Problém škálovatelnosti Bitcoinu

Matyáš Mechl

Bakalářská práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Matyáš Mechl**
Osobní číslo:	**A17099**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**Prezenční**
Téma práce:	**Problém škálovatelnosti Bitcoinu**
Téma práce anglicky:	**Bitcoin Scalability Problem**

Zásady pro vypracování

1. Vypracujte literární rešerši dané problematiky.
2. Nastudujte a popište historii, základní vlastnosti a principy kryptoměn se zaměřením na Bitcoin.
3. Nastudujte a popište možnosti nákupu, prodeje, platebních transakcí a těžby kryptoměny Bitcoin.
4. Detailněji se zaměřte na problém škálovatelnosti Bitcoinu.
5. Analyzujte možná řešení tohoto problému.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing, 2018.
2. NARAYANAN, Arvind, Joseph BONNEAU, Edward FELTEN, Andrew MILLER a Steven GOLDFEDER. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016.
3. AJIBOYE, Timi, Luis BUENAVENTURA, Alex GLADSTEIN, Lily LIU, Alexander LLOYD, Alejandro MACHADO, Jimmy SONG a Alena VRÁNOVÁ. *The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future*. Amazon Digital Services LLC, 2019.
4. EXTANCE, Andy. The future of cryptocurrencies: Bitcoin and beyond. *Nature News*, 2015, roč. 526, č. 7571, s. 21-23.
5. Kryptomagazin.cz – Bitcoin, Blockchain, zpravodajský portál o kryptoměnách [online]. [cit. 2019-09-17]. Dostupné z: https://kryptomagazin.cz
6. CROMAN, Kyle, Christian DECKER, Ittay EYAL, Adem Efe GENCER, Ari JUELS, Ahmed KOSBA, Andrew MILLER, Prateek SAXENA, Elaine SHI, Emin Gün SIRER, Dawn SONG, Roger WATTENHOFER. On Scaling Decentralized Blockchains. In: Financial Cryptography and Data Security, FC 2016. Lecture Notes in Computer Science, Vol. 9604. Springer, Berlin: Heidelberg, pp. 106-125, 2016.
7. GEORGIADIS Evangelos. How many transactions per second can bitcoin really handle? Theoretically. *Cryptology ePrint Archive*, Report 2019/416, 2019.

Vedoucí bakalářské práce: **doc. Ing. Radek Matušů, Ph.D.**
Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce: **19. prosince 2019**
Termín odevzdání bakalářské práce: **27. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Ing. Martin Sysel, Ph.D.
garant oboru

Ve Zlíně dne 19. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské prácevyužito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně Matyáš Mechl, v.r.

ABSTRAKT

Bakalářská práce na téma „Problém škálovatelnosti Bitcoinu“ si dává za cíl uvést čtenáře do světa kryptoměn, představit hlavní zástupce a hlouběji se zaměřit na největší kryptoměnu na trhu – Bitcoin a jeho problém škálovatelnosti. Začátek práce pojednává o kryptoměnách obecně, nastiňuje historii a základní vlastnosti. Většina teoretické části je věnována samotnému Bitcoinu. Shrnuje princip jeho funkce, možnosti nabytí, používání a jeho výhody a nevýhody. Celá praktická část je zaměřena na uvedení do problematiky škálovatelnosti. Autor práce prvně definuje, co tento pojem znamená a následně vysvětluje, jakou to má spojitost s Bitcoinem. Součástí je i popis možných řešení, kdy autor analyzuje nejvíc diskutované možnosti, jak škálovatelnost Bitcoinu zlepšit.

Klíčová slova: Bitcoin, škálovatelnost, blockchain, kryptoměny, on-chain, off-chain, SegWit, Lightning Network

ABSTRACT

The bachelor's thesis "Bitcoin Scalability Problem" aims to introduce to readers the world of cryptocurrencies, the main representatives and to focus more deeply on the largest cryptocurrency on the market - Bitcoin and its scalability problem. The beginning of the work deals with cryptocurrencies in general, outlines the history and basic properties. Most of the theoretical part is devoted to Bitcoin itself and summarizes the principle of its function, the possibility of acquisition, usage and Bitcoin’s advantages and disadvantages. The whole practical part is set aside for Bitcoin scalability problem. The author first defines what this term means and then describes how it relates to Bitcoin. It also includes a description of possible solutions, where the author analyzes the most discussed options for improving Bitcoin scalability.

Keywords: Bitcoin, scalability, blockchain, cryptocurrencies, on-chain, off-chain, SegWit, Lightning Network

Tímto bych chtěl poděkovat panu doc. Ing. Radku Matušů, Ph.D. za odborné vedení, ochotu vždy pohotově reagovat a cenné rady poskytnuté při zpracovávání této bakalářské práce. Zároveň bych rád poděkoval své matce, bratrovi a prarodičům za podporu při vysokoškolském studiu.

„The Times 03/Jan/2009 Chancellor on brink of second bailout for banks“

-Satoshi Nakamoto

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Zájem o Bitcoin a celkově o kryptoměny v posledních letech rapidně roste. Vypovídá o tom i jeho cena, která momentálně balancuje mezi 9 až 10 tisíci USD za jeden bitcoin. Nejedná se ovšem o maximální cenu, kterou kdy v historii dosáhl. V roce 2017 jeho cena prudce rostla, a to až na hodnotu přibližně 20 tisíc USD. Extrémní nárůst ceny přilákal široku veřejnost, která s vidinou velkého zisku začala bitcoiny nakupovat. Počet transakcí, které Bitcoin musel zpracovávat, narůstal a s nimi i spojené poplatky, které v jednom okamžiku činily až 53 USD. Na povrch začal vyplouvat jeden z jeho velikých nedostatků, kterým je špatná škálovatelnost. Bitcoin je příliš pomalý na to, aby byl schopen zpracovat velké množství transakcí, a přitom si udržel přijatelné poplatky za jejich provedení.

Tento problém se stal hlavním předmětem této bakalářské práce, která si klade za cíl vypracovat literární rešerši pojednávající o problému škálovatelnosti Bitcoinu. Jde o problematiku, o které mnoho investorů ani neví, že jí Bitcoin čelí. Výstupem této práce by tedy měl být přehled, který uvede čtenáře do problematiky. Vysvětlí, co to škálovatelnost je a analyzuje možnosti, jak škálovatelnost této kryptoměny zlepšit.

Možností, jak zlepšit škálovatelnost Bitcoinu je několik. Autor práce provede analýzu těch v současné době nejdiskutovanějších, což bude obsahovat vysvětlení principu jejich funkce a do jaké míry jsou schopny škálovatelnost Bitcoinu zlepšit. Budou také rozebrány pozitivní a negativní vlastnosti, které jsou s jednotlivými řešeními spjaty. Práce se bude nejvíce upínat k Lightning Network, což je off-chain řešení, kterému se v poslední době dostává nejvíce pozornosti a je v něj vkládána veliká naděje.

Práce je zajímavá i pro čtenáře, kteří o Bitcoinu a obecně kryptoměnách slyší poprvé. Před hlubším ponořením do problému škálovatelnosti se bude práce věnovat úvodu do světa kryptoměn. Bude popsána jejich historie, základní vlastnosti a princip funkce se zaměřením na Bitcoin.

Práce bude členěna na teoretickou a praktickou část. Teoretická část čtenáři vysvětlí, co to kryptoměny jsou, jaká je jejich historie, základní vlastnosti a způsob dělení. V této části dojde také k detailnějšímu rozboru samotného Bitcoinu. Zde se čtenář mimo jiné i dozví, jak bitcoin získat, kde ho uložit a jak ho používat. Dále dojde k zaměření na praktickou část, která bude obsahovat uvedení do problému škálovatelnosti Bitcoinu a analýzu, jejíž výstupem by měl být přehled kladů a záporů jednotlivých řešení spolu s detailním popisem principu jejich funkce.

I. TEORETICKÁ ČÁST

1 KRYPTOMĚNY

Kryptoměny představují relativně novou formu aktiv, a to aktiv digitálních. Hlavním důvodem jejich vzniku bývá uváděna snaha o zvýšení bezpečnosti a rychlosti peněžních převodů. Digitální jsou proto, že existují pouze v digitálním prostředí, kde jsou reprezentovány jako zápisy v paměti počítačů a nelze je tedy hmotně vlastnit. Kryptoměny umožňují provádět finanční transakce bez ohledu na hranice států a jejich národní měny. I přesto, že kryptoměny existují relativně krátkou dobu, na trhu se jich vyskytuje celá řada. Stránka coimarketcap.com, zabývající se kryptoměnami, značí přibližně 5 tisíc existujících projektů. [1; 2; 3]

Samotné slovo „kryptoměny“ představuje překlad složeného anglického slova „cryptocurrencies“, kde „crypto“ znázorňuje kryptografii, která se používá k zabezpečení kryptoměnové sítě a slovo „currencies“ znamená měny. Kryptografie je obor představující rozsáhlé pole akademického výzkumu, které využívá mnoho složitých matematických technik. Mezi nejznámějším nástroje kryptografie, které kryptoměny používají patří například hashování[1] a digitální podpis. Tyto nástroje tvoří absolutní základ kryptoměn, bez kterého by se nad jejich existencí dalo jenom polemizovat. [2; 4]

1.1 Historie

Mnoho lidí je přesvědčeno, že za den vzniku kryptoměn je považován 3. leden roku 2009, kdy Satoshi Nakamoto[2] vypustil do oběhu první jednotky digitální měny Bitcoin. Avšak samotné kořeny kryptoměn sahají až do osmdesátých let minulého století, kdy se odehrála řada událostí, která se stala pro Bitcoin inspirací. Většina dříve vytvořených digitálních měn však ztroskotala na problémech, jako je dvojitá útrata[3] nebo centralizace. O Bitcoinu se tedy hovoří jako o první plně decentralizované kryptoměně, která byla schopna se prosadit na globálním trhu. Níže jsou popsány koncepty, které měly zásadní vliv na jeho vznik. [5; 6]

1.1.1 Digicash

První pokus o vytvoření digitální měny provedla firma DigiCash, za jejíž založením stojí americký kryptograf David Chaum. Chaum bývá také nazývám otcem digitálních měn či

[1] Matematická funkce, která slouží k přeměně vstupu libovolné délky na výstup o délce jednotné (tzv. hash). K hashovací funkci neexistuje funkce inverzní.
[2] Osoba nebo skupina, která navrhla a vytvořila Bitcoin.
[3] Dvojitá útrata neboli double-spending znamená, že uživatel využije stejné mince k provedení dvou plateb.

anonymní komunikace, jelikož do světa digitálních komunikací přišel s řadou inovací. Za zmínku stojí hlavně kryptografický systém pro anonymní transakce, který byl Chaumem předveden v roce 1982 pod názvem eCash. Později, roku 1990 došlo k jeho samotné realizaci. Jeho hlavním účelem bylo vytvoření jednoduší alternativy s větší anonymitou ve vztahu k tehdejším peněžním převodům. I přesto, že se jednalo o zcela výjimečný projekt, v roce 1998 celá firma DigiCash zbankrotovala. Jedním z hlavních důvodů jejího bankrotu je uváděna posedlost Chaