VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

KRYPTOMĚNY A MOŽNOSTI JEJICH OBCHODOVÁNÍ
CRYPTOCURRENCIES AND THEIR TRADING OPTIONS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

Lubomír Kubík

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Jan Luhan, Ph.D., MSc

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Lubomír Kubík**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Jan Luhan, Ph.D., MSc**
Akademický rok:	2018/19

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Kryptoměny a možnosti jejich obchodování

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Charakterizovat základní fungování kryptoměn a trhu s virtuálními měnami. Analyzovat možnosti získávání kryptoměn, jejich těžby a nákupu prostřednictvím bankomatů a online prostředků. Porovnat služby pro získávání a obchodování s kryptoměnami se zaměřením na výhodnost pro specifického zájemce.

Základní literární prameny:

ANTONOPOULOS, A. M. Mastering Bitcoin: Programming the Open Blockchain. 2nd ed. Sebastopol: O'Reilly, 2017. 416 p. ISBN 978-1-491-95438-6.

DRESCHER, D. Blockchain Basics: A Non-technical Introduction in 25 Steps. 1st ed. Berkeley: Apress, 2017. 276 p. ISBN 978-1-4842-2603-2.

NARAYANAN, A. et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. 1st ed. Princeton University Press, 2016. 336 p. ISBN 978-0-691-17169-2.

STROUKAL, D. a J. SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2. rozš. vyd. Praha: Grada Publishing, 2018. 200 s. ISBN 978-80-271-0742-1.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Bakalářská práce se věnuje vývoji a začátkům kryptoměn v čele s nejrozšířenější kryptoměnou Bitcoin. Popisuje principy fungování blockchainu a decentralizovaných měn. Zaměřuje se také na srovnání jednotlivých kryptoměn, které jsou porovnávány z několika hledisek, jako je například jejich vznik, princip fungování a hodnota. Následně jsou analyzovány a porovnávány možnosti získání a obchodování kryptoměny. Tyto možnosti zahrnují těžbu, nákup pomocí směnáren a obchodování na burzách. Jednotlivá řešení jsou porovnávána s důrazem na výhodnost pro konkrétního uživatele.

Klíčová slova

kryptoměny, virtuální měny, bitcoin, směnárny, obchodování

Abstract

The bachelor thesis focuses on the development and formation of cryptocurrencies especially the most common cryptocurrency Bitcoin. It describes the principles of blockchain and decentralized currencies. It focuses on the comparison of individual kinds of cryptocurrencies which are compared from several points of view, such as their origin, the principle of their functioning and value. Furthermore the possibilities of acquiring and trading cryptocurrencies are analyzed and compared. These options include extraction, purchase through digital currency exchange and exchange trading. Individual solutions are compared in terms of their convenience for a particular user.

Keywords

cryptocurrency, virtual currency, bitcoin, cryptocurrency exchange, trading

Bibliografická citace

KUBÍK, Lubomír. Kryptoměny a možnosti jejich obchodování [online]. Brno, 2019 [cit. 2019-05-06]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119815. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Jan Luhan.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 7. května 2019

……

podpis autora

Poděkování

Rád bych poděkoval vedoucímu této bakalářské práce Ing. Janu Luhanovi Ph.D., MSc, za poskytnutí cenných rad při tvorbě této práce. Velké díky patří také mým kamarádům, kterými jsou Ing. Marian Kopeček a Martin Miksa, za rady a tipy z oblasti kryptoměn.

Obsah

Úvod

Kryptoměny jsou v dnešní době široce medializované téma. Velký zájem veřejnosti si získaly především díky odvěké touze po finančním bohatství, kterého lze na první pohled nákupem a včasným prodejem těchto virtuálních měn dosáhnout. Největší mediální zájem vyvolal příběh o ztraceném harddisku, na kterém měl nešťastný vlastník uloženo mnoho jednotek některé z úspěšných kryptoměn, které získaly během několika let několikanásobnou hodnotu. Také lze zmínit reálný příběh o počátcích Bitcoinu, kdy si jeden z jeho fanoušků pořídil nejdražší pizzu na světě.

Všechen tento zájem, popularita a někdy také nízká znalost problematiky vede často širokou veřejnost ke spekulacím, zda je tento druh měny bezpečný, jaké jsou jeho možnosti využití a jaké typy kryptoměn kromě nejznámějšího Bitcoinu mohou získat nebo vytěžit.

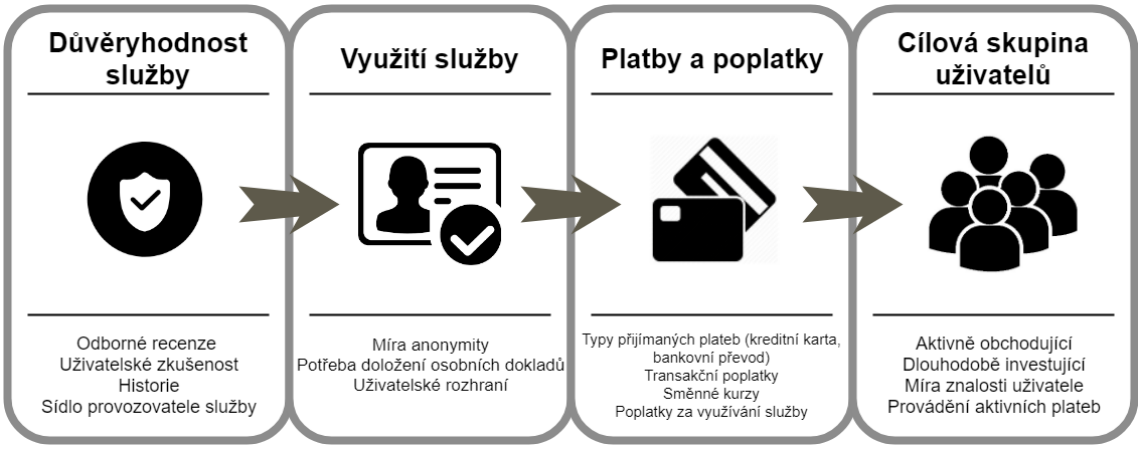
Původně vznikaly jako programátorský koncept neovlivnitelné, decentralizované měny, která není závislá na žádném centrálním řízení. Tento projekt, který byl původně určený spíše pro nadšence do IT technologií a měl otestovat schopnosti existence tohoto konceptu nakonec vyústil až k vytvoření nového typu elektronických peněz, o které se zajímá nejen široká veřejnost, ale i bankovní instituce a státy samotné.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem práce je přiblížit fungování kryptoměn a kryptoměnových sítí. Představit způsob a důvod vzniku decentralizovaných měn, ukázat technologické rozdíly distribuovaných a centralizovaných sítí, jejich klady a zápory s vysvětlením základního technologického fungování transakcí v síti Bitcoin s příkladem uživatelského využití. Uvést praktické příklady, kde se již dnes kryptoměny aktivně používají a k jakým účelům je lze využívat. Popsat principy získání kryptoměny jako je těžba nebo směna za národní měnu a vyhodnotit vhodnou metodu nákupu. Následně provést analýzu jednotlivých kryptoměn a způsobů jejich nákupu. Konkrétní způsoby porovnat a zjistit jejich výhodnost pro konkrétní typy uživatelů.

Při zpracování základních principů kryptoměn byla využita technická analýza jednotlivých řešení. Pro zpracování informací pro analytickou a praktickou část práce bylo využito analýzy uživatelských potřeb a technické analýzy.

Postup zpracování teoretické části práce spočíval ve zpracování syntézy relevantních informací o fungování distribuovaných počítačových sítí a jejich využití pro decentralizované měny. V analytické části byly zpracovány informace ke konkrétním kryptoměnám a bylo poukázáno na jejich historii, způsoby využití nebo rozšířenost. Praktická část se věnovala řešení samotného nákupu kryptoměny. Byly provedeny analýzy společností z pohledu tradice, bezpečnosti, výhodnosti, uživatelské přívětivosti a nabízených služeb. Důraz byl také kladen na to, aby byly dostupné pro případné zájemce z České republiky.



Obrázek 1 - Analyzované oblasti služeb praktické části práce (Vlastní zpracování)

1 TEORETICKÁ ČÁST

1.1 Národní měny, Bitcoin a počátky decentralizace

Fungování blockchainu a většiny nejrozšířenějších kryptoměn je založeno, na rozdíl od klasických bankovních a platebních systémů, na decentralizované platformě. Místo centrální autority, kterou je v případě standartních měn národní banka, je systém založen na důvěře vznikající při samotné interakci všech účastníků blockchain systému. Samotný Bitcoin je technologií, ale většina lidí si jej představí spíše jako peníze, základní jazyk pro výměnu hodnot mezi lidmi. (1)

Samotné kryptoměny jsou vynálezem kombinací různých oborů jako je kryptografie, počítačové sítě, open-source software, nebo třeba peněžní teorie. V širším měřítku zkoumání kryptoměn lze využít poznatky sociálních i humanitních věd a to především při odhadu budoucí hodnoty.

Ve světě bez národních měn by v dnešní době stále existoval směnný obchod založený na potřebách dvou lidí, kteří mezi sebou smění zboží za zboží, případně za službu. Tato metoda obchodování sebou však nesla i řadu nedostatků. Jedním z nich je například potřeba takového zboží, které člověk touží vlastnit, protistrana jej nabízí, ale není ochotna vyměnit jej za nabízený produkt nebo službu. V takovém případě je nutné vyhledat třetí osobu, která nabídne jiné zboží za které již bude možné první směnu uskutečnit. Právě podobné situace umožnily vznik univerzálních prostředků k platbě. Nejdříve pomocí žádoucích a trvanlivých předmětů jako jsou mušle a plátna, později se však přešlo na drahé kovy, které předcházely vzniku mincí a bankovek. (2)

Aby byla každá měna životaschopná, ať už jde o decentralizovanou kryptoměnu vydanou počítačovým algoritmem nebo tradiční fiat měnu vydanou vládou, musí získat důvěru lidí, kteří ji chtějí nebo jsou nuceni používat. Cílem kryptoměn je nabídnout alternativní model této důvěry. Poskytují systém plateb, v němž příjemce nemusí důvěřovat institucím třetích stran, například bankám nebo vládám, aby zajistil, že plátce může poskytnout sjednané finanční prostředky. Kryptoměny se snaží přinášet důvěru nedotknutelnosti a decentralizovanosti počítačového programu, jehož zdrojový kód je veřejně dostupný pod licencí open-source a kdokoliv může ověřit jeho fungování. Na stejných principech staví

také samotný blockchain. Ten si lze představit jako účetní knihu, která obsahuje všechny provedené transakce za celou historii fungování, do které může kdokoliv nahlédnout.

V roce 2011 si Bitcoinu všimli i přední ekonomové. Nahlíželi na něj většinou velmi kriticky. Bylo mu vytýkáno, že není ničím krytý, podivovali se nad jeho plánovanou emitací a byl považován za podvodnou hru s cílem vylákat co nejvíce peněz od lidí. Již o dva roky později se začalo o Bitcoinu mluvit i v médiích a široká veřejnost se chtěla o této nové technologii dozvědět více. Celý svět se navíc stále ještě vyrovnával s ekonomickou krizí a například v Řecku přetrvávala dluhová krize. Z aktuálnějších událostí lze zmínit měnovou krizi v Argentině. Selhání ekonomiky státu potkalo také Zimbabwe, kde reformy prezidenta Mugabeho způsobily v roce 2008 hyperinflaci. Tato situace měla za následek prudké zvýšení nezaměstnanosti, nedostatek potravin, vznik chaosu a bídy. Lidé si uvědomili křehkost národních a nadnárodních peněz a viděli jejich rizika v praxi. (3)

Ze zkušeností některých těchto míst se dozvídáme, že hlavním problémem nejsou nezodpovědná politická rozhodnutí centrálních bank v oblasti tisku peněz. Základ problému pramení spíše z hluboce zakořeněného zhroucení důvěry mezi lidmi, kteří měnu používají a nemají důvěru v autoritu, která ji vydává. Vzhledem k tomu, že tyto měnové orgány jsou obvykle řízeny vládou, odráží se tak ona nedůvěra společnosti právě k ní. Kryptoměna, která zakládá svoji důvěryhodnost peněžní směny na matematickém algoritmu je tak často férovou alternativou, které jsou miliony lidí ochotny důvěřovat.

Pokud občané nedůvěřují vládě, která by měla zastupovat jejich zájmy, nebudou důvěřovat měnovému systému, kolem kterého je jejich ekonomika organizována. V případě možnosti raději smění tuto měnu za takovou, které důvěřují. To samé lze pozorovat i v případě kryptoměn, kde chování komunity, tvůrců a technologická vyspělost rozhodují o tom, zda bude zájemce ochoten kryptoměnu nakoupit nebo směnit. (3)

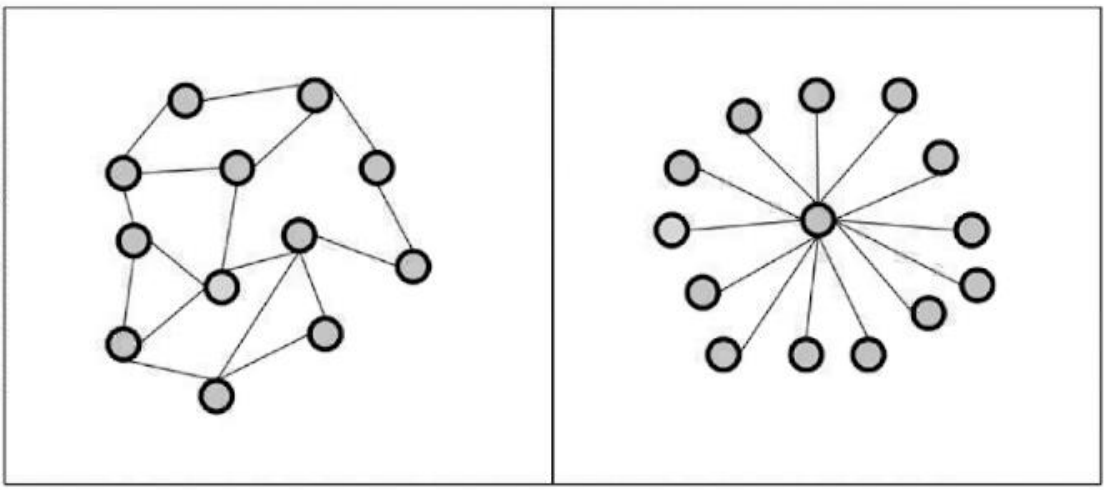
V dnešní době existuje více než 2000 kryptoměn. Vzhledem k dostupnosti zdrojových kódů a nenáročnosti na technologické vybavení autora si tak může vlastní decentralizovanou měnu vytvořit každý, kdo má přístup k internetu a základní znalosti programování. V silné konkurenci zavedených kryptoměn je ovšem velmi obtížné získat uživatele na svoji stranu, nabídnout jim přidanou hodnotu a přesvědčit je, aby dali šanci nové kryptoměně. Z tohoto důvodu vládne dnešnímu světu virtuálních měn jen několik

desítek měn, které dokázaly přinést inovaci v technologii, pojetí nebo dokázaly skloubit marketingovou kampaň a poutavý příběh vzniku a získali tak na tomto trhu významný podíl, jméno a silnou komunitu.

1.2 Centralizované a decentralizované platformy

Běžné počítačové i mobilní programy fungují na principu centralizovaného systému. I samotná kosmologická teorie velkého třesku je postavená na tom, že třesk začal z „centralizovaného“ bodu, ze kterého se vesmír začal rozpínat. Následně vznikly i takové galaxie, které mají decentralizované rozložení hvězdných soustav. (4)

Na obrázku níže lze vidět porovnání distribuované a centralizované platformy. Šedé kruhy reprezentují uzly, které jsou propojeny přímkami. Důležité je uvědomit si, že v případě decentralizovaného systému jsou uzly propojeny bez existence centrálního prvku, který by je vzájemně spojoval. Oproti tomu v centralizovaném spojení jsou všechny prvky propojeny přes jeden centrální uzel. (4)



Obrázek 2 - Porovnání distribuovaného a centralizovaného modelu systémové architektury (Zdroj: 4)

1.2.1 Výhody a nevýhody distribuovaného systému

Mezi hlavní výhody distribuovaného modelu patří:

- Větší výpočetní síla
- Redukce nákladů na provoz
- Vyšší spolehlivost
- Redundantní propojení uzlů
- Možnost jednoduchého rozšíření (4)

Větší výpočetní síla distribuovaného systému je dosažena spojením výpočetní síly všech připojených uzlů. Aby byl centralizovaný model podobně výkonný, centrální prvek by musel být stejně výkonný jako součet výpočetní síly všech decentralizovaných prvků.

S tím souvisí také nižší náklady. Ceny běžných osobních počítačů jsou mnohem nižší, než jeden výkonný „superpočítač“ schopný obstarat provoz centralizované platformy. (4)

Vyšší spolehlivost je dosažena redundantním propojením a zastupitelností jednotlivých uzlů. V případě selhání uzlu převezme jeho roli uzel vedlejší. Distribuované systémy tedy na rozdíl od centralizovaných, nemají jediný prvek, na jehož provozu závisí fungování celé sítě. (4)

Schopnost rozšíření sítě závisí na možnostech agregace výpočetní síly všech uzlů. Při rozšíření sítě o další uzel je k dispozici ihned jeho výpočetní síla, která je započítána a může být rovnou využita v celé síti tak, aby byly uzly zatíženy rovnoměrně. (4)

Distribuovaný model má ale také několik nevýhod. Mezi ty hlavní patří:

- Složitá koordinace
- Složitá komunikace
- Závislost na síťové infrastruktuře
- Nároky na vyšší komplexnost softwaru
- Bezpečnostní rizika (4)

Koordinace sítě a celé platformy je závislá na jednotlivých uživatelích, tedy vlastnících uzlů. Koordinace jednotlivých uživatelů a udržení kompatibility sítě sebou nese náročnost jak na samotné uživatele, kteří musejí udržovat aktuální vývojovou verzi např. provozovaného softwaru, tak také na výpočetní výkon uzlu, který nemůže být v plné míře využitý k původním účelům. I náklady na samotnou komunikaci mezi uzly v síti jsou vyšší. (4)

Koordinace vyžaduje také komunikaci. Komunikovat mezi sebou musí jak samotná zařízení v síti, tak v případě řešení problémů i uživatelé uzlů. Síťová komunikace vyžaduje často speciální protokoly, které umožňují pracovat v distribuovaných sítích. Součástí těchto protokolů jsou zprávy, které musí uzly přijímat, posílat a zpracovávat. To ve finále opět stojí náklady na vývoj a vyžaduje vyšší náročnost na výpočetní výkon. (4)

Každý druh komunikace vyžaduje přenosové médium, pomocí kterého bude komunikace probíhat. To je odpovědné za přenos informací mezi komunikačními uzly. Tyto informace je nutné přenášet pomocí sítě. Kvalita síťové infrastruktury vysoce ovlivňuje výkon celé distribuované sítě a silně tak ovlivňuje rychlost i spolehlivost celého modelu. (4)

Řešení výpočetních problémů zahrnuje psaní programů pro danou síť. Díky zmíněným nevýhodám musí programy fungující v distribuovaných sítích zvládnout také koordinaci, komunikaci a rovnoměrné rozložení výkonu sítě. Jejich tvorba je tedy složitější a časově náročnější. (4)

Komunikace prostřednictvím síťě znamená odesílání a sdílení dat, která jsou důležitá k výpočetnímu úkonu. Zasílání informací prostřednictvím sítě však zahrnuje bezpečnostní hrozby, protože nedůvěryhodné subjekty mohou zneužít síť k neautorizovanému přístupu a využití neoprávněných informací. Jakýkoli distribuovaný systém proto musí řešit otázky týkající se bezpečnosti. Čím méně je omezen přístup k síti přes kterou distribuované uzly komunikují, tím vyšší jsou bezpečnostní rizika tohoto systému. (4)

1.2.2 Distribuované peer-to-peer systémy

Peer-to-peer sítě jsou speciálním druhem distribuovaného systému. Skládají se z jednotlivých zařízení (uzlů), které nabízejí své výpočetní zdroje ostatním členům sítě bez existence centrálního prvku. Mezi sdílené zdroje může patřit například výpočetní výkon procesoru, paměť nebo třeba síťové připojení. Všechny uzly v síti jsou si rovny, mají stejná práva i role. (4)

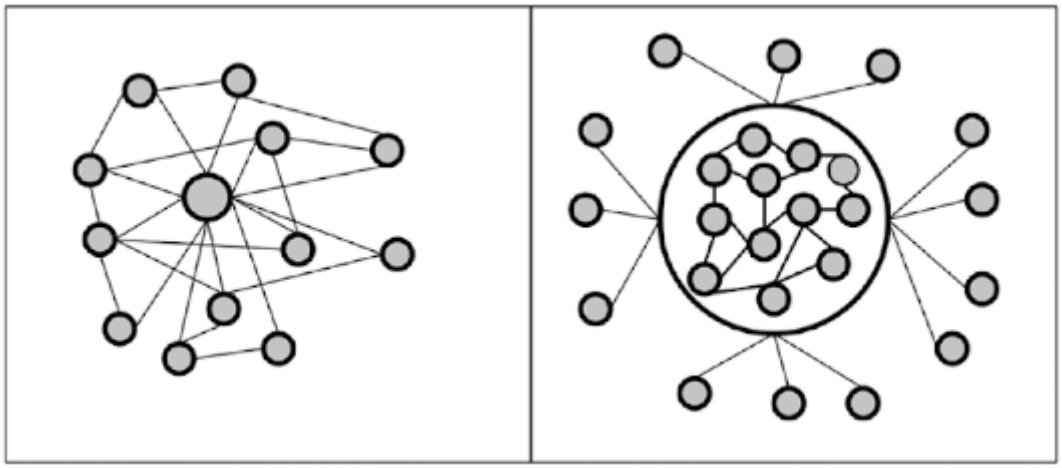
Peer-to-peer systémy mají různé možnosti využití. Mezi nejznámější patří sdílení dat, tedy distribuce obsahu (často ilegálního). Například ale také šíření aktualizací operačního systému Windows probíhá částečně tímto principem a uživatel si často stahuje nový

bezpečností balíček z počítače jiného uživatele, aniž by o tom měly obě strany tušení. Cílem tohoto řešení je snížení zátěže pro servery Microsoftu a tím také rychlejší distribuce aktualizací. Stejného řešení je využito u některých verzí Linuxu. (4)

Dalším využitím je také komunikační protokol BitTorrent, který je za pomocí klienta schopen sdílet a přijímat obsah jako jsou filmy, hudba, počítačové hry apod. od ostatních uživatelů tohoto protokolu. (4)

1.2.3 Kombinace distribuovaných a centralizovaných systémů

Je potřebné zmínit také existující kombinace centralizovaných a distribuovaných systémů. Existují dvě základní cesty jak zkombinovat tyto dvě odlišné technologie. Jejich porozumění je velmi důležité k pochopení samotného blockchainu.



