jste připraveni udělat další krok, podívejte se do další sekce doplňkových zdrojů, kde jsme vybrali nejlepší zdroje pro další vzdělávání.“

Další zdroje

1. Proč používat bitcoin?

a **'Bitcoin je budoucnost' od autora Vijaye Boyapatiho:**

Tento článek (i kniha) vysvětluje, proč je Bitcoin cenným aktivem a proč má potenciál stát se dominantní globální měnou. Autor se zabývá technickými a ekonomickými aspekty Bitcoinu, které z něj činí silnou investiční příležitost.

b **'Why Bitcoin Matters' od Aleks Svetski (1 hodina):**

Toto video se zabývá důležitostí Bitcoinu jako decentralizovaného digitálního aktiva a tím, jak může ovlivnit současný finanční systém. Autor zkoumá potenciál Bitcoinu přinést finanční svobodu lidem na celém světě.

c **'Why Bitcoin' od Wiz:**

Tento článek poskytuje přehled výhod používání Bitcoinu jako měny a úložiště hodnoty. Zdůrazňuje decentralizovanou povahu Bitcoinu a to, jak umožňuje větší finanční svobodu a bezpečnost.

2. Co to je Bitcoin?

a **'How Bitcoin Works Under the Hood' od CuriousInventor:**

https://www.youtube.com/watch?v=Lx9zgZCMqXE Toto video podrobně vysvětluje technické aspekty bitcoinu a jeho fungování.

b **'What Is Bitcoin' od Greg Walker:**

Tento článek poskytuje komplexní vysvětlení toho, co je Bitcoin, včetně jeho historie, technologie a toho, jak se liší od tradičních měn.

c **'Bitcoin - The Genesis' od RT (30 minut):**

Toto video se věnuje vzniku a počátkům Bitcoinu. Zkoumá motivaci tajemného tvůrce Satoshiho Nakamota a vývoj konceptu Bitcoinu, jako takového.

3. Další učení:

a **'Bitcoinový Standard' (1 hodina 40 minut):**

Tato audiokniha se zabývá ekonomickými a historickými souvislostmi, které vedly ke vzniku Bitcoinu. Zabývá se výhodami decentralizované měny a potenciálem Bitcoinu stát se globálním standardem.

c **"Bitcoin Babies"**

od Naomi Wambui - **https://bitcoinbabies.com/**
Twitter: **@btcbabies - @ngachanaomi1**
Volně stažitelný pdf zdroj pro posílení postavení matek v zemích třetího světa.

b **'Intro to Bitcoin Austrian Thought' (1 hodina):**

Tato audio přednáška se zabývá rakouskou ekonomickou školou a jejím vztahem ke konceptu Bitcoinu. Poskytuje podrobný pohled na ekonomické principy, které stojí za Bitcoinem, a na to, jak se shodují s rakouským myšlením.

d **BTC Sessions**

Vzdělávací kanál YouTube zaměřený pouze na bitcoiny s užitečnými návody a průvodci: **https://www.youtube.com/@BTCSessions**

4. Kurzy:

a **Summer of Bitcoin**

https://www.summerofbitcoin.org/: globální online program letních stáží zaměřený na seznámení vysokoškolských studentů s vývojem a designem open-source kódu Bitcoinu.

b Chaincode Labs

https://learning.chaincode.com/#FOSS: online kurzy a rezidenční program, který studentům umožňuje osvojit si dovednosti potřebné k práci na vývoji protokolu Bitcoinu.

c Saylor Academy

Bezplatné vzdělávání v různých oborech: **https://www.saylor.org/**

5. Vzdělávací obsah pro české čtenáře:

a Bitperia.cz

Bitcoinový průvodce v českém jazyce, který je rozcestníkem k dalšímu vzdělávacímu obsahu. Najdete zde zajímavé články, knihy s českým překladem, podcasty jak pro začátečníky, tak i pokročilé, možnost najít si práci v předních firmách, které budují byznys okolo Bitcoinu v České republice, a další.

b Bitcoinovej kanál:

Největší český YouTube kanál s užitečnými návody a rozsáhlou sérií videí s názvem – Úvod do Bitcoinu. Dále zde najdete rozhovory se zajímavými osobnostmi a také novinky ze světa financí, Bitcoinu.

