

MICHAEL MERTA

JAK POCHOPIŤ

BITCOIN





MICHAEL MERTA

## Jak pochopit Bitcoin

*Elektronická kniha v češtině obsahující všechny  
potřebné informace pro začátečníky a pokročilé, kteří se  
chtějí zorientovat ve světě Bitcoinu.*

*Copyright © 2021 by Michael Merta*

*All rights reserved. No part of this publication may be reproduced, stored or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without written permission from the publisher. It is illegal to copy this book, post it to a website, or distribute it by any other means without permission.*

*First edition*

*This book was professionally typeset on Reedsy.*

*Find out more at [reedsy.com](https://reedsy.com)*

“The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.”

- SATOSHI NAKAMOTO



# Contents

<i>Předmluva</i>	ii
<i>Disclaimer</i>	v
Otázka č. 1 : Co je Bitcoin?	1
Otázka č. 2: Jak může někdo bitcoin „těžit“?	8
Otázka č. 3 Jaký je smysl Bitcoinu?	12
Otázka č. 4: Jak lze bitcoiny koupit a pracovat s nimi?	16
Otázka č. 5: Jaká je cena bitcoinu?	24
Otázka č. 6: Jak Bitcoin vzniknul?	30
Otázka č. 7: Jaká jsou rizika Bitcoinu?	35
Otázka č. 8: Proč se o Bitcoin zajímat teď, a ne až bude...	41
Referraly (Odkazy na doporučené služby)	43
Závěr	46
Rady a tipy	47
Slovník pojmů a zkratek	49
Kam dál?	52
<i>About the Author</i>	56

# Předmluva

Tato stručná kniha o základech Bitcoinu je určena každému, kdo má zájem co nejjednodušeji pochopit, co to Bitcoin je a proč by ho mohl zajímat. V rozhodnutí tuto knihu napsat mě inspirovalo zejména to, že jsem chtěl vysvětlit své vlastní rodině a přátelům podstatu Bitcoinu tak, aby jí rozuměli a Bitcoin snad i jednou aktivně používali, stejně jako si zvykli používat např. internetové bankovníctví, ke kterému mohli být možná také na jeho začátku skeptičtí. Přestože se o Bitcoin zajímám přibližně 4 roky a již několikrát jsem se snažil vysvětlit např. svým rodičům, co je to Bitcoin, stále vnímám jejich skepsi. Mají pocit, že se jedná pouze o nějakou finanční bublinu pro mladou generaci, které se radši vyhnou, protože jí nerozumí a myslí si, že je zajímat nemusí. Už viděli za svůj život mnoho slibů zázračného zbohatnutí a informace z večerních zpráv o Bitcoinu a jeho rekordních hodnotách či propadech v nich tento dojem pouze zesiluje.

Každá generace zažívá změny, které přináší příležitosti a pasti, jak vydělat peníze, či o ně přijít. Když jejich generace vstupovala do produktivního věku, podobným momentem mohla být např. kupónová privatizace. Bylo spoustu lidí, kteří díky ní zbohatli (někteří nepatrně, jiní pohádkově), a bylo také spoustu lidí, kteří o veškerou svou investici přišli úplně. Podobných příležitostí a pastí bychom v průběhu času našli určitě více, tou současnou,



kteřá nás ale bude zajímat v této knize, bude právě Bitcoin.

Když jsem se poprvé v roce 2014 o Bitcoinu dozvěděl, příliš jsem se o něj nezajímal. Studoval jsem v té době ekonomii na univerzitě ve Francii, a protože Bitcoin s tímto oborem souvisí, ptal jsem se svých profesorů na jejich názor ohledně této problematiky. Bitcoin si už v té době získal pozornost médií, ale byl stále v plenkách a málokdo ho bral vážně. Profesoři se vždy tedy nad jeho myšlenkou pouze zasmáli, protože Bitcoin byl opakem toho, co se sami o penězích doposud naučili a co učili své žáky, což jim nelze mít za zlé. Těžko věřit něčemu, co nemá historii, známého zakladatele, není nikým řízené a bourá establishment finančního a vlastně i politického světa. Sám jsem poté na Bitcoin úplně zapomněl a vrátil se k němu až v roce 2016, kdy mě k němu přivedl zpět kamarád. Řekl mi, že opouští práci ve Švýcarsku, odjede do Asie a bude se živit kryptoměny. Nápad to byl asi šílený, ale věřil jsem mu, proto jsem přes něj koupil svůj první bitcoin za 700 dolarů. Ondra dnes vede projekt [Baserank.io](http://Baserank.io) a já jsem mu vděčný, že mě k Bitcoinu dovedl.