Obrázek 3 - Kombinace distribuovaných a centralizovaných sítí (Zdroj: 4)

Na obrázku vlevo je zobrazena architektura, která vytváří centrální komponentu v distribuovaném systému. Na první pohled vytváří distribuovaný systém, nicméně všechny uzly jsou připojeny napřímo k centrálnímu prvku uprostřed. Může tak vzniknout dojem distribuovaného systému. Ve skutečnosti jde ovšem o systém centralizovaný.

Obrázek vpravo ukazuje odlišný přístup. Na první pohled vypadá jako systém centralizovaný, jelikož jsou všechny okrajové uzly připojeny do hlavního kruhu uprostřed. Nicméně kruh uprostřed se skládá z vlastního vnitřního distribuovaného systému. Uzly na vnější straně velkého kruhu tak ani nemusejí být schopny rozpoznat, že jsou připojeny k distribuovanému systému, který funguje uvnitř kruhu.

Tyto dva systémy mají společné to, že je velmi složité poznat nebo pojmenovat o jaký typ systému se jedná. Důležité je poukázat na jejich složení ze dvou typů.

Rozpoznání centrální nebo distribuované platformy uvnitř nemusí být snadné. V případě, kdy je obtížné rozlišit typ sítě, je vhodné se zaměřit na jednotlivé komponenty jako jsou databáze, registry uživatelů, přihlašovací komponenty, nebo třeba tlačítko pro vypnutí uzlu. Pokud existuje taková komponenta, která dokáže celý systém v případě výpadku nebo smazání vyřadit z provozu, nejedná se o distribuovaný systém. (4)

Obrázek 4 - Mapa centralizovaných internetových služeb ukazuje, jak velký dopad může mít výpadek jednoho z těchto "velikánů" (Zdroj: www.internet-map.net)

Obrázek výše zobrazuje největší světové internetové služby. Na jejich fungování jsou dále závislé miliony dalších webů, které využívají některé z jejich služeb (Google Analytics, Youtube, Facebook plugin,..). Vzájemná propojenost a centralizovanost těchto systémů je závislá především na kvalitě zabezpečení jednotlivých poskytovatelů. V extrémní situaci je ale teoreticky možné, že např. hackerský útok může způsobit výpadek jedné i více služeb společnosti právě díky centralizované platformě. Příkladem může být výpadek sítě Facebook, který v dubnu 2019 postihl evropské i asijské uživatele této sociální sítě včetně jeho aplikací WhatsApp a Instagram.

1.3 Blockchain a síť Bitcoin

Každý uživatel má možnost připojit se do blockchainové sítě a podílet se na jejím fungování. Jako příklad poslouží nejrozšířenější síť Bitcoin.

Pro připojení do sítě musí uživatel použít klienta nebo webovou aplikaci. Jejich základní rozdělení je:

- **Úplný klient**
  Klient ve formě aplikace, který uchovává kompletní historii bitcoinových transakcí. Uživatel si musí stáhnout kompletní záznamy blockchainu od jeho počátku. To je vzhledem k jeho stále narůstající velikosti velmi náročné na kapacitu uložiště. V dubnu 2019 byla velikost blockchainu 210 GB. Uživatel zde může spravovat své peněženky a provádět libovolné bitcoinové transakce. Velká část těchto klientů také často umožňuje provádět samotnou těžbu, která je ovšem, jak bude zobrazeno v analytické části práce, již delší dobu ekonomicky velmi nevýhodná.

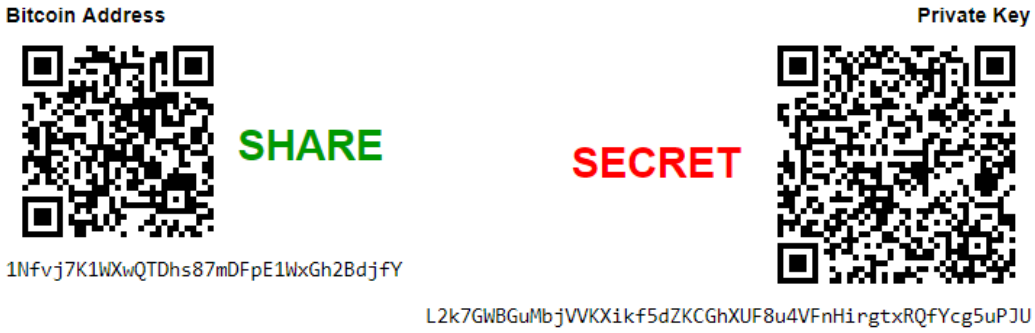
- **Odlehčený klient (Lite)**
  Odlehčený klient uchovává peněženky uživatele ale historické transakce a výpisy z blockchainu ověřuje pomocí serverů třetích stran, na kterých je stažený kompletní soubor. Tento klient je tedy mnohem méně náročný na HW stanice uživatele na úkor důvěry třetí straně.

- **Webový klient**
  Je dostupný pomocí webového prohlížeče. Peněženky uživatele jsou ukládány na server poskytovatele služeb. Web je dostupný odkudkoliv, ale uživatel často nemá plný přístup ke své peněžence. Většina služeb praktické části práce je založena právě na webovém klientu.

- **Mobilní klient**
  Klient ve formě aplikace pro chytré mobilní telefony. Většinou funguje na principu odlehčeného nebo webového klienta. Většina webových služeb nabízí i vlastní mobilní aplikaci. Mnoho služeb z praktické části poskytuje uživateli také přístup z mobilního telefonu. (4)

V těchto aplikacích si uživatel vygeneruje nebo získá vždy svoji Bitcoinovou adresu, která je většinou sled znaků Pay-to-PubkeyHashe a v některých aplikací také privátní klíč, který opravňuje uživatele k provádění transakcí s danou bitcoinovou adresou. Privátní klíč tedy nikdy nesmí získat nikdo jiný než sám majitel adresy. Privátní adresu

lze přirovnat k údajům jako je heslo PayPal účtu nebo heslo do internetového bankovnictví. (1)



Obrázek 5 - Vygenerovaná Bitcoin adresa a privátní klíč (Zdroj: www.bitaddress.org)

1.3.1 Provádění transakcí v bitcoinové síti

Jak již bylo zmíněno, bitcoinové transakce a celá bitcoinová síť jsou založeny na důvěře, která vzniká automaticky při interakci účastníků v systému, kteří v ní provádějí libovolný úkon. Uvedený příklad bude popisovat několik uživatelských scénářů a jejich interakci v bitcoinové síti.

Uživatel má vlastní Bitcoin peněženku, ve které má 0.10 BTC. Získat je mohl některým ze způsobů uvedených v praktické části práce. Tento uživatel si nyní chce zakoupit nová sluchátka v obchodě s elektronikou, kde jsou Bitcoiny přijímány jako platidlo (např. kamenná pobočka Alza.cz). Cena sluchátek je uvedena v českých korunách a stojí 1799,- Kč. Platební systém, který podporuje platbu v Bitcoinech, převede tuto částku dle kurzu daného obchodníkem. V Bitcoinech se jedná o částku 0.015 BTC. Platební systém vygeneruje QR kód, který lze skenovat pomocí aplikace mobilní peněženky v chytrém telefonu. Jeho definice je vytvářena dle BIP0021 (Bitcoin Improvement Proposals), což jsou vylepšení schvalovaná a implementovaná komunitou Bitcoin uživatelů a fanoušků na webu github.com.

Obrázek 6 - Příklad QR kódu pro provedení Bitcoin transakce (Vlastní zpracování)

Tento QR kód obsahuje po naskenování následující:

„bitcoin:1CkVXswCRnEtbwxzzFTQMr94Lobv9TDdV5?amount=0.015&label=Objednávka 0125499 na Alza OC CAMPUS“

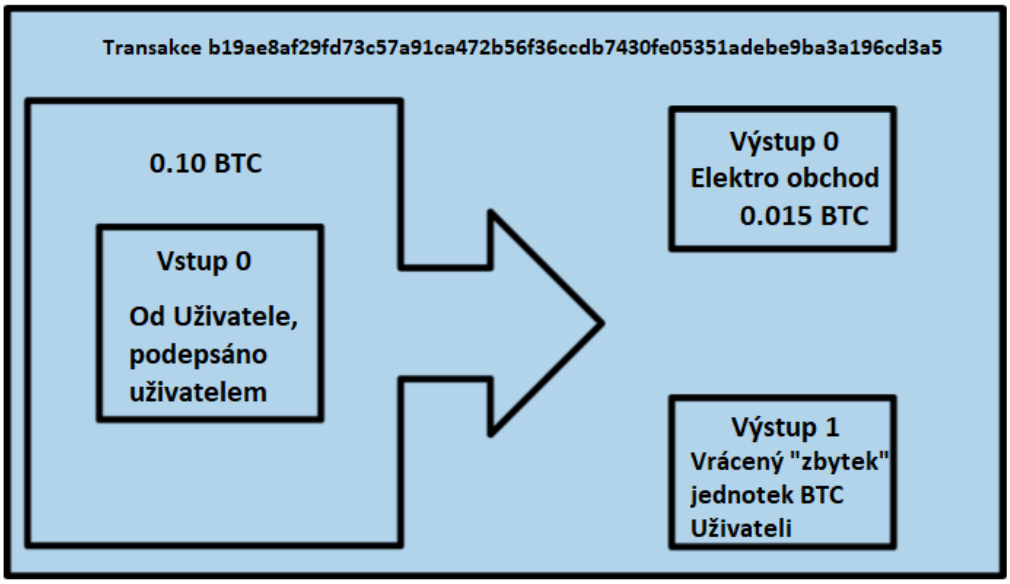
- **bitcoin:** - Bitcoinová adresa příjemce dané částky (prodejna elektra)
- **amount:** - Odesílaná částka v BTC
- **label:** - libovolný text k dané transakci. (např. číslo objednávky v systému prodejce). Tento prvek je nepovinný a nemá žádný vliv na provedení transakce.

Po naskenování QR kódu se předvyplní platba v aplikaci uživatele a ten ji následně odešle ve prospěch prodejce. Prodejce tuto platbu do několika sekund zaregistruje a vydá uživateli zboží.

Transakce v sítí říká, že majitel určitého množství Bitcoinů převedl jejich část jinému uživateli. Ten tyto přijaté Bitcoiny může utratit vytvořením nové transakce, ke které přiřadí nového vlastníka. Takto postupuje řetěz transakcí dále a lze jej přirovnat principu účetní knihy. Každá transakce obsahuje vstupy a výstupy. Vstupy jsou transakce vzniklé vydáním prostředků z jednoho nebo více účtů (adres). Výstupy jsou příjmy jiného bitcoinového účtu nebo účtů. Součty vstupů a výstupů se přes ně nerovnají díky existenci transakčních poplatků, které jsou malé částky z platby, náležící těžaři.

Transakce přesouvá hodnotu vstupů do výstupů. Původ vstupu je vždy z některého předchozích výstupu (předešlé transakce). Výstup z transakce přiřadí nového vlastníka

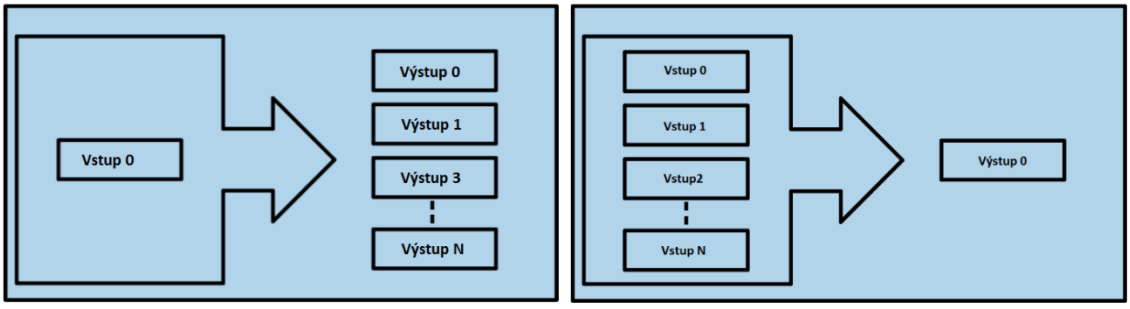
určité hodnoty. Ten se tak stane novým majitelem a k manipulaci s danou částkou je nutné použít podpis (privátní klíč) pro její budoucí uvolnění. (1)



Obrázek 7 - Příklad provedení transakce platby s vratnou částkou (Zdroj: Vlastní zpracování dle: 1)

Daný uživatel nakoupil Bitcoiny například pomocí automatu a jeho vlastněná částka činí 0.10 BTC. Tato částka vznikla jako výstup transakce poskytovatele bankomatu a byla zamčena klíčem uživatele. Jeho nová transakce při nákupu elektra se odkazuje na tuto předchozí transakci jako vstup a vytváří nový výstup (0.015 BTC) pro zaplacení částky za sluchátka a následné obdržení neutracených jednotek Bitcoinu zpět.

Klíč uživatele obsahuje podpis, který tyto prostředky odemkne, bitcoinové síti poskytne důkaz že je jejich vlastníkem a výstup pro elektro zatížil požadavkem, aby bylo právě dané elektro schopno podepsat budoucí požadavek na novou transakci s touto částkou. Tato situace je zobrazena na obrázku výše.



Obrázek 8 - Transakce slučující (vpravo), rozdělující prostředky (vlevo) (Zdroj: Vlastní zpracování dle:1)

V Bitcoinové síti mohou také probíhat transakce z několika sloučených vstupů do jednoho výstupu (transakce která slučuje prostředky) nebo transakce z jedno vstupu do několika výstupů (transakce rozdělující prostředky). (1)

1.3.2 Fungování transakcí v bitcoinové síti

Z uživatelského hlediska stačí pro placení kryptoměnou, v tomto případě Bitcoinem, ovládání jednoduchého uživatelského rozhraní aplikace.

Nyní je ale třeba prozkoumat samotné fungování aplikací a sítě, které tyto transakce zpracovávají. Aplikace uživatele musí najít vstupy, ze kterých lze započíst transakci a uhradit částku obchodníkovi. Většina „lite“ aplikací udržuje pouze malou databázi výstupů předchozích transakcí, které jsou zamčeny klíčem uživatele. Může jich být velké množství a aplikace by měla vědět s jakými prostředky může pracovat. Aplikace tak již ví o transakčním výstupu, který získal uživatel nákupem Bitcoinu pomocí automatu. Pokud by tento výstup nezaregistrovala, může učinit dotaz do bitcoinové sítě a zjistit všechny výstupy, ke kterým se váže klíč uživatele. V rozhraní aplikace tak lze vidět konečný zůstatek na dané Bitcoinové adrese. (1)

V našem případě tedy aplikace zjistila jediný výstup z předchozí transakce (0.1 BTC). Vytvoří transakci, která uhradí částku za sluchátka (0.015 BTC) a zároveň do této transakce zahrne také vrácení přebytečných peněž zpět uživateli (0.085BTC). Rozdělí tak prostředky na dvě platby. Aby byla transakce zpracována, přidá aplikace transakční poplatek. Tento poplatek není zobrazen v transakci. Je vytvořen z rozdílů součtů vstupů a výstupů. Aplikace tedy vytvoří „vratku“ pouze 0.0845 BTC. Odměna za vytěžení tak bude 0.0005 BTC. (1)

Transakce je odeslána a rozšířena do bitcoinové sítě. Součástí samotného blockchainu se stane ale až po ověření a vložení do bloku pomocí procesu těžby. Transakce uživatele se stane součástí bloku, pro jehož vytvoření je nutné velké množství výpočtů. Tyto výpočty jsou součástí těžby, která funguje jako ověřovací prvek a také vytváří každým vytěženým blokem nové Bitcoiny. Množství těchto nových Bitcoinů je pevně dané a snižuje se v čase. Férovost je zajištěna tím, že pro dané potvrzení bloku je vyžadováno velké množství výpočetní síly. Samotné těžbě se dále věnuje analytická část práce. (1)

1.4 Možnosti využití kryptoměn

Jaké možnosti otvírá uživateli nákup kryptoměn? Na tuto otázku se jistě mnoho uživatelů zajímajících se o virtuální měny zeptá. V počátcích svého konceptu měly fungovat jako pokus o vytvoření měny bez centrální autority. Před několika lety byl středem zájmu technologických nadšenců. Zájem ze strany velkých společností i bank byl zanedbatelný. Byli to až samotní uživatelé a vlastníci většinou Bitcoinu, kteří dokázali přesvědčit některé firmy, že akceptací tohoto typu platidla se jim otevře cesta k novým zákazníkům, kteří chtějí tuto technologii používat. Využití kryptoměn je ale mnohem širší.

Základní možnosti využití jsou :

- Nákup výrobku nebo platba za službu
- Uchovatel hodnoty
- Prostředek k obchodování na burze

Postupem času a s příchodem dalších kryptoměn založených na různých technologických odlišnostech se jejich spektrum využití rozšířilo.

Další možnosti využití:

- **Nízkonákladové peněžní převody**
  Některé kryptoměny mají za cíl nabídnout uživatelům rychlé transakční převody za minimální poplatky. Například nedávná transakce s litecoinem (LTC) v hodnotě 99 milionů dolarů trvala pouze dvě a půl minuty a náklady odesílatele byly pouze ve výši 0.40 USD. Pokud by tento převod peněz probíhal běžným finančním zprostředkovatelem, poplatky by byly pravděpodobně mnohem vyšší a převod by trval, v případě kdyby se jednalo o přeshraniční transakci, mnohem déle.

