VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

KRYPTOMĚNY A JEJICH PENĚŽENKY

CRYPTOCURRENCY WALLETS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Tomáš Mařík
AUTHOR

VEDOUCÍ PRÁCE — Ing. Jan Luhan, Ph.D., MSc
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Tomáš Mařík**
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 jejich peněženky

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:

Posoudit investiční a technologický potenciál kryptoměn na základě technické, ekonomické a právní analýzy se zaměřením na analýzu a výběr vhodné krypto–peněženky dle konkrétních požadavků s užším zaměřením na měnu Bitcoin.

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.

CHAFFEY, D. Digital Business and E-commerce Management. 6th ed. Harlow: Pearson, 2015. 679 p. ISBN 978-0-273-78654-2.

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

Cílem práce je posouzení investičního a technologického potenciálu kryptoměn na základě jejich technické, ekonomické a právní analýzy. Práce se zabývá kryptoměnami, analýzou a výběrem peněženky.

Klíčová slova

Kryptoměna, Bitcoin, blockchain, virtuální peněženka, trezor

Abstract

The aim of the thesis is to assess investment and technological potential cryptocurrencies on the basis of their technical, economic and legal analysis. The work deals cryptocurrencies, analysis and wallet selection.

Key words

Cryptocirreny, Bitcoin, blockchain, virtual wallet, safe

Bibliografická citace

MAŘÍK, Tomáš. *Kryptoměny a jejich peněženky* [online]. Brno, 2019 [cit. 2019-05-12]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119817. 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 12. května 2019

……

podpis studenta

Poděkování

Tímto bych chtěl poděkovat panu Ing. Janu Luhanovi Ph.D., MSc za vedení bakalářské práce a poskytnutí potřebných rad a svých dlouholetých zkušeností.

V Brně dne 12. května 2019 .....

podpis autora

OBSAH

ÚVOD

Kryptoměny jsou vynálezem posledních let. Zastřešují několik oborů: ekonomie, finance a informační technologie. Lidé jejich potenciál využívají hlavně ke zhodnocení svých financí. Kryptoměny budou mít bezpochyby dopad na celý svět a ovlivní fungování financí ve společnosti.

Bakalářská práce se nejprve zaměřuje na kryptoměny obecně, popisuje získávání kryptoměn, jejich vývoj a vznik první kryptoměny Bitcoin. Popisuje fungování blockchainu a jeho jedinečnost.

Práce analyzuje Bitcoin i obecně kryptoměny z pohledu právní úpravy, jejich budoucího vývoje a poukazuje na možné budoucí využití Blockchainu.

V závěrečné části se práce zaměřuje na krypto-peněženky. Poukazuje na jejich výhody rizika.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem práce je přiblížit fungování kryptoměn, na jakém principu jsou založeny, co umožnilo jejich vznik a důvody jejich rostoucí obliby. Převážně se práce zaměřuje na Bitcoin. Dále je v práci popsán způsob získávaní kryptoměn. Analýza obsahuje předpokládaný budoucí cenový vývoj Bitcoinu a využití potenciálu blockchainu v dalších odvětvích. Hlavním cílem je informovat o různých způsobech uložení a udržování vlastnictví kryptoměn, rizika a bezpečnosti jednotlivých peněženek.

Tvorbě bakalářské práce předcházelo teoretické studium kryptoměn. Autor práce se účastnil několika seminářů, kde získával potřebné zkušenosti a rady od odborníků.

1 TEORETICKÁ VÝCHODISKA PRÁCE

Tato část bakalářské práce se bude zabývat fungováním blockchainu, popisu těžby a samotným kryptoměnám.

1.1 Virtuální měna

Virtuální neboli digitální měnu můžeme charakterizovat jako měnu, která je vytvořena elektronicky. Vznikaly původně spíš jako programátorský teoretický koncept decentralizované nepadělatelné a neovlivnitelné měny, v současné době však existují stovky virtuálních měn (můžeme též nazývat jako digitální měny nebo kryptoměny), které mohou mít několik praktických využití, nejčastěji jako investiční nástroj či platidlo. Jako platidlo se používá mnohem méně, většina lidí spíše vidí ve virtuálních měnách skryté bohatství a možnost snadného obohacení díky rychlému vývoji kurzu, proto do nich ve většině případů investují a snaží se přijít na způsob, jak je co nejlépe zhodnotit. (3)

Základní vlastností těchto měn je transparentnost, to znamená, že veškeré provedené transakce jsou veřejné a každý může na tyto transakce nahlédnout v databázi zvané blockchain, ke které se dostaneme později. Další, velmi pozitivní vlastností, jsou minimální nebo žádné poplatky za provedené transakce. Kryptoměny byly navrženy tak, aby transakční poplatky byly co nejnižší, což je opak klasických bankovních transakcí.

Jednotlivé kryptoměny se od sebe navzájem samozřejmě mohou lišit, např. hodnotou, poplatky či využitím. (4)

	KRYPTOMĚNA	SYMBOL	KURZ	ZMĚNA (24H)	TRŽNÍ KAPITALIZACE	GRAF VÝVOJE (7D)	
	Bitcoin	BTC	$ 6287.05	3.59%	$ 111,703,316,933		Obchodovat
	Ethereum	ETH	$ 173.01	1.14%	$ 18,366,711,081		Obchodovat
	Ripple	XRP	$ 0.2976	-0.35%	$ 12,607,329,867		Obchodovat
	Bitcoin Cash	XBC	$ 285.71	0.37%	$ 5,125,680,733		Obchodovat
	Litecoin	LTC	$ 75.62	2.84%	$ 4,733,678,931		Obchodovat
	EOS	EOS	$ 4.89	-0.99%	$ 4,425,027,794		Obchodovat
	Tether	USDT	$ 1	-0.04%	$ 2,780,165,812		Obchodovat

Obrázek 1: Kryptoměny podle tržní hodnoty
(Zdroj: 12)

Všechny virtuální měny mají však jedno společné – fungují na principu peer-to-peer sítě. Peer-to-peer síť je označení pro typ sítí, ve kterých spolu komunikují jednotliví uživatelé bez užití serveru, nepoužívá tedy server jako prostředníka v komunikaci mezi počítači. Veškeré počítače jsou tedy navzájem propojené. (4)

Za výhodu virtuálních měn lze považovat to, že jsou naprosto decentralizované. Decentralizace znamená, že nad žádnou kryptoměnou nemá moc stát ani žádní jiní jednotlivci. Není tedy možno měnu padělat či jakkoliv ovlivňovat. (4)

1.2 Blockchain

Od začátku existence internetu byly tendence o vytvoření virtuální měny. Kryptografové, bankéři, ekonomové a podnikatelé hledali způsob, jak přijít s konceptem, který by byl životaschopný. Největším problémem virtuální měny je možnost duplikace, virtuální měna je pouze digitální informace, což znamená, že by se tato informace dala duplikovat a touto virtuální měnou zaplatit vícekrát. Toto byl zásadní problém při vývoji digitální měny. Tento problém by se dal vyřešit existencí centrální autoritou, které by uživatelé důvěřovali. U centrální autority nastává problém, že v případě útoku se centrální server dá zničit nebo by server mohla odstranit sama vláda, které by se měna znelíbila, v případě by mohla zasahovat do vývoje kurzu. Těmto problémům chtěli vývojáři předejít vytvořením decentralizovaného systému. (1)

Autor proto vytvořil tzv. blockchain, což je jakási účetní kniha, která je veřejná a sdílená všemi uživateli. Každý uživatel potvrzuje transakce stejně jako u centrální autority jen v případě digitální měny decentralizovaně. Každý uživatel si může stáhnout databázi záznamů a vidět každou transakci v historii. Díky systému veřejně uložených záznamů o transakcích si každý uživatel může všimnout, že nějaký podvodník se snaží zaplatit něčím, co nevlastní. (3)

V případě uskutečněné transakce, která je v dostatečném počtu potvrzena na blockchainu, nemůže dojít k vrácení transakce. Banka má vždy nějakou pojistku stornování transakce pro případ, že bychom transakci spletli a poslali finance na jiny účet. Kryptoměny žádnou pojistku nemají a pokud se tedy při převodu spleteme, tak už svoje coiny nikdy nedostaneme zpět. (3)

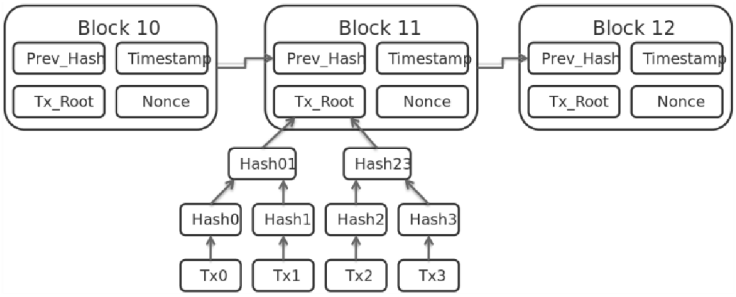
Přes blockchain se utrácí coiny bez nutnosti jakéhokoliv účtu nebo verifikace, nákupy jsou tedy anonymní, neexistuje žádná centrální instituce, která by prostředky ovládala. Naši jedinou identifikací na síti blockchain jsou dlouhé adresy, kterých může mít každý uživatel neomezené množství. Pro založení adresy nepotřebuje žádný doklad a nikdo tedy neví, kolik a jakých coinů uživatel vlastní. Blockchain zaznamenává všechny operace na každé adrese a v případě zájmu si každý uživatel může tedy stáhnout blockchain a podívat se kolik jakých operací bylo na jaké adrese provedeno. (3)

Historie virtuálních měn není dlouhá, ale od vzniku blockchainu dochází k velkému boomu v tomto odvětví.

Blockchain pomohl vyřešit několik problémů, a to:

- znemožňuje kopírování peněz,
- zabraňuje dvojité útratě,
- pomáhá s důvěrou na P2P síti,
- ověřuje a podepisuje transakce. (3)

Blockchain je spojový seznam bloků. Blok je nejdůležitější datovou strukturou coinového protokolu. Blok kóduje množinu transakcí, ty svým zahrnutím potvrzuje. Jedna z transakcí v boku je generující a pouze touto vlastností vznikají nové coiny. Tento takzvaný validní blok je velice náročné na výpočetní výkon díky svým kryptografickým vlastnostem. Každý takto zapsaný vygenerovaný block obsahuje hashe předchozího blocku. Hash výstup hashovací funkce, matematické funkce, (resp. Algoritmus), pro převod vstupních dat na malé číslo. Každý blok má jednoznačně zapsaného svého předka.(4)



Obrázek 2: Obsah bloků
(Zdroj:10)

Popis obsahu bloků v blockchainu:

- Timestamp – čas, kdy byl blok vytvořen
- Prev_hash – odkaz na hash předcházejícího bloku
- Tx_root – Zde se nachází seznam všech transakcí, obsažených v bloku. Blok musí obsahovat minimálně jednu transakci, zvanou Coinbase a v ní jsou zapsány nově vytěžené coiny.
- Nonce – náhodné číslo které slouží k odlišení bloku.(3)

1.3 Typy virtuálních měn

Virtuální měna si lze představit jako řetězec digitálního kódu, který obsahuje určitou hodnotu, která v určitém systému slouží k nákupu statků a služeb. Nejvíce známou a používanou měnou je Bitcoin, ale není vše samozřejmě jen o Bitcoinu. Vzhledem k tomu, že zdrojový kód této digitální měny je volně k dispozici, každý má možnost ho předělat, upravit, pozměnit nebo udělat jeho kopii. Díky tomuto aspektu na světě vzniklo a vzniká nespočetné množství virtuálních měn. (5)

Dnes už můžeme i bez velké námahy najít několik kryptoměn, které se zhodnocují lépe než Bitcoin. Byl to ale právě Bitcoin, který dalším měnám vydláždil cestu – nesmíme

proto zapomenout, že i když se v souvislosti s Bitcoinem neustále dočítáme o různých konspiračních teoriích, bublinách či úpadku, jedná se stále o největší „jistotu“ světa kryptoměn. Nyní se podíváme na další kryptoměny. (5)

1.3.1 Litecoin

Litecoin je decentralizovaná virtuální měna, která funguje na stejném principu jako Bitcoin, ke kterému se dostaneme později. Litecoin začal jako první ze všech kryptoměn využívat algoritmus Scrypt, což je speciální hardware na těžení virtuálních měn. Tento způsob těžení později začala používat velká spousta dalších digitálních měn, Litecoin tedy nese velkou zásluhu na vzniku nových měn jako je např. Dark Coin. Množství Litecoinu je omezeno na 54 milionů, přičemž v prosinci 2018 bylo již vytěženo cca 60 milionů mincí. (5)

Jeden Litecoin má momentálně hodnotu přibližně 705 Kč.

