provozně ekonomická

fakulta



**Katedra informačních technologií**

Kryptoměny

|  |
| --- |
| Zpracoval: Lukáš Holub  KS Klatovy ZS 2018/2019 |

**Obsah**

[1 Úvod 2](#_Toc531540240)

[2 Vymezení pojmů 2](#_Toc531540241)

[3 Kryptoměny 2](#_Toc531540242)

[4 Způsob nabytí kryptoměn a možnosti jejich držení 3](#_Toc531540243)

[5 Historie a současné použití kryptoměn 4](#_Toc531540244)

[6 Pád cen kryptoměn 4](#_Toc531540245)

[7 Budoucnost kryptoměn 5](#_Toc531540246)

[8 Závěr 6](#_Toc531540247)

# Úvod

Informační a komunikační technologie patří dlouhodobě k nejvýznamnějším hybným silám ovlivňujícím náš každodenní život. Mnoho služeb a oborů proměnilo ICT natolik dramaticky, že už si jejich fungování bez počítačové techniky ani nedovedeme představit. Jedním z těchto oborů je finanční sektor. Bankovnictví spoléhá na IT jako nikdy předtím. Tradiční trezory nahrazují servery s firewally a fyzické peníze zase jedničky a nuly. Přirozeným vývojem finančnictví dochází k postupné digitalizaci peněz. Jedním z pozitivních důsledků digitalizace peněz je nepochybně utažení pomyslných kohoutků šedé a černé ekonomiky. Na druhou stranu, elektronizace peněz ubírá na svobodě jedince, kdy ztrácíme volbu platbu bez identifikace příjemce. Cílem mojí práce je seznámení čtenáře s alternativní formou digitálních peněz. S fenoménem kryptoměn a hlavním představitelem těchto měn, Bitcoinem.

# Vymezení pojmů

**Kryptoměna** - je typ digitální měny či elektronických peněz, což je novodobý druh měny/peněz

**Bitcoin** – jedna z hlavních kryptoměn, co do objemu největší

**Blockchain** – speciální decentralizovaná databáze uchovávající neustále se rozšiřující počet záznamů. Blockchain je někdy označovaný za hlavní „účetní“ knihu kryptoměn.

**Digitalizace** – převod fyzických nebo analogových dat do digitálních

**Těžba kryptoměn** – činnost která se podílí a provozu kryptoměn výpočetní podporou. Tyto operace jsou honorovány z poplatků za pohyby digitálních měn.

**Virtuální peněženka** – on-line i off-line řešení pro uchování kryptoměn.

**Private key** – privátní klíč slouží k identifikaci uživatele virtuální peněženky

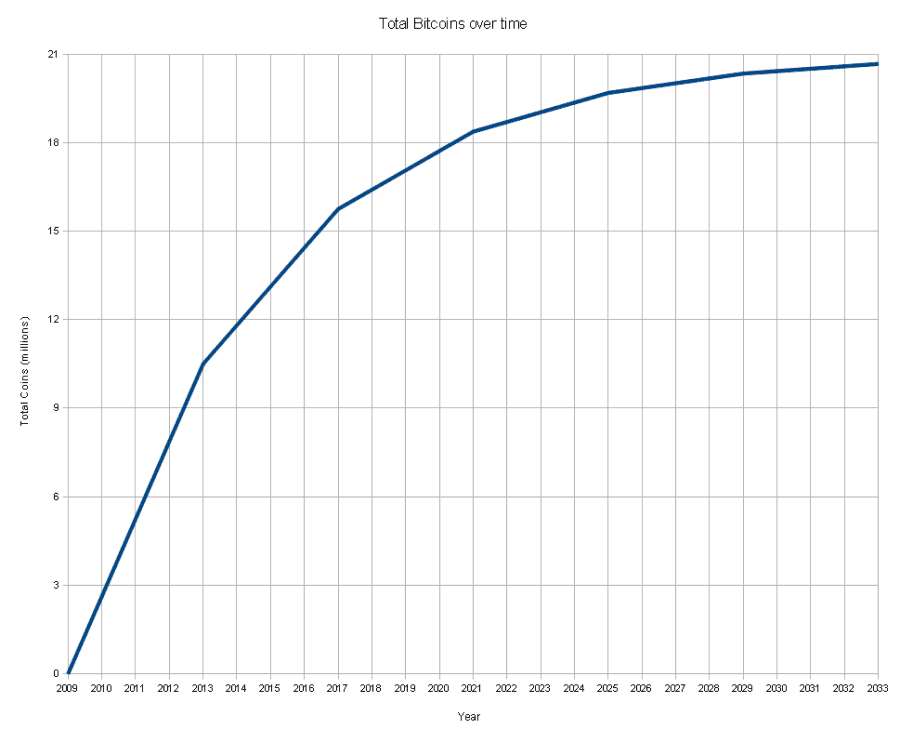
**Peer-to-peer** – označení pro takový typ spojení, kdy spolu komunikují klienti (počítače) napřímo, nikoliv prostřednictví serverů.

# Kryptoměny

Kryptoměny definujeme jako **digitální měny**, která nemají žádnou fyzickou podobu. Oproti běžným penězům na bankovním učtu jsou platby v kryptoměnách rychlé, levné a anonymní. Digitální měny typu Bitcoin využívají speciální druh decentralizované databáze který se nazývá Blockchain. Tento Blockchain si můžeme představit jako veřejnou účetní knihu, která je složená z transakcí a bloků. Transakce je nějaký uskutečněný převod (neboli data vložená uživateli). Blok (anglicky block) je naproti tomu poplatek za uskutečněnou transakci.

**Decentralizované kryptoměny jsou navrženy tak, aby fungovaly bez centrálních autority a centrální banky.** Měnu tak nemohou ovlivňovat ani vlády, ani jiné instituce. Další výhodou je transparentnost. Díky použití Blockchainu není možné kryptoměny falšovat, ani zatajit jednotlivé transakce (ale uživatele ano).

Celkový počet virtuálních mincí v rámci většiny měn je pevně stanovený. Nejznámější kryptoměna Bitcoin bude mít po úplném vytěžení 21 000 000 mincí. Uvolňování nových mincí se postupně zpomaluje a veškeré mince budou vytěženy až v roce 2140.



(zdroj: Bitcoin.it)

# Způsob nabytí kryptoměn a možnosti jejich držení

1. **Nákupem**

Nákup Bitcoinu nebo jiných kryptoměn je možný pomocí směnáren, burzy, nebo speciálních bankomatů. U nákupů mincí z bankomatu odpadá zdlouhavý proces registrace. Za zprostředkování nákupu, nebo prodeje se účtuje poplatek nejčastěji 5-10%. Od února 2018 se značně zpřísnilo používání kreditních karet pro nákup kryptoměn, proto je třeba před nákupem digitálních měn složit jistinu, nebo zálohu kterou bude transakce jištěna. Mezi nejznámější společnosti pro nákup kryptoměn patří Coinbase, LiteBit, nebo třeba BitMEX.

1. **Těžbou**

Vlastníci kryptoměn se mohou podílet na ověřování finančních transakcí v rámci Blockchain. V takovém případě o nich hovoříme jako o „těžařích“ takzvaných bloků. Těžař je slovo odvozené od anglického mining. Abychom mohli těžit některou z kryptoměn, potřebujeme alespoň trochu výkonnou grafickou kartu (např. AMD nebo Nvidia) a vhodný software. Tento software pro provedení dostatečného počtu početních operací odešle odměnu na předem definovanou adresu. Platí zde přímá úměra že vyšší výkon počítače zajišťuje vyšší efektivitu těžby.

1. **Z prodeje**

Některou z kryptoměn lze také získat směnou za zboží. Česká republika patří ke světovým lídrům v možnosti placení kryptoměnami. Asi nejznámějším obchodníkem u nás je společnost Alza.cz. Ale zboží na kryptoměny může získat i soukromá osoba například z prodeje zboží na portálu bazos.cz.