- **Alternativní sklad bohatství odolný vůči cenzuře**
  Zejména v jurisdikcích s pochybným právním řádem a v zemích, které sužuje velká míra korupce jsou častá obvinění z finančního pochybení ze strany konkurence nebo nepřátel. Lidé se tak mohou ocitnout v situaci, kdy nemají přístup k hotovosti, i když neudělali nic špatného. Kryptoměny jsou v tomto případě výbornou alternativou, kterou lze v případě dobře zvolené metody nákupu ukrýt před úřady.

- **Způsob investice do inovativních startupů**
  Vznik fundraisingu založeného na digitálních tokenech umožnil každému, kdo má připojení k internetu stát se investorem v inovativních začínajících technologických startupech a zároveň podporovat nové projekty potřebným základním kapitálem.

Počáteční nabídky mincí (ICO) jsou novou formou fundraisingu, která poskytuje začínajícím hráčům příležitost zvýšit kapitál prodejem nově vytvořeného digitálního tokenu výměnou za zavedené kryptoměny investorů, jako je Bitcoin (BTC) nebo Ethereum (ETH).

- **Provádění soukromých a anonymních transakcí**
  Digitální měny zaměřené na soukromí jako jsou Monero (XMR), Zcash (ZEC) a PIVX (PIVX) umožňují uživatelům provádět anonymní finanční transakce bez dohledu jakéhokoliv finančního regulátora.

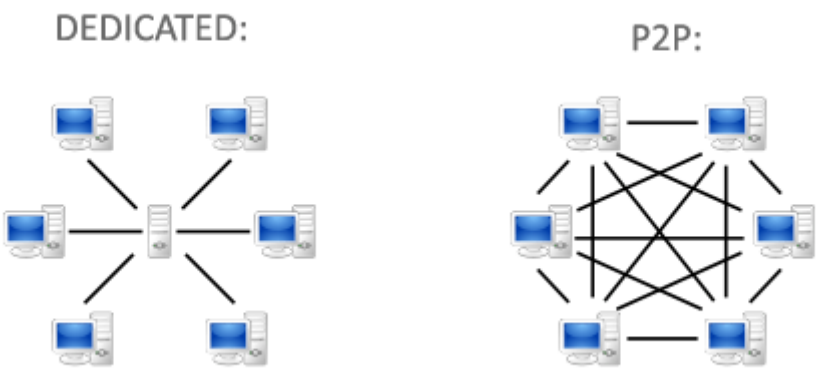
- **Provádění nepeněžních plateb**
  Dalším případem použití kryptoměn je bezhotovostní úhrada. Nigerijský startup SureRemit například umožňuje svým uživatelům odesílat nepeněžní platby z libovolného místa na světě vybraným africkým národům.
  Afričané si mohou zakoupit nativní tokeny SureRemit RMT, které se pak používají v aplikaci k provádění bezhotovostních plateb jako jsou například nákupy mobilních dat, dobití kreditu nebo platby za služby pro své příbuzné v Africe. Tento způsob využívají především Afričané pracující v některé z vyspělých zemí, kteří finančně pomáhají svým rodinám ve své vlasti. (5)

2 ANALÝZA SOUČASNÉHO STAVU

2.1 Nejznámější kryptoměny

2.1.1 Bitcoin

Bitcoin je nejznámější, nejrozšířenější a také první kryptoměnou, která přiblížila fungování decentralizovaných měn široké veřejnosti. Pojem P2P je v oblasti kryptoměn, stejně jako v případě počítačových sítí, označení pro takový typ sítě, kde si jsou všechny uzly rovnocenné. Jednotliví klienti zde mezi sebou komunikují napřímo. Není zde tedy žádný centrální uzel, který by sloužil jako prostředník pro distribuci dat v síti, jak je tomu u modelu klient-server. V případě P2P sítí také platí, že s narůstajícím počtem uživatelů se zvyšuje také přenosová kapacita sítě.



Obrázek 9 - Porovnání architektury klient-server a P2P (Zdroj: www.neogaf.com)

Bitcoin vznikl v roce 2009. Vytvořil jej dodnes anonymní vývojář pod přezdívkou Satoshi Nakamoto. Stejně jako jeho autor je pojmenována také nejmenší jednotka kryptoměny Bitcoin. 1 Satoshi je roven 0.00000001 BTC tedy Bitcoin Classic.

Sám autor zdrojového kódu kryptoměny ve svém průvodním článku psal, že na Bitcoinu pracoval od roku 2007. Vytvořil oficiální internetovou doménu Bitcoin.org, kterou po rozšíření jeho měny předal do rukou jeho fanouškovi a později hlavnímu vývojáři Gavinu Andresenovi. Po tomto kroku se odmlčel a jeho profil na původním fóru P2P Foundation zůstal neaktivní. O jeho osobě se vede mnoho spekulací. Sám o sobě tvrdí, že je Japonec a v roce 2009 mu bylo 34 let. Tato informace je často zpochybňována vzhledem k jeho dokonalé angličtině. Mezi další adepty, které se snažila média i jednotlivci vypátrat patřili

také matematik Shinichi Mochizuki a mladý irský student Michael Clear, který se aktivně věnoval P2P sítím. Oba adepti ale razantně spojení s Bitcoinem odmítli. V roce 2014 našel reportér časopisu Newsweek Japonce Doriama Nakamoto žijícího v USA, jehož rodné jméno bylo Satoshi Nakamoto. Pracoval jako systémový inženýr v oblasti financí. Tuto informaci však dementoval sám tvůrce této kryptoměny, když po několika letech napsal na původní internetové fórum svým uživatelským profilem „Nejsem Doriam Nakamoto“. Mnoho lidí se naopak snažilo využít mediální popularity této měny a označovali sami sebe za tvůrce Bitcoinu. Přestože se pravý tvůrce zřejmě nikdy nedohledá, důležité je, že na fungování měny tento fakt nebude mít žádný vliv. Nad sítí zařízení, které jsou zapojeny do tohoto procesu nemá, a již ze samotného principu Bitcoinu ani nemůže mít, jedinec kontrolu. (6)

2.1.2 Důležité milníky vývoje Bitcoinu

- **2009 – Vznik Bitcoinu**
  Zdrojový kód Bitcoinu je zpřístupněn veřejnosti. Počátek těžby, tedy procesu, kterým vznikají nové jednotky této kryptoměny a ověřují se transakce provedené v blockchainu.

- **2010 – Poprvé stanovena hodnota Bitcoinu**
  Vzhledem k tomu, že Bitcoin nebyl touto dobou ještě obchodován ale pouze těžen, bylo nemožné přiřadit peněžní hodnotu jednotce této vznikající kryptoměny. V roce 2010 se americký programátor Laszlo Hanyecz rozhodl poprvé prodat své vytěžené jednotky pomocí nabídky na fóru bitcointalk.org. Vyměnil 10 000 BTC za dvě pizzy. Ke dni 24.2.2019 by ho tyto dvě pizzy vyšly na 860 000 000,- Kč.

- **2011 – Vznik alternativních kryptoměn**
  Popularita Bitcoinu roste a poptávka po decentralizovaných a šifrovaných měnách se zvyšuje, začínají se objevovat první alternativní kryptoměny (altcoiny). Některé se snaží vylepšit úskalí Bitcoinu jako je například nízká rychlost ověření transakce, větší anonymita a podobně. Jako jedny z prvních lze zmínit Namecoin a Litecoin.

- **2013 – Pád cen Bitcoinu**
  Krátce poté, co cena jednoho Bitcoinu poprvé dosáhla 1000 dolarů, cena začala rychle klesat. Mnozí lidé, kteří investovali peníze v tomto okamžiku utrpěli vysoké ztráty, protože cena klesla na zhruba 300 dolarů. Trvá více než dva roky, než opět dosáhne hodnoty 1000 dolarů.

- **2014 – První velké podvody a krádeže**
  Bitcoin se ukázal vzhledem ke své anonymitě a neexistujícímu dozorujícímu orgánu také atraktivním a lukrativním cílem pro zločince. V lednu 2014 zkrachovala největší světová burza Bitcoinu Mt.Gox. Majitelé 850 000 Bitcoinů obchodujících na této burze je již nikdy nedostali zpět. Tato kauza ukázala světu také velká rizika obchodování s kryptoměnami.

- **2016 – Ethereum a ICOs**
  Kryptoměna Ethereum byla velmi blízko tomu, aby sesadila Bitcoin z první příčky trhu. Tato platforma využívá kryptoměnu známou jako Ether k usnadnění inteligentních smluv a aplikací založených na blockchainu. Příchod Etherea byl poznamenán vznikem počátečních nabídek mincí (ICO). Jedná se o platformy pro získávání finančních prostředků, které investorům poskytují možnost obchodovat s tím, co jsou často v podstatě akcie nebo podíly zakladatelských akcií. Komise pro kontrolu cenných papírů Spojených států sdělila investorům, že kvůli nedostatku dohledu mohou být ICO podvody nebo investiční operace na základě podvodného Ponziho schématu, vypadající jako legitimní investice. Čínská vláda je zcela zakázala.

- **2017 – Magická hranice pokořena**
  Bitcoin překračuje hranici 10 000 USD za jednotku a pokračuje v růstu na své ATH (all time high), kterého dosáhlo v prosinci 2018 částkou 20 089 USD za jednotku.
  Nárůst míst, kde lze s Bitcoinem platit a obchodovat postupně roste. Světové banky jako Barclays, Citi Bank, Deutsche Bank a BNP Paribas se vyjádřily, že hledají cesty, jak svým klientům Bitcoin nabídnout či uchovávat.

- **2018, 2019 – Pád kryptoměn**
  Cena Bitcoinu klesla již v únoru 2018 k hranici 6500 USD. Po šokovém pádu ceny následoval strmý nárůst až k 12 000 USD. Tento stav však vydržel pouze do poloviny března, kdy se ceny začaly opět propadat. Hranice 10 000 USD již v tomto roce nebylo dosaženo. Ke konci roku Bitcoin klesl pod hranici 3000 USD. Během ledna a února 2019 nedošlo k výraznějšímu nárůstu a jeho cena se pohybuje kolem 4000 USD.
  (7)

2.1.3 Ethereum

Ethereum je označení pro kryptoměnu fungující od roku 2015. Její jednotkou je Ether (ETH). Autorem je rusko-kanadský programátor Vitaly Dmitriyevich Buterin, který se již ve svých sedmnácti letech aktivně zajímal o Bitcoin. Díky znalostem fungování Bitcoinu chtěl vytvořit novou decentralizovanou síť, jejíž využití může být širší než jako pouhá platební platforma. Koncept Etherea představil v roce 2013. (6)

Kryptoměna Ethereum funguje stejně jako Bitcoin na decentralizované blockchain síti. Samotný projekt ovšem nebyl spuštěn za účelem vytvoření platební sítě, jako tomu je u Bitcoinu. Účelem Etherea je vytvoření platformy pro chytré kontrakty. Chytré kontrakty si lze představit jako software, který ověřuje jednání dvou nebo více stran, kteří mezi sebou daný kontrakt provádějí. Díky tomu zajistí, že všechny zúčastněné strany budou jednat podle stanovených podmínek. Aplikace fungující na principu chytrých kontraktů zaručí uživateli transparentní vykonání kódu daného programu pomocí ověření v blockchainu Etherea. Celá síť tak v tomto případě funguje jako vykonavatel daného výpočetního procesu a všichni „těžaři“ v síti se tak podílejí na jejím správném a transparentním fungování. (8)

Pro vytvoření aplikace na bázi Etherea je třeba vytvoření cloudového účtu, tedy adresy, na kterou samotný tvůrce aplikace odešle určitý obnos Etherů, které jsou následně distribuovány mezi jednotlivé těžaře, kteří ověřují transakce blockchainu, poskytují svůj výpočetní výkon a umožňují tak fungování programu podle představ jeho tvůrce.

Využití v praxi můžeme vidět na stovkách různých aplikací založených na platformě Etherea. Jedná se o aplikace jako je webový prohlížeč Brave, hudební streamovací služba Ujo hra CryptoKittes nebo směnárny IDEX a AirSwap.

Díky chytrým kontraktům je možné také jednoduše vytvářet nové kryptoměny na technickém standardu ERC-20, který běží právě v síti Ethereum. Největší tržní kapitalizaci na daném standardu si drží kryptoměny BNB, Maker a VeChain.

Také dříve zmiňované ICO kontrakty fungují na standardu ERC-20.

Hlavními rozdíly mezi Bitcoinem a Etherem:

- Způsob použití blockachainu Bitcoinu je určený ke sledování a zaznamenávání změn při transakcích s kryptoměnou. Blockchain Etherea je využíván především ke spouštění zdrojových kódů decentralizovaných aplikací

- Vytěžení jednoho bloku Bitcoinu trvá v průměru 10 minut. U Etherea trvá těžba jednoho bloku 12 sekund. Proto je zde potvrzování transakcí rychlejší, což je vhodnější především při běhu zmiňovaných aplikací

- Jsou založeny na různých bezpečnostních protokolech: Ethereum využívá systém "proof of stake" na rozdíl od systému "proof of work" u Bitcoinu

- Odhaduje se, že do roku 2021 bude vytěžena pouze polovina mincí Ethera, zatímco většina Bitcoinů již byla vytěžena (konečný počet bude 21 000 000 BTC). (9)

Ani Ethereu se nevyhýbají hackerské útoky. V roce 2016 bylo odcizeno v přepočtu více než 50 milionů amerických dolarů organizaci DAO, jejíž cílem bylo poskytnutí decentralizovaného obchodního modelu jak neziskový organizacím, tak i komerčním institucím. Přestože se nejednalo o nedokonalost samotného Etherea, ale chybu systému této nové organizace, díky této události došlo k tzv. „hard forku" neboli rozdělení sítě. Jedna skupina uživatelů preferovala vrácení odcizené měny zpět organizaci DAO, zatímco druhá skupina preferovala ponechání stávajícího fungování blockchainu. Provedením vrácení prostředků organizaci a zásahu do blockchainu tak vznikla nová kryptoměna Ethereum Classic jejíž zastánci nebyli podporovatelé tohoto rozhodnutí a pokračují tak v původní podobě blockchainu. (8)

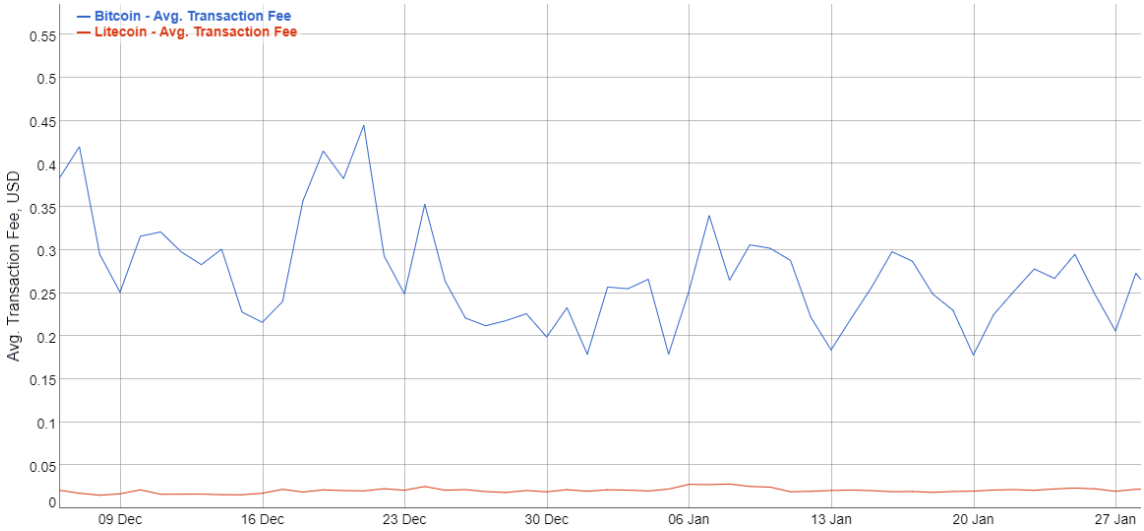
Vytvoření vlastní Ethereum peněženky je velmi jednoduché a existuje mnoho nástrojů, které dokáží vygenerovat adresu peněženky pomocí skriptu probíhajícího off-line ve webovém prohlížeči, aby byla zajištěna vyšší bezpečnost pro uživatele.

2.1.4 Litecoin

Kryptoměna Litecoin je oblíbenou alternativou Bitcoinu. Cena za jednotku Litecoinu (LTC) je v průměru asi 70krát nižší než za jednotku Bitcoinu. První blok této měny byl vytěžen v říjnu roku 2011. Další dva roky trvalo, než hodnota jednotky Litecoinu překonala hranici jednoho amerického dolaru. Její vznik se tedy datuje o necelé tři roky později než Bitcoin. Princip fungování je Bitcoinu velmi podobný a sám autor Charlie Lee, který dříve pracoval pro společnost Google se jeho inspirací netají. Také způsoby těžby a ověřování transakcí jsou velmi podobné. Těžení zpočátku probíhalo pomocí grafických karet, později těžaři přešli na specializované ASIC čipy, které si lépe poradily s hashovacím algoritmem Scrypt, který Litecoin využívá. (10)

Litecoin má od začátku sloužit jako rychlejší a levnější alternativa Bitcoinu, určená především pro transakční převody. Jeho bloky jsou vytěženy průměrně 4x rychleji a celkový počet finálních vytěžených mincí bude 4x vyšší než u Bitcoinu. Nejen tyto parametry předurčují Litecoin jako lepší alternativu k provádění drobných transakcí, vzhledem k rychlejšímu ověřování transakcí ale také velmi nízkým transakčním

poplatkům. I samotní obchodníci reagují na atraktivitu Litecoinu jako platebního prostředku a zákazníkům často nabízejí platby jak Bitcoinem tak i Litecoinem. Příkladem české firmy akceptující platby touto kryptoměnou je např. největší internetový obchod Alza.cz, která tuto možnost nabízí od února 2018. (11) (10)



Graf 1 - Porovnání průměrné výše transakčního poplatku Bitcoinu a Litecoinu v prosinci 2018 a lednu 2019 (Zdroj: www.bitinfocharts.com)

2.1.5 Monero

Monero vzniklo v dubnu 2014 rozdělením (forkem) kryptoměny Bytecoin. Na svém oficiálním webu se prezentuje jako soukromý, bezpečný a anonymní měnový systém. Jeho anonymita je dána především díky implementací protokolu CryptoNote, pro jehož hashovací systém je velmi těžké sestavit výkonnostně dostačující ASIC minery. Tento fakt nahrál do karet především těm těžařům, kteří nakoupili výkonné GPU a CPU jednotky, ale jejich efektivita se pro těžbu Bitcoinu nebo Etherea postupem času snižovala právě na úkor specializovaných ASIC jednotek. I přesto však v roce 2018 představil čínský výrobce Bitmain ASIC minery, které její těžbu umožnovaly. Její tvůrci na tuto situaci zareagovali hard forkem, který situaci vyřešil. V roce 2016 skokově vzrostla jeho tržní kapitalizace z 5 milionů na 185 milionů dolarů. Tomuto skoku pomohla také jeho implementace pro platby na dark webu AlphaBay. (12)

Jak již z předchozích vlastností vyplývá, přednosti této kryptoměny jsou především v její anonymitě a omezené možnosti vystopování iniciátora např. platby Monerem. To sebou

nese i stinné stránky, jelikož tato měna může být často použita i pro praní špinavých peněz z kriminálních aktivit nebo k ilegálním obchodním transakcím.

Výhodou Monera jsou nízké transakční poplatky a také anonymita, kde např. oproti Bitcoinu není v blockchainu možnost vystopovat původ a tok daných transakcí.