Obrázek 3: Logo Litecoin
(Zdroj:13)

1.3.2 Peercoin

Tato měna byla vytvořena v roce 2012 a od ostatních měn se liší tím, že nemá definovaný přesný počet mincí. Využívá algoritmus Proof of Stake (PoS), který funguje na principu toho, že čím více digitálních peněz daná osoba vlastní (zpravidla Bitcoiny nebo altcoiny), tím více virtuálního jmění může vytěžit. (15)

Jeden Peercoin je momentálně přibližně 22Kč.

Obrázek 4: Logo Peercoin
(Zdroj:14)

1.3.3 Namecoin

Další známou virtuální měnou je Namecoin. Tato měna byla vytvořena jako decentralizované DNS (Domain name system), což je systém doménových jmen, který slouží k vyměňování informací, např. IP adres uzlů sítě. Později tento systém začal fungovat i jako např. elektronická pošta. (5)

Jeden Namecoin má momentálně hodnotu přibližně 46 Kč.

Obrázek 5: Logo namecoin
(Zdroj:16)

1.3.4 Ethereum

Ethereum je další ze známých a velmi používaných kryptoměn, která se dostává stále více do popředí digitálního světa. Bitcoin je etherem stále více nahrazován. Zakladatelem této měny je Vitalik Butarin, který tuto síť virtuální měny spustil v polovině roku 2015. Rozdíl mezi Bitcoinem a Ethereuem je tedy takový, že Ethereum je řízeno centrálně, má přesně

danou strukturu a plán, což se dá považovat za výhodu, především co se investic do této měny týče. (5)

Ethereum má narozdíl od ostatních měn jednu velkou výhodu – nadaci Ethereum Foundation. Tuto nadaci si můžeme představit jako formu fondu, kam pro rozvoj Etherea přispívají největší firmy z oblasti IT a internetu, jako např. Google či Microsoft. Hodnota Etherea tak díky nejen Ethereum Foundation, ale především práci a investicím drobných těžařů v letošním roce silně roste. (5)

Kurz se nyní pohybuje okolo 2400Kč, jeho kurz prošel za poslední rok pádem, v lednu 2018 jeho cena byla kolem 30 000Kč.

Obrázek 6: Logo ethereum
(Zdroj:17)

1.4 Bitcoin

Nejznámější a zároveň nejpoužívanější digitální měnou je Bitcoin, jedná se zároveň o stejnojmennou internetovou platební síť. Tato síť je veřejně dostupná a funguje na principu již zmíněné peer-to-peer sítě. Bitcoin nepodléhá žádné centrální bance, tato měna je zcela decentralizovaná, neexistuje tedy žádná instituce, která by nad Bitcoinem měla moc nebo ji mohla jakkoliv ovlivňovat. (3)

Konečný počet Bitcoinů v oběhu je předem znám, bylo stanoveno, že poslední se mají dostat do oběhu v roce 2140 a mělo by jich být vytvořeno celkem 21 milionů. (3)

V případě, že by někdy v budoucnu hodnota Bitcoinu dosahovala extrémně vysoké částky za jednotku je možné využít dělitelnosti Bitcoinu. Díky této dělitelnost je možné mít ve své peněžence jenom například 0.000001 BTC a používat tuto sumu k placení.

Před investicemi do virtuálních měn však v době jejich největšího rozmachu varovala největší německá banka Deutsche Bank, která tyto investice označila za vysoce rizikové kvůli jejich nadměrným výkyvům a kvůli tomu, že jsou neregulované. (3)

Bitcoin je založen na dvou fundamentálních technologiích z kryptografie. První je asymetrická kryptografie. Pro šifrování a dešifrování se používají dva odlišné klíče, privátní a veřejný. Veřejný klíč slouží k ověřování uživatele. Je to jako bychom měli schránku, kdokoliv může do schránky něco vložit, uzamknout ji svým veřejným klíčem. Otevřít ji a vybrat co se v ní nachází ovšem dokáže pouze vlastník privátního klíče. Pokud uživatel ztratí privátní klíč, ztratí vše, co bylo tímto klíčem asociováno. Privátní i veřejný klíč jsou v matematickém vztahu, veřejný klíč má korespondující privátní klíč. K poslání transakce ji musíme digitálně podepsat privátním klíčem. Digitálním podpisem se uživatel nemusí zabývat, to obsluhuje uživatelské rozhraní. (1)

Druhá používána technologie je kryptografické ověřování transakcí, transakce se musí řídit pravidly protokolu Bitcoinu. Nepovolují se transakce, které mají například špatnou syntaxi či špatnou velikost. (1)

Obrázek 7: Logo Bitcoin
(Zdroj:18)

1.4.1 Zakladatel Bitcoinu

Za autora Bitcoinu je považován Satoshi Nakamoto. Satoshi Nakamoto je pseudonym osoby nebo skupiny lidí, kteří stojí za vytvořením Bitcoinu. Přikládá se jim také návrh

první blockchainové databáze, bez které by Bitcoin nemohl vzniknout. Není známa skutečná identita osoby, která za založením stojí, existuje však několik teorií. (4)

Satoshi v překladu z japonštiny znamená „moudrý" nebo „jasné myšlení". Jako první teorie byla, že Satoshi je muž okolo 37 let s japonskými kořeny, to však podnítilo celou řadu pochybností, neboť software i veškeré dokumenty týkající se Bitcoinu jsou pouze v angličtině. (4)

Dále se spekuluje, že Satoshi je zkrátka skupina spolupracovníků, která stojí za vydáním této měny, z toho vznikla myšlenka, že je to kolektivní pseudonym skupiny lidí. (4)

Ve zdrojovém kódu i různých komentářích Satoshi používá britskou angličtinu, s největší pravděpodobností se tedy jedná o někoho z Commonwealthu, může to být tedy někdo z Británie, Irska, Nového Zélandu, Austrálie či Jižní Afriky. (4)

Švýcarský kodér a aktivní člen komunity digitálních měn Stefan Thomas vytvořil graf s časovými údaji příspěvků od Satoshiho na diskuzním fóru (který zahrnuje více než 500 jeho příspěvků) a výsledek ukázal, že pokud je to s osoba s běžnými spacími návyky, s největší pravděpodobností se nachází v časovém pásmu UTC−05 nebo UTC−06. Tyto pásma odpovídají východní části Severní Ameriky, Střední Ameriky, Karibiku a části Jižní Ameriky. (4)

V prosinci roku 2015 vydal australský časopis Wired článek, ve kterém je za zakladatele Bitcoinu považován australský podnikatel Craig Steven Wright, který se k tomu později i přiznal. (4)

Podle britské televizní stanice BBC poskytl technické důkazy, které dokládají jeho tvrzení. Jako důkazní materiál použil mince, o kterých je známo, že je vlastní pouze zakladatel Bitcoinu. (4)

Zveřejněním své identity doufá, že tím zastaví spekulace o tom, kdo je Satoshi Nakamoto. Ačkoliv teorie o tom, že Craig Wright je skutečným zakladatelem této virtuální měny, je nejvíce uvěřitelná, britský týdeník The Economist o tom není zcela přesvědčen. (4)

1.4.2 Vývoj kurzu

Cena Bitcoinu neustálé snižuje a zase zvyšuje, a tak hodnota Bitcoinu neustále kolísá. Dlouhou dobu probíhají spekulace o tom, co se zapříčiňuje hodnotu Bitcoinu. Největším mýtem je domněnka, že cena Bitcoinu je určena počtem uživatelů, kteří Bitcoin těží, tedy čím více uživatelů těží, tím se zvyšuje cena měny. Stoupající cena měny zvyšuje počet těžařů, to znamená, že tito uživatelé nemohou ovlivňovat skutečnou hodnotu. Nejpravděpodobnější teorie tedy je, že kurz této měny závisí především na poptávce a nabídce na trhu, tak jako tomu je u každé jiné měny. (4)

Obrázek 8: Vývoj kurzu Bitcoinu
(Zdroj:21)

V uvedeném grafu můžeme vidět vývoj kurzu od roku 2013 do roku 2019 (cena Bitcoinu je uváděna v USD). Jak je z grafu zřejmé, největší nárůst a následný propad měny byl mezi léty 2017 a 2018, kdy se cena kurzu přiblížila hodnotě 20 000 USD.

Momentálně by se obecně dalo říct, že hodnota Bitcoinu klesá, i když se občas objeví nějaký krátkodobý nárůst.

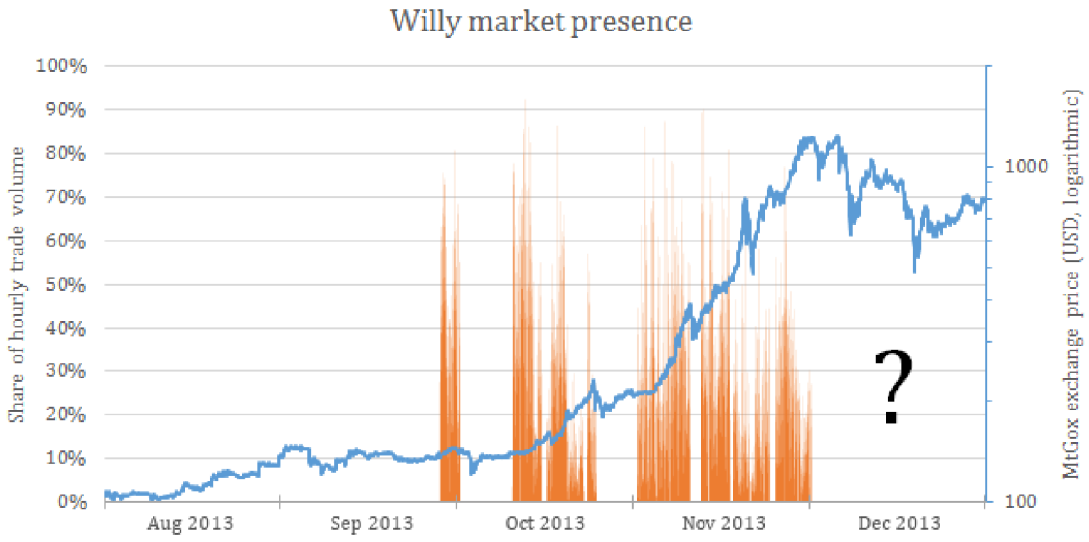
Co se historie Bitcoinu týče, v roce 2010 to byla čistě záležitost jisté skupiny nadšenců a hodnota byla prakticky nulová, možnost platby touto měnou byla velmi omezená. Historicky první platba údajně proběhla v květnu 2010 - jednalo se o dvě pizzy v hodnotě 10 000 BTC (pro představu dnes by to bylo v přepočtu zhruba 770 000 000 Kč). (4)

Zatímco rok 2017 byl pro kryptoměny velmi úspěšný, začátek roku 2018 pro ně nebyl vůbec příjemný. Prakticky všechny měny v lednu 2018 začaly ztrácet na své hodnotě, Bitcoin ztratil na své hodnotě nejvíce za tři roky, nicméně zatím si stále drží poměrně vysokou hodnotu. Příčiny mohou být různé, nejpravděpodobnější teorie je ta, že se trhy obávají regulace obchodů po oznámení jihokorejského ministra financí, že země stále zvažuje zákaz obchodu s kryptoměnami. (5)

Další nejistoty vyvolaly úvahy o tom, že virtuální měny se stanou zakázanými v Číně, což je momentálně největší těžařská velmoc. V Číně vzrostly obavy, že by tamní vláda mohla požádat o regulaci z důvodu nadměrné spotřeby energie při těžbě. I tento fakt může být v Číně jeden z důvodů, proč se uvažuje o zákazu digitálních měn.

Dalším zajímavým faktem o růstu kurzu Bitcoinu je informace, že největší nárůst ze 150 USD na 1000 USD byl zmanipulovaný. Studie o možnosti manipulaci s virtuálními měnami byly podrobně rozebrány ve vědeckém časopise Journal of Monetary Economics, kde autoři článku přišli na to, že takový růst by se dal „uměle vyvolat" za necelé dva měsíce. (22)

V této studii se píše, že zmanipulovat tento velký cenový skok lze pomocí falešných obchodů na Bitcoinové burze MT GOX, kde se obchodovala normální měna za virtuální. Čím více se obchodovalo, tím více kurz stoupal. Během těchto falešných obchodů stoupala cena kurzu o 4% za den. Pak nastala doba, kdy burza ležela bez jakékoliv manipulace a tak hodnota Bitcoinu začala zase zpátky klesat. Princip tohoto falešného obchodování spočíval v napadení této burzy hackery. Prodávající přišel o své Bitcoiny, ale nic za ně nedostal. Tyto akce, které měly za úkol vylákat z kupujících virtuální jmění, prováděly softwarové automaty. Ty měly dokonce vlastní názvy – automat, který byl ve falešných obchodech nejvíce aktivní, měl název Willy. Tyto automaty si stanovovaly za virtuální měny stále vyšší a vyšší částky peněz. Mezi únorem a zářím v roce 2013 odcizily lidem přes 500 000 Bitcoinů, důvodem pro falešný obrovský nárůst kurzu byl tedy pravděpodobně čistě finanční motiv. Podle dohadů odborníků za tímto vším stojí jeden člověk, jehož jediným cílem byla krádež Bitcoinů a moc manipulovat s kurzem. Podle mého názoru nikdy nebude možné pravého pachatele dohledat, největší podezření zatím však padá na samotného provozovatele této burzy Marka Karpelese. (22)



Obrázek 9: Růst Bitcoinu při falešném obchodování
(Zdroj:22)

Na obrázku můžeme vidět reálné tempo růstu Bitcoinu vzhledem k obchodování na burze (zobrazeno modře) a působení automatu (robota) Willyho. Tento robot nakupoval 10-20 Bitcoinů každých 5-10 minut, obchodoval jen v dolarech a nikdy žádné Bitcoiny neprodal. (22)

Celá tato burza později zkrachovala a bylo z ní ukradeno zhruba 6% veškerých vytěžených Bitcoinů. Provozovatelé burzy později upřesnili, že všichni klienti přišli celkem o 850 000 BTC včetně těch burzy, v tehdejším kurzu to byla škoda přibližně 9,5 miliardy korun. Investoři své peníze už pravděpodobně nikdy neuvidí, protože Bitcoiny nejdou dohledat. (22)

Výzkumníci proto varují: „Jelikož své finance investuje do kryptoměnových aktiv už i hlavní proud investorů a země přistupují k legalizaci Bitcoinu jako platebního systému (jak se to stalo v Japonsku v dubnu 2017), je důležité pochopit, jak jsou trhy s kryptoměnami náchylné k manipulaci.” (22)

V následujících bodech se můžeme podívat na několik mezníků při vývoji Bitcoinu v průběhu posledního desetiletí:

- 1/2009 - nulová cena BTC, téměř žádný trh neexistoval
- 2/2011 - BTC dosáhl hodnoty 1 $
- 6/2011 - první velký nárust kurzu, BTC v hodnotě 31$
- 4/2013 - cena BTC vzrostla na 266 $

- 11/2013 - BTC překročil hranici 1000 $
- 1/2015 - BTC klesl na 152 $
- 1/2017 - BTC vzrostl na zatím nejvyšší cenu 1 022 $
- 5/2017 - hodnota 1 BTC překonala 2 000 $
- 8/2017 - cena se pohybuje okolo 3 000 $
- 10/2017 - BTC se vyšplhal až na 6 000 $
- 11/2017 - hodnota přesáhla 11 200 $
- 12/2017 - cena se pohybuje nad 18 700 $ (cca 411 400 Kč)
- 1/2018 - cena spadla až na 11 425 $
- 11/2018 - cena spadla pod 6 000 $
- 1/2019 - cena spadla pod 4 000 $

1.4.3 Těžba

Těžba Bitcoinů, neboli mining, je způsob „výroby" této měny. Těžbu virtuální měny můžeme také vysvětlit jako potvrzování správností transakcí v síti. Mining je poměrně náročná a nákladná investice s nejistou návratností. (3)

V prvopočátcích se pro těžení používaly procesory počítače. Stačilo spustit speciální program a počítač se pustil do práce. Tento způsob těžení se v dnešní době už vůbec nepoužívá a to kvůli jeho neefektivnosti (vysoká spotřeba elektřiny za minimum Bitcoinů). Tím, že uživatelé pro těžbu Bitcoinu používali svůj osobní PC, byla zároveň i vyřešena otázka distribuce měny mezi širší spektrum uživatelů. (3)

Dalším způsobem byla těžba pomocí grafické karty v PC. Přišlo se totiž na to, že je to podstatněji efektivnější metoda těžby. Grafické karty se používaly poměrně dlouho, nicméně pak je nahradily tzv. ASIC jednotky, což je v dnešní době, kromě speciálních a velmi výkonných grafických karet, jediný způsob výroby měny. ASIC jednotky jsou specializované stroje pro těžení Bitcoinů. Jedná se vlastně o procesory, které jsou navrženy tak, aby měly co nejnižší spotřebu elektřiny a zároveň co nejvyšší výkon. (3)

Jelikož se Bitcoin stává stále více používanějším, začaly vznikat tzv. těžební farmy. Tyto farmy se vyskytují převážně v Číně, kde zároveň probíhá velkovýroba ASIC přístrojů potřebných k těžbě. Čína je vhodná pro velkotěžbu Bitcoinů zejména proto, že je tam

levná elektřina, dobrá dostupnost ke příslušnému HW a neplatí se clo nebo DPH při odeslání mimo kontinent. (3)

Těžba Bitcoinů se stává stále populárnější záležitostí, a proto se tyto speciální HW a grafické karty stávají nedostatkovým zbožím, za minulý rok vzrostla poptávka po tomto druhu zboží až o 700%. „Díky těžení kryptoměn nastal celosvětový problém v dodávkách grafických karet. V této souvislosti pozorujeme značné zvýšení poptávky a nákupu hotových skladových sestav," prohlásila mluvčí Alzy Patricie Šedivá. I spousta dalších obchodů se specializací na výpočetní techniku evidují nárůsty poptávky po grafických kartách. „Růst prodeje tohoto zboží zaznamenáváme až do takové míry, že velká část sortimentu je momentálně vyprodaná a vzhledem ke stavu trhu ve světě se nezdá, že by se tato situace měla v dohledné době nějak výrazně změnit. I tak ale sledujeme možné příležitosti pro nákup zboží v zahraničí, abychom uspokojili poptávku hráčů i těžařů", prohlásila tisková mluvčí internetového obchodu CZC.cz v roce 2018. (6)

Samozřejmě existuje i několik nadšenců do kryptoměn, kteří se rozhodli těžit si měny sami z pohodlí svého domova. Není to nic složitého, jen je potřeba pořídit si na to kvalitní a specializovaný hardware, rozmyslet si, jakou měnu chce vlastně těžit a samozřejmě stáhnout si program pro těžbu. (6)

Český internetový obchod Alza.cz a. s. se stal velkým podpůrcem Bitcoinu a jeho uživatelů. Kromě toho, že je možno tam nakoupit veškeré zboží za digitální měny, prodává také příslušenství pro těžbu a používání Bitcoinů (Bitcoin trezory, HW pro těžbu, procesory, grafické karty…). (6)

Obrázek 10: Težba grafickými kartami
(Zdroj:11)

Při těžbě Bitcoinu je důležité narazit na tzv. blok. Blok je zpracované uskupení velkého množství transakcí, jehož výsledkem je „hash", což je stručně řečeno obrovské číslo.

Cílem je, aby byl tento hash co nejnižší, a to kvůli jeho složitým výpočtům. Mineři mezi sebou soupeří o to, kdo první najde co možná nejnižší hash a co nejdříve ho spočítá. Komu se tento proces podaří jako prvnímu, získá za odměnu emisi aktuálně 12.5 BTC. To je pro těžaře Bitcoinů v současné době největší motivace. Tento nový blok je zaznamená do Blockchainu a celý proces začíná znovu. (3)

Bitcoin bude mít v budoucnosti 21 milionu jednotek, které v roce zavedení přibývali 50 BTC za každých 10 minut, po 4 letech už to bylo pouze 25 BTC za 10 minut a nyní už je to pouze 12,5. A v květnu roku 2020 dojde ke snížení opět o polovinu na 6,25 BTC. (5)

Kvůli neustále rostoucímu počtu těžařů se těžba v jistých směrech stává stále více náročnější, proto vzniká tzv. „Těžební pool". Je to seskupení těžařů, kteří zkoušejí štěstí v dosažení zisku pomocí těžby společně, jelikož pro malé těžaře je nález bloku velmi nepravděpodobný. Pokud se některému z nich podaří tento blok najít, o zisk se pak rozdělí společně. Tyto těžařská seskupení mají velkou výhodu v tom, že se zvyšuje předvídatelnost zisku. (4)

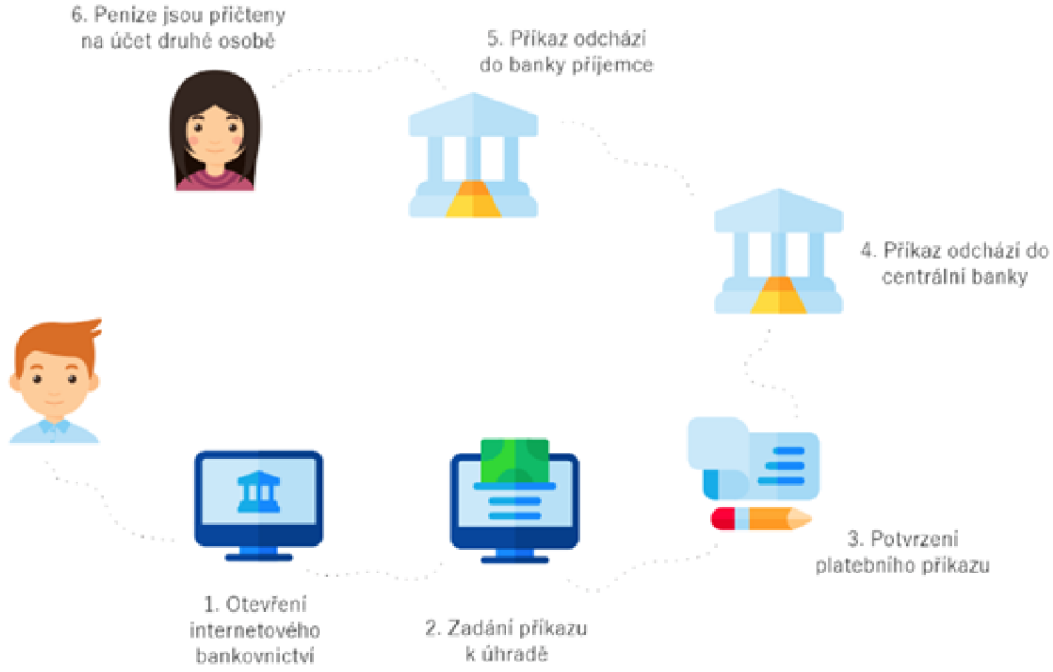
Malý těžař s průměrnou grafickou kartou by byl schopen najít blok v průměru cca až za 5 let, zatímco v seskupení těžařů (také nazýváno jako „Mining pool") by mohl dosahovat menších zisků klidně několikrát denně. Jedinou nevýhodou jsou poplatky, které každý člen musí platit správcům seskupení. (4)

Do světa kryptoměn se začínají stále častěji zapojovat i velké firmy, např. Siemens. Společnost Siemens přišla na trh se speciálním procesorem pro těžbu virtuálních měn. Kvůli náročné těžbě je momentálně na trhu velká poptávka po kvalitních a výkonných grafických kartách, a to v Česku i zahraničí. Siemens se rozhodl tuto situaci změnit, společnost navrhla speciální procesor, který je narozdíl od klasických grafických karet již od základu stavěn pro těžbu virtuálních měn. Zajímavostí je, že tento procesor má být mnohem výkonnější, ale podstatně energeticky úspornější. To se zdá být velkým přínosem do virtuálního světa, a především jako velká výhoda pro těžaře, jediný problém by snad mohla být cena, která se bude pohybovat mnohem výš než klasické prostředky pro těžbu. (5)

1.5 Transakce

Než se podíváme na transakce Bitcoinu, tak se nedříve podíváme na běžný způsob, jakým dnes bezhotovostně posíláme peníze.

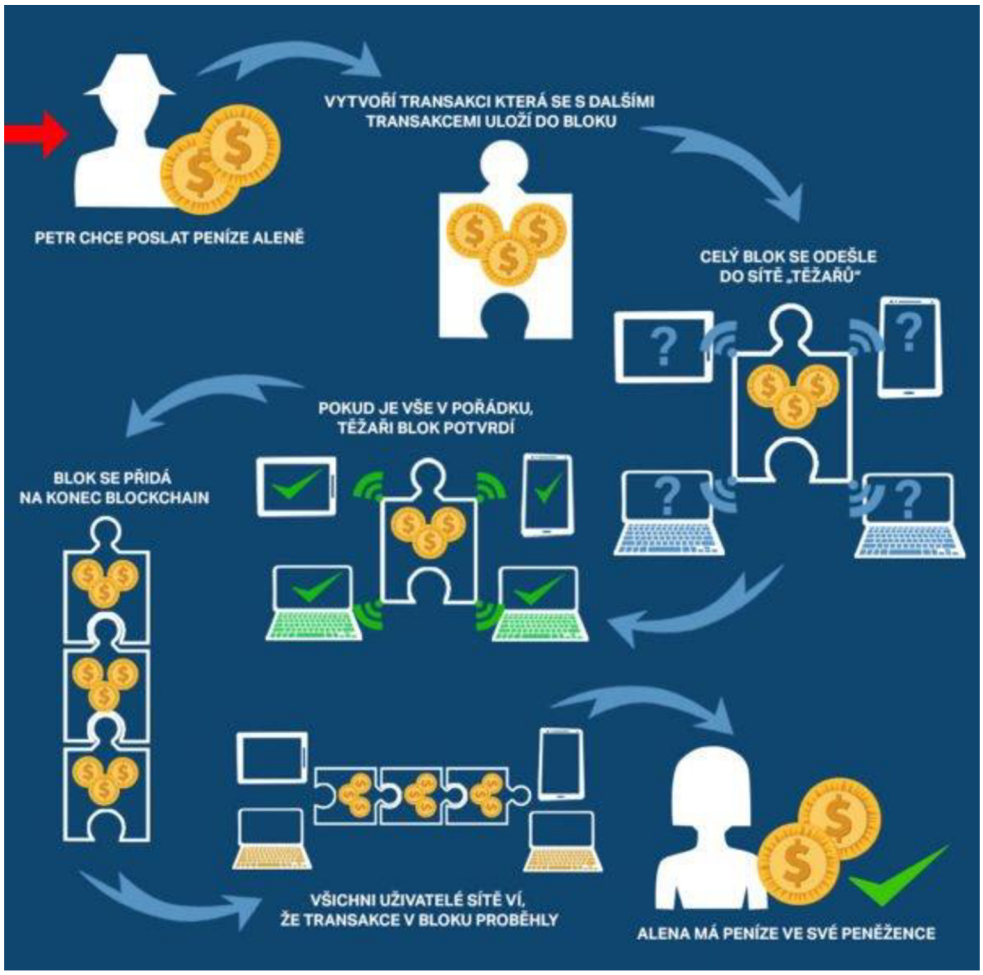
Nedříve se musíme otevřít internetové bankovnictví, zvolit příkaz k úhradě, zadat číslo účtu, kam peníze posíláme, potvrdit příkaz a odeslat ke zpracování. V tuto chvíli důvěřujeme bance, že peníze správně odešle z našeho účtu a částku připíše na správný účet příjemce. Bance musíme důvěřovat v peníze jsou dostatečně chráněny proti krádeži či zfalšování. (9)



Obrázek 11: Bezhotovostní platba
(Zdroj:9)

Z tohoto příkladu je jasné, že důvěřujeme bankám a prostředníkům v bezhotovostních platbách. V případě Bitcoinu, nedůvěřujeme žádně bance ani prostředníkovi. Diky decentralizaci, mezi odesílatelem a příjemcem není žádná společnost, ale obrovská sít propojených počítačů všude po světě, která zpracovává transakce. Při posílání Bitcoinu, naši transakci musí nejprve ověřit decentralizovaná sít uzlů, tzv nodes. Nodes je označení několika tisíc počítaču rozmístěných po světě, které díky vzájemnému propojení spolu neustále komunikují. Nodes ověřuje, zda je transakce platná, jestli je v peněžence dostatečné množství Bitcoinu. Poté přichází na řadu těžaři, ti musí transakci zpracovat a vložit jí do bloku k dalším transakcím. Blok si můžeme představit jako složku s příkazy

k úhradě banky. Tento blok je následně zařazen k dlouhému řetězci bloků, tedy do Blockchainu. (9)



Obrázek 12: Platba přes blockchain
(Zdroj: 8)

1.6 Peněženky kryptoměn

Bitcoin i ostatní kryptoměny zůstávají v blockchainu, nenakládáme s nimi fyzicky. Z technického hlediska jsou peněženky pouze schránky, do kterých ukládáme přístupové kódy kryptoměnových adres. (5)

Rozlišujeme dva základní druhy kryptoměnových peněženek, takzvané „hot wallet" (online peněženky) a „cold wallet" (offline peněženky). (3)

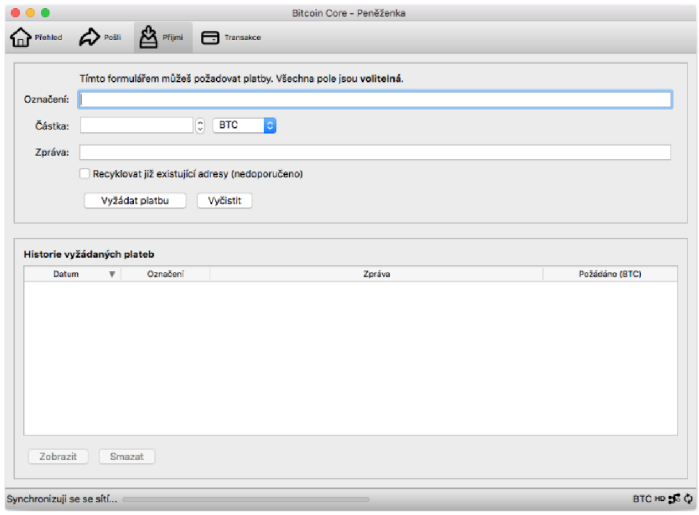
Hot wallet peněženky jsou připojené k internetu (mobilní peněženky/virtuální peněženky). Tyto peněženky jsou obecně méně bezpečné, díky přístupu k internetu představují pro vaše peníze i pro vaše osobní údaje bezpečnostní riziko. Pokud máme

zařízení, na kterém peněženku používáme zabezpečenou pomocí antivirových programů a hesel tak je bezpečnost na vysoké úrovni a nemusíme mít velký strach o bezpečnost. Výhodou hot wallet je dynamičnost, transakce se uskutečňují téměř okamžitě v závislosti na aplikaci a druhu transakce. Většina kryptoměnových peněženek je typu hot wallet. Tyto peněženky jsou převážně určené k častému obchodování a využívaní k platbám. (3)

Cold wallet jsou naopak ty peněženky jež nejsou k internetu připojeny (hardwarové peněženky, papírové peněženky). Tudíž jsou naprosto bezpečné k útokům hackeru. Bezpečnost cold wallet je i značnou nevýhodou. Cold wallet nemívají vlastní uživatelské rozhraní. Přistup se provádí přes program, který vám umožní přístup na blockchain síť. Cold wallet peněženky jsou určené pro uchovávaní kryptoměn na dlouhou dobu, kdy očekáváme, že cena kryptoměny v budoucnosti značně poroste. (3)

1.6.1 Softwarová peněženka

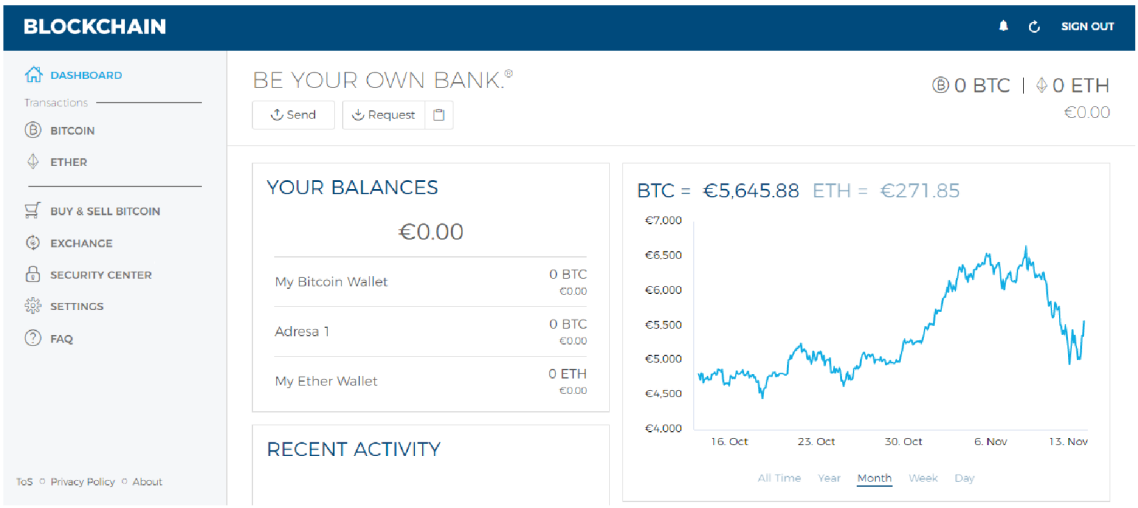
V současnosti existuje obrovské množství softwarových peněženek. Nejvíce se doporučuje používat „oficiální" peněženky virtuálních měn, pro Bitcoin tedy Bitcoin Core Wallet nebo pro Ethereum je to Ethereum Wallet. Softwarové peněženky lze stáhnout jako v plné verzi nebo v odlehčené verzi. Plná verze uchovává celou kopii blockchainu a odlehčená verze jen část z blockchainu. Na každé peněžence si lze vygenerovat neomezené množství adres. Tyto adresy lze zveřejnit, pokud nám někdo přepošle na tuto adresu digitální mince, obdržíme je ve své peněžence. Součástí každé peněženky je privátní klíč. Každý klíč je matematicky spojen s adresami naší peněženky. Tento klíč musíme udržovat bezpečně uschován a nikdy nezveřejnovat. Bez klíče nemůžeme přijímat ani odesílat transakce. (7)



Obrázek 13: Softwarová peněženka Bitcoin Core
(Zdroj: 7)

1.6.2 Online peněženka

Online peněženka je taková peněženka, která se nám vytvoří při vytvoření účtu na nějaké burze. Je to velice efektivní a jednoduché, nemusíme si speciálně zakládat peněženku. Tento způsob ovšem není příliš bezpečný. Digitální mince svěřujeme třetí straně. Když burza zkrachuje, nemusíme svoje digitální bohatství už nikdy spatřit. A jsou tu další rizika, jako vykradení burzy nebo může burza peníze svých klientů zpronevěřit. Klienti burz nejsou jediní, kdo má přístup k privátnímu klíči. Klienti jsou odkázaní na férovost dané burzy a na to, že burza udělá vše pro dostatečné zabezpečení. (7)



Obrázek 14: Online peněženka Blockchain.info
(Zdroj: 7)

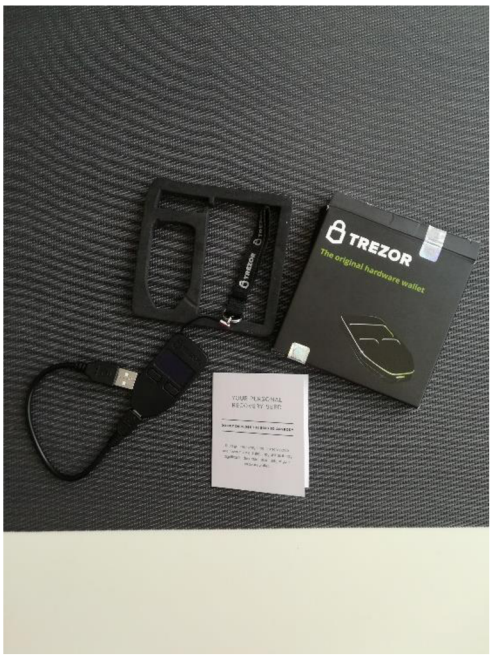
1.6.3 Mobilní peněženka

Mobilní peněženka je aplikace, kterou si stáhneme do mobilu a v které můžeme uchovávat krypto peníze. Hlavní výhodou peněženky je možnost aktivně používat vytěženou kryptoměnu k placení zboží a služeb, protože mobil máme většinou u sebe a v něm i tudíž svoje digitální peníze. Některé mobilní peněženky fungují na principu online peněženek, takže má privátní klíč k dispozici i třetí strana. (23)

1.6.4 Hardwarové peněženky

Stejně jako peníze, i Bitcoiny vám někdo může ukrást nebo zpronevěřit. Nejbezpečnější způsob, jak mít pod kontrolou své Bitcoiny, je uchovat si je ve své hardwarové peněžence. Je to zařízení podobné USB zařízení. Jde o nejbezpečnější řešení uschovávání kryptoměn. Bez znalosti hesla a hardwarové peněženky s vlastněnou kryptoměnou nic nenaděláte.

Hardwarové peněženky složí jako jednoúčelová zařízení, z důvodů nepřipojení k internetu je nelze napadnout. V případě s manipulací uložených kryptoměn musíme hardwarovou peněženku připojit k počítači, který je připojen na internet, ale komunikace počítače s peněženkou je jednosměrná. K větší bezpečnosti slouží navíc i to, že každou transakci musíme potvrdit fyzickým tlačítkem na hardwarové peněženky. (7)



Obrázek 15: Hardwarová peněženka Bitcoin Trezor
(Zdroj: Vlastní zpracování)

1.6.5 Papírová peněženky

Papírová peněženka obsahuje privátní klíč vytištěný na papíře. Nákup z automatu pro kryptoměny vám právě vytiskne takovouto papírovou peněženku. Papírová peněženka je náchylná ke krádežím a zničení, doporučuje se pouze jako krátkodobé řešení. (7)

2 ANALÝZA SOUČASNÉHO STAVU

V analytické časti se práce zabývá budoucím využitím blockchainu. Popíše výhody i rizika virtuálních měn, zaměří se na využití při nelegálních obchodech. Bude se zabývat Bitcoinem jeho právní úpravou a jeho předpokládaným vývojem a posouzení kryptoměn obecně.