Knih je rozdělena do 8 kapitol, z nichž každá zodpovídá na jednu ze zásadních otázek týkající se této kryptoměny. Z mého pohledu se jedná o ty nejdůležitější informace, které by měl znát každý, kdo o investici do Bitcoinu uvažuje. Věřím, že po přečtení těchto několika stránek bude každý jejich čtenář o něco jistější v chápání Bitcoinu a bude tak schopen si na něj udělat vlastní názor. Neočekávám (a ani to není cílem této knihy), aby přesvědčila všechny čtenáře o tom, že „Bitcoin je budoucnost“. Přál bych si ale, aby donutila každého podívat se do budoucnosti a zvážit, zda má takovýto nástroj šanci v globálním digitálním

světě uspět, a co jemu osobně může přinést.

Tato kniha se zaměřuje pouze na jednu jedinou kryptoměnu – Bitcoin. Žádná z dalších kryptoměn, které se snažily následovat úspěch Bitcoinu, nikdy takové adaptace nedosáhla a s velkou pravděpodobností ani nedosáhne.

8 otázek, na které se zaměříme:

1. Co je Bitcoin?
2. Jak může někdo bitcoin „těžit“?
3. Jaký je smysl Bitcoinu?
4. Jak lze bitcoiny koupit a pracovat s nimi?
5. Jaká je cena bitcoinu?
6. Jak Bitcoin vzniknul?
7. Jaká jsou rizika Bitcoinu?
8. Proč se o Bitcoin zajímat teď, a ne až bude užíván masově (pokud se tak stane)?

Tak pojďme na to!

# Disclaimer

Autor knihy není finančním poradcem, nelze tedy s touto knihou pracovat jako s investičním doporučením nebo radou. Kniha slouží primárně k získání základních informací o nejdůležitější kryptoměně, Bitcoinu, a má pouze informační charakter.

Tato kniha pracuje s hodnotami, které se jistě v čase budou měnit. Místa, kde bude mít výše ceny nebo kapitalizace vliv na výpočty v knize, budou označena kurzívou. Všechny údaje tedy jsou platné k 1. lednu 2021. Zde jsou ty hlavní z nich:

- Cena za 1 bitcoin: \$29 380 = 630 788 Kč
- Tržní kapitalizace všech bitcoinů : 544 miliard dolarů = 11,7 bilionů korun
- Kurz USD/CZK = \$1 = 21,47 Kč
- Kurz EUR/CZK = 1€ = 26,22 Kč

V knize se objevují výrazy Bitcoin, bitcoin a BTC. Bitcoin s velkým písmenem odkazuje na kryptoměnu jako systém, bitcoin s malým písmenem pak na jeho jednotku transakce. BTC je pak zkratkou pro tuto jednotku.



## Otázka č. 1 : Co je Bitcoin?

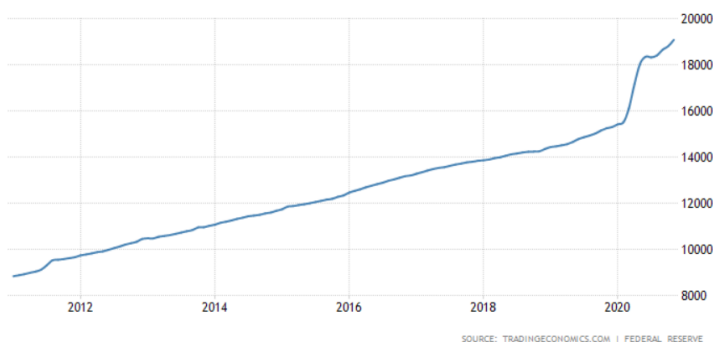
Definici Bitcoinu najdeme mnoho. Zde jsou 3 hlavní z nich:

Bitcoin je kryptoměna.

Tuto definici jste už určitě slyšeli. Bitcoin slouží jako měna, tedy jako prostředek směny. Vizí Bitcoinu je používat ho ke směně stejně jako dnes používáme koruny, eura nebo dolary (tzv. **fiat měny**) k platbě za zboží a služby. Rozdílů od těchto fiat měn je ale několik.

Běžné fiat měny tiskne centrální banka dané země a vláda země zaručuje, že jsou akceptovány jako platidlo. Centrální banka kontroluje její množství v oběhu tím, že je půjčuje za velmi malý úrok komerčním bankám, které je dále půjčují firmám a jednotlivcům. Centrální banka tak používá měnu jako nástroj pro naplňování politiky své vlády. Pokud potřebuje ekonomiku podpořit, sníží úrokovou sazbu, za kterou půjčuje bankám, aby banky mohly přilákat firmy a jednotlivce na levné úvěry a hypotéky. Čím více peněz ale v oběhu je, tím více ztrácejí na své hodnotě, což vede k inflaci, tedy ke zvyšování cen.

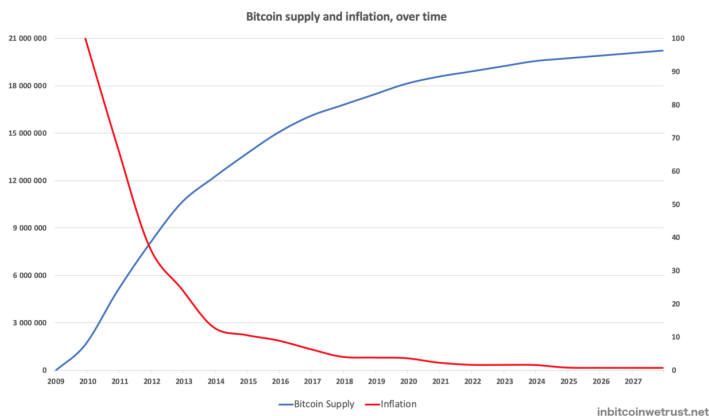
Naopak pokud má vláda pocit, že ekonomika jede příliš rychle a hrozí její přehřátí, nařídí centrální bance zvýšit úrok a úvěry pro firmy a jednotlivce tak prodražit a od investic či zadlužení je odradit. Tyto změny objemu peněz v ekonomice mají zásadní vliv na naše úspory a investice. Obecně se ví, že **inflation** se pohybuje okolo 2–3 % ročně, což nepůsobí dramaticky – to je také důvodem, proč ji většina lidí ignoruje. Porovnejte si ale, jaký dopad to má na vaše úspory např. za 10 let. Narážíme tak na první z mnoha problémů dnešních peněz.



*Peněžní zásoba (nabídka peněz) amerických dolarů za rok 2020 rostla jako z vody. Každý patý dolar na světě byl vytisknut a napumpován do ekonomiky právě v tomto pandemickém roce.*

Jak je na tom v tomto případě **Bitcoin**? Bitcoin žádnou centrální banku nemá. Neexistuje instituce, která by ovlivňovala množství peněz, protože jeho množství je od jeho vzniku v roce 2009 jasně dané, a to 21 milionů bitcoinů, které se postupně do oběhu uvolňují. K dnešnímu dni (rok 2021) je v oběhu cca 18,5 milionů bitcoinů, tedy 89 % z celkového počtu. Zbýlých 11 % bude vznikat postupně až do roku 2140, kdy vznikne poslední bitcoin, a jeho těžba tak bude završena.

## OTÁZKA Č. 1 : CO JE BITCOIN?



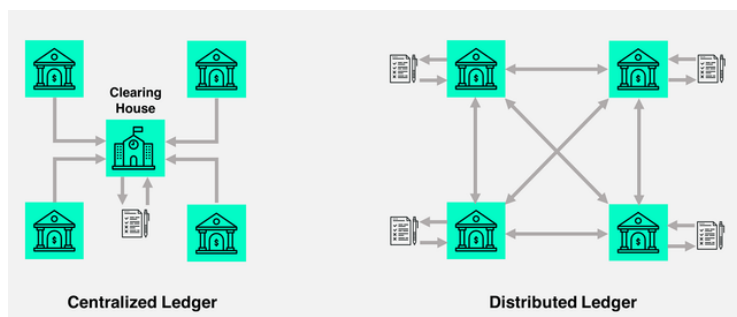
*Graf znázorňující množství bitcoinů v oběhu (modrá linie) na časové ose X. Červená linie představuje inflaci.*

Fiat peníze i Bitcoin jsou založené na naší víře a důvěře v ně. V případě fiat peněz věříme ve vládu, její centrální banku a další instituce, že ochrání naše prostředky a zajistí jejich platnost. V případě Bitcoinu věříme v jeho technologii. Jak je to možné? Jak může něco fungovat bez nějakého kontrolního úřadu, bez centrální banky, bez autority, která vše řídí a o všem rozhoduje? O tom si povíme více v další definici.

**Bitcoin je distribuovaná účetní kniha.**

Dobře, co to ale znamená? Představte si síť tisíců počítačů (aktuálně okolo 100 000 tzv. uzlů), které obsahují stejnou účetní knihu. V této knize jsou zaznamenány všechny transakce (od historicky první až po tu poslední před několika okamžiky). Tato kniha je tedy neustále aktualizována a to zároveň na celé

počítačové síti. Díky tomu jsme schopni sledovat stavy všech účtů, kterým říkáme adresy. Každý nový záznam se zapíše do této distribuované účetní knihy a je tak uložen na tisících míst najednou. Tato vlastnost zaručuje bezpečnost, na rozdíl od bankovních serverů, protože je technicky nemožné napadnout ve stejnou chvíli tisíce počítačů a některý z údajů změnit, např. připsat si nové bitcoiny do své peněženky nebo smazat některý z historických údajů.



*Porovnání mezi centralizovanou a distribuovanou účetní knihou. Centralizovaná účetní kniha sbírá údaje z více míst a ukládá je do centrálního depozitáře. Decentralizovaná účetní kniha ukládá všechny nové údaje najednou na více míst, která spolu vzájemně komunikují. Jednotlivé uzly ověřují mezi sebou, že mají správné údaje.*

Co je důležité říci, že tato účetní kniha je veřejná a digitální. Každý si může vyhledat jakoukoli transakci mezi dvěma peněženkami. Nikdo z nás by si ale asi nepřál, aby každý věděl, že se jedná o naši peněženku a věděl, jak se svými prostředky nakládáme. Proto nevidíme údaje o majiteli, ale pouze její adresu. Pod adresou peněženky si představme kód (šifru), podobný číslu bankovního účtu, které známe z internetového



bankovníctví.

Příklad transakce:

- Odchozí adresa: 1NyqNQW8H1QLhQhALcbGGDoPJP-FiVwEKiG
- Příchozí adresa: 12WR5ePaRYwXHNbkeZuLBho3kk5TPvf9ii
- Částka: 10 BTC
- Poplatek: 0.00050000 BTC

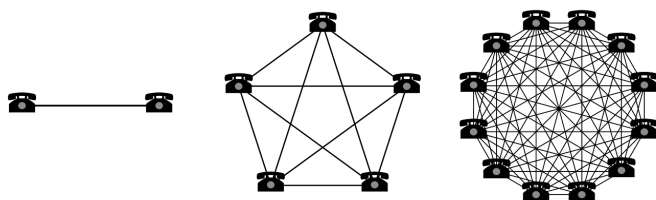
Složitý název adresy, který vypadá, jako by se nám kočka prohnala přes klávesnici, je kód automaticky vygenerovaný pomocí šifrovacího (kryptovacího) algoritmu. Díky tomu je prakticky nemožné, aby ve stejnou chvíli vznikly dvě peněženky se stejnou adresou a mohlo tak dojít k jejich záměně. Proto lze Bitcoin označit slovem kryptoměna, ale šifer a šifrování obsahuje celá technologie mnohem více a určitě se na ně v této knize ještě zaměříme.

Dobře, už víme, že Bitcoin je tedy síť počítačů obsahující veřejné záznamy všech plateb. Tím, že veškerá historie transakcí je veřejná a je uložena na tisících počítačů, není možné si nějaké bitcoiny vymyslet a přidat je jen tak do své peněženky. Jak ale bitcoiny vznikají, když je netiskne žádná centrální banka? Asi jste slyšeli o tom, že někdo bitcoiny těží. Protože se ale jedná o obsáhlejší téma, které je poměrně technické, podíváme se na něj zvlášť ve 3. otázce.

## Bitcoin je digitální zlato.

Toto přirovnání vychází z mnoha vlastností Bitcoinu, kterými nám zlato může připomínat. Už víme, že Bitcoinu je omezené množství, stejně jako zlata. Odhaduje se, že celkovou zásobu zlata (vytěženého i nevytěženého) si lze představit jako krychli o délce 20 metrů (= 8 000m<sup>3</sup>) a váze 170 000 tun, díky čemuž věříme, že má hodnotu, protože je **vzácné**. Technologie nám už dnes umožňují vytvořit nové syntetické zlato, které by bylo nerozpoznatelné všemi vlastnostmi od pravého zlata, ale samotný proces je tak ekonomicky nevýhodný, že postrádá smysl. Protože je tedy nabídka zlata omezená, dokud po něm bude existovat poptávka, bude si zlato držet svoji hodnotu.

Dalším důvodem, proč má zlato hodnotu, je, že je **užitečné**. Lidé ho už tisíce let používají jako uchovatele hodnoty. Výše hodnoty je úzce spojena s množstvím lidí, kteří ho jako uchovatele hodnoty používají. A to ne lineárně, ale exponenciálně. Čím více lidí bude takový nástroj používat, tím je pro nás hodnotnější.



*Síťový efekt (z angl. Network Effect)*

Kdybychom na Facebooku nenašli své přátele, nebudeme na něm trávit tolik času. Kdybychom se telefonem dovolali jen