Cena za jednotku Monera (XMR) se v březnu 2019 pohybovala kolem 50 USD. (13)

2.1.6 Bitcoin Cash

Tato kryptoměna vznikla stejně jako Monero hard forkem původního Bitcoinu. Již několik let od spuštění Bitcoin sítě byly vedeny diskuse o tom, jaká technická vylepšení bude třeba implementovat pro to, aby síť dostačovala stále se zvyšujícímu počtu uživatelů a transakcí. Velikost jednoho bloku je limitována na 1 MB, který ve výsledku znamená maximální počet sedmi transakcí za sekundu. Toto neflexibilní řešení se snažilo několik předních vývojářů změnit, nicméně nikdy se nesetkalo s potřebným souhlasem komunity pro implementaci. Jedním z navrhovaných řešení bylo zvětšení velikosti bloku, které by ovšem vyžadovalo provedení hard forku, tedy takových změn v síti, které nejsou zpětně kompatibilní se staršími verzemi programů pracujících s Bitcoinovou sítí. Výsledným řešením problému bylo nasazení Segwit, jehož podstata je zmíněna v teoretické části práce a mělo za cíl vylepšit fungování sítě bez nutnosti provedení zpětně nekompatibilních změn.

Toto řešení ovšem nebylo akceptovatelné pro skupinu těžařů především z důvodu ponechání velikosti bloku na 1 MB. Proto se skupina těžařů pohybující se kolem čínského výrobce těžebního hardwaru provozovatele velkého těžebního poolu Bitmain rozhodla k vytvoření vlastní odnože Bitcoinu s možností velikosti bloku až 8 MB. 1.8.2017 došlo k oddělení od sítě Bitcoin a vytvoření Bitcoin Cash (BCH).

Uživatelé vlastnící Bitcoin, kteří měnu získali před tímto datem a mají přístup k privátnímu klíči, tak získali i podíl nové kryptoměny. Některé burzy také implementovali Bitcoin Cash jakožto další měnový pár. Cena za jednotku se pohybovala v prvních měsících na 20% Bitcoinu. V březnu 2019 cena 1 BCH odpovídá 130 USD. Jeho hodnota je tedy zhruba 30x nižší než hodnota 1 BTC. (6) (1)

2.1.7 Dash

Kryptoměna Dash vychází ze zdrojového kódu bitcoinu s vlastním blockchainem. Je jednou z kryptoměn s nejsilnější aktivní komunitou. V lednu 2014 byl spuštěn jako XCoin a po měsíci fungování přejmenován na Darkcoin, tedy na název, který lépe vystihuje jeho sklony k anonymizaci uživatelů. Po dalším roce již získal svůj nynější název Dash. Jeho autorem je Evan Duffield, který za účelem přejmenování na nynější název odkoupil přístup na web a přístup k softwaru kryptoměny Dashcoin, která je dnes již ve své původní podobě téměř zapomenutým projektem a jejíž hodnota se blíží nule. (14)

Jeho fungování se částečně odlišuje od logiky většiny ostatních kryptoměn. Používá hashovací algoritmus X11, který využívá kombinaci jedenácti různých těžících algoritmů. V síti existují kromě uživatelů a těžařů ještě tzv. master uzly, které poskytují vysoký výpočetní výkon a za odměnu jim připadá 45% všech nových mincí. Master uzly mají také zároveň anonymizační funkci PrivateSend a funkci InstantSend, díky které lze ověřit transakci rychle, bez nutnosti ověřování transakce menšími těžaři. Provozovatel toho uzlu je schopen získat plnou odměnu a zajistit si tak vysoký pasivní příjem z těžby. Pro založení tohoto uzlu je ovšem nutné vlastnit alespoň 1000 DASH. To je v přepočtu ke dni 5.5.2019 částka 2 704 371 Kč. Dalších 45% připadá klasickým těžařům a 10% je investováno do vylepšování ekosystému a fungování kryptoměny. Díky tomuto způsobu financování tak vývojáři nemusí vynakládat vlastní finanční prostředky pro implementaci změn nebo hledat sponzory. O těchto prostředcích poté rozhodují vlastníci master uzlů a pomocí hlasování volí, jakým způsobem budou prostředky investovány pro zlepšení sítě. (6) (14)

2.2 Porovnání uvedených kryptoměn

Tabulka 1 - Porovnání kryptoměn dle vybraných parametrů k 8.3.2019 (Vlastní zpracování)

	Bitcoin	Ethereum	Litecoin	Monero	Bitcoin Cash	Dash
Jednotka	BTC	ETH	LTC	XMR	BCH	DASH
Tržní kapitalizace (USD)	68 655 351 607	14 018 925 798	3 399 762 493	872 697 746	2 278 581 172	792 051 798
Cena za jednotku (USD)	3862	131	55	50	127	89
Algoritmus těžby	SHA 256, proof of work	Ethash	Scrypt, proof of work	CryptoNight, proof of work	SHA 256, proof of work	X11, proof of work
Konečný počet tokenů	21 000 000	Neomezeno	84 000 000	Neomezeno	21 000 000	18 900 000
Vznik	03.01.2009	30.07.2015	07.10.2011	18.04.2014	01.08.2017	01.01.2014
Průměrný čas těžby bloku	10 minut	15 sekund	2 minuty	2,5 minuty	10 minut	2,5 minuty
Počet maximálně provedených transakcí za sekundu	7	20	56	1700	60	48
Oficiální webové stránky	https://www.bitcoin.org	https://www.ethereum.org	https://www.litecoin.org	https://www.getmonero.org	https://www.bitcoincash.org	https://www.dash.org

V uvedené tabulce vybraných parametrů kryptoměn lze porovnat vlastnosti výše zmíněných kryptoměn. Tržní kapitalizace odpovídá součinu všech vydaných jednotek kryptoměny v oběhu a ceny za jednotku dané kryptoměny. Zde lze pozorovat suverenitu Bitcoinu jakožto úspěšného průkopníka technologie blockchainu. Následuje Ethereum, které přestože funguje teprve od roku 2015, získalo mnoho příznivců ze stran obchodníků s ICO tokeny. Také mnoho menších alternativních kryptoměn staví svůj základ právě na Ethereu a pomocí chytrých kontraktů si jej lidé kupují pod jménem jiné alternativní kryptoměny postavené na standardu ERC (ERC20, ERC223, ERC777).

Algoritmus těžby určuje hashovací funkci, kterou jsou ověřovány transakce dané kryptoměny. Konečný počet tokenů udává stav, při kterém již nebudou vznikat nové jednotky kryptoměny a zaručí tak držiteli větší „vzácnost“. Neomezenost například u kryptoměny Monero znamená, že od roku 2022 bude do sítě přibývat již pouze 0.3 XMR za minutu jako odměna za ověřování. Tato odměna se bude postupem času snižovat. I samotný tvůrce Etherea již navrhl, aby se komunita shodla na mezní hranici Etherea, kdy již nebudou přibývat nové tokeny. (1)

Vznik kryptoměny datuje první vytěžení bloku nové kryptoměny a měl by zaručit určitou míru etablovanosti kryptoměny a s tím i nižší riziko možného podvodu při jejím nákupu.

Průměrný čas těžby bloku a počet transakcí za sekundu naznačují rychlost samotné sítě a provádění transakcí. Zatímco komerční systémy ke zpracování transakcí dokáží zpracovat až 4400 transakcí za sekundu (VISA) např. Bitcoin jich zvládne pouhých 7. Řešením tohoto problému je např. Lighting Network u Bitcoinu. Samotné číslo by ovšem mohlo zájemci napovědět, zda je kryptoměna vhodná i pro drobné platby (Monero 1700, 2.5 minuty/blok) nebo je lepší ji spíše využít jako uchovatel hodnoty (Bitcoin 7, 10 minut/blok). S tím také souvisí výše transakčního poplatku, který většinou není závislý na výši splatné částky. Ve většině případů může odesílatel transakce zvolit i výši

transakčního poplatku. Zde platí, že čím vyšší poplatek uživatel zvolí, tím rychleji bude jeho transakce zpracována. (15)

2.3 Možnosti obchodování

Při nákupu virtuální měny je důležité si uvědomit, jakým způsobem s ní budeme chtít pracovat a uchovávat ji. Jinou metodu zvolí uživatel, který chce měnou aktivně platit a využívat ji pro nákup zboží nejen v internetových obchodech, opačný způsob zvolí ten, kdo chce pouze jednorázově směnit určitou peněžní sumu a držet ji v podobě virtuální měny s vidinou budoucího růstu hodnoty. Jiné prostředky si vybere ten, kdo se chce aktivně věnovat obchodování na kryptoměnovém trhu a potřebuje mít k dispozici analytické nástroje s predikčními modely. Ocení také možnost převodu držené měny do měny alternativní v co možná nejkratším čase.

S uvedenými scénáři souvisí také výše částky, kterou je daný člověk ochoten investovat, ať už jednorázově, nebo pravidelně. Od toho se odráží také důraz na bezpečnost jednotlivých řešení a jejich předpoklady pro bezpečné uložení prostředků. Proto by si i sami uživatelé měli uvědomit všechna finanční i bezpečnostní rizika, která mohou z nesprávně zvolené metody vyplynout.

Cílem je tedy zvolení správné cesty k získání, nebo směně prostředků rovnou z několika pohledů specifických zákazníků, vhodné především k uspokojení jejich potřeb jak již z hlediska komfortu nákupu, složitosti metody, bezpečnosti i míry likvidity daného způsobu.

2.3.1 Těžba kryptoměn

Těžba v dnešním digitálním světě nemusí nabývat pouze významu získávání nerostného bohatství, ale i získávání bohatství kryptografického. Jako příklad si vezmeme nejpoužívanější virtuální měnu Bitcoin, a to jak z důvodu historických dat, tak i z rozšířenosti této měny.

Těžba je založená na ověřování transakcí v síti, tedy takových transakcí, jako je například převod mezi peněženkami. Za ověření transakce získává těžař neboli „miner“ odměnu ve formě nově vzniklých bitcoinů a také poplatek za transakci. Vhodně zvolená výše

poplatku zaručí uživateli, že jeho transakce bude zahrnuta do nejbližšího bloku a tím dříve potvrzena. Výše poplatku se odvíjí především od množství právě probíhajících transakcí a celkové oblíbenosti měny v daný okamžik. Pokud bude v danou dobu probíhat malé množství transakcí, těžaři budou provádět i ta ověření, u kterých nebyl zvolen vysoký poplatek. Naopak při velkém vytížení sítě je nutné zvýšit hodnotu poplatku, aby byla ověření provedena. V případě, že bude poplatek příliš nízký, k ověření transakce nemusí vůbec nikdy dojít. Velikost poplatku je určována v jednotkách satoshi/byte (satoshi = 0.00000001 BTC). Většina dostupných služeb dnes tento poplatek dokáže vypočíst automaticky ke konkrétnímu typu transakce. (6)

V následujících grafech lze pozorovat závislost mezi cenou za jednotku bitcoinu a hodnotou průměrného poplatku za transakci v období od prosince 2017 do července 2018. Nelze zde mluvit o přímé úměrnosti, nicméně závislost mezi vyšší poptávkou po měně s růstem cen za jednotku, a tudíž i následným zvýšením poplatku za transakci, je zde zřejmá.

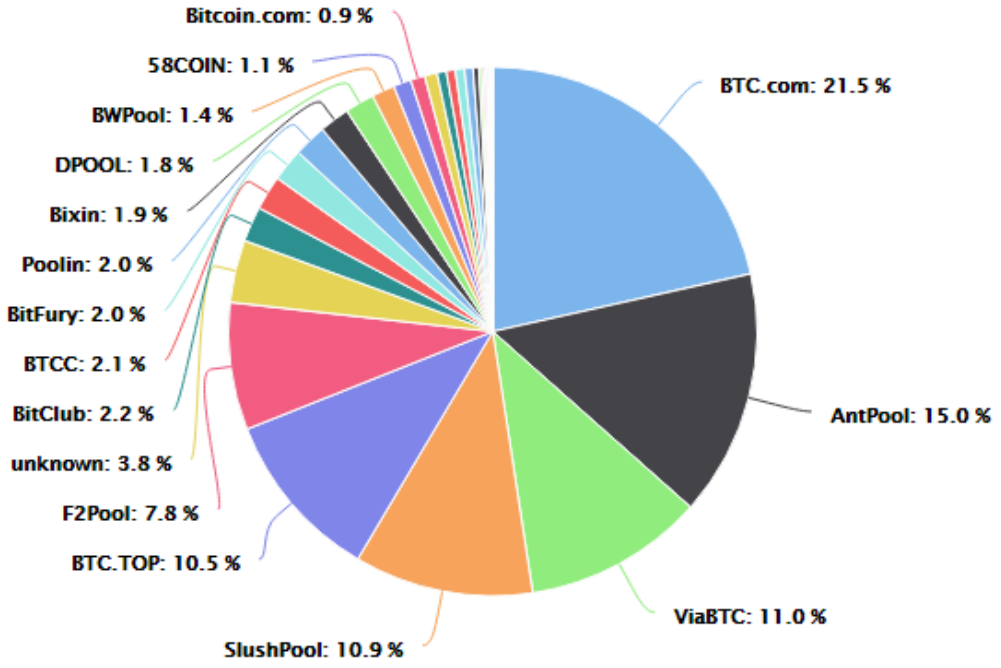
Graf 2 - Kurz BTC v daném období v USD (Zdroj: www.bitinfocharts.com)

Graf 3 - Výše průměrného transakčního poplatku za dané období v USD (Zdroj: www.bitinfocharts.com)

Druhá složka, ze které se skládá odměna pro těžaře je odměna za vytěžený blok. Transakce jsou ověřovány jednotlivými těžaři. Těžař, který nalezne nový blok získá také odměnu z vytěženého bloku. Ta je postupně snižována z původních 50 BTC z roku 2009

na dnešních 12,5 BTC. Tato hodnota je vždy redukována po zhruba čtyřech letech na polovinu (halving). Jelikož je ale k nalezení správného bloku nutný obrovský výpočetní výkon, shlukují se těžaři do tzv. poolů, ve kterých sdílejí jak výpočetní výkon, tak i odměny za nalezení nových bloků. Pooly jsou reakcí na velké množství těžařů v síti, které snižuje jejich šanci na včasné nalezení „šifry“ nad daným blokem. (1) (16)

Jednou z těchto největších komunit je i původem český „SlushPool“. Jedná se také o vůbec první pool, který stál za počátkem tohoto sdružování těžařů. Jeho autorem je český programátor Marek Palatinus a byl založen 27.11.2010. Tedy ještě v dobách, kdy povědomí o samotných kryptoměnách nebylo veliké. (17)



Graf 4 - Podíl jednotlivých poolů na těžbě Bitcoinu pro rok 20017/2018 (Zdroj: www.btc.com)

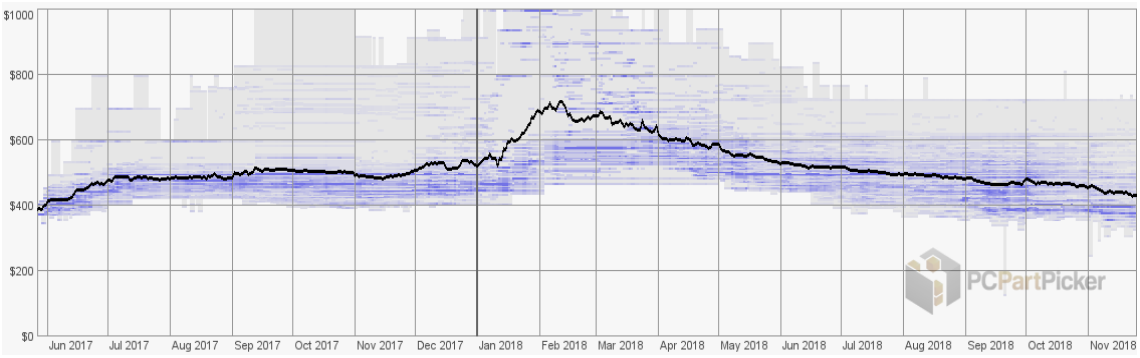
Pro samotné těžení je třeba podstoupit několik kroků, které jsou nutné pro každého začínajícího těžaře. Téměř nutností je vybrat si pool, ke kterému se lze často volně připojit. Těžba na klasickém desktop zařízení se využívala především v počátcích virtuální měny. K výpočtům byly využívány vyšší řady grafický karet, především od AMD, které byly pro těžbu Bitcoinu vhodnější. Neznamenalo to ale univerzálnost pro těžbu jakékoliv kryptoměny. Jelikož každá z těchto měn využívá jiný „hashovací algoritmus“, je třeba brát v potaz vhodnost pro konkrétní kryptoměnu. Dále je nutné vytvořit si účet u vybraného poolu. Po tomto kroku následuje výběr softwaru pro těžbu. Mezi nejrozšířenější programy pro těžbu Bitcoinu patří například Bitcoin Miner,

BTCMiner, NiceHash miner nebo CGMiner. Vždy je ale potřebné, aby daný program podporoval i vybraný pool. Funkce programů jsou velmi podobné. U některých programů je nutné stáhnout si na své uložiště kompletní blockchain soubor, obsahující historii všech uplynulých transakcí od jeho počátku (v době psaní má 210 GB a stále narůstá), zatímco některé si vystačí pouze s jeho částmi.

Dnes nicméně probíhá většina těžby na tzv. „ASIC minerech“. Tato zařízení mají speciální hardware optimalizovaný pro maximální výkon a nízkou spotřebu energie při výpočtu dané „hashovací“ metody (např. SHA-256 u Bitcoinu). Také většina „těžebních farem“ je založena na zařízeních typu ASIC. Většina těchto farem se nachází na území Číny, kde jejich majitelé využívají především levnější zdroje elektřiny i prostor. Také dostupnost těžebního hardwaru je pro ně snazší a levnější. (18)

Přestože má tedy i běžný uživatel vybavený klasickým stolním počítačem teoretickou šanci kryptoměny těžit, reálné náklady na danou těžbu jsou již nezanedbatelným výdajem. V konečném výsledku se takovému těžaři za aktuálních podmínek nikdy těžba nevyplatí. Tato situace se dá implikovat na příkladu těžby zlata. Velké těžařské společnosti, které mají technicky vyspělé technologie a do těžby investovaly miliardy dolarů, těžbu úspěšně provádějí. Vytěžené zlato se ziskem prodávají menším odběratelům, pro které je získání cenného kovu tímto způsobem výhodnější. (6)

Růst hodnoty Bitcoinu tak způsobil, že menším těžařům se přestávala těžba vyplácet, ale předchozí investice do těžebního hardwaru byly vysoké. Proto se především ti, kteří ještě neměli těžbu prováděnou pomocí ASIC zařízení, ale výkonnými grafickými kartami, uchýlili k těžbě jiných kryptoměn jako je například Ethereum, Monero nebo Zcash. Jejich hodnota nebyla tak vysoká a byla pro ně vhodnější těžba pomocí grafických karet. I tato situace přispěla k nedostatku jejich množství a růst cen především u výkonnějších řad ke konci roku 2017. (6)



Graf 5 - Cena grafických karet s čipem NVIDIA GTX 1070 v USA za dané období (Zdroj: www.pcpartipicker.com)

Výpočet vytěžených jednotek Bitcoin lze vypočíst následujícím způsobem jako:

$$\frac{N * B * H * 86400}{D * 2^{32}}$$

kde:

- H = výpočetní výkon (hashs/s)
- D = obtížnost vytěžení bloku
- B = odměna za vytěžený blok (v roce 2018 = 12,5 BTC)
- N = počet dní v měsíci
- 86400 (počet sekund v jednom dni)

Existuje ale také spousta online kalkulaček, které kromě výše uvedených parametrů berou v úvahu i náklady za energie. Níže uvedený příklad zobrazuje neziskovost těžby na desktopovém PC za pomocí grafické karty NVIDIA GTX 1050. V úvahu je brána průměrná cena elektrické energie v ČR, která za rok 2018 činila v distribuční oblasti ČEZ 4,07 Kč za kWh. (19)

	1 DAY	1 WEEK	1 MONTH
Income	0.00002050 BTC 1.74 CZK	0.00012300 BTC 10.43 CZK	0.00052440 BTC 44.46 CZK
El. costs	-0.00006864 BTC -5.82 CZK	-0.00048339 BTC -40.98 CZK	-0.00207326 BTC -175.78 CZK
Profit	**-0.00004814 BTC** -4.08 CZK	**-0.00036039 BTC** -30.56 CZK	**-0.00154886 BTC** -131.32 CZK

Tabulka 2 – Výpočet výhodnosti těžby BTC pomocí GPU NVIDIA GTX 1050 (Zdroj: www.nicehash.com)

Uvedená tabulka nám tedy jasně zobrazuje měsíční ztrátu 131,- Kč a to pouze za elektrickou energii. V úvahu nejsou brány náklady na pořízení hardware a náklady obětované příležitosti. Výsledná ztráta by byla tím pádem ještě několikanásobně vyšší.