2.1 Výhody a rizika virtuálních měn

Z faktu, že virtuální měny používá po celém světě stále více uživatelů, se dá vyvodit to, že jsou schopny svým klientům poskytnout celou řadu výhod. Za první výhodu můžeme považovat to, že mají relativně krátkou dobu ověřování a provedení transakce (standardně je to méně než 1 hodina, u Bitcoinu to zpravidla netrvá déle než 10 minut). Nemusíme však čekat, až bude transakce potvrzena, protože jsou přijímány i transakce nepotvrzené.

Velkým rizikem u platby pomocí kryptoměn je tzv. „double-spending“ (přeloženo jako „dvojí útrata”). Jedná se o jev, kde mohou být jednotky virtuální měny utraceny dvakrát. Tento problém je pro virtuální měny typický, neboť virtuální informace lze velmi snadno reprodukovat. U standardních měn si tento jev můžeme představit jako padělání mincí či bankovek.

Dalším rizikem, a zároveň největší nevýhodou, je nenávratnost. Pokud jste Bitcoin či jakoukoliv jinou měnu omylem poslali na špatnou adresu, nedá se dohledat a je nenávratně ztracená. Toto vede i ke krádežím, tedy hackerskému napadení virtuálních peněženek. Jako příklad si můžeme uvést doposud největší krádež na japonské burze Coincheck, která se stala koncem ledna 2018. Celková škoda dosáhla 58 miliard jenů, tedy 10,8 miliardy korun. Jednalo se o virtuální měnu NEM (z hlediska tržní hodnoty je to desátá největší měna) a posléze byly odcizovány i všechny ostatní typy digitálních měn obchodovány na burze s výjimkou Bitcoinu.

Jednatelé burzy oznámili, že je velká pravděpodobnost najít virtuální adresu místa, kam hackeři odcizené měny odeslali. Došlo také k vyjádření, že všechny uživatele burzy, kteří kvůli útoku přišli ke škodě, odškodní v japonských jenech. Mělo by to být zhruba 260 000 klientů.

Další příklady můžeme uvést z roku 2014, kdy kvůli krádeži 650 tisíc BTC zkrachovala burza MtGox. Burza Bitstamp v roce 2016 ztratila skoro 20 BTC a dalších 120 tisíc BTC hackeři ukradli z burzy Bitfinex.

Co se potenciálního zisku z investic týče, nelze zcela určit, zda je to výhoda či nevýhoda. Zisk může být velmi velký bez jakékoliv námahy – stačí „pouze" počkat na to, až bude kurz minimální a prodat, až bude podstatně vyšší – tedy za málo nakoupit, za draho prodat. Principem těchto investic je umět odhadnout, jak na tom aktuální trh bude, zda cena půjde nahoru či dolů.

Spousta lidí v dnešní době si z těchto velmi rizikových investice udělala živobytí, někteří si na tyto obchody dokonce půjčují finanční prostředky a potom se je na online Bitcoin burzách snaží zhodnotit. Největší riziko tohoto obchodování je zcela jasné – nevyzpytatelné chování měny. Tento způsob za obstarávání peněz bych tedy stručně přirovnal k ruletě a hře na náhodu a štěstí. Problematika investic do Bitcoinu tkví ještě někde jinde – je třeba umět rozpoznat, co je falešný obchod a lákadlo. Můžete se totiž velmi snadno zaplést na falešnou burzu či e-shop, kde za své Bitcoiny či jinou měnu nic nezískáte – naopak proděláte a své virtuální jmění už nikdy nedohledáte.

2.2 Virtuální měny a nelegální obchody

Naprostá anonymita virtuálních měn může jistě představovat velkou výhodu, nicméně také to umožňuje nezákonné obchodování, např. na internetových černých trzích s nelegálním zbožím, kde se jak prodejce, tak ani kupující nedá dohledat. Toto téma mě přivádí k tomu, kde a jak se Bitcoin skutečně nejvíce rozšířeně používá.

Virtuální měny se jako platidlo mnohem více využívají v „podsvětí" internetu („dark webu"), než v běžném životě, a to právě kvůli naprosté anonymitě, kterou Bitcoin a další měny umožňují. Pokusím se toto fungování černého trhu a Bitcoinu stručně předvést na jednoduchém příkladě:

Pokud by nějaká osoba chtěla uskutečnit obchod s nelegálním zbožím (zbraně, léky, kradená elektronika atd.), na běžném internetu, který všichni známe a téměř denně používáme, samozřejmě nemá možnost. Využije k tomu tedy „zakázanou" část internetu, na kterou se dostane přes speciální prohlížeč. Klíčovou vlastností tohoto prohlížeče je to, že skrývá vaši identitu a vámi přenesená data. Obsah toho, co hledáte, tedy nelze nikdy

dohledat. Vyberete si zboží a dále postupujete jako na každém jiném e-shopu, na virtuální peněženku prodejce pošlete částku. Platby probíhají samozřejmě pouze prostřednictvím digitálních měn, nejčastěji Bitcoinu, nicméně vzhledem k tomu, že Bitcoin se stává stále populárnějším a je více pozorován, uchylují se uživatelé dark webu k platbám jinými měnami, momentálně se Bitcoin začal hojně nahrazovat Etherem či Monerem.

Nejznámějším e-shopem s nelegálním zbožím, kde můžete své virtuální měny zužitkovat, je „Silk road“. Nejčastěji nakupovaným zbožím byly drogy, ale taky falešné pasy a uniklé vládní dokumenty, což samozřejmě FBI brzy zjistila a dokázala vypátrat jednoho ze zakladatelů a prostřednictvím něj se jim podařilo tento trh zastavit, nicméně brzy začaly vznikat jiné verze „Silk roadu“ a černých trhů teď existuje mnohem více.

Dále se na tomto internetu shromažďují také nadšenci do techniky, kteří se zajímají o tzv. hacking. Existuje několik diskuzních fór, kde se tito hackeři shromažďují a plánují společně útoky. Představme si to něco jako skupinu zločinců, kteří se chystají přepadnout banku – tito hackeři místo toho však zakládají falešné e-shopy, které jsou velmi dobře propracované, jejich účelem totiž je, aby z lidí vylákali jejich Bitcoiny. Domnívám se, že i přes snahu nahrazovat Bitcoin, 99 % veškerých služeb či zboží na dark webu lze zaplatit pouze jím, a když už o své Bitcoiny jednou přijdete, nikdy je nezískáte zpět.

Regulační úřady a vyšetřovací orgány se již naučily lépe zpracovávat data o transakcích provedených v Bitcoinech, v mnoha případech se tak již podařilo vypátrat snahy o financování trestné činnosti a „praní špinavých peněz”. Důvodem je veřejná povaha blockchain sítě, na které je Bitcoin postaven. Blockchain Bitcoinu si můžeme představit jako formu veřejně přístupné účetní knihy. Adresy Bitcoinu, na které jsou platby posílány, jsou tedy v blockchain síti známé. Vyšetřovatelům tedy stačí nějakou dobu pozorovat transakce prováděné na udané adrese a pak stačí jen zločince dopadnout. Platby pomocí Bitcoinu na černých trzích tedy pomalu upadají, nicméně je to stále nejvíce používanou měnou. Největší šanci dohnat jeho slávu má již zmiňovaná měna Monero, která vznikla v roce 2014 a je navržena tak, aby chránila identitu odesílatele, příjemce ale taky množství odesílaných virtuálních peněz. Hodnota Monera za poslední rok vzrostla o 1000 % a momentálně je to přibližně 8,6 tisíc Kč.

Obrázek 16: Logo monera
(Zdroj:19)

2.2.1 Bitcoin a jeho právní úprava

Vzhledem k tomu, že je tato virtuální měna poměrně mladá (první transakce proběhly až v roce 2010), není vázána na žádnou zemi a tudíž na žádný právní systém, není tedy řešena otázka její právní úpravy. Jelikož kurz Bitcoinu neustále stoupá/klesá a virtuální měny obecně se stávají stále větším fenoménem, začal si jich všímat i stát. Zákonodárci zamýšlejí právní regulaci Bitcoinu. Nabízí se hned několik způsobů. Některé zahraniční země uznávají měnu jako soukromé prostředky, jiné země ho však dokonce zakazují nebo velmi omezují.

V České republice otázka právní úpravy Bitcoinu zůstává nezodpovězena. V současnosti obchodování či měna samotná stále nepodléhá normám ČNB. Ministerstvo financí však označilo obchodování s Bitcoiny jako velice rizikové a vyzývá, aby byla platba nad 1000 EUR posouzena jako riziková, a aby byl každý obchod nad 15 000 EUR označen jako podezřelý.

Názory na to, zda je právní regulace virtuálních měn nutná nebo ne, se liší. Skupina lidí, která je pro regulaci, se domnívá, že jejich rychlý a nekontrolovaný vývoj může způsobit velkou nestabilitu finančních trhů a celkově může mít negativní dopad na ekonomickou situaci země. Zastánci Bitcoinu se naopak domnívají, že virtuální měny by mohly změnit mnohé nedokonalosti ve fungování finanční trhů, nicméně je nutno postupovat tak, aby nedošlo k narušení vývoje měn.

Největší regulace virtuálních měn nastaly v Číně, a to kvůli oslabování jejich domácí měny jüan, která se oproti dolaru propadla o sedm procent. Čínská vláda za tento propad

viní právě Bitcoin, který údajně způsobuje odliv peněz ze země. Dne 5. prosince 2013 čínská vláda vydala zákazu provádění jakýchkoliv převodů Bitcoinu pro finanční instituce. Jednotlivce zákaz neohrožoval. Tamní vláda zavedla zpřísnění kapitálových kontrol, kdy každý obyvatel může za jeden rok vyměnit jüany maximálně za 50 tisíc dolarů. Nicméně investoři v této regulaci velmi brzo našli skulinu a za čínskou měnu nakupují Bitcoiny, které mohou bez jakéhokoliv omezení převést na dolary.

Velká regulace Bitcoinu započala v Číně v září 2017, kdy byly uzavřeny burzy a kryptoměnové směnárny. Pozastavení obchodování proběhlo pouze na čínských burzách, zahraniční směnárny a burzy fungovaly dále. Velké čínské burzy proto přesunuly svá sídla, aby opustili čínskou jurisdikci a mohli i nadále obchodovat. Jednotlivci se po uzavření čínského trhu obraceli na zahraniční burzy a směnárny. Počátkem roku 2018 se čínská vláda rozhodla zamezit přístup i k zahraničním platformám nabízejícím virtuální měnu. Dále byli čínští těžaři vyzváni, aby přestali těžit kryptoměny z důvodů vysoké energetické náročnosti.

Podle Zennona Kaprona, zakladatele firmy Kapronasia, je jen otázkou času, kdy Čína přijde s ještě přísnějšími regulacemi, které by mohly mít povahu přísnějších kapitálových kontrol. Vláda by např. mohla určit, kolik Bitcoinů jedna osoba může vlastnit, v úvahu připadá i zavedení daně za držení kryptoměn. Další způsob, jak získat nad Bitcoinem úplnou kontrolu, je poněkud extrémní, Čína plánuje zakázat ho úplně. Už delší dobu se diskutuje o tom, zda k zákazu dojde a jestli se bude týkat pouze těžby, nákupu, prodeje či existence kryptoměn obecně.

Budoucnost právního řešení pro Bitcoin v Číně je podle mého názoru zcela zásadní, jelikož čínské obchodování s Bitcoinem představuje drtivou většinu všech transakcí v digitálních měnách. Kromě toho je Čína doposud největší těžařskou velmocí těchto měn.

Další velmi diskutovanou otázkou je to, zda jsou samotné virtuální měny legální. ČNB vydala stanovisko, že obchodování s Bitcoiny nepodléhají dohledu ČNB a není potřeba ani žádného povolení. Soudní dvůr Evropské komise dále potvrdil, že nákup ani prodej Bitcoinu prozatím nepodléhá odvodu DPH, podobně jako nákup např. EUR nebo jakékoliv jiné cizí měny. Nicméně jelikož se investice do Bitcoinu dá využít jako způsob zbohatnutí, řeší se otázka zdanění. Dle stanovisek ČNB se Bitcoin z pohledu práva považuje za věc, a to za věc nehmotnou, movitou a zastupitelnou. Dále z těchto stanovisek

vyplývá, že se Bitcoin není považován ani za bezhotovostní finanční prostředky či elektronické peníze. Směna Bitcoinů za oficiální měnu (např. převést si měnu z vaší virtuální peněženky na CZK) nenese znaky směnárenské činnosti. Bitcoiny dále nemají znaky investičního nástroje – nemají povahu CP ani derivátu.

Z daňového hlediska je zdanitelným příjmem zpeněžení vytěžených Bitcoinů nebo jejich směna za zboží či služby. Příjem dosažený prodáním měny či směnou za měnu oficiální může být u fyzických osob brán jako předmět daně, tedy jako příjem ze samostatné činnosti. U právnických osob je řazen mezi tzv. ostatní příjmy. Jelikož jsou tedy virtuální měny obecně brány jako příjmy, podléhají dani z příjmu. Ta se vypočte jako 15 % z rozdílu nákupní a prodejní ceny. Zdanit zisk z virtuálních měn však není jednoduché, protože stále není jasno v tom, zda se jedná o dočasný příjem, který je od daně do 30 tisíc korun osvobozen.

Judikatura kolem kryptoměn je velice složitá a nejednotná. Americký soud vynesl verdikt, že Bitcoin nejsou peníze, evropský soud judikoval, že Bitcoin je měna a Japonský soud judikoval, že Bitcoin nelze vlastnit, tudíž veškeré diskuze o jeho finančním přínosu jsou bezpředmětná.

2.3 Výhody a nevýhody blockchainu

Blockchain nemá budoucnost pouze v kryptoměnách. Blockchain může sloužit jako účetní kniha, databáze, ale i jako platforma. Blockchain udržuje data v neměnné podobě, bylo by velmi namáhavé něco změnit, bylo by potřeba změnit všechny následující data. Blockchain by se mohl využívat i v účetnictví a v auditech, protože obsahuje všechny data od začátku vzniku. Půjde prověřit každou transakci pomocí speciálního kódu, místo namátkových kontrol transakcí. Bude mnohem jednoduší objevovat podvody. Posílání transakcí přes celý svět bez verifikace a zprostředkovatele.

Blockchain by mohl také sloužit jako databáze klientů. Banky by měly ověřený centrální záznam a tam by měly informace o klientech a zakládání nových účtů by bylo efektivnější. V tomto případě by blockchain byl datové uložiště s vysokou integritou.

V oblasti převodu peněz, by mohl sloužit pro lidi, kteří se snaží vyhnout poplatkům u bank. Banky vydělávají na poplatcích, provizích a na směnných kurzech jako jiné

instituce. V případě blockchainu by se lidé těmto poplatkům mohli vyhnout, transakce by posílali sami, levněji a rychleji.

Blockchain je možnost pro lidi z rozvojových zemí. V rozvojových zemí je snadnější vlastnit mobilní telefon než vlastnit účet. Nebo se lidé setkávají s problémy, že kvůli chudobě jim banky žádný účet založit ani nemůžou nebo nechtějí. Těmto lidem přinesla naději kryptoměna Humaniq se svojí mobilní aplikaci. V této aplikaci si lidé můžou půjčit peníze od třetích stran a dalších uživatelů.

Blockchain by v budoucnu mohl být užíván jako technologie pro skutečně demokratické volby. O tomto tématu se začalo mluvit po kauze ve státu Georgia, kdy byly smazány elektronické volební hlasy na příkaz neznámo koho. V případě blockchainu by ke smazání dat dojít nemohlo.

Nevýhodou blockchainu je jeho neustále se zvětšující velikost, protože každý block v sobě uchovává informace o předcházejících blocích. Ovšem v dnešním světě, kdy velikost pevných disku neustále stoupá se to nedá považovat za velký problém. Aktuální velikost blockchainu se pohybuje okolo 210 GB.

Další nevýhodou blockchainu může být jeho zatížení. Pokud by síť byla přetěžována může dojít ke zpomalení celé sítě. Každý blok pro svoje vytvoření potřebuje nějakou dobu a výpočetní výkon. Toto by měl být však pouze dočasný problém, protože se neustále pracuje na zlepšování blockchainové technologie. V případě, že by tento problém nebyl vyřešen, nemá cenu zavádět technologii blockchainu celosvětově.

Pro přidáváni záznamů do blockchainu potřebujeme výpočetní výkon počítače. To má samozřejmě za následek zvyšování energetické náročnosti. Aktuálně se odhaduje, že udržování Bitcoinové databáze a přidávání nových záznamu má stejnou spotřebu jako 30 % spotřeby energie České republiky.

Jednou z komplikací je nerozvinutost třetího světa, k zavedení blockchainu je nutnost internetu. Což v některých oblastech světa není možné.

Největší nevýhoda blockchainu je v 51 % útoku. Je to velice nebezpečný útok, kdy domluvená skupina uživatelů nebo jednotlivec vlastní nadpoloviční většinu celé sítě. Pokud takové množství sítě kontroluje jedna entita, může se pokoušet sama rozhodnout o osudu celé sítě. Například o tom, které transakce budou uloženy v blockchainu. Ve velkých měnách jako je Bitcoin je dost nepravděpodobné, že by jedna entita vlastnila

nadpoloviční většinu, ovšem v případě menších měn to není nic nemožného. Takový útok ovšem není nic jednoduchého. Je velice náročný a hlavně nákladný. Útočníkovi nestačí pouze mít jen dostatečné množství kryptoměny, musí mít taky vetší výpočetní výkon. I kdyby útok byl úspěšný, nejspíše by to znamenalo degradaci sítě a tím také pád hodnoty kryptoměny. Útok by zcela pozbyl smysl.

2.4 Posouzení kryptoměn

Vnitřní hodnotu kryptoměny získávají díky trhu. Kryptoměny svoji hodnotu nezískávají díky svému průmyslovému využití nebo dalšímu fyzickému využití jako jiné obchodní komunity. Panují obavy, že hodnota kryptoměn je tvořena pouze takzvanými mylnými představami trhu, tudíž jde o čistě spekulativní hodnoty, které nemají žádný reálný základ. Jakákoliv hodnota na trhu je odvozena subjektivním posouzením dané služby či předmětu. Hodnota se odvozuje od toho, kolik jsou za službu ochotni kupující zaplatit a za kolik jsou prodávající ochotni prodat.

Kryptoměny prokazují odolnost vůči makroekonomickým vlivům a na rozdíl od obyčejné měny si hodnotu udržují nehledě na situaci. Dlouhodobě bylo za bezpečné považované například zlato.

Kryptoměny se hojně používají v oslabených ekonomikách, kdy lidé nevěří místní měně, ať už kvůli vysoké inflaci, čí měnovým reformám. Kryptoměnám napomáhá špatná ekonomická situace na úrovni státu.

2.5 Budoucí vývoj

Na začátku minulého roku byl zaznamenán značný propad Bitcoinu. Tato měna dosahovala hodnoty téměř 19 000$ za BTC. Minulý rok tato měna téměř neustále oslabovala, teď se ovšem zdá, že by mohla znovu posilovat. Ovlivňující faktory jsou chystaný brexit, tedy nesourodé ekonomické uspořádání Evropy, to zda Velká Británie opustí EU nebo nikoliv už není podstatné. Další faktorem může být oslabení čínské ekonomiky a vyostřené vztahy se zahraniční politikou USA.

Vliv na cenu Bitcoinu bude mít i to, že v následujícím roce, přesněji v květnu 2020, dojde k půlení odměny těžařů. K tomuto půlení dochází každé 4 roky, takže už i v minulosti se tam stalo a z toho můžeme vycházet.

Budoucí vývoj ceny Bitcoinu může ovlivnit i podle analytiků budoucí recese, kterou začali předpovídat. Nikdo neví, jak se v takové krizi bude kurz pohybovat, protože za dobu Bitcoinu ještě krize nebyla.

Při aktuálním trendu zvyšování cen Bitcoinu je možné, že dojde k opětovnému boomu nákupu jako v roce 2017. V tomto roce začali Bitcoin nakupovat všichni, protože se všude psalo o tom, jak na kryptoměnách každý vydělává, a to mělo nejspíše za následek zvýšení ceny Bitcoinu. Ovšem v následují roce, kdy cena Bitcoinu mírně klesla se právě tito obchodníci snažili co nejrychleji zbavit svých Bitcoinu, aby zamezili ztrátě, a to mělo za následek zaplnění trhu a pád ceny. Řada těchto retailových obchodníku jistě čekalo, až Bitcoin začne znovu růst, aby ho nakoupili za co nejméně.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V praktické části bakalářské práce nastíním, jak může vypadat nákup Bitcoinu a práce s jednotlivými peněženkami. Dále popíši, jak si vybrat podle svých potřeb ideální peněženku.

3.1 Nákup Bitcoinu

Pro nákup Bitcoinu byl vyzkoušen Bitcoinmat. Bitcoinmatů je v celé české republice deset, jeden z nich se nachází v Brně na Náměstí Svobody v obchodním centru Omega. Automat je v češtině a velice jednoduchý na ovládání. Automat přijme nejmenší bankovku hodnoty 500 Kč a bankomat nepřímá karty, tudíž musíme mít hotovost. Do automatu vložíte svoje peníze, následně je potřeba zadat adresu peněženky, na kterou mají být Bitcoiny zaslány. Adresu můžeme zadat ručně na dotykové klávesnici na obrazovce nebo můžeme naskenovat QR kód ze svého mobilního telefonu. Poté už stačí pouze potvrdit a nákup je hotov.

Obrázek 17: Bitcoinmat
(Zdroj:20)

3.2 Peněženky

V této části se práce zabývá několika vybraných peněženkami a poukazuje na jejich výhody a nevýhody.

3.2.1 Bitcoin trezor

Stejně jako peníze, i Bitcoiny vám někdo může ukrást nebo zpronevěřit. Nejbezpečnější způsob, jak mít pod kontrolou své Bitcoiny, je uchovat si je ve svém Bitcoin trezoru. Bitcoin trezor je hardware o velikost klíčenky s displejem a dvěma tlačítky, který slouží k bezpečnému uchování nejen Bitcoinu, ale i Litecoinu, Dash zcash a dalších kryptoměn.

S Bitcoin trezorem transakci provádíte na obrazovce počítače, potvrzení transakce však provádíte mimo počítač pomocí svého Bitcoin trezoru, který je k počítači připojen USB kabelem. Díky tomuto fyzickému potvrzení se vám nemůže stát, že by vám peněženku někdo vykradl po síti.

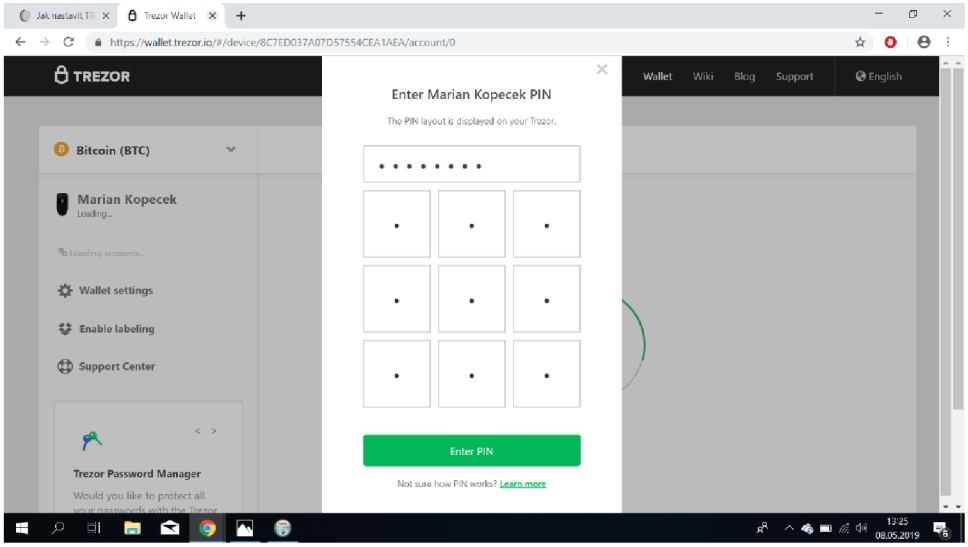
Bitcoin trezor je tedy samostatná počítačová jednotka, ve které je uložen váš privátní klíč. Výhodou je, že je to bezpečné úložiště vašich virtuálních peněz, relativně jednoduše se používá, jde o velmi lehké a dobře přenosné zařízení, nezabírá téměř žádné místo. Velkou výhodou je, že i při ztrátě peněženky se k obsahu můžete dostat online díky kódu, který se vám vygeneruje při prvním použití. Kód obsahuje 24 náhodných slov. Trezor je možné používat i za pomoci mobilního telefonu, stačí si pořídit redukci a stáhnout mobilní aplikaci.

Za nevýhodu tohoto trezoru lze považovat to, že instalace a veškerá práce s ním je zatím vedena pouze v angličtině a pořizovací náklady, které ovšem s rostoucími financemi úložnými v kryptoměnách stojí za investici, a hlavně pocit bezpečí. Cena Bitcoin trezoru se pohybuje kolem 2000 Kč.