6. Důležití Autoři

a Alex Gladstein: *Check Your Financial Privilege*

b Alex Swan: *Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications*

c Amanda Cavaleri: *Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide*

d Anita Posch: *Learn Bitcoin: Become Financially Sovereign*

e Eric Yakes: *The 7th Property: Bitcoin and the Monetary Revolution*

f Jeff Booth: *The Price of Tomorrow: Why Deflation is the Key to an Abundant Future*

g Jimmy Song: *The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future*

h Nik Bhatia: *Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies*

i Robert Breedlove: *Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money*

j Lyn Alden: *Broken Money*

7. Citovaní Autoři

a Curious Inventor:

https://www.youtube.com/@CuriousInventor

b Anil Patel:

Twitter: @anilsaidso

8. Další zdroje:

1 **Bitcoin.org:** Oficiální stránka Bitcoinového protokolu.

2 **Bitcointalk.org:** Bitcointalk je fórum, kde mohou uživatelé diskutovat o tématech souvisejících s bitcoinem, klást otázky a sdílet informace. Jedná se o vhodné místo, kde se můžete učit od ostatních nadšenců a odborníků na Bitcoin.

3 **Bitcoincore.org:** Jedná se o původní software, který je stále hojně využíván mnoha uživateli a vývojáři. Poskytuje rozsáhlou sadu nástrojů pro práci s Bitcoinovou sítí a vytváření aplikací.

4 **Bitcoinwiki.org:** Je komunitní zdroj informací, který poskytuje podrobného průvodce vším, co souvisí s Bitcoinem. Zahrnuje tak vše od technických aspektů Bitcoinu až po jeho historii a případy použití.

5 **Bitcoinmagazine.com:** Jedná se o online publikaci, která se zabývá novinkami a poznatky týkajícími se Bitcoinu a dalších kryptoměn. Poskytuje tak skvělý přehled o nejnovějším vývoji v tomto ekosystému.

6 **Bitcoin.Design:** Open-source úložiště designových souborů pro ilustrace, webové stránky, šablony a ikony.

Další zdroje

7. **NOSTR:** https://nostr.com/ - decentralizovaná sociální síť, kde vám nikdo nemůže cenzurovat vaše data a příspěvky.
8. **Simple X:** https://simplex.chat/ - decentralizovaná aplikace zaměřena na soukromí uživatelů.
9. **Set up a Bitcoin Node:** Raspberry Pi DIY od Keith Mukai: https://github.com/kdmukai/raspi4_bitcoin_node_tutorial?tab=readme-ov-file
10. **How to select a Bitcoin wallet:** https://bitcoin.org/en/choose-your-wallet - využijte nově nabyté znalosti k výběru té správné peněženky.
11. **BitcoinIcons.com:** - https://bitcoinicons.com/ - Kolekce icon souvisejících s Bitcoinem.
12. **Bitcoin For Local Business:** https://bitcoinforlocalbusiness.com/ - Sada letáků, které vám pomohou sdílet hodnotu Bitcoinu s vašimi oblíbenými místními podniky.
13. **Mempool.Space:** https://mempool.space/ - Opensource projekt, který obsahuje také data a grafy sítě Lightning Network.

Klíčové Pojmy

Kapitola 1:

Úvod do kurzu:

Seznamte se s cíli a očekáváními kurzu Bitcoinového diplomu.

Úvaha - Definice peněz:

Zapojte se do úvahového cvičení a odpovězte na pět klíčových otázek o penězích.

Diskuse ve třídě - Proč potřebujeme peníze:

- Zúčastněte se diskuse v rámci celé třídy a prozkoumejte základní potřebu peněz.
- Sdílejte a porovnávejte jednotlivé pohledy ohledně potřeby peněz.
- Stanovte si důvody pro pochopení úlohy peněz v ekonomických systémech.