Z výše uvedených informací tedy lze vyhodnotit, že na těžbě většiny rozšířených kryptoměn mohou profitovat především velcí investoři, kteří jsou ochotni investovat statisíce až miliony korun do vybavení, zázemí, energií a vzdělání v této oblasti. Ve výhodě jsou zájemci ze zemí, kde je k dispozici levná elektrická energie (Čína), nebo ze zemí s chladnějším podnebím a možností výroby elektrické energie z geotermálních zdrojů, jako je například Island. Nižší teploty pozitivně ovlivňují nároky na chlazení těžebních strojů a geotermální získávání elektrické energie je levnější a efektivnější. Díky tomu je výroba i samotná těžba také mnohem ekologičtější. Pro zájemce o zavedenější kryptoměnu, který je ochoten investovat maximálně desítky tisíc korun je lepší variantou využít některý ze způsobů směny za běžnou fiat měnu následujícími způsoby. (20)

2.3.2 Burzy kryptoměn

Stejně jako na klasických burzách, tak i na burzách kryptoměn dochází ke střetu nabídky a poptávky uživatelů, kteří chtějí prodat nebo nakoupit určitý obnos dané kryptoměny. I na těchto burzách lze směnit kryptoměnu za peněžní prostředky, ale některé burzy také nabízejí směnu kryptoměny za kryptoměnu jinou. Na rozdíl od směnáren zde tedy obchodujete se samotnými uživateli a burzovní společnost je pouhým prostředníkem, který obchod zprostředkuje.

Nejobvyklejšími jsou zde objednávky typu „limit“ a „market“. U objednávky typu „limit“ uživatel vyplní množství v jednotkách dané kryptoměny a cenu, za kterou chce kryptoměnu prodat nebo koupit. Objednávka je zařazena do seznamu nabídek a čeká na svého zájemce.

Druhý typ objednávky je typ „market“. Ten slouží k rychlému nákupu nebo prodeji. Uživatel vyplní pouze požadované množství a burzovní systém mu poskytne nejvhodnější nabídku, vhodnou pro jeho potřeby. Vzhledem k vysoké volatilitě kryptoměn je typ objednávek „market“ vhodnější pro uživatele, kteří nechtějí na danou směnu dlouho čekat a riskovat tak, že se rychle změní nákupní, nebo prodejní kurz. Na druhou stranu nemusí být tento typ objednávky natolik výhodný oproti objednávce typu „limit“, kde si uživatel sám určí hodnotu, za kterou je ochoten obchodovat. (21)

Obchodování na kryptoměnových burzách je vhodnější především pro obchodníky s kryptoměnami, kteří spekulují o růstu, či poklesu určité kryptoměny. Tito uživatelé většinou nedrží konkrétní obnos v dané kryptoměně, ale aktivně jej obchodují v čase za kryptoměnu jinou, nebo provádějí převody na fiat měnu. Burzy mají obvykle nižší transakční poplatky a jsou často koncipovány pro zkušenější obchodníky, kteří preferují intradenní obchodování a provádějí tak velké množství transakcí za den. Nižší transakční poplatky a pokročilé funkce aplikace dané burzy jsou pro ně prioritou. (22)

2.3.3 Směnárny kryptoměn

Kryptoměnové směnárny jsou webové služby umožňující nákup a prodej kryptoměn, a to směnou za klasickou fiat měnu, nebo za alternativní kryptoměnu. Portfolio kryptoměn je u každého poskytovatele individuální. Základem většiny z nich se staly známe měny jako je Bitcoin, Ethereum a Litecoin. Rozdíly jsou také v samotných možnostech a nástrojích služeb. Existuje mnoho služeb, které poskytují komplexní analytické a automatizované obchodní nástroje, ale i naprosto základní služby umožňující jednorázovou směnu bez nutnosti registrace a ověření uživatele. Oproti burzám je zde pevně daný kurz, za který je možné obchodovat.

Před samotným nákupem je vhodné si zjistit o směnárně co možná nejvíce informací. Na internetu i dnes existují stovky podvodných webů, které se vydávají za důvěryhodné společnosti poskytující směnu virtuálních prostředků. Neopatrný zákazník tak může velmi rychle přijít o vložené finance. Vymáhání těchto prostředků je zpravidla velmi složité a nákladné, často i díky nejasné zemi původu společnosti. Pokud na webové stránce směnárny nenalezneme informace o sídle a původu společnosti, je vhodné se službě úplně vyhnout, nebo důkladně prověřit její důvěryhodnost. Nejlepší způsob, jak zjistit důvěryhodnost společnosti, je vyhledat uživatelské i odborné recenze, zjistit původ společnosti, historii a případné problémy, které mohla mít v minulosti. Důraz také musí být kladen na důvěryhodnost zdrojů. Častým jevem mohou být falešné recenze webů, nebo komerční články, které vypadají jako autentické zkušenosti uživatelů. Proto je také vhodné ověřit dobu fungování společnosti. U několik let dobře fungující firmy je riziko podvodů menší než u nové služby. I u nových služeb, které fungují ze začátku dobře a často lákají nové klienty například na velmi výhodný směnný kurz nebo podobné konkurenční výhody, je riziko krachu nezanedbatelné. Ať už z důvodů finančních, legislativních, bezpečnostních nebo předem promyšleného obchodního modelu pyramidového schématu.

Dalším faktorem, kterým je vhodné se při výběru směnárny řídit jsou poplatky. Většina ověřených společností má na svém webu zveřejněny všechny poplatky, které mohou při využívání jejich služeb připadat v úvahu. Nutno podotknout, že rozdíly v poplatcích mezi jednotlivými společnostmi se mohou dramaticky lišit a při obchodování s menšími obnosy mohou být samotné poplatky vyšší než obchodovaná částka. Pokud informace o poplatcích a provizích na webu společnosti chybí, je nutné zpozornět.

V neposlední řadě je třeba zjistit platební metody a podmínky pro uskutečnění transakce. Obecně lze říci, že platba kreditní nebo debetní kartou vždy vyžaduje ověření identity uživatele. Většinou je nutné provést sken občanského průkazu nebo pasu. V některých případech je nutná ještě fotografie uživatele, kdy drží svůj občanský průkaz nebo pas. Tento způsob je také často dražší díky nutnosti ověření údajů o uživateli za pomoci fotografií. Pro uživatele zde plyne vyšší riziko zneužití osobních údajů, ať už v podobě podvodné společnosti, nebo napadení serverů poskytovatele hackery. Transakce převody z bankovního účtu často dodatečné ověření nevyžaduje. Uživatel je zde také dohledatelný, a to především podle čísla svého bankovního účtu. Odpadá zde riziko zneužití dokladu totožnosti, ale čas provedení převodu je zde výrazně delší než u kreditní nebo debetní karty. Některé služby nabízejí platbu pomocí PayPal, Alipay a dalších online platebních služeb. Rizika u těchto typů plateb korespondují s riziky samotné služby, která platbu poskytuje. (23) (21)

3 VLASTNÍ NÁVRHY ŘEŠENÍ

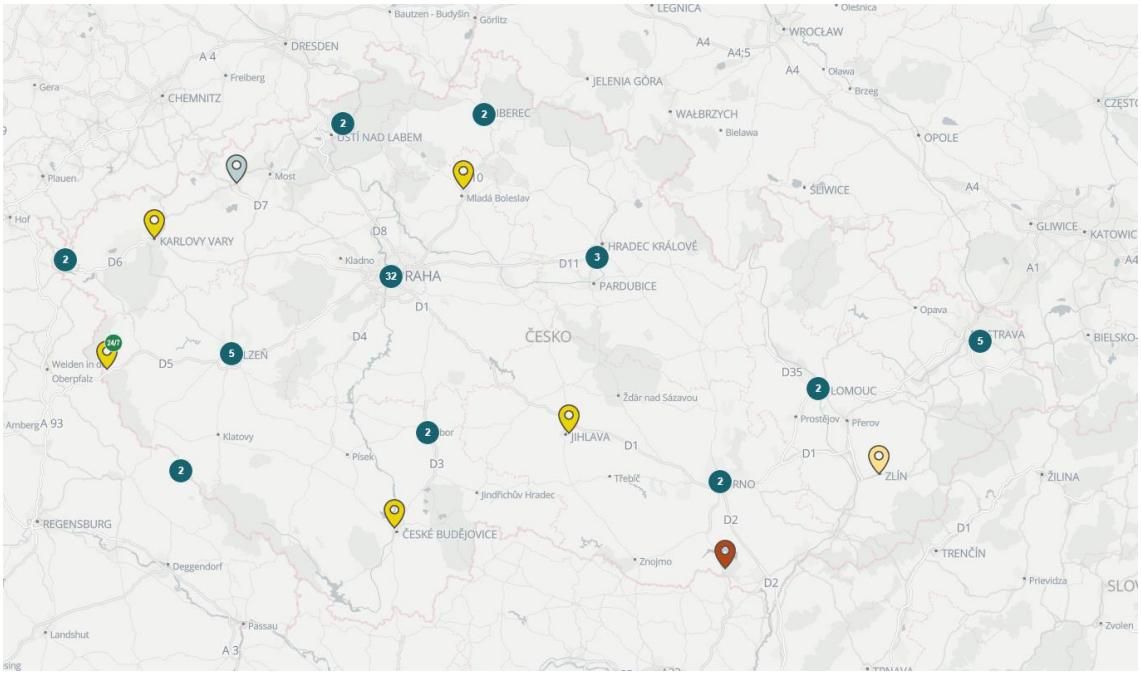
3.1 Bankomaty

V České republice je poměrně hustá síť automatů umožňující provádět směnu z fiat měny na některou z kryptoměn a naopak. Tento způsob nákupu je velmi vhodný především pro začátečníky, kteří nechtějí riskovat své peníze výběrem nesprávné online služby, nebo nemají důvěru k online platbám a elektronickému obchodování obecně. Tento postup je také jeden z velmi anonymních způsobů nákupu či prodeje kryptoměn, nevyžadující identifikaci zájemce o prodej či nákup.

Z hlediska bezpečnosti se jedná také o jednu z vhodných alternativ například pro nákup Bitcoinu. Jelikož má držitel k dispozici veřejný i privátní klíč, je reálným vlastníkem daného obnosu ve virtuální měně a jeho daná transakce i zůstatek jsou zapsány přímo v blockchainu. Zabezpečení jeho obnosu závisí tedy pouze na jeho schopnostech uchování veřejné části klíče. Odpadá zde riziko např. hackerského útoku na online burzu nebo jejího krachu.

Poskytovatelem těchto automatů jsou společnosti WBTCB a General Bytes. Společnost WBTCB s.r.o. se sídlem v Praze je zároveň také provozovatelem služby EasyCoin, která bude zmíněna později. Nabízí také službu s názvem Bitcoin Banking, fungující na principu online směnárny. Společnost General Bytes s.r.o. je původem také česká společnost se sídlem v Praze. Kromě kryptoměnových automatů poskytuje také produkty, díky kterým může podnikatel přijímat platby virtuálními měnami. Společnost WBTCB byla založena v roce 2014, General Bytes v roce 2013. Jejich působení na daném trhu je tedy již dostatečně dlouhé na to, aby mohly být považovány za důvěryhodné a spolehlivé.

Využití kteréhokoliv bankomatu daných poskytovatelů je tedy pro začínajícího uživatele bezpečnou a jednoduchou možností, jak získat vybranou kryptoměnu. Nevýhodou může být méně výhodný kurz oproti průměrnému kurzu na trhu a omezení 25 000,-Kč jak pro nákup i výběr na jednoho zákazníka denně.



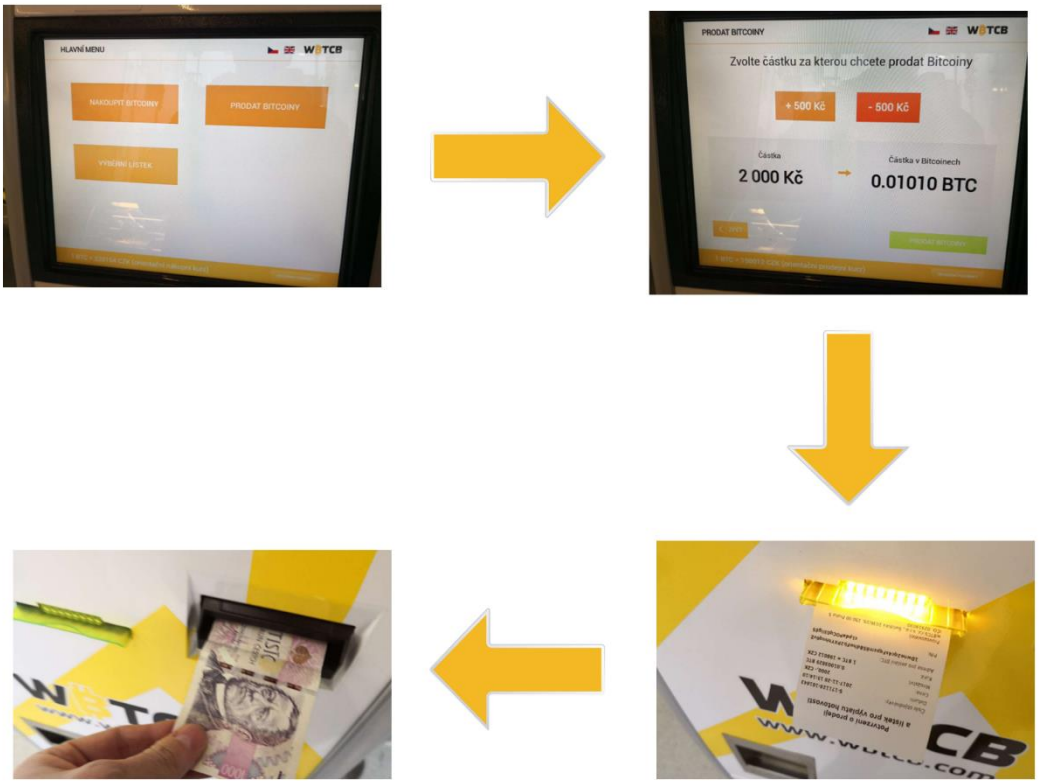
Obrázek 10 - Mapa automatů pro nákup kryptoměn v ČR (Zdroj: www.coinatmradar.com)

Příkladem může být automat WBTCB umístěný v brněnském OC Omega na náměstí Svobody. Na úvodní obrazovce vybere uživatel, zda chce prodat nebo nakoupit kryptoměnu. V tomto případě prodej Bitcoinu.

Dalším krokem je zvolení částky, za kterou chceme Bitcoin prodat. Zvolená částka lze navolit jak v hodnotě fiat měny, tak v dané kryptoměně. V dolní části obrazovky můžeme také vidět aktuální prodejní kurz. Minimální částka pro prodej je 500,-Kč stejně jako hodnota, o kterou lze danou částku navyšovat.

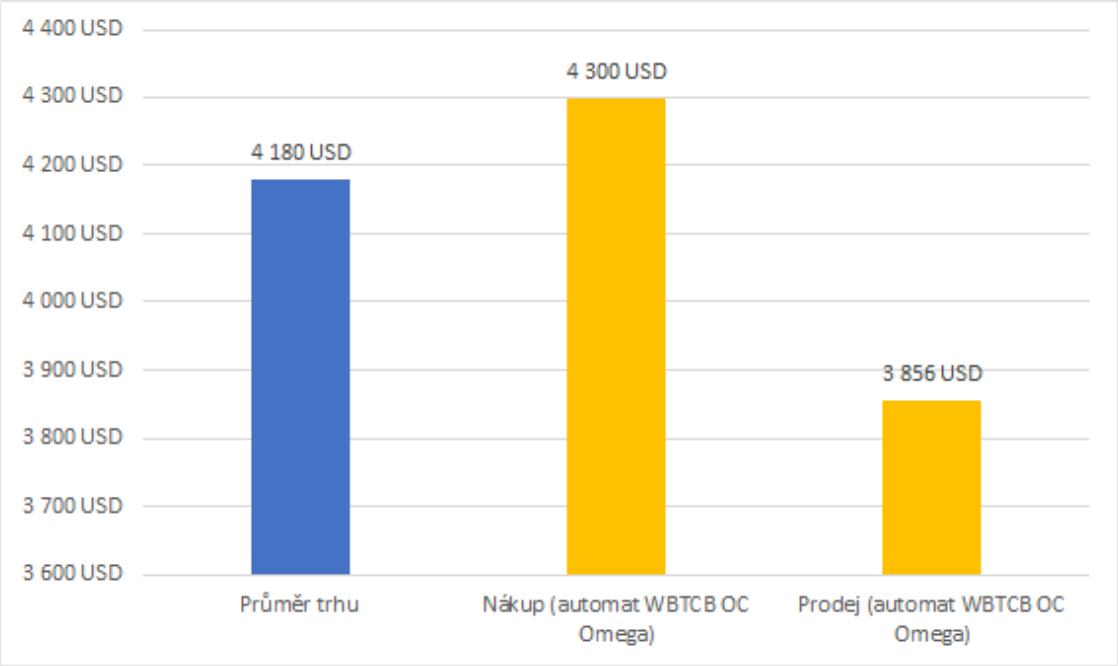
Po zvolení dané částky vygeneruje automat peněženku, na kterou je třeba danou částku do 30minut odeslat. Uživatel získá účtenku s vytištěným QR kódem peněženky pro zaslání hodnoty kryptoměny a PIN, který bude použit pro výběr hotovosti. Zároveň také startuje 30minutová lhůta pro zahájení transakce. Během této lhůty je nutné zadat požadovanou transakci přes některou z aplikací nebo služeb. Ověření transakce může trvat několik minut, ale i hodiny. Vše závisí na aktuální vytíženosti sítě a volbě transakčního poplatku, který vždy zaplatí zákazník navíc.

Posledním a nejpříjemnějším krokem je vyzvednutí hotovosti. Tu je možné si vyzvednout po ověření zadané transakce. Automat vyplácí pouze bankovky hodnoty 1000,-Kč. Jinou hodnotu je nutné si vyzvednout v klientském centru WBTCB v Praze. (24)



Obrázek 11 - Postup pro výběr kryptoměny Bitcoin z automatu WBTCB (Zdroj: Vlastní zpracování dle: 11)

Výhodou využití automatu je jednoduchost použití, které zvládne i začátečník. Při nákupu i prodeji kryptoměn je ale vždy nutné počítat s méně výhodným kurzem, než nabízejí online směnárny.



Graf 6 - Porovnání kurzu automatu WBTCB a průměru trhu v USD ke dni 2.12.2018 (Zdroj: Vlastní zpracování dle: www.coinatmradar.com)

Pro prodej kryptoměn potřebuje zákazník odeslat danou část tokenů na peněženku zřizovatele automatu. Tím se uživatelsky proces komplikuje, jelikož je již nutné použít např. některou z online peněženek, kterou zákazník musí mít zřízenou.

Zatímco prodej kryptoměny pomocí automatu nemusí být pro každého uživatele triviální záležitostí, je nákup pomocí automatu nejjednodušším řešením, jak si kryptoměnu obstarat. Pokud uživatel nemá zřízenou vlastní peněženku, kterou lze jednoduše vytvořit například pomocí online generátoru na adrese www.bitaddress.org, je možné nechat si vygenerovat novou peněženku přímo pomocí automatu, a to hned v prvním kroku. Poté je uživatel vyzván k naskenování QR kódu jeho peněženky a vložení hotovosti. Po ověření se částka v kryptoměně připíše na jeho peněženku.

3.2 Směnárny kryptoměn

Směnárny kryptoměn jsou nástrojem pro směnu peněžních prostředků za kryptoměnu, kryptoměny na fiat měnu nebo směnu jednotlivých kryptoměn mezi sebou. Na rozdíl od kryptoměnových burz je zde pevně daný kurz, za který transakce proběhne. Výběr vhodné směnárny je důležitým faktorem k úspěšnému a co možná nejvýhodnějšímu provedení směny. Při výběru směnárny je třeba dbát několika základních hledisek, které by měl

uživatel vyhodnotit před odesláním svých prostředků ve prospěch provozovatele směnárny:

- **Reputace** – ověření společnosti především z uživatelských recenzí na internetu. Na internetu existuje spoustu podvodných webů, vydávajících se za směnárnu kryptoměn. Také fungující zavedené směnárny mývají často finanční nebo technické potíže a v určitém okamžiku přestávají vyplácet uživatelům směněné prostředky. Je velká pravděpodobnosti, že vyhledáním a pročtením co možná nejaktuálnějších diskusí o dané společnosti lze těmto nepříjemnostem předejít a vybrat si spolehlivější alternativu.

- **Poplatky** – poplatkům za využívání služby se téměř nelze vyhnout. Je tedy důležité si předem zjistit jeho výši. Mezi základní patří poplatky za vklady, transakce a výběr. Poplatky se také často liší v závislosti na použití platební metody převodu, nákupu dané kryptoměny a výši směnné částky.

- **Platební metody** – způsob převedení peněžních prostředků, který je pro uživatele nejvýhodnější. Mezi základní možnosti patří platba debetní nebo kreditní kartou online, převod na bankovní účet, PayPal. Platba platební kartou většinou znamená rychlejší převod peněžních prostředků, vyšší poplatek a nutnost ověření identity. Převod z bankovního účtu trvá déle, zvyšuje se riziko chybného zadání údajů, ale poplatky za převod jsou nižší a často stačí k ověření identity váš bankovní účet, ze kterého byly přijaty prostředky v případě, že souhlasí se jménem uvedeným při registraci.

- **Požadavky na ověření** – většina obchodních platforem vyžaduje ověření totožnosti uživatele a tím téměř jistou ztrátu anonymity při nákupu kryptoměn. Při ověření je vyžadován sken osobního dokladu jako je občanský průkaz, pas nebo řidičské oprávnění, u některých poskytovatelů i kombinace těchto dokladů. Ověření je často zdlouhavý proces, jehož zpracování ze strany obchodní platformy může trvat i několik dní. I zde je důležité klást důraz na pověst obchodní platformy vzhledem k odesílání svých citlivých osobních údajů. Přestože se u většiny platforem nelze tomuto ověření vyhnout, najdou se alternativy, u kterých je ověření vyžadováno až při větším objemu transakcí.

- **Geografická omezení** – některé uživatelské funkce nemusí být v dané zemi podporované. Přestože je v tomto ohledu Česká republika otevřená země bez konkrétní právní úpravy pro obchodování s kryptoměnami, mohou být některé funkce směnáren omezeny z důvodů obecných nařízení orgánů EU jako je např GDPR. (25)

3.2.1 EasyCoin

Služba EasyCoin nabízí především zákazníkům v ČR možnost nákupu i prodeje Bitcoinu prostřednictvím partnerských prodejen GECO za hotovost nebo online. Na rozdíl od většiny online směnáren je tato služba založena na jednorázových transakcích, které se přímo zapisují do blockchainu. Provozovatelem této služby je dříve zmiňovaná česká společnost WBTCB.

Nákup v hotovosti je nejjednodušším způsobem, jak získat Bitcoin v případě, že v místě pobytu zákazníka není dostupný automat. Uživatel vyplní částku v korunách, za kterou chce Bitcoin nakoupit. Zadá adresu svojí peněženky, na kterou chce alternativní měnu zaslat a kontaktní e-mail, kde je informován o stavu své objednávky. Následně je třeba odsouhlasit obchodní podmínky. Uživatel obdrží potvrzení objednávky, kterým se identifikuje na kterékoliv ze 300 prodejen tabáku GECO. Zde objednávku zaplatí a následně mu je Bitcoin převeden na jeho adresu.

Podobným způsobem funguje i prodej Bitcoinu. Uživatel vyplní sumu, kterou chce směnit, zadá e-mail a odsouhlasí obchodní podmínky. Po odeslání objednávky získá objednávkový list, kde je uvedený PIN kód. Následně získá e-mailem odkaz na zadání daného PIN kódu. Po správném zadání získá číslo peněženky a sumu v Bitcoin měně, kterou je třeba na danou peněženku odeslat. Po odeslání a jednom potvrzení transakce je možné jít na pobočku GECO a vyzvednout si hotovost v korunách.

Výhodou této služby je jednoduchost nákupu bez nutnosti ověření, jednoduchost provedení transakce a dostupnost téměř kdekoliv v ČR. Nevýhodami jsou transakční limity, které jsou totožné pro nákup i prodej. Minimální limit pro obchodování je 2000,- Kč, maximální 25 000,- Kč. Při prodeji kryptoměny zde nastává stejný problém jako u automatu, a to ten, že uživatel již musí mít zřízený učet u některé z online služeb nebo aplikací, díky kterým může provádět převody mezi peněženkami. Jako poslední nevýhodu lze také, stejně jako u automatů, zmínit méně výhodné kurzy pro nákup i prodej oproti průměrné hodnotě na online burzách. Služba EasyCoin ponese od 20.4.2019 název BitStock, kvůli sjednocení názvu služby na všech trzích, kde tato společnost působí. Její fungování se z uživatelského hlediska nijak nemění. (26)

3.2.2 SimpleCoin

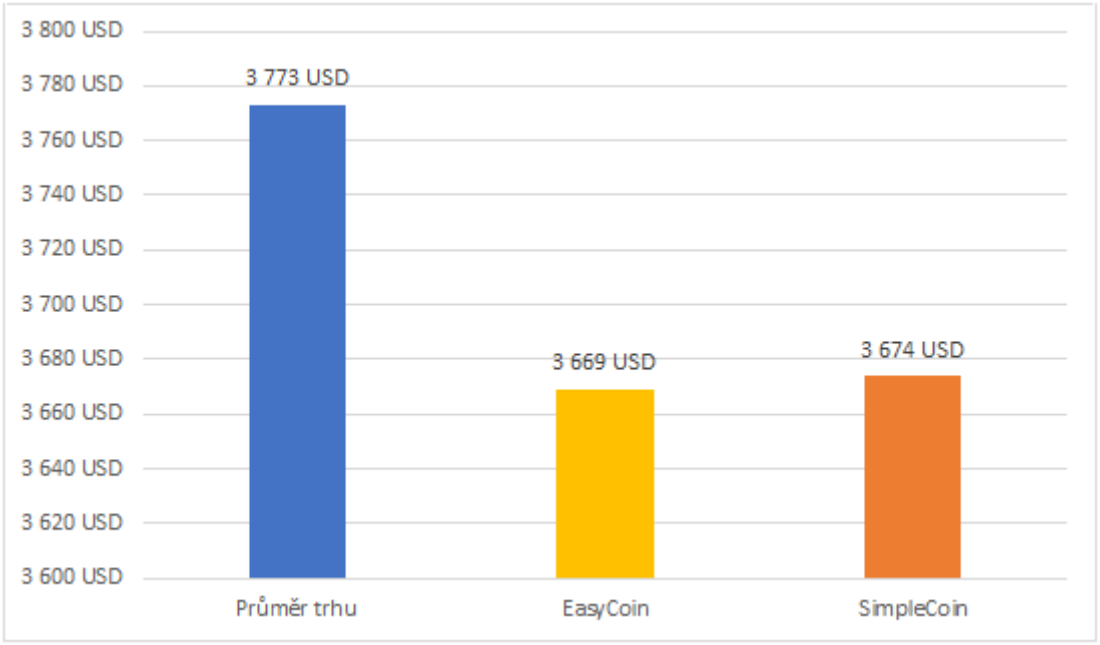
Za velmi podobnou službu, jakou je EasyCoin, můžeme považovat také službu SimpleCoin. Společnost Simple Coin s.r.o. se prezentuje jako česká směnárna kryptoměn, která chce zjednodušit českým zájemcům nákup a prodej kryptoměn, a to i bez nutnosti ověření do částky 400 Euro za měsíc. Po překročení této částky je nutné vytvořit bezplatný účet, který dovoluje obchodovat až do částky 10 000 Euro za měsíc. Obchodování nad limit této částky je třeba ověřit doložením zdroje příjmu, fotografií a občanským průkazem uživatele.

Samotný nákup a prodej je velmi podobný jako u předchozí služby s tím rozdílem, že nelze využít hotovostní platby u partnerských kamenných poboček. Veškeré nákupy kryptoměn je nutné uhradit převodem na bankovní účet společnosti. Prodej funguje na opačném principu. Uživatel zadá číslo svého účtu, na který mu bude vyplacena částka za prodej kryptoměny. (27)

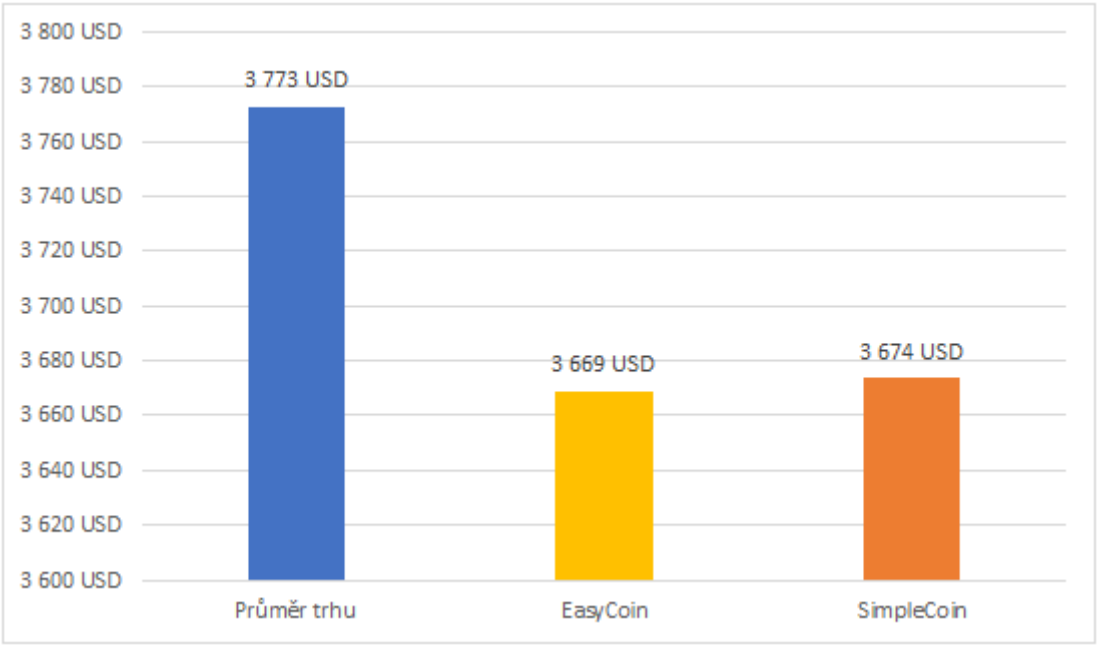
Výhodou této služby oproti službě EasyCoin je možnost prodeje a nákupu alternativních kryptoměn. Koupit zde lze kromě Bitcoinu i Litecoin, Bitcoin Cash, Ethereum a Ripple. Prodat je možné pouze Bitcoin, Litecoin a Bitcoin Cash. Registrovaný uživatel má také přehled o všech svých provedených objednávkách a stavu jejich vyřízení, možnost uložení svých bankovních účtů a kryptoměnových peněženek. (28)

Obě zmíněné služby mají výhodu především pro české zákazníky v jednoduchosti, přehlednosti, lokalizaci a tradici, která by měla i začínajícímu uživateli zaručit, že nákup nebo prodej proběhne bez komplikací. Daní za tyto výhody je u obou především méně výhodný kurz pro nákup i prodej.

V následujících grafech jsou zobrazeny kurzy v USD pro nákup a prodej kryptoměny Bitcoin u obou služeb a pro srovnání také průměrná cena jednoho Bitcoinu na burzách a směnárnách. Z grafů ke dni 4.1.2019 lze vyčíst, že výhodnější kurz pro nákup i prodej získá zákazník u služby SimpleCoin.



Graf 7 - Porovnání kurzu služeb pro nákup 1 BTC a průměrná hodnota 1 BTC na burzách v USD ke dni 4.1.2019 (Zdroj: Vlastní zpracování dle: www.coinatmradar.com, www.easycoin.cz, www.simplecoin.cz)



Graf 8 - Porovnání kurzu služeb pro prodej 1 BTC a průměrná hodnota 1 BTC na burzách v USD ke dni 4.1.2019 (Zdroj: Vlastní zpracování dle: www.coinatmradar.com, www.easycoin.cz, www.simplecoin.cz)

3.2.3 Coinbase

Společnost Coinbase je největší celosvětovou směnárnou kryptoměn. Vznikla v roce 2012 a je dostupná ve 42 zemích včetně České republiky. Provozovatelem je stejnojmenná americká společnost se sídlem v Kalifornii a její sesterská společnost se sídlem v Londýně.

Obrázek 12 - Logo společnosti Coinbase (Zdroj: www.coinbase.com/press)

Společnost je podporována důvěryhodnými investory a využívají ji miliony zákazníků na celém světě. Umožňuje jak směnu prostředků, tak i vytváření kryptoměnových peněženek za účelem uložení v alternativních měnách. Uživatelům jsou k dispozici také aplikace pro chytré telefony na platformách Android a iOS.

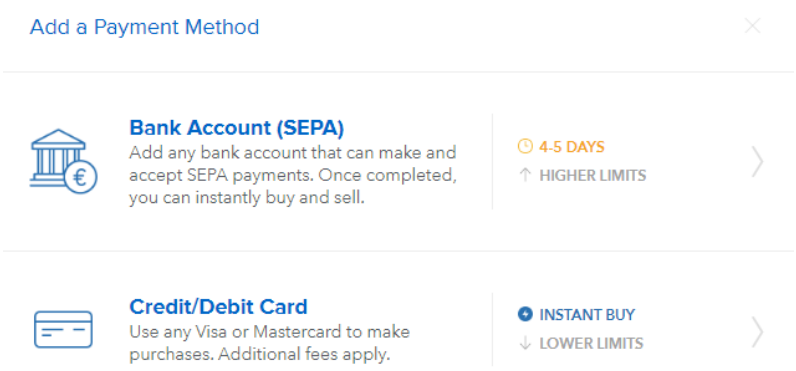
Platforma podporuje obchodování s 11-ti kryptoměnami, mezi kterými nechybí Bitcoin, Ethereum, Ripple, Litecoin a Bitcoin Cash. Podporuje také jejich vzájemnou směnu. Poplatek za běžnou transakci (nákup/prodej) zde činí 1,49% z částky, při nákupu kreditní kartou 3,99%. Při směně kryptoměn je účtován poplatek 1%.

Z uživatelských recenzí je platformě vytýkána velmi špatná uživatelská podpora, vyšší poplatky, dlouho trvající, často problematické a nutné ověření identity uživatele a především chybějící možnost získání privátního klíče k peněženkám uvnitř aplikace. Uživatel tak nemá 100% přístup ke svým prostředkům a je tak závislý na dané platformě v případě, že chce provést jakoukoliv transakci.

Za výhodu lze považovat kvalitní zabezpečení platformy, která se od roku 2012 obešla bez větších problému s hackery, přehledné prostředí s mobilními aplikacemi, které je vhodné i pro začátečníky a v neposlední řadě také široké portfolio podporovaných kryptoměn. (29)

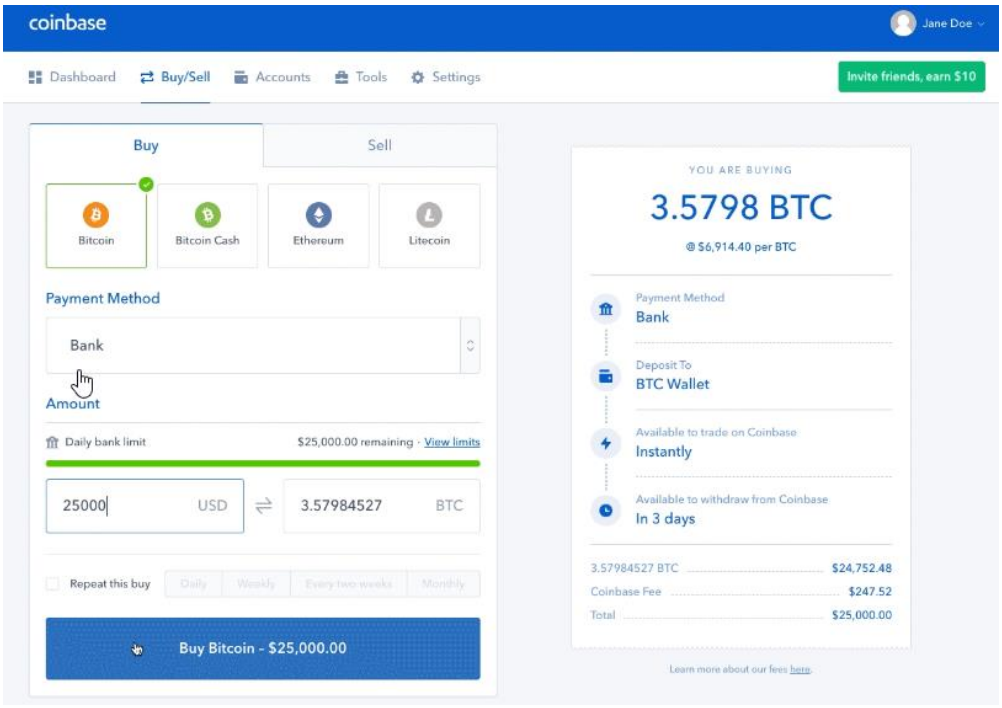
Jak již bylo zmíněno, pro provedení směny na Coinbase je potřeba vytvoření uživatelského účtu. K dispozici jsou typy účtu Individual a Business. Účty typu Business jsou určeny především pro právnické osoby. Nabízí jim možnosti jako je akceptace kryptoměnových plateb ve svém podniku nebo zprostředkování obchodu s kryptoměnami. Pro jednotlivce je určen typ účtu Individual. Při registraci je nutné vyplnit jméno, příjmení, email a potvrdit dosažení věku 18 let. Po ověření e-mailu je nutné provést druhou fázi ověření zadáním telefonního čísla. Následuje doplnění údajů o uživateli, které je již poněkud zvídavější. Kromě jména, příjmení a data narození je nutné vyplnit adresu bydliště, k čemu chce uživatel Coinbase využívat, zaměstnání a zaměstnavatele. Tímto krokem ještě proces nekončí. K dokončení je nutné nahrát kopii cestovního pasu, řidičského oprávnění nebo občanského průkazu. Po nahrání dokladů je následně nutné provést „selfie“ fotografii za pomoci webkamery.

Po komplikovaném procesu ověření, kde je velmi často problém s provedením „selfie“ pomocí webkamery (dle uživatelských recenzí je snazší provést ověření pomocí mobilní aplikace) se zobrazí uživateli rozhraní aplikace s možností nabití peněžního účtu v eurech nebo využití okamžité směny z účtu uživatele na vybranou kryptoměnu.



Obrázek 13 - Výběr platební metody na Coinbase (Zdroj: www.coinbase.com)

Samotné uživatelské rozhraní je již velmi přehledné, a přestože nepodporuje český jazyk, uživatel se v něm rychle zorientuje. Mezi základní záložky patří Dashboard, kde uživatel vidí vývojové grafy cen kryptoměn a jeho portfolio. Další je záložka Buy/Sell pomocí níž lze nakupovat a prodávat kryptoměny. Poslední důležitou záložkou je Account, kde uživatel vidí své peněženky včetně provedených transakcí.