Obrázek 18: Bitcoin Trezor
(Zdroj: Vlastní zpracování)

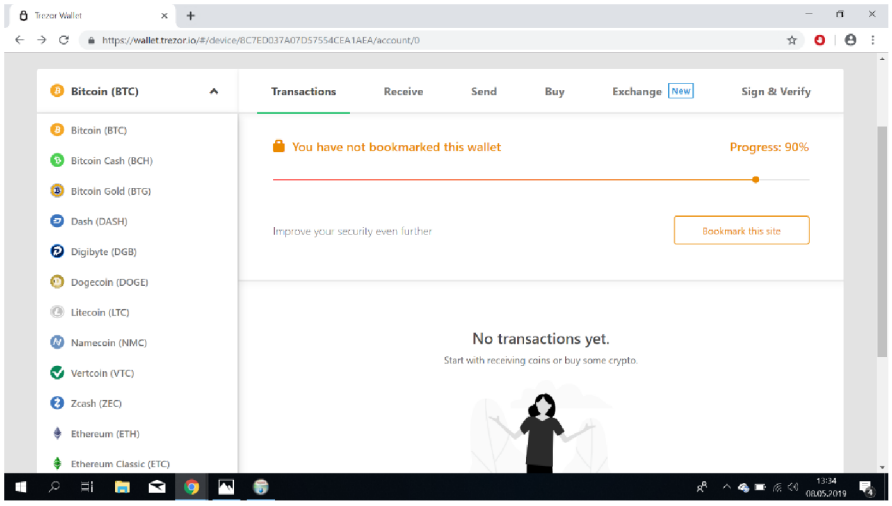
Po vybalení Trezoru jej připojíme k počítači pomocí USB. Po připojení se na obrazovce Trezoru objeví ikona zámku a pokyny k navštívení webové stránky „trezor.io/start“. Na stránce si zvolíme zařízení, které vlastníme. Automaticky jsme přesměrováni na další stránku, ze které si stáhneme můstek pro váš operační systém. Při dalším kroku po nás zařízení požaduje povolení pro instalaci firmwaru. Firmware v zařízení není nahrán z výroby, proto toto povolení instalace. Po instalaci firmwaru se na obrazovce Trezoru i prohlížeče objeví kód, který musíme porovnat, jestli je shodný na obou zařízení a potvrdit na zařízení. Po tomto kroku musíme zařízení odpojit a znovu připojit. Poté zařízení můžeme pojmenovat. Dále nastavíme PIN, který je potřeba ke každému potvrzení transakce a přístupu do zařízení. V prohlížeči máme mřížku čtverců s tečkami 3x3 a na zařízení vidíme mřížku 3x3 s přeházenými čísly. V prohlížeči si vybereme čtverce pro PIN, které představují pozici čísel na Trezoru. PIN musíme potvrdit ještě jednou, ovšem musíme se podívat znovu na zařízení, protože pozice čísel se mění pro každé zadávání PIN kódu. Potvrzením PIN kódu na zařízení přecházíme k seedu, na obrazovce trezoru se zobrazuje slovo po slovu, která si musíme co nejlépe zapsat a uložit na bezpečné místo tak, aby nám tento řetězec slov nikdo nezcizil a abychom ho v případě potřeby nalezli.

Ověřme si, že seed máme dobře opsaný a můžeme kliknout na ukončení a nyní můžeme se zařízením pracovat.



Obrázek 19: Zadávání PINu
(Zdroj: Vlastní zpracování)

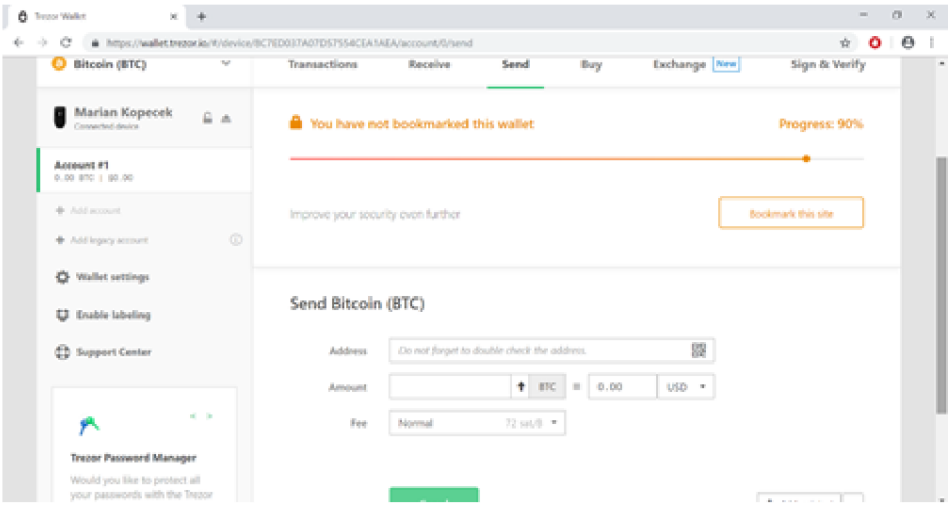
Pro přihlášení do zařízení musíme zadat opět PIN. Rozhraní Trezoru je velice intuitivní a žádný uživatel se základní znalostí angličtiny s ním nebude mít problém.



Obrázek 20: Vzhled peněženky
(Zdroj: Vlastní zpracování)

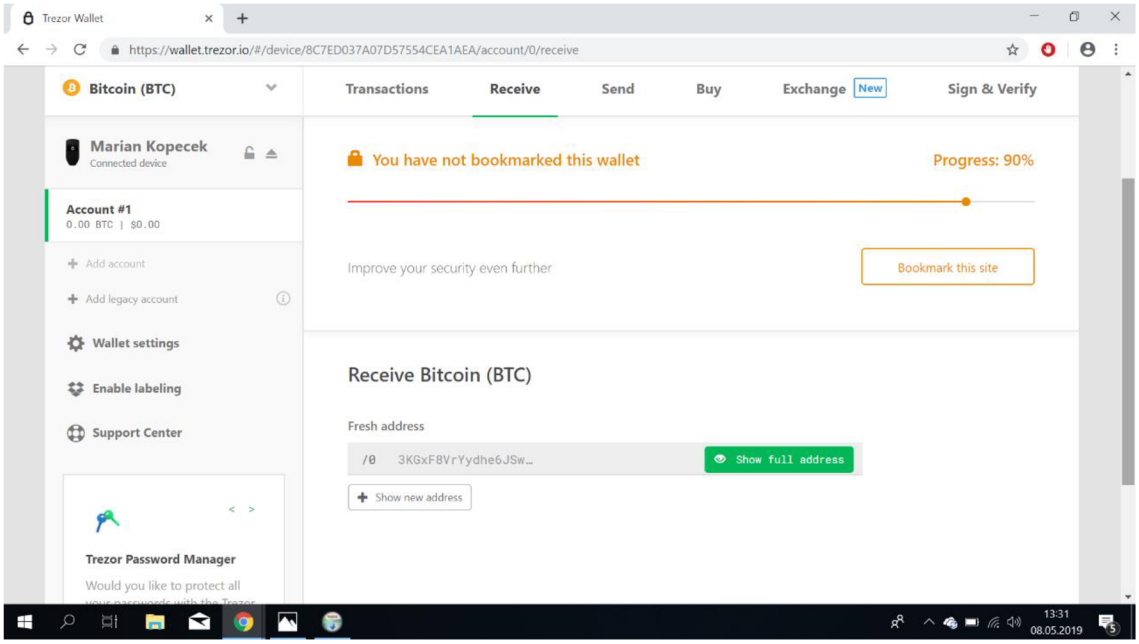
Po levé straně máme podporované coiny a na horní liště co s jednotlivými coiny chceme dělat. Po rozkliknutí měny se nám objeví naše účty se stavem a možnosti pro vytvoření účtu a dalšího nastavení. Pro odeslání měny nám stačí znát adresu peněženky, kam coiny

posíláme, vybereme částku a poplatek, který zaplatíme za poslání (čím nižší poplatek, tím delší je doba ověření).



Obrázek 21: Bitcoin trezor – odesílání
(Zdroj: Vlastní zpracování)

V případě, že nějaké coiny posíláme do peněženky, stačí znát adresu naší peněženky, ta se nachází v „Receive“.



Obrázek 22: Bitcoin Trezor – adresa
(Zdroj: Vlastní zpracování)

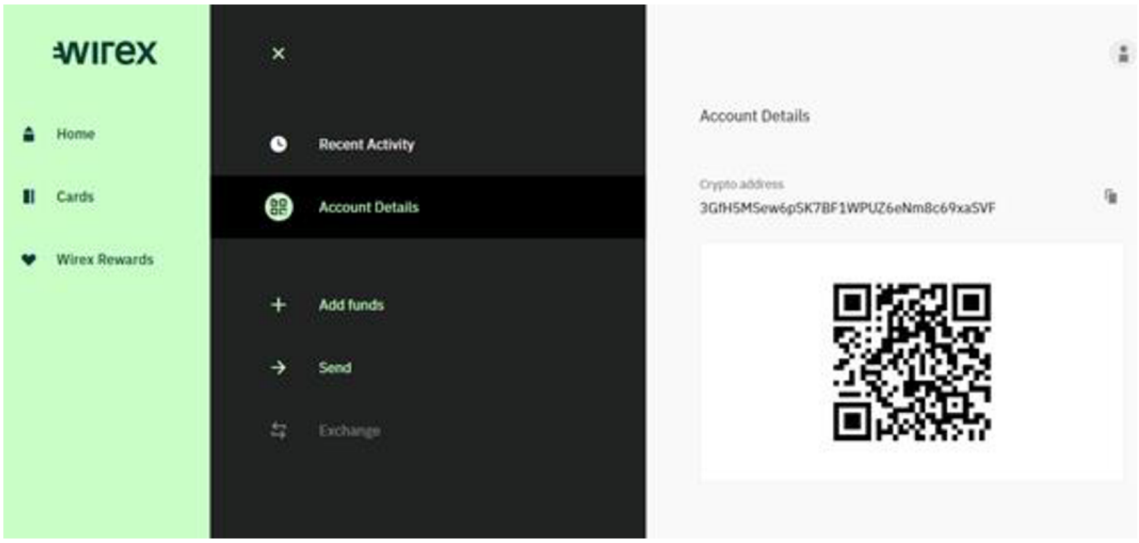
3.2.2 Wirex

Wirex je dostupný ke stažení uživatelům operačních systému Android a iOS. Wirex je jednotná platforma pro prodej, nákup, převod i uchovávání kryptoměn. Při registraci se neplatí žádný poplatek za vedení. Žádné poplatky aplikace nevyžaduje za uchovávání ani přijímání kryptoměn, pouze při odesílání platíme transakční poplatek jako u všech transakcí kryptoměn. Společnost Wirex v případě vašeho zájmu zašle platební kartu, kterou můžete využívat k placení kryptoměnami, které máte ve své peněžence. Za kartu si společnost účtuje 1 euro měsíčně a za každý výběr z bankomatu 1.70 euro. Při platbách kartou se vám bude na kartu vracet 0.5 % z nákupu. Pro případ směny reálných peněz za ty virtuální aplikace vyžaduje minimální částku 25 eur s 0% poplatkem což je výhoda oproti konkurenci, která vyžaduje za každou směnu částku kolem 10 eur. Za výhodu lze považovat to, že je na vás, v jaké měně chcete peněženku vést, můžete si vybrat mezi eurem, americkým dolarem a britskou librou, většinou se však Bitcoiny uvádí v dolarech. Aplikace podporuje zabezpečení 2FA ochranou, ověřuje transakce pomocí SMS a emailem a umožňuje přihlášení otiskem prstu. Wirex neuchovává vaše data o platební kartě (pokud nechcete), kterou jste použili k nákupu, takže není potřeba mít strach o svoje údaje. Další výhodou je to, že tato peněženka nám umožňuje vidět naše „opravdové" peníze. Tato částka se mění v závislosti na tom, jak se mění kurz Bitcoinu a vzhledem k tomu, že v současnosti Bitcoin neustále opět roste, s velkou radostí můžete sledovat, jak každý den vaše investovaná částka roste. Wirex má vlastní webové rozhraní, což znamená, že se k peněžence můžeme připojit i přes webový prohlížeč. Při použití webového rozhraní jsou vaše privátní klíče uloženy někde na cloudu. Je to zvýšení rizika, že o svoje kryptoměnové bohatství můžete přijít ne svojí vinou, na úkor pohodlí.

Aplikace je ke stažení na Google Play i na App Store. Při spuštění aplikace se musíme nejprve registrovat. Aplikace požaduje pouze jméno, příjmení, email, heslo a PIN. Přijde potvrzovací email, který musíme potvrdit a už můžeme pracovat s aplikací. Pro přihlášení do aplikace budeme vždy zadávat PIN kvůli ochraně.

V aplikaci si můžeme uložit naši kreditní či debetní kartu a využívat jí k nakupování kryptoměn, přímo z aplikace.

Wirex má i webové rozhraní, takže všechny svoje virtuální měny můžeme ovládat pomocí počítače.



Obrázek 23: Wirex – vzhled
(Zdroj: Vlastní zpracování)

3.2.3 Mycelium Bitcoin Wallet

Jako jedna z prvních mobilních kryptoměnových peněženek vznikala Mycelium Bitcoin Wallet. Od svého uvedení se drží na špičce mobilních kryptoměnových peněženek dodnes. Mycelia si drží svoje jednoduché a intuitivní prostředí, a proto si udržuje svoji oblíbenost. Mycelium nepodporuje webové rozhraní, tudíž ji lze používat pouze v mobilním zařízení, což obsahuje nevýhodu v omezeném přístupu ke svému bohatství, ale poskytuje výhodu bezpečnosti, všechny vaše privátní klíče jsou v bezpečí na vašem mobilním zařízení. V případě krádeže vašeho mobilního zařízení je aplikace chráněna PIN kódem, který musíte zadávat jak pro přístup do aplikace, tak pro posílání peněz. Aplikace má bezpečnostní systém i pro případ krádeže nebo rozbití mobilního zařízení, což by většinou znamenalo ztrátu vašeho virtuálního bohatství. Princip je téměř shodný jako u hardwarové peněženky Trezor. Mycelium je hierarchicky deterministická virtuální peněženka, tudíž svoji peněženku máte zálohovanou pomocí 12 náhodně vygenerovaných slov. Těchto 12 slov je potřeba mít zapsaných a uchovat je na bezpečném místě, nejlépe na papíru mimo sít. Výhodou pro české uživatele je, že aplikace je přeložená do češtiny. Hlavni nevýhodu vidím v tom, že aplikace podporuje pouze Bitcoin, což v dnešním světe, kdy investoři kombinují více kryptoměn aplikaci znevýhodňuje.

Pro stažení aplikace stačí jít na Google Play. Aplikace pro spuštění nevyžaduje žádné přihlášení ani PIN. Zabezpečení si v tomto případě musíme nastavit v aplikaci sami a podle svých potřeb. Aplikace je velice jednoduchá a částečně v češtině. Bitcoiny si

můžeme koupit přímo v aplikaci, budeme přesměrování na stránku, kde si můžeme koupit okamžitě Bitcoiny v hodnotách od 50 eur po 2000 eur.

Obrázek 24: Mycelium – vzhled
(Zdroj: Vlastní zpracování)

3.2.4 Bread Wallet

Bread Wallet sází na jednoduchost, do této mobilní peněženky lze jednoduše vložit Bitcoin a další desítku menších kryptoměn jako například Tron. Aplikace bohužel nepodporuje Litecoin, Ripple nebo Ethereum což jsou dnes stále populárnější měny. Aplikace i přes chybějící češtinu je velice jednoduchá a se znalostí základní angličtiny s ní není žádný problém. Přímo v aplikaci si kryptoměny můžeme zakoupit, ovšem tento nákup je zpoplatněn částkou 10 eur. Pokud tedy nakupujete kryptoměny po malých částkách, poplatky jsou opravdu nesmyslné, v případě velkých finančních nákupu tato částka příliš nesmyslně nepůsobí. Aplikace poskytuje zobrazování reálné hodnoty peněz vlastněných kryptoměn v českých korunách, tak ve světcových měnách dolaru či euru. Aplikace je chráněna PIN kódem a dále pro případ ztráty mobilního zařízení poskytuje i seed, tedy 12 náhodných slov.

Aplikace při spuštění požaduje zabezpečení mobilního telefonu gestem, PINem nebo heslem. Dále aplikace vyžaduje pro přístup do ní další 6místný PIN. Poté nám aplikace generuje náhodný 12 slovný seed. Aplikace si ověřuje zapsaní seedu, je zapotřebí naspat několik slov ze seedu, jinak není možné dokončit spuštění aplikace.

Obrázek 25: Bread Wallet – vzhled
(Zdroj: Vlastní zpracování)

3.3 Výběr peněženky

Výběru krypto-peněženky je potřeba věnovat pozornost, protože mince nevlastníme do doby, dokud je nemáme ve své peněžence. V případě, že je máme uložené u směnárny či burzy, pořád o ně můžeme přijít. Kryptoměny jsou naše až ve chvíli, kdy je uložíme do peněženky, ke které máme přístupový klíč pouze my. Druhů peněženek je celá řada a výběr není jednoduchá záležitost. Budeme muset volit mezi kompromisy bezpečnosti a jednoduchosti.

Na vyzkoušení byly vybrány krypto-peněženky s různým zaměřením na zákazníka, porovnány a vybrána ta nejvhodnější pro potřeby daného uživatele. Další virtuální a

hardwarové peněženky se od těch testovaných moc neliší, většinou jen v podporovaných měnách, stylu zabezpečení a poplatcích.

Výběrem vhodné peněženky si ulehčíme práci. V případě, že s měnami denně obchodujeme si určitě nebudeme vybírat hardwarovou peněženku, jenom bychom neustále ztráceli čas jejím připojováním k počítači a zadáváním složitého systému PINu. Ovšem pro někoho, kdo si nakoupí velké množství kryptoměny a bude čekat až její hodnota vzroste má hardwarová peněženka nepopsatelný pocit bezpečí. Hardwarová peněženka je nejbezpečnější způsob, jak uchovávat Bitcoiny a další měny. Zařízení uchovává Bitcoiny offline a proto nehrozí útoky hackerů. Hardwarová peněženka je ideální na středně velké a velké obnosy.

Pokud s kryptoměnami teprve začínáme, je dobré si zvolit nějakou mobilní peněženku nebo online peněženku, jsou velice jednoduché, intuitivní a pohodlné. Nesmíme ovšem zapomínat na nebezpečí online peněženek, kvůli poskytování klíčů třetí straně. Mobilní peněženky fungují na podobném principu, jako ty webové, jen máte svůj privátní klíč pouze vy u sebe a nespoléháte se na třetí stranu. Mobilní a online peněženky jsou vhodné pro menší objemy Bitcoinu.

Softwarové peněženky jsou snadné a intuitivní. Jednoduše si je naistalujete na počítač. Jejich bezpečnost je odvozená od bezpečnosti samotného počítače. Pokud nemáte počítač dostatečně zabezpečen antivirem, počítač se při připojení do sítě může stát snadným přístupem k Vašemu bohatství. Softwarové peněženky jsou vhodné pro menší a střední obnosy peněz.

Papírové peněženky se dají považovat za hardwarovou peněženku. Má výhodu, že je naprosto zdarma, protože se jedná pouze o papír s adresou a privátním klíčem. Bitcoiny papírová peněženka udržuje offline, mimo dosah hackerů. Ovšem papír můžeme lehce ztratit, či zničit. Problém nastává i s manipulací, budeme muset totiž vkládat klíč do mobilní peněženky.

Při výběru správné peněženky bychom si měli odpovědět na pár otázek:

- Budu kryptoměny používat v placení a obchodování nebo pouze budu čekat na jejich zhodnocení?
- Jakým obnosem budu disponovat?
- Vyplatí se investice do hardwarové peněženky?

Pokud jste si na otázky odpověděli, že si plánujete koupit vetší množství virtuální měny a čekat na její zhodnocení a nevadí Vám utratit přibližně 2000 Kč, tak je jasná volba hardwarová peněženka. V případě, že nechceme platit za hardwarovou a chce podobný pocit bezpečí, tak je ideální použít papírovou peněženku. V kombinaci s uložením v sejfu, je to výborná možnost. Pokud se bojíme, že papír zničíme, další možnost je testovaná peněženka Mycelium Bitcoin Wallet, která nepodporuje webové rozhraní, tudíž máte privátní klíče v bezpečí, ovšem Mycelium podporuje pouze Bitcoin.

Pokud hodláme aktivně platit za služby, tak je ideální mobilní peněženka Wirex, která v případě našeho zájmu, společnost wirex zašle kartu, pomocí které můžeme platit kryptoměnami jako běžnou platební kartou.

V případě častého obchodování s kryptoměnami nám nezbývá než vsadit na online peněženku. Musíme najít věrohodnou burzu a svěřit jí finance.

4 ZÁVĚR

Ač kryptoměny už existují deset let, jedná se stále o jejich počátek. Kryptoměny, potažmo blockchain v sobě ukrývají obrovský potenciál. Práce se zabývala pohledem na kryptoměny na jejich budoucí vývoj, skrytý potenciál i nebezpečí z pohledu ekonomického, technického i právního s přihlédnutím k hlavnímu zástupci Bitcoinu.

V první části práce byly předloženy základní teoretické znalosti blockchainu, na které se navázali znalosti o kryptoměnách a těžbě kryptoměn. Velká část byla věnována Bitcoinu, jeho vzniku a vývoji kurzu. Na konci teoretické části byly představeny druhy krypto-peněženek.

Analytická část se na základě teorie blockchainu pokouší předpovídat jeho budoucí využití napříč obory. Předpovídá výhody a nevýhody virtuálních měn obecně a jejich rizika využití v ilegálním obchodě. Na konci analytické části je optimistická předpověď vývoje kurzu Bitcoinu.

V poslední části se práce zaobírá krypto-peněženkami. Popisuje několik náhodně vybraných. Popisuje jejich rizika i výhody oproti konkurenci a na konci poskytuje návod pro výběr té správné.

SEZNAM POUŽITÝCH ZDROJŮ

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

(2) CHAFFEY, D. Digital Business and E-commerce Management. 6th ed. Harlow: Pearson, 2015. 679 p. ISBN 978-0-273-78654-2.

(3) 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.

(4) 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.

(5) 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.

(6) V obchodech rychle docházejí grafické karty do počítačů. In: *Hospodářské noviny* [online]. [cit. 2019-05-12]. Dostupné z: https://byznys.ihned.cz/c1-66026770-v-obchodech-rychle-dochazeji-graficke-karty-do-pocitacu-lide-je-hromadne-skupuji-kvuli-tezbe-kryptomen

(7) Peněženky pro kryptoměny, kde uchovat virtuální měny, co je TREZOR?. In: *INVESTPLUS* [online]. [cit. 2019-05-12]. Dostupné z: https://investplus.cz/investice/penezenky-pro-kryptomeny-kde-uchovat-virtualni-meny-co-je-trezor/

(8) Blockchain v praxi. In: *Finex* [online]. [cit. 2019-05-12]. Dostupné z: https://finex.cz/blockchain/

(9) Jak fungují převody Bitcoinů. In: *Jaknakrypto* [online]. [cit. 2019-05-12]. Dostupné z: https://jaknakrypto.cz/bitcoinove-transakce-poslat-bitcoin/

(10) Blockchain. In: *Wikipedia* [online]. [cit. 2019-05-12]. Dostupné z: https://en.wikipedia.org/wiki/Blockchain

(11) Bitcoin je už tak levný, že se nevyplácí jeho těžba. Náklady na elektřinu i chlazení začínají převyšovat jeho hodnotu. In: *Ihned*[online]. [cit. 2019-05-12]. Dostupné z: https://byznys.ihned.cz/c1-66081620-bitcoin-je-uz-tak-levny-ze-se-nevyplaci-jeho-tezba-naklady-na-elektrinu-i-chlazeni-zacinaji-prevysovat-jeho-hodnotu

(12) SEZNAM KRYPTOMĚN. In: Investplus [online]. [cit. 2019-05-12]. Dostupné z: investplus.cz/investice/seznam-kryptomen-kurzy/

(13) HOW TO INVEST IN LITECOIN. In: *The college investor* [online]. [cit. 2019-05-12]. Dostupné z: https://thecollegeinvestor.com/19673/how-to-invest-in-litecoin/

(14) Trade Recommendation: Peercoin. In: *Hacked* [online]. [cit. 2019-05-12]. Dostupné z: https://hacked.com/trade-recommendation-peercoin/

(15) Pioneer of Proof of Stake. In: *Peercoin* [online]. [cit. 2019-05-12]. Dostupné z: https://peercoin.net/

(16) Namecoin. In: *Bountysource* [online]. [cit. 2019-05-12]. Dostupné z: https://salt.bountysource.com/teams/namecoin

(17) Ethereum. In: *Kryptomagazin* [online]. [cit. 2019-05-12]. Dostupné z: https://kryptomagazin.cz/co-je-ethereum/

(18) Podcast: Buying Bitcoin. In: *Justonelap* [online]. [cit. 2019-05-12]. Dostupné z: https://justonelap.com/buying-bitcoin/

(19) Monero. In: *Kryptomagazín* [online]. [cit. 2019-05-12]. Dostupné z: https://kryptomagazin.cz/co-je-to-monero/

(20) Jak vybrat peníze za bitcoiny z automatu. In: *Zive* [online]. [cit. 2019-05-12]. Dostupné z: https://www.zive.cz/clanky/jak-vybrat-peniz

(21) Vývoj kurzu kryptoměny Bitcoin. In: *Kurzy* [online]. [cit. 2019-05-12]. Dostupné z: https://www.kurzy.cz/bitcoin/

(22) MtGox investigation update and preliminary release. In: *Wizsec* [online]. [cit. 2019-05-12]. Dostupné z: https://blog.wizsec.jp/2015/02/mtgox-investigation-release.html

(23) Co je to Bitcoinová peněženka? A jejich porovnání. In: *Jak na krypto* [online]. [cit. 2019-05-12]. Dostupné z: https://jaknakrypto.cz/co-je-to-bitcoinova-penezenka-a-jejich-porovnani/

SEZNAM OBRÁZKŮ