Kapitola 2:

Pochopení peněz:

- Prozkoumejte základní definici peněz.
- Diskutujte o různých pohledech na peníze v rámci třídy, abyste pochopili jejich rozmanitou povahu.

Funkce, vlastnosti a druhy peněz:

- Seznamte se s hlavními funkcemi, vlastnostmi a druhy peněz.
- Poznejte důležitost těchto aspektů při definování a používání peněz.

Psychologie peněz:

- Pochopte psychologické aspekty peněz, včetně nedostatku, časových preferencí a kompromisů.
- Zapojte se do aktivity „Časové preference“ a propojte psychologické prvky s reálnými scénáři.

Kapitola 3:

Úvod do historie a vývoje peněz:

- Prozkoumejte historii a vývoj peněz.
- Pochopte, jak starověké formy obchodování vedly ke vzniku měny, kterou používáme dnes.

Revoluce digitálních měn:

- Objevte současný vrchol peněžní revoluce - digitální měny.
- Pochopte, že existují pouze v elektronické podobě a umožňují okamžité a levné transakce po celém světě.
- Seznamte se s významnou rolí, kterou sehrál Bitcoin při řešení prvních problémů digitálních měn, a připravil je tak na celosvětové použití.

Vývoj měny:

Prozkoumejte přechod od starověkých forem peněz, jako jsou mušle a korálky, až po vznik mincí a papírových peněz. Sledujte cestu od „papíru k plastu“ a poznejte evoluci peněz v průběhu celé historie.

Barter:

Zapojte se do praktické hry na směnný obchod, abyste pochopili problémy přímé směny a uvědomili si potřebu efektivnějšího systému.

Kapitola 4:

Počátky fiat měn:

Prostřednictvím stručné historie se seznámíte s původem fiat měn a pochopíte, jak se staly dominantní formou platidla.

Bankovnictví částečných rezerv:

Zapojte se do aktivity „Bankovnictví s frakčními rezervami“, abyste získali přehled o fungování tohoto systému, zdůraznili jeho závislost na dluhu a důsledky pro širší ekonomiku.

Systém Fiat měn:

Pochopte základní aspekty dnešní ekonomiky, včetně povahy fiat měn jako nuceného peněžního systému. Aále pochopíte úlohu bankovnictví s částečnými rezervami a klíčových hráčů, kteří tento systém ovládají.

Kapitola 5:

Snižování kupní síly:

- Porozumějte konceptu měnové inflace a jejímu dopadu na kupní sílu.
- Důsledky inflace: Vyzkoušejte si na vlastní kůži, jaké dopady má inflace.

Důsledky Fiat systému:

Zapojte se do aktivity „Důsledky Fiat systému“, která osvětlí širší dopady současného měnového uspořádání.

Digitální měny centrálních bank (CBDC):

Prozkoumejte vyvíjející se prostředí digitálních měn centrálních bank (CBDC) a jejich potenciální vliv na budoucnost peněz.

Globální dluhová zátěž a sociální nerovnost:

Prozkoumejte dvojí dopad globální dluhové zátěže a sociální nerovnosti. Poznejte individuální a společenské důsledky s důrazem na ztrátu kupní síly a zvětšující se rozdíly v bohatství.

Cypherpunkeři a decentralizace:

Seznamte se s příběhem Cypherpunkerů a jejich motivací k hledání decentralizované měny. Rozlišujte mezi centralizovanými a decentralizovanými systémy a získejte poznatky ze stručné historie digitálních měn.

Kapitola 6:

Satoshi Nakamoto a vznik Bitcoinu:

Prozkoumejte tajemnou postavu Satoshiho Nakamota a příběh vzniku Bitcoinu, kde pochopíte prvotní motivaci k jeho vzniku.

Aktivita ve třídě - Vytváření shody:

Zapojte se do aktivity Vytváření shody v síti Peer-to-Peer a získejte praktické poznatky o tom, jak se dosahuje konsenzu v síti Bitcoin.

Přijetí osobní odpovědnosti:

Zdůraznění konceptu osobní odpovědnosti v souvislosti s Bitcoinem, podpora pochopení individuálních rolí a odpovědnosti v rámci decentralizovaného ekosystému.

Jak Bitcoin funguje:

Pohled na mechaniku Bitcoinu včetně Nakamotova mechanismu konsenzu. Identifikujte klíčové hráče v bitcoinové síti, jako jsou těžaři, uzly, uživatelé, vývojáři a projekty. Pochopíte tak dynamiku spolupráce mezi nimi.

Bitcoin jako zdravé digitální peníze:

Prozkoumejte Bitcoin v roli zdravých digitálních peněz, diskutujte o jeho vývoji, funkcích a vlastnostech a zúčastněte se diskuse ve třídě o tom, zda je Bitcoin považován za zdravé peníze.

Klíčové Pojmy

Kapitola 7:

Peer-to-Peer transakce:

Zapojte se do transakcí na decentralizované bázi a vyzkoušejte si základní principy směny bitcoinu.

Nastavení bitcoinové peněženky:

Podívejte se na základní kroky ke stažení peněženky, vytvoření klíčů a zálohování pro bezpečné operace s Bitcoinem.

Spoření a DYOR:

Pochopte spoření v bitcoinu jako uchování kupní síly a význam zkratky DYOR (Do Your Own Research).

Typy Bitcoinových peněženek:

Rozlišujte mezi peněženkami s otevřeným zdrojovým kódem, s uzavřeným zdrojovým kódem a dále mezi non-custodial a custodial peněženkami. Také se seznamte se s úlohou jednotlivých klíčů v zabezpečení bitcoinu.

Pořizování bitcoinu:

Prozkoumejte metody, jako jsou peer-to-peer transakce a nebo směnárny/burzy. Diskutujte o otázkách ochrany osobních údajů souvisejících s procesy KYC, AML.

Kapitola 8:

Úvod do sítě Lightning Network:

Poznejte vývoj na Bitcoinu prostřednictvím technologií, jako je Lightning Network. Ten rozšiřuje jeho možnosti, zejména v oblasti škálovatelnosti.

Nastavení Lightning peněženky:

Přečtěte si základní kroky k nastavení Lightning peněženky, která usnadňuje rychlejší a škálovatelnější transakce.

Praktická aktivita:

Zapojte se do štafetového závodu Lightning peněženek, který podporuje dynamické porozumění transakcí na síti Lightning.

Typy Lightning peněženek:

Rozlišujte mezi open source, closed source, custodial a noncustodial Lightning peněženkami pro různé preference uživatelů.

Transakce přes Lightning:

Prozkoumejte proces odesílání a přijímání bitcoinu přes Lightning s důrazem na rychlost a efektivitu sítě.

Kapitola 9:

Bitcoinová účetní kniha:

Pochopte koncept decentralizované účetní knihy, kterou vedou uzly a těžaři a která zajišťuje transparentnost a bezpečnost.

Model UTXO:

Pochopte model UTXO (Unspent Transaction Output) jako základní aspekt transakčního procesu Bitcoinu.

Uzly a těžaři bitcoinu:

Podívejte se na roli uzlů a těžařů při udržování bitcoinové sítě, která zahrnuje aspekty, jako je emise, vzácnost, půlení a obtížnost.

Veřejné a soukromé klíče:

Prozkoumejte význam kryptografického zabezpečení v bitcoinových transakcích prostřednictvím veřejných a soukromých klíčů spolu s aktivitou demonstrující hashování SHA 256.

Jak fungují bitcoinové transakce:

Získejte přehled o celém cyklu bitcoinové transakce, do kterého jsou zapojeni odesílatel, příjemce, uzly, těžaři a mempool, se speciální aktivitou zaměřenou na mempool.

Kapitola 10:

Filozofické základy bitcoinu:

Prozkoumejte základní filozofii bitcoinu a pochopte, proč vznikl jako reakce na kolabující ekonomickou situaci ve světě. A to zejména se zaměřením na finanční svobodu a na to, jak se liší od tradičních měn.

Budoucnost bitcoinu:

Prozkoumejte potenciální směr a budoucí vývoj Bitcoinu jako revoluční digitální měny.

Poznatky:

- Shrnutí klíčových poznatků z učebnice Bitcoinový diplom a povzbuzení studentů, aby se zamysleli nad svou cestou a získanými zkušenostmi.
- Aktivity zahrnují sledování videa na téma „Proč Bitcoin?“ a zopakování otázek z kapitoly 1, abyste zhodnotili svůj osobní růst.

Slovník pojmů

51% útok: Jedná se o typ útoku na blockchainovou síť, při kterém jeden subjekt nebo skupina ovládá většinu výpočetního výkonu sítě, což jim umožňuje manipulovat s transakcemi (utrácet stejné mince vícekrát) a potenciálně narušit síť.

Adresa peněženky: Jedinečný identifikátor používaný k odesílání a přijímání bitcoinů, obvykle reprezentovaný jako řetězec písmen a čísel.

Altcoinová sezóna: Období, kdy alternativní kryptoměny zaznamenávají výrazný nárůst cen, často v důsledku zvýšeného zájmu investorů a jejich adopce.

Altcoiny: Všechny digitální měny, které vznikly po Bitcoinu.

Atomic Swap: Výměna jedné kryptoměny za jinou bez potřeby centralizované burzy nebo zprostředkovatele.

Aukce: Proces, při kterém se zboží nebo majetek prodává tomu, kdo nabídne nejvyšší cenu.

Bitcoin: Digitální měna/systém, který umožňuje lidem posílat si navzájem peníze bez nutnosti použití banky nebo jiné instituce.

Burza/směnárna kryptoměn: Platforma, kde mohou uživatelé nakupovat, prodávat a vyměňovat kryptoměny za jiná aktiva, jako je fiat měna nebo jiné kryptoměny.

Blockchain: Veřejný záznam všech uskutečněných transakcí s bitcoiny.

BTC: Jednotka používaná pro bitcoiny. Digitální měna, kterou lze používat k nákupům nebo k obchodování.

Centrální banka (Fed, ECB, ČNB...): Vládou kontrolovaná a řízená instituce, která řídí měnovou politiku země.

Centralizace: Soustředění moci nebo kontroly v jediném subjektu.

Centralizovaný systém: Systém, v němž je moc nebo kontrola soustředěna v rukou jediného subjektu.

Cold storage: Metoda ukládání bitcoinů v režimu offline, mimo dosah hackerů nebo jiných online hrozeb.

Chytrý kontrakt: Samostatně realizovatelná smlouva, jejíž podmínky jsou zapsány v kódu.

Dluh: Peníze, které jsou dluženy někomu jinému.

Decentralizace: Rozdělení moci a kontroly mezi všechny členy sítě namísto centrální autority.

Decentralizovaná autonomní organizace (DAO): Organizace nebo síť řízená smartkontrakty a provozovaná na blockchainu bez centrální autority nebo řídicí struktury.

Decentralizované finance (DeFi): Hnutí v kryptoměnovém průmyslu, jehož cílem je vytvořit decentralizované finanční produkty a služby, které fungují na blockchainu.

Decentralizovaný systém: Systém, ve kterém je moc nebo kontrola rozdělena mezi více subjektů.

Digitální aktivum: Digitální vyjádření hodnoty, se kterým lze obchodovat nebo které lze použít jako uchovatel hodnoty, například bitcoiny.

Distribuovaná účetní kniha: Databáze, která je rozprostřena v síti počítačů a není uložena na jednom konkrétním místě.

Dovoz: Zboží a služby vyrobené v jiné zemi a prodávané na domácím trhu.

Dvojí shoda potřeb: V barterové ekonomice mají obě strany to, co chce jiná strana, a zároveň chtějí to, co má druhá strana.

Dvojnásobná útrata: Když se člověk pokusí poslat své bitcoiny dvěma různým příjemcům současně.

Dvoufaktorové ověřování (2FA): Pro přístup k účtu nebo dokončení transakce je nutné použít dva způsoby ověření, obvykle heslo a samostatný kód nebo zařízení.

Dust Transaction: Transakce, při níž se posílá velmi malé množství bitcoinů, které je příliš malé na to, aby bylo ekonomicky výhodné.

Etický hacker: Osoba, která využívá své schopnosti k identifikaci a opravě zranitelností v počítačových systémech a sítích.

FOMO: Fear of missing out (strach z promeškání příležitosti) je termín používaný k popisu pocitu úzkosti nebo lítosti, že člověk může propásnout ziskovou příležitost na trhu.

FUD: Fear, uncertainty and doubt, termín používaný k popisu negativních zvěstí nebo informací, které mohou způsobit paniku nebo pokles trhu.

HDP: Hrubý domácí produkt neboli celková hodnota zboží a služeb vyprodukovaných v dané zemi za určité období.

Hard Fork: Změna protokolu, která vytvoří novou verzi blockchainu, která není kompatibilní s předchozí verzí (např. Bitcoin Cash).

Hardwarová peněženka: Fyzické zařízení používané k ukládání soukromých klíčů a správě kryptoměn, které poskytuje vyšší bezpečnost než softwarové peněženky.

Hashovací funkce: Matematická funkce, která přijímá vstupní data libovolné velikosti a na jejímž výstupu je řetězec znaků pevné velikosti. Běžně používaná v kryptografii a blockchainové technologii.

Slovník pojmů

Hash Rate (rychlost hašování): Je to způsob měření výpočetního výkonu bitcoinové sítě.

HODL: : Termín používaný v kryptoměnové komunitě pro označení dlouhodobého držení kryptoměny namísto jejího prodeje nebo obchodování s ní.

Hodnota peněz v čase: princip, podle kterého mají peníze větší hodnotu v současnosti než v budoucnosti.

Hot Wallet: Peněženka, která je připojena k internetu a umožňuje snadný přístup k bitcoinům.

ID transakce: Řetězec čísel a písmen, který v bitcoinovém blockchainu zobrazuje podrobnosti o bitcoinovém převodu (například odeslanou částku, adresy odesílatele a příjemce a datum převodu).

Inflace: Zvýšení obecné cenové hladiny zboží a služeb v ekonomice. Jinými slovy zvýšení peněžní zásoby v oběhu, které zvyšuje poptávku a tím tak tlačí ceny nahoru.

Komoditní peníze: Předměty, které mají hodnotu samy o sobě a používají se jako prostředek směny, v historii například zlato nebo stříbro.

Kontrola kapitálu (peněz): Omezení pohybu peněz přes hranice.

Kryptoměnová peněženka: Softwarový program, který uchovává soukromé klíče a umožňuje uživatelům posílat, přijímat a spravovat kryptoměny.

Kryptografie: Obor matematiky, který pomáhá vytvářet bezpečné systémy.

Kupní síla: Určuje cenu peněz, za které lze nakupovat zboží a služby.

Lightning Network: Platební protokol druhé vrstvy, který umožňuje rychlejší a levnější bitcoinové transakce pomocí otevřených kanálů mimo hlavní řetězec. Slouží pro malé a každodenní transakce.

Mechanismus Konsensu: Zároveň je to metoda používaná v blockchainové technologii k ověřování transakcí a zajištění integrity blockchainu.

Merkle Tree: Datová struktura používaná v bitcoinovém blockchainu k efektivnímu ověřování integrity velkých souborů dat.

Mempool: V tomto nástroji si uživatelé mohou prohlížet jednotlivé bloky, transakce a adresy peněženek.

Měnová a fiskální politika: Politika centrální banky a vlády, která ovlivňuje nabídku peněz a úrokové sazby v ekonomice.

Multi-Signature: Je bezpečnostní funkce, která vyžaduje více než jeden soukromý klíč k autorizaci bitcointové transakce.

Nabídka a poptávka: Ekonomický princip, podle kterého je cena zboží nebo služeb určena vzájemným působením množství dodávaného zboží nebo služeb a poptávky.

Non-Fungible Token (NFT): Z překladu „nezaměnitelný token" je typ digitálního aktiva, které představuje jedinečný nebo unikátní předmět, často používaný k reprezentaci uměleckých děl, sběratelských předmětů nebo jiných předmětů.

Nonce: Náhodné číslo přidané do hlavičky bloku za účelem vytvoření hashe, který odpovídá cíli obtížnosti.

Odměna za blok: Množství nových bitcoinů, které jsou těžařům přiděleny za přidání nového bloku do blockchainu.

Osiřelý blok: Blok, který nebyl zařazen do hlavního řetězce blockchainu, protože byl zneplatněn předchozím konkurenčním řetězcem.

Obnovovací fráze/seed: Série 12, 18, 20 nebo 24 slov, která lze použít k vygenerování několika párů soukromých a veřejných klíčů. Ty lze použít k obnovení bitcoinové peněženky.

Obchodní pár: Sada dvou měn nebo aktiv, která lze vzájemně obchodovat na kryptoměnové burze.

Potvrzení: Proces, při kterém je transakce zpracována sítí a je velmi nepravděpodobné, že by byla zrušena. Metoda „těžařů", která slouží k ověřování pravosti transakcí pomocí jejich počítačového hardwaru a softwaru. Doporučuje se počkat na nejméně šest potvrzení, aby se zabránilo dvojímu utracení.

Počáteční nabídka mincí (ICO): Způsob získávání finančních prostředků, při kterém se investorům prodává nová kryptoměna výměnou za fiat nebo za zavedenější kryptoměnu, jako je například Bitcoin.

Protokol na první vrstvě: Základní vrstva blockchainové sítě, která se stará o základní aspekty konsensu, ověřování transakcí a ukládání dat.

Protokol na druhé vrstvě: Sekundární vrstva postavená nad blockchainovou sítí první vrstvy, která se často používá ke zvýšení škálovatelnosti, rychlosti a funkčnosti.

Prostředky směny: Jakýkoliv předmět/prostředek, který je všeobecně přijímán výměnou za zboží a služby.

Peněžní zásoba: celkové množství peněz v oběhu.

Papírová peněženka: Vytištěná kopie soukromých a veřejných klíčů uživatele, která slouží k ukládání a správě kryptoměn off-line.

Peer-to-Peer (P2P): Decentralizovaná síť, ve které účastníci komunikují přímo mezi sebou, nikoli prostřednictvím centrální autority.

Slovník pojmů

Peg: Pevný směnný kurz mezi dvěma měnami, kdy je jedna měna navázána na hodnotu druhé měny.

Proof-of-Stake (PoS): Mechanismus konsensu používaný v některých blockchainových sítích, který vyžaduje, aby uživatelé drželi určité množství kryptoměny, aby se mohli podílet na ověřování transakcí.

Proof-of-Work (Důkaz o vykonané práci): V tomto případě se jedná o mechanismus konsensu, který vyžaduje, aby uživatelé provedli určité množství výpočetní práce, aby se mohli podílet na ověřování a zabezpečování sítě.

Poměr rezerv: Podíl vkladů, které musí banka držet jako rezervy.

Podpis: Digitální matematický mechanismus, který někomu umožňuje prokázat vlastnictví.

Peněženka: Virtuální schránka na bitcoiny, která obsahuje soukromý klíč (klíče) umožňující odesílat, přijímat a spravovat bitcoiny.

Restriktivní bankovnictví: Omezení bankovních služeb nebo přístupu k bankovním službám.

Síť: Skupina vzájemně propojených subjektů.

Síť uzlů: Síť propojených počítačů nebo zařízení, které podporují a udržují bitcoinovou síť.

Soukromý blockchain: Blockchain, který je kontrolován jednou organizací, není tedy decentralizovaný.

Soukromý klíč: Tajný klíč, který prokazuje právo osoby utrácet bitcoiny z konkrétní peněženky prostřednictvím kryptografického podpisu.

Satoshi Nakamoto: Pseudonym, který používá anonymní tvůrce Bitcoinu.

Satoshi: Nejmenší jednotka bitcoinu, která se rovná 1/100 000 000 bitcoinu. Je pojmenována po tvůrci Bitcoinu, Satoshi Nakamotovi.

Satoshi na bajt (sat/b): Jednotka používaná k měření výše poplatku za bitcoinovou transakci zaplaceného za jeden bajt transakčních dat.

SegWit (Segregated Witness): V případě Bitcoinu se jedná o upgrade protokolu, který mění způsob ukládání dat v blockchainu, což umožňuje zvýšit kapacitu a snížit transakční poplatky.

Sidechain: V tomto případě se jedná o blockchain, který je připojen k jinému blockchainu a umožňuje přenos aktiv nebo informací mezi oběma řetězci.

Soft Fork: Změna protokolu Bitcoinu, která je zpětně kompatibilní se staršími verzemi softwaru.

Stablecoin: Typ kryptoměny navržený tak, aby si udržoval stabilní hodnotu často tím, že je vázán na fiat měnu nebo jiné aktivum.

Směnný kurz: Hodnota jedné měny ve vztahu k jiné měně.

Směnný obchod: Výměna zboží a služeb bez použití peněz.

Spotřební koš: Soubor zboží nebo služeb, který se používá k měření změn životních nákladů (často k měření inflace).

Těžební pool (Mining Pool): skupina těžařů, kteří spolupracují, aby zvýšili své šance na nalezení nových bloků a získání bitcoinů. Odměny jsou následně rozdělovány podle výpočetního výkonu.

Těžba: Proces, při kterém se pomocí počítačového hardwaru provádějí matematické výpočty, aby se potvrdily transakce a zvýšila bezpečnost sítě.

Token: Hodnotová jednotka vytvořená na blockchainu, která často reprezentuje konkrétní aktivum nebo užitek v rámci určitého ekosystému.

Tokenizace: Proces vytvoření digitální reprezentace aktiva nebo třídy aktiv na blockchainu, který umožňuje částečné vlastnictví a převoditelnost.

Transakční poplatek: Malá částka, kterou platí odesílatel transakce a která motivuje těžaře, aby transakci zařadili do bloku a přidali ji do blockchainu.

Transakce: Převod bitcoinů z jedné adresy na druhou v bitcoinové síti.

Unbanked („Bez bankovního účtu“): Jednotlivci nebo komunity bez přístupu k tradičním bankovním službám.

Uzel: Počítač nebo zařízení, které je připojeno k bitcoinové síti a podílí se na ověřování, přenosu transakcí. Dále zabezpečují, že pravidla v síti jsou dodržována.

Účetní kniha: Záznam o finančních transakcích.

Účetní jednotka: Standardní měrná jednotka používaná k vyjádření hodnoty zboží a služeb.

Vícepodpisová peněženka (Multisig): peněženka, která vyžaduje více podpisů nebo schválení před provedením transakce, což poskytuje dodatečné zabezpečení a kontrolu.

Veřejný blockchain: Blockchain je otevřený komukoli, kdo se může účastnit a ověřovat transakce, čímž se stává decentralizovaným.

Veřejný klíč: Jedinečný identifikátor používaný pro příjem bitcoinů odvozený ze soukromého klíče uživatele pomocí matematického procesu.

Slovník pojmů

Veřejný klíč/adresa bitcoinu: Jednoduše řečeno adresa používaná k přijímání bitcoinů.

Veřejná účetní kniha: Veškeré transakce v bitcoinové síti se zaznamenávají do decentralizované databáze.

Volatilita: Míra kolísání ceny aktiva v čase.

Velryba: Jednotlivec nebo organizace, která drží značné množství bitcoinů a je schopna ovlivňovat ceny na trhu prostřednictvím velkých obchodů.

Whitepaper: Dokument, který vysvětluje problém a řešení, které se blockchainový projekt nebo kryptoměna snaží řešit.

XBT a BTC: Zkratky pro označení bitcoinu. XBT se dnes již nepoužívá.

Záloha peněženky: Kopie soukromých klíčů pro obnovení bitcoinové peněženky, kterou lze použít k opětovnému získání přístupu k peněžence v případě ztráty nebo krádeže originálu.

Znehodnocení: Snížení hodnoty dané měny, často snížením množství drahého kovu v minci (v historii příměs levnějších kovů, ořezávání, děrování mincí).

ČESKÁ REPUBLIKA

český překlad | 2024