Pro úspěšné nabytí peněz je třeba **virtuální peněženka**. To je místo kde budete skladovat například vaše Bitcoiny. Virtuální peněženka může vygenerovat libovolné množství adres, na které můžete vaše digitální peníze přijímat. Součástí virtuální peněženky je privátní klíč (private key). Ten je propojený se všemi adresami a je proto důležité ho mít bezpěčně uložený. Bez privátního klíče nemůžete uskutečnovat žádné transakce! Zájemce o kryptoměny může využít i některou z on-line vituálních peněženek, které jsou zpravidla zdarma v případě registrace na tržišti, nebo burze. U této varianty je nutná zvýšená obezřetnost. Pokud poskytovatel on-line peněženky zkrachuje, zpronevěří peníze nebo bude okraden, šance na vrácení ztracených peněz je téměř nulová.

# Historie a současné použití kryptoměn

Bitcoin a další od něj odvozené kryptoměny začaly vznikat od roku 2008. Cílem projektu bylo zajištění okamžité, levné a pokud možno anonymní **mikro platby**. Jednalo se tedy spíše o konkurenci platebním kartám a šekům, než skutečným penězům. Za otce novodobých digitálních měn je považován vývojář vystupující pod pseudonymem Satoshi Nakamoto. Tento inovátor a velký fanoušek kryptografie jako první představil veřejnosti koncept pojmenovaný „**A Peer-to-Peer Electronic Cash System**“.

V prvopočátku nevyvolal Bitcoin téměř žádnou reakci veřejnosti a nebýt komunity nadšenců kryptologie, je pravděpodobné že by tato revoluční digitální měna upadla v zapomnění. Trvá 3 roky než Bitcoin vstoupí na veřejnou scénu. Stalo se tak v roce 2011, kdy byla uvedena první oficiální aplikace umožňující zpracování Bitcoinových transakcí. S přibývajícím počtem uživatelů začala vznikat i první místa kde bylo možné novou kryptoměnou platit. V roce 2011 stála jedna pizza přibližně 10 000 Bitcoinů, což je v dnešním kurzu přibližně 55 milionu dolarů.

Anonymitu plateb kterou kryptoměny zaručují bohužel využívá ve velké míře i černý trh pro své nelegální obchody. Na dnes již neexistujícím serveru Silk Road (hedvábná stezka) bylo možné za Bitcoiny směnit drogy, zbraně a jiné kontroverzní zboží.

Oficiální místa kde je možné provádět platby v kryptoměnách monitoruje nevýdělečná společnost Coinmap.org. **Podle informací této instituce existuje ve světě více než 15 tisíc míst kde lze platit Bitcoinem.** V ČR je to tak přibližně 300 míst. V obou případech je vykazován meziroční růst.

# Pád cen kryptoměn

Dosud nepoznanou dynamiku růstu cen zažily virtuální měny v druhé polovině roku 2017, a to zejména v jeho posledních měsících. V této době plnily stránky i seriózních medií skoro až neuvěřitelné příběhy lidí kteří pohádkově zbohatli. Bitcoin, který funguje jako lakmusový papírek pro ostatní měny, atakoval v prosinci 2017 hranici 20 000 USD. Vše se zdálo být v pořádku a hospodské řeči o politice vystřídala diskuze o budoucím vývoji kryptoměn. Novodobá zlatá horečka lákala nové a nové investory a riziko přehřátí na sebe nenechalo dlouho čekat. Bylo krátce před Vánoci a všechny významné měny bez výjimky se začínaly propadat. V té době lidé věřili že pokles souvisí s nákupem vánočních dárků a že se po Novém roce kryptoměny vrátí zpět na výsluní kam patří. Tak se skutečně stalo a začátkem ledna se začaly umazávat ztráty. Ani další korekci kurzu se digitální měny nevyhnuly a nastal prudký pád. Pro graf vývoje se vžil pojem „**Dead cat bounce**“, což se překládá jako efekt mrtvé kočky která spadne z výšky. I ta se po dopadu na zem odrazí a dočasně povyskočí.