Obrázek 14 - Uživatelské prostředí Coinbase (Zdroj: www.coinbase.com)

Směnárnu Coinbase lze považovat za zavedeného partnera v oblasti obchodování kryptoměn. Výhodou je intuitivní ovládání jak webové, tak i mobilní aplikace, podpora nejrozšířenějších kryptoměn, zabezpečení na vysoké úrovni a přiměřené poplatky za transakce. Vhodná je jak pro začínající, tak pro pokročilé uživatele a díky podpoře plateb z českých bankovních účtů zde není omezení nabití Coinbase účtu pouze pomocí platební karty. Z hlediska zabezpečení je na velmi vysoké úrovni s povinným použitím dvoufázové autentizace pro provádění transakcí. Jako další prvek zabezpečení účtu lze také přidat ověření pomocí Google Authenticator nebo Authy. (29)

Nevýhodami lze shledat špatnou uživatelskou podporu, nemožnost získání privátního klíče své peněženky nebo složité ověření při zakládání účtu. Za zmínku také stojí nutnost vyplnění velmi detailních informací o uživateli včetně fotografií jeho dokladů totožnosti, které jsou také po dobu fungování účtu uchovávány.

3.2.4 Changelly

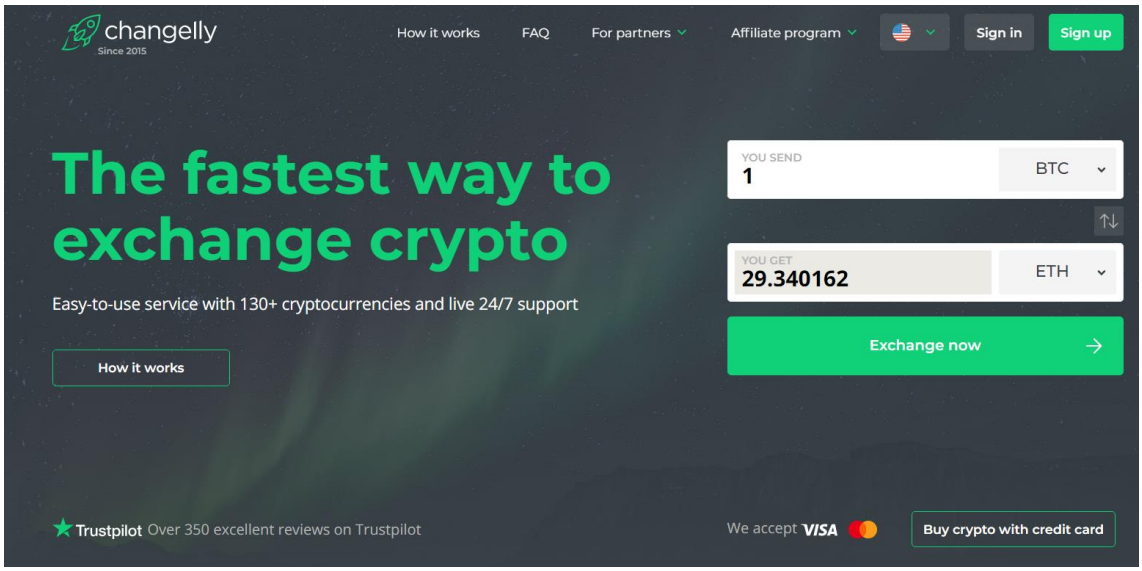
Changelly je rychlá služba poskytující možnost směny kryptoměn i transakce, kde je kryptoměna směněna za měnu národní. Funguje od roku 2015 a její sídlo je na Maltě. Nabízí přístup jak ze svých webových stránek www.changelly.com nebo pomocí svojí

aplikace pro mobilní platformy Android. Uživatelům umožňuje také jako doplňkovou službu umístit si platební kryptoměnový widget na vlastní webové stránky, což může být užitečné jak pro tvůrce webového obsahu, tak pro jeho fanoušky, kteří ho mohou snadno podpořit příspěvkem ve formě kryptoměny přímo z jeho webové stránky.

Obrázek 15 - Logo společnosti Changelly (Zdroj: www.changelly.com)

Sama společnost na svých webových stránkách přiznává, že princip fungování platformy spočívá ve vytváření nabídek a poptávek pomocí vlastního algoritmu na burzovních serverech jako je Binance, Poloniex, Bitrex apod. Zde najde v nejkratším možném čase vhodnou nabídku nebo poptávku po dané měně a provede směnu. Proto si za provedení transakce účtuje poplatek 0,5% z ceny při konverzi mezi kryptoměnami, který se ovšem může drobně lišit, vzhledem k určité časové prodlevě provedení transakce na výše zmíněných serverech. (30)

Směnárna podporuje více než 130 existujících alternativních měn a při nákupu kryptoměn za běžnou měnu nabízí pouze možnost platby debetní nebo kreditní kartou online. Nákup kartou online ovšem využívá služeb sprostředkovatelů Indacoin a Simplex, a tak nenabízí příliš výhodný směnný kurz. Pro srovnání lze vzít v úvahu kurz k 26.3.2019 ve 21:44, kdy se průměrná cena na burzách pohybovala okolo 3969 USD za jednotku Bitcoinu. Česká směnárna EasyCoin prodávala 1 BTC za 4052 USD a směnárna Changelly si za jednotku Bitcoinu žádala 4496 USD. Neznalý uživatel tak může jednoduše provést velmi nevýhodnou transakci, a to za podmínek, kdy si může společnost Changelly kdykoliv vyžádat ověření jeho identity. To vyžaduje kvalitní scan cestovního pasu nebo řidičského průkazu, doložení zdroje příjmů a ostatní potřebné dokumenty. (31)



Obrázek 16 - Jednoduché uživatelské rozhraní platformy Changelly (Zdroj: www.changelly.com)

Platforma Changelly nabízí vlastní algoritmus pro vyhledávání nejlepších nabídek na velkých burzovních platformách. To zajistí uživateli komfort při hledání nejlepší nabídky při směně kryptoměny za kryptoměnu. Zároveň posílá ihned všechny převedené prostředky na peněženku uživatele, který má tak veškeré své privátní klíče pod vlastní kontrolou. Poplatek 0,5% za transakci tohoto typu je velmi nízký a uživateli ušetří vyhledávání nejvýhodnější transakce, vytváření a často i ověřování účtu u nejvhodnější burzovní platformy. Hodí se tedy především pro tento případ použití. Výhodou je také podpora více než 130-ti různých kryptoměn.

Využití platformy pro nákup kryptoměny pomocí kreditní karty sebou přináší velmi nevýhodný kurz a nejasné podmínky, za kterých je vyžadováno ověření uživatele. Pro tento typ využití jsou na trhu mnohem lepší alternativy zmíněné výše. V uživatelských recenzích je také často kritizován čas provedení transakce. Na druhou stranu je platforma Changelly již dlouho fungující služba s velmi dobrou uživatelskou podporou a zajímavou technologií vyhledávání transakcí, která je vhodná pro směnu kryptoměny za alternativní kryptoměnu.

3.3 Kryptoměnové burzy

Burzy kryptoměn jsou založeny, stejně jako většina ostatních burz, na principu nabídky a poptávky, kde jedna část uživatelů nabízí své kryptoměny k prodeji a druhá má zájem

o jejich nákup v daném množství za určitou částku. Na rozdíl od směnáren zde uživatel nakupuje kryptoměny od ostatních uživatelů a burzovní společnost je pouhým prostředníkem pro obě strany. Jejich software by měl uživatelům nabídnout jistotu spravedlivého obchodu, při kterém budou obě strany po dokončení obchodu spokojeny.

Na burzách existují základní dva typy objednávek a to typu „Limit“ a „Market“. Objednávky typu limit umožňují obchodníkovi nakoupit nebo prodat kryptoměnu za jeho požadovanou cenu. Může například vystavit poptávku po kryptoměně za cenu nižší, než je jeho aktuální cena, nebo naopak prodat za cenu vyšší. Tento typ objednávky ovšem proběhne pouze tehdy, pokud se najde protistrana, která je ochotna danou nabídku akceptovat. Při tomto typu objednávky má tedy obchodník jistotu, že dostane cenu, jakou požaduje, ale nemá jistotu, že se pro jeho nabídku najde protistrana, která jeho objednávku přijme.

Objednávky typu market slouží k okamžitému nákupu nebo prodeji. Uživatel vyplní pouze množství, které chce prodat a systém burzy pro něj vybere nejlepší možnou nabídku v daném čase. Při nízkém počtu nabídek je tak větší riziko, že uživatel nedosáhne natolik výhodného obchodu jako v případě použití nabídky typu limit.

Většina projektů je postavena na centrálním systému, který shromažďuje data uživatelů na svém serveru. Existují ale i decentralizované burzy jejichž princip fungování je plně založený na blockchain technologii, a to především na chytrých kontraktech Etherea. Převážný objem obchodů zde tak tvoří ERC-20 tokeny, které jsou právě na Ethereu založeny.

U většiny zahraničních burz je třeba dobití účtu dané platformy pomocí bankovního převodu nebo pomocí online platby kreditní kartou. Další možností je převedení již držené kryptoměny k účtu uživatele na konkrétní platformě.

I u burz s kryptoměnami je třeba počítat s potřebou ověření totožnosti uživatele, která probíhá většinou stejným způsobem jako v případě směnáren. Většinou se jedná o scan dokladu totožnosti, někdy i o vyplnění dotazníku o výši a původu příjmů uživatele. Při výběru burzy je dále vhodné zohlednit výši poplatků, uživatelské recenze, dobu působení na trhu, nabídku obchodovatelných kryptoměn nebo jazyk uživatelského rozhraní platformy. (32)

3.3.1 Binance

Binance je burza kryptoměn fungující od roku 2017. Od té doby se stala jednou z největší kryptoměnových burz. Její fungování začalo v Číně, nicméně později bylo její sídlo přesunuto na Maltu a to především díky nižším právním omezením obchodu s kryptoměnami ze strany státu.

Obrázek 17 - Logo burzy Binance (Zdroj: www.binance.com)

Burza nabízí dva různé pohledy uživatelského prostředí nazvané jako Basic a Advanced. Hlavní rozdíl mezi těmito verzemi je, že verze Advanced nabízí podrobnější technickou analýzu hodnoty digitální měny v čase. Nyní nabízí panel základní verze několik grafů a grafů pro páry, které se obchodují, knihy objednávek a historii obchodů.

Burza nabízí velmi široké portfolio více než 110 kryptoměn, mezi kterými nechybí nejznámější kryptoměny. Pro uživatele jsou k dispozici virtuální peněženky, na kterých má uživatel své prostředky. Nemá tedy přímý přístup k privátním klíčům a je tak pouze na něm, jak moc burze důvěřuje. K nedůvěře není příliš mnoho důvodů. Od počátku svého fungování se burza nesetkala s většími problémy jako jsou hackerské útoky nebo jiné typy zneužití prostředků uživatelů.

Poplatek za transakci činí standardních 0,1%. S objemem obchodů se transakční poplatky snižují, nicméně běžný uživatel nejspíše těchto výhod nedosáhne. Burza totiž snižuje poplatek na 0,09% až při měsíčním objemu transakcí nad 100 BTC.

Při objemu transakcí do 2 BTC za den není třeba ověření identity vlastníka účtu. Burza tak o uživateli neshromažďuje žádné osobní údaje. Případné ověření pro větší objemy obchodu lze provést pomocí fotografie osobního dokladu uživatele.

Nákup kryptoměny lze provést platební kartou online. Zde je ovšem využita technologie společnosti Simplex včetně velmi nevýhodného směnného kurzu pro jakoukoliv kryptoměnu. Řešením pro uživatele, který chce tuto burzu využívat je tedy nákup kryptoměny jinde a odeslání do virtuální peněženky ve svém Binance účtu.

Binance je velmi uživatelsky přívětivá služba umožňující dva odlišné pohledy na aktuální vývoje a grafy na trhu. Hodí se tedy jak pro začínající uživatele, tak i pro pokročilé obchodníky. Nabízí vlastní kryptoměnu Binance coin, dvoufázové zabezpečení uživatelského účtu i možnost obchodování bez ověření uživatelské identity a tím jistou míru anonymity. Uživatelské recenze a zkušenosti jsou veskrze pozitivní, a tak se toto řešení jeví jako jeden z dobrých partnerů pro vstup na kryptoměnovou burzovní platformu. (33)

3.3.2 Coinbase Pro

Vlastníkem burzy Coinbase Pro je stejná společnost Coinbase sídlící ve San Franciscu v Kalifornii, která provozuje i výše zmíněnou směnárnu Coinbase. Burza vznikla pod názvem GDAX a jednalo se o jednu z největších kryptoměnových burz, která vznikla již v roce 2012. V roce 2018 se burza přejmenovala právě na Coinbase Pro, a to především proto, aby se uživatelé směnárny Coinbase neobávali přechodu na burzovní platformu, kterou již dobře znají. Změny se neudály ve vlastnické struktuře burzy, ale pouze v designu webové aplikace.

Obrázek 18 - Logo Coinbase Pro (Zdroj: www.pro.coinbase.com)

Jak naznačuje současný název, Coinbase Pro je verze Coinbase doplněná o funkce, které ocení pokročilí obchodníci. Zatímco směnárna Coinbase nabízí pouhé uchování kryptoměn nebo fiat měny na svém účtu, Coinbase Pro nabízí standardní burzovní příkazy, podrobné grafy a analýzy historie vývoje cen. Zároveň neztrácí výhodu pohodlného nabití prostředků uživatelského účtu pomocí online kreditní karty nebo převodem pomocí SEPA platby.

Uživatel, který má vytvořený a ověřený účet u směnárny Coinbase se může totožným uživatelským profilem přihlásit bez problémů i do účtu na burze Coinbase Pro. Vytváření

nového uživatelského profilu a často složitá fáze ověření identity uživatele tak nejsou pro tyto zákazníky nutné.

Transakční poplatky se pohybují od 0,15% do 0,25% za provedenou transakci. Pro obchodníky s měsíčním objemem nad 100 000 USD se poplatky snižují i pod tuto hranici.

Nabití účtu pomocí SEPA platby sebou obnáší poplatek ve výši 0,15 EUR, stejně jako při výběru pomocí platby na účet uživatele.

Coinbase Pro je navržen tak, aby oslovil pokročilejší obchodníky, kteří chtějí vědět více než jen základy tržních výkyvů souvisejících s dvojicemi krypto měn a nabízí jim k tomu potřebné nástroje. Rozhraní Coinbase Pro je zároveň velmi intuitivní a umožňuje obchodníkům rychlou orientaci v uživatelském rozhraní. (34)

3.3.3 Kraken

Kryptoměnová burza Kraken působí na trhu již od roku 2013. Přestože je provozovatelem americká spolčenost Payward Inc., zaměřuje se především na evropské a japonské zákazníky.

Obrázek 19 - Logo kryptoměnové burzy Kraken (Zdroj: www.kraken.com)

Burza nabízí přes 20 obchodovatelných kryptoměn, mezi kterými nechybí ty nejznámější jako Bitcoin, Ethereum nebo Litecoin. Vytvoření uživatelského účtu je velmi snadné a postačí k němu vyplnění e-mailu, jména, data narození a telefonního čísla. Při pouhém obchodování s kryptoměnami není třeba vyšší uživatelské ověření. Pro převody mezi kryptoměnou a fiat měnou, například pro vklady a výběry, je nutné vyplnění adresy bydliště. Dalším stupněm je zaslání osobních údajů formou scanu osobního dokladu jako je např. občanský průkaz nebo pas. Díky tomuto ověření je možné obchodovat vyšší částky, a to až do 25 000 USD za den. Běžnému uživateli ovšem bohatě postačí druhá fáze ověření. Burza podporuje kromě amerického dolaru také vedení účtu v eurech. Další

národní měny jako jsou japonské jeny (JPY) nebo kanadské dolary (CAD) nejspíše uživatel z Evropy nevyužije a jejich použití vyžaduje třetí fázi ověření uživatelského účtu. (35)

Společnost si zakládá na transparentnosti a přehlednosti uživatelských poplatků. Do měsíčního objemu 50 000 USD se poplatek za objednávku typu „limit“ („maker“) platí 0,16% z obchodované částky. Za objednávku typu „market“ („taker“) si burza účtuje 0,26%. Alternativní názvy v závorce vyjadřují, jak jsou dané typy obchodů nazývány v uživatelském rozhraní Krakenu. Při vyšším obchodním obratu (nad 50 000 USD) se procentuální poplatky za obchody postupně snižují.

Burza neměla během let provozu žádné větší skandály a problémy s hackery. Většina uživatelů také jistě ocení dnes již standardní dvoufázové ověřování pro přihlášení nebo provedení transakce. Dle uživatelských recenzí se jedná o spolehlivého poskytovatele s občasnou kritikou pomalých vkladů a výběrů fiat měny a nepříliš aktivní zákaznickou podporou. (36)

Tato burza by tak mohla být pro začínajícího obchodníka přijatelným kompromisem mezi úrovní anonymity, zabezpečením a příjemného uživatelského prostředí s podporou SEPA bankovních převodů bez poplatku s mobilní aplikací.

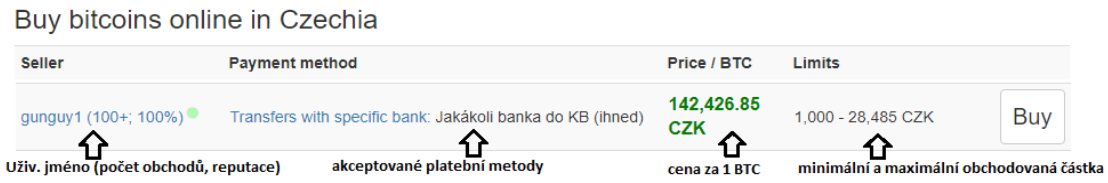
3.3.4 LocalBitcoins

LocalBitcoins je alternativní možnost pro nákupu Bitcoinu. Nejedná se přímo o klasický koncept burzy kryptoměn, ale spíše o inzertní portál, který propojuje zájemce a prodejce Bitcoinu pomocí platformy peer-to-peer. Celý web je pak koncipovaný jako velké tržiště, kde si uživatelé mohou vybrat nejvýhodnější nabídku z jejich okolí a domluvit se na formě provedení obchodu.

Obrázek 20 - Logo platformy LocalBitcoins (Zdroj: www.localbitcoins.com)

Přestože lze nabídky prodejců zobrazit i bez uživatelského účtu, pro provedení obchodu je nutné se zaregistrovat zadáním uživatelského jména a e-mailu. Po potvrzení ověřovacího e-mailu je možné plně využívat svůj účet a začít obchodovat. Není třeba provádět žádné ověření uživatele a způsob nákupu je vždy anonymní podle toho, jaké pravidla si obě strany mezi sebou dohodnou. (37)

Prvním krokem je vyhledání prodejců Bitcoinu v okolí. Zde si uživatel může vybírat z mnoha filtrů jako jsou akceptované platební metody, měna, lokalita prodejce nebo například jeho reputace za jeho historii transakcí. Případně lze prodávajícího před obchodem kontaktovat a domluvit se spolu takřka na čemkoliv. Uživatel si vybere nejvýhodnější nabídku a klikne na tlačítko „Buy“.



Obrázek 21 - Zobrazení uživatelské nabídky na platformě LocalBitcoins.com (Vlastní zpracování)

LocalBitcoins nabízí desítky metod převodu peněz na účet obchodníka. Mezi nimi nechybí platba na bankovní účet (ať už SEPA platba nebo platba na účet konkrétní banky), platba kreditní kartou i předání peněz v hotovosti na předem domluveném místě. Právě možnost osobního předání peněz je na této platformě unikátní. Všechny možnosti platby závisí také na tom, zda je daný obchodník podporuje.

Aby se předešlo podvodům na této platformě, každý uživatel má své reputační skóre, které se odvíjí od hodnocení ostatních uživatelů. Pokud uživatelé dokončí transakci, vzájemně se ohodnotí a získají tím větší reputační skóre. Pokud některý z účastníků nebyl s obchodem spokojen, může uživatele hodnotit i negativně. Pro zajištění vyšší bezpečnosti nabízí LocalBitcoin Escrow service, který zajistí, že odeslané prostředky budou připsány na účet obchodníka až poté, co kupec potvrdí úspěšnou směnu.

Mezi další bezpečnostní vylepšení patří služba sporů vedená společností LocalBitcoin pro případy, kdy mezi uživateli vznikne spor (např. kupující obdrží nižší částku, než byla dohodnuta). V neposlední řadě ani na této platformě nechybí možnost dvoufázového

ověření pro přihlášení nebo provedení transakce. Poplatek za provedení transakce je 1%. Tento poplatek je většinou hrazen prodávajícím. (38)

Výhodami platformy LocalBitcoins je bezesporu míra anonymity, podpora mnoha platebních metod a možnost nalézt nejvýhodnější nabídku ve svém okolí. Dále také uživatelská podpora a Escrow service, který má zajistit spravedlivé provedení obchodu. Na druhou stranu nízký poplatek za provedení transakce je často vykoupený méně výhodným směnným kurzem ze strany prodávajících. Také podpora pouze jedné kryptoměny (Bitcoin) může být pro mnoho uživatelů důvodem, proč službu nevyužít. Lze jej ovšem vyzkoušet spíše jako zajímavou alternativu k zavedeným, centralizovaným burzám a směnárnám s vysokou mírou anonymity.

3.3.5 Porovnání vybraných burz

Výše uvedené burzy kryptoměn si jsou často v mnoha prvcích podobné. Tudíž mohou hrát roli drobné rozdíly, které je uživatel schopen zjistit až při přímém porovnání. V následující tabulce je uvedeno několik důležitých parametrů, které jsou při volbě správné burzy rozhodující.

Tabulka 3 - Porovnání vybraných parametrů kryptoměnových burz (Zdroj: Vlastní zpracování)

	Binance	Coinbase Pro	Kraken	LocalBitcoins
Země původu	Japonsko	USA	USA	Finsko
Rok založení	2017	2012 (Původně jako GDAX)	2013	2012
Fiat měny	Ne	USD, EUR, GBP	USD, JPY, CAD	Dle nabídky prodejce (včetně nabídek v CZK)
Počet podporovaných kryptoměn	více než 110	19	Více než 20	1 (Bitcoin)
Možnost platby kartou online	Ne	Ano	Ne	Ano (pouze u učtitých nabídek)
Nutné ověření osobních dokumentů	Ne (pouze při vyšších objemech)	Ano	Ne (pouze při vyšších objemech)	Ne
Výše poplatku za transakci	0.1%	0.15% - 0.25%	0.16% - 0.26%	0.1%
Jiné výhody	Dvoufázová autentizace	SEPA platby, Dvoufázová autentizace	SEPA platby, Dvoufázová autentizace	Dvoufázová autentizace, Escrow service
Oficiální webové stránky	https://www.binance.com/	https://pro.coinbase.com	https://www.kraken.com	https://www.localbitcoins.com

Z tabulky lze zjistit, že výši poplatku za transakci 0,1% nabízí dva poskytovatelé - Binance i LocalBitcoins. Zde je ale potřeba zohlednit rozdílné fungování klasické burzy, služby pro vyhledávání prodejců Bitcoin v okolí a rozmanitost nabízených kryptoměn. Nabízí se zde spíše kombinace obou těchto služeb. Jelikož Binance nenabízí možnost vedení účtu v národní měně, uživatel si může koupit Bitcoin pomocí obchodníka na LocalBitcoins, kde může u některých typů nabídek zaplatit i v hotovosti. Zakoupené Bitcoiny lze převést na účet v platformě Binance a zde obchodovat za nízký transakční poplatek bez nutnosti ověření osobních údajů. Alternativou k převedení peněžních prostředků na kryptoměnový účet burzy může být také využití některé z výše uvedených směnáren, kde uživatel získá pravděpodobně i lepší směnný kurz.

Snadnějším řešením je využití služeb Coinbase Pro. V případě, kdy se jedná již o mírně pokročilého uživatele, který například nakoupil kryptoměny pomocí směnárny Coinbase a má zde založený a ověřený uživatelský účet, může s těmito prostředky zakoupenými pomocí směnárny začít jednoduše obchodovat na burze Coinbase Pro bez nutnosti jakéhokoliv dodatečného převodu klasické měny nebo kryptoměny. Pro uživatele, kteří Coinbase nemají a nechtějí odesílat své osobní údaje poskytovateli služeb, je zde burza Kraken. Za podobné poplatky jako u Coinbase je zde možnost obchodování na burze kryptoměn bez nutnosti ověření osobních dokladů. U obou z nich jsou podporovány evropské SEPA platby za nulové nebo minimální poplatky za provedenou platbu. Oběma těmto službám také hraje do karet delší doba působení na trhu oproti burze Binance.

ZÁVĚR

Technologie kryptoměn a jejich odlišný princip fungování je důkazem toho, že inovace technologického a finančního sektoru lze provádět ve vzájemném souznění. Důkazem toho jsou milióny aktivních uživatelů kryptoměn po celém světě. Mnoha lidem dopomohly až k pohádkovému bohatství, ale i k chudobě. V afrických a méně vyspělých zemích pomáhají k udržení minimálního finančního bohatství místních lidí. Ve vyspělých zemích jsou zase novým nástrojem k placení nebo obchodování.

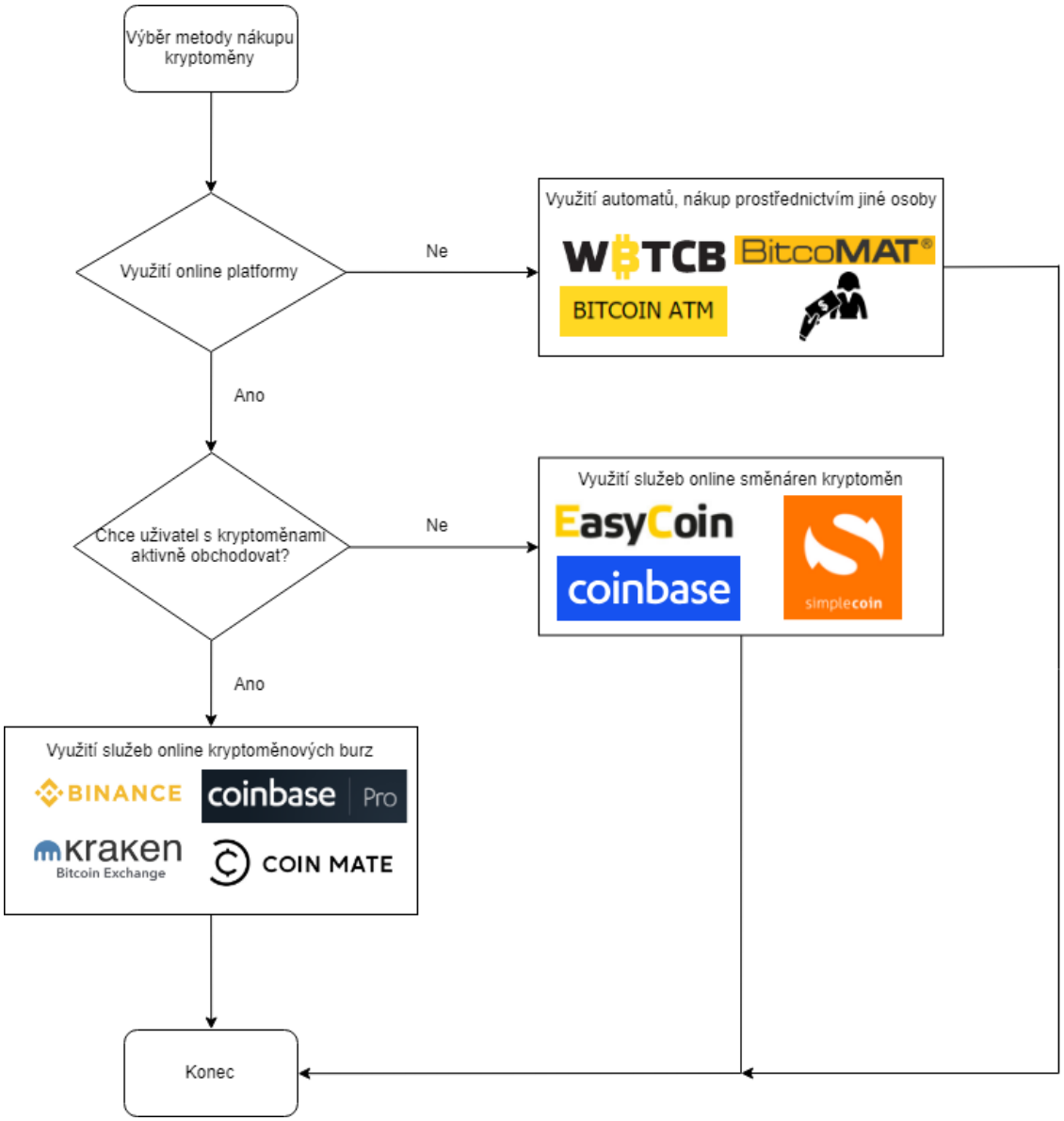
Teoretická část práce popsala základní fungování kryptoměnových sítí a měn. Nastíněn zde byl samotný uživatelský průběh transakce všech zúčastněných stran. Bylo také naznačeno fungování blockchainu, který je nedílným prvkem téměř každé kryptoměny.

V další části práce byla provedena analýza konkrétních a nejpoužívanějších virtuálních měn, kterým je věnována největší pozornost. Díky tomu je velmi jednoduché získat je využitím některé ze služeb uvedených v praktické části. Zde byla porovnávána řešení, které mají možnost uživatelé využít k získání, směně nebo obchodování.

Velmi jednoduchým způsobem, jak získat kryptoměnu bez většího bezpečnostního rizika, jsou kryptoměnové bankomaty. Toto řešení je vhodné pro kohokoliv, kdo si chce vyzkoušet fungování této moderní technologie na vlastní kůži. Není nic jednoduššího, než vyhledat nejbližší kryptoměnový bankomat a zakoupit si zde jednotky některé z podporovaných kryptoměn. Toto řešení není samozřejmě vhodné pro uživatele, kteří

chtějí kryptoměnu využívat každý den k placení nebo s ní obchodovat. To se odráží také na menší podpoře jednotlivých kryptoměn a méně výhodném směnném kurzu.

Dalšími porovnávanými službami byly kryptoměnové online směnárny. Zde byly vybrány jedny z nejrozšířenějších služeb a porovnávány napříč různými uživatelskými preferencemi. Za nejvhodnější řešení lze považovat zavedené platformy Coinbase a Kraken, které nabízí velmi nízké transakční poplatky, vysokou mírou zabezpečení a snadné uživatelské rozhraní včetně mobilní aplikace. Nevýhodou většiny takových služeb je omezený přístup k soukromým klíčům peněženek uživatele a nízká míra anonymity.



Obrázek 22 - Diagram volby metody k nákupu nebo obchodování kryptoměn (Zdroj: Vlastní zpracování)

Poslední oblastí byly kryptoměnové burzy. Ty jsou vhodné pro uživatele, kteří se rozhodli obchodovat s kryptoměnami a nabízejí jim tak často komplexní nástroje pro řízení svých investic v oblasti virtuálních měn. Vhodné jsou pro pokročilé a zkušené uživatele.

Ať už se uživatel rozhodne pro jakoukoliv variantu, vždy by měl mít na paměti, že kryptoměny jsou vysoce volatilní aktivum, se kterým je nutné nakládat velmi uváženě. Nákup velkého objemu v nevhodnou dobu tak může způsobit nemalé ztráty. To ovšem platí i naopak. Většina samotných služeb jsou často velmi mladými startupy, které se vezou společně na vlně boomu kryptoměn. Přestože není jisté, zda konkrétní virtuální měny a služby vydrží fungovat ve stávající podobě, decentralizované měny a sítě jsou technologií, se kterou je do budoucna nutné počítat.

SEZNAM POUŽITÝCH ZDROJŮ

(1) ANTONOPOULOS, Andreas. *Mastering Bitcoin: programming the open blockchain* [online]. Second edition. Sebastopol, CA: O'Reilly, 2017 [cit. 2018-11-20]. ISBN 978-149-1954-386.

(2) NARAYANAN, Arvind. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, 2016. ISBN 978-069-1171-692.

(3) VIGNA, Paul a Michael CASEY. *The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order*. New York: St. Martin's Press, 2015. ISBN 978-125-0065-636.

(4) DRESCHER, Daniel. *Blockchain basics: a non-technical introduction in 25 steps*. 1st ed. Berkeley, California: Apress, 2017. ISBN 14-842-2603-8.

(5) LIELACHER, Alex. 10 Awesome Uses of Cryptocurrency. *Brave NewCoin* [online]. Auckland: A Techemy company, 2018 [cit. 2019-04-27]. Dostupné z: https://bravenewcoin.com/insights/10-awesome-uses-of-cryptocurrency

(6) STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-80-271-0742-1.

(7) A Short History Of Bitcoin And Crypto Currency Everyone Should Read. *Forbes.com* [online]. New Jersey: Forbes Media, 2017 [cit. 2019-02-24]. Dostupné z: https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/

(8) Ethereum. *InvestPlus* [online]. InvestPlus, 2018 [cit. 2019-03-06]. Dostupné z: https://investplus.cz/kurzy/aktualni-kurz-ethereum-online-graf-kde-koupit-tezba-kryptomeny-cena-hodnota

(9) Blockchain: A Very Short History Of Ethereum Everyone Should Read. *Forbes.com* [online]. New Jersey: Forbes Media, 2018 [cit. 2019-03-06]. Dostupné z: https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/#48924f61e892

(10) Litecoin – zmrtvýchvstání podceňovaného altcoinu. *Btctip.cz* [online]. 2017 [cit. 2019-03-07]. Dostupné z: https://btctip.cz/litecoin-zmrtvychvstani-podcenovaneho-altcoinu/

(11) *Litecoin.org* [online]. 2011 [cit. 2019-03-07]. Dostupné z: https://litecoin.org/cs/

(12) Monero – Kurz, mining, graf a další. *Finex.cz* [online]. 2018 [cit. 2019-03-08]. Dostupné z: https://finex.cz/kryptomena/monero/

(13) Monero (XMR). *KRYPTOMAGAZIN.sk* [online]. 2018 [cit. 2019-03-08]. Dostupné z: https://kryptomagazin.sk/co-je-monero/

(14) MIKSA, Martin. Dash: populární kryptoměna, kterou se dá rychle platit a sama si financuje vývoj. *Živě.cz* [online]. Brno: CZECH NEWS CENTER, 2018 [cit. 2019-05-05]. Dostupné z: https://www.zive.cz/clanky/dash-popularni-kryptomena-kterou-se-da-rychle-platit-a-sama-si-financuje-vyvoj/sc-3-a-192565/default.aspx

(15) KWAASTENIET, Aat de. The nonsense of…. TPS (transactions per second). *Medium* [online]. Medium Corporation, 2018 [cit. 2019-03-16]. Dostupné z: https://medium.com/@aat.de.kwaasteniet/the-nonsense-of-tps-transactions-per-second-2d7156df5e53

(16) Češi se řadí mezi průkopníky v těžbě bitcoinu, ta ale bude generovat stále méně „mincí“. *E15.cz* [online]. Praha: CZECH NEWS CENTER a.s, 2018 [cit. 2018-11-20]. Dostupné z: https://www.e15.cz/bitcoin-tezba

(17) Kryptocelebrity – (11. díl) Marek Slush Palatinus, vizionář z Česka. *Kryptomagazin* [online]. Medial Base, 2018 [cit. 2018-11-20]. Dostupné z: https://kryptomagazin.cz/serial-kryptocelebrity-11-dil-marek-slush-palatinus-vizionar-ceska/

(18) *TĚŽBA KRYPTOMĚN: Jak těžit kryptoměny, princip, návratnost, návod na MINING* [online]. InvestPlus, 2018 [cit. 2018-11-20]. Dostupné z: https://investplus.cz/investice/tezba-kryptomen-jak-tezit-kryptomeny-princip-navratnost-navod/

(19) Cena elektřiny za kWh v roce 2018 poskočila na 4,1 Kč. Proč koukat i na jiné částky?. *Elektřina.cz* [online]. Praha: Ušetřeno.cz, 2018 [cit. 2018-11-25]. Dostupné z: https://www.elektrina.cz/cena-elektriny-za-kwh-2018-cez-eon-pre-a-jini-dodavatele-elektriny

(20) Těžba kryptoměn na Islandu spotřebuje víc energie, než domácnosti. *Kryptomagazin.cz* [online]. Medial Base, 2018 [cit. 2018-11-28]. Dostupné z: https://kryptomagazin.cz/island-tezba-kryptomen-ziskava-popularite/

(21) JAK KOUPIT KRYPTOMĚNY – kde provést nákup, burzy a směnárny, návod. *Investplus.cz* [online]. InvestPlus.cz, 2018 [cit. 2019-01-06]. Dostupné z: https://investplus.cz/investice/jak-koupit-kryptomeny-kde-provest-nakup-burzy-a-smenarny-navod/

(22) Intradenní obchodování: Průvodce do začátků. *Lynx Broker* [online]. Praha: Lynx Czech Republic, 2018 [cit. 2019-01-06]. Dostupné z: https://www.lynxbroker.cz/vzdelavani/intradenni-obchodovani-pruvodce-pro-zacatecniky/

(23) Nejlepší směnárny kryptoměn – kde nakoupit Bitcoin a jiné kryptoměny. *Crypto Svět* [online]. CryptoSvet.cz, 2017 [cit. 2019-01-13]. Dostupné z: https://cryptosvet.cz/nejlepsi-smenarny-kryptomen-kde-koupit-bitcoin-a-jine-kryptomeny/

(24) Jak vybrat peníze za bitcoiny z automatu. V Praze, Brně a dalších městech krok za krokem. *Živě* [online]. Brno: CZECH NEWS CENTER, 2017 [cit. 2018-12-02]. Dostupné z: https://www.zive.cz/clanky/jak-vybrat-penize-za-bitcoiny-z-automatu-v-praze-brne-a-dalsich-mestech-krok-za-krokem/sc-3-a-190703/default.aspx

(25) Best Cryptocurrency Exchanges: The Ultimate Guide. *Blockgeeks* [online]. 2019 [cit. 2019-03-20]. Dostupné z: https://blockgeeks.com/guides/best-cryptocurrency-exchanges/

(26) *EasyCoin* [online]. Praha, 2018 [cit. 2018-12-03]. Dostupné z: https://www.easycoin.cz

(27) *Simple Coin* [online]. Praha, 2018 [cit. 2019-01-04]. Dostupné z: https://exchange.simplecoin.eu/

(28) Simplecoin návod – rychlá platba bez registrace. *Kryptomagazin.cz* [online]. Medial Base, 2018 [cit. 2019-01-04]. Dostupné z: https://kryptomagazin.cz/simplecoin-navod-rychla-platba-bez-registrace/

(29) *Coinbase* [online]. California, 2019 [cit. 2019-03-20]. Dostupné z: https://www.coinbase.com

(30) Changelly Review and Comparison From Changelly Review (2019 Updated). *99bitcoins* [online]. Trivex, 2019 [cit. 2019-03-26]. Dostupné z: https://99bitcoins.com/bitcoin-exchanges/changelly-review/

(31) *Changelly* [online]. 2019 [cit. 2019-03-26]. Dostupné z: https://changelly.com

(32) Místa, kde se protočí miliardy. Seznamte se s burzami kryptoměn a jejich fungováním. *E15* [online]. Praha: CZECH NEWS CENTER, 2018 [cit. 2019-03-31]. Dostupné z: https://www.e15.cz/burza-kryptomen

(33) *Binance* [online]. 2019 [cit. 2019-04-02]. Dostupné z: https://www.binance.com/en

(34) *Coinbase Pro* [online]. Kalifornie, 2019 [cit. 2019-04-02]. Dostupné z: https://pro.coinbase.com

(35) *Kraken* [online]. San Francisco, 2018 [cit. 2019-04-04]. Dostupné z: https://www.kraken.com

(36) Kryptoměnová burza Kraken – recenze, zkušenosti, návod, poplatky, diskuze. *InvestPlus* [online]. Praha: InvestPlus, 2019 [cit. 2019-04-04]. Dostupné z:

https://investplus.cz/investice/kryptomenova-burza-kraken-recenze-zkusenosti-navod-poplatky-diskuze/

(37) *LocalBitcoins* [online]. Helsinki, 2019 [cit. 2019-04-06]. Dostupné z: https://localbitcoins.com/

(38) Recenze LocalBitcoins – kde koupit Bitcoin?. *CryptoSvet.cz* [online]. 2017 [cit. 2019-04-06]. Dostupné z: https://cryptosvet.cz/recenze-localbitcoins/

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