****

(zdroj: Finanzen.net)

# Budoucnost kryptoměn

Pokud bych svůj odborný referát ukončil u předchozí kapitoly, ochudil bych čtenáře o to nejpodstatnější a to je budoucnost a vlastně i současnost kryptoměn. Jedním z českých expertů, který pravidelně publikuje své názory v této oblasti je Dominik Stoukal, který pracuje pro internetový deník E.15. Ten v listopadu napsal článek na téma Bitcoinu. V něm velmi široce vysvětluje nejen že Bitcoin potažmo kryptoměny ještě neřekl poslední slovo, ale naopak se domnívá, že se Bitcoinu nikdy nedařilo líp. Své tvrzení opírá o fakt, že současný kurz je o 500% vyšší než tomu bylo před 2 lety. Osobně bych rád rozvinul dvě roviny budoucího vývoje kryptoměn:

**Investiční příležitost –** V současné době se zdá, že se potenciál investic do kryptoměn dočasně omezil, nebo minimálně zpomalil. Na nepříznivém jevu se projevuje snaha vlád a bank omezit nekontrolovaný pohyb peněz i potencionální financování černého trhu, případně terorismu. Současně s tím klesá podíl investorů kteří jsou ochotni podstoupit riziko ztráty investovaných peněž, především po zkušenostech začátku roku 2018. Na druhou stranu, Bitcoin i jiné klíčové kryptoměny zažívají velmi stabilní období které se dá označit jako ideální pro pokrytí mikro plateb kvůli kterým vznikly.

**Technologický potenciál –** Blockchain díky svým vlastnostem nabízí téměř téměř nekonečné možnosti využití. Japonsko a Jižní Korea uvažují o Blockchainu jako o hlasovacím nástroji. V případě dostatečného množství uživatelů dokáže sdílená databáze výrazně omezit podvody, což je důvod, proč nadnárodní korporace vidí v technologii potenciál pro kontrolu digitálního vlastnictví.

# Závěr

Cílem mojí práce bylo představení kryptoměn a Bitcoinu jako alternativy k tradičnímu bankovnictví a principu jeho fungování. V první části jsem shrnul základ technologie digitálních měn a způsob jejich možného nabytí. Druhá část se věnuje historii kryptoměn a popisu současného stavu. V závěru, na základě zjištěných informací, sestavuji predikci vývoje z pohledu investic a technologií.

Pokud se kryptoměny neprosadí jako prostředek směny, věřím že Blockchain, tedy sdílená databáze, neupadne v zapomnění a bude se v budoucnu využívat jako účinný prostředek proti podvodům a padělání.

Seznam použitých zdrojů

Autor Stroukal, 2018. Bitcoin spadl, ve skutečnosti se mu ale nikdy nedařilo víc [online]. 25.11. [cit. 28.11.2018]. Dostupné z: https://kryptoportal.cz/nakup-kryptomen-pomoci-kreditnich-karet-omezen/. Path: Homepage; články; 28.11.2018.

Autor Karma, 2018. Nákup kryptoměn pomocí kreditních karet omezen [online]. 8.2. [cit. 28.11.2018]. Dostupné z: https://kryptoportal.cz/nakup-kryptomen-pomoci-kreditnich-karet-omezen/. Path: Homepage; články; 28.11.2018.

Autor Redakce Finanzen.net, 2018. Tabulka vývoje cen Bitcoinu [online]. 8.2. [cit. 28.11.2018]. Dostupné z: https://www.finanzen.net/devisen/bitcoin-euro/chart/. Path: Homepage; články; 28.11.2018.

Autor Tým TradeSmart, 2018. Co to je Odraz mrtvé kočky (Dead Cat Bounce)? Trading Terminologie! [online]. 27.10. [cit. 28.11.2018]. Dostupné z: https://www.tradesmart.cz/co-to-je-odraz-mrtve-kocky-dead-cat-bounce-trading-terminologie/ Path: Homepage; články; 28.11.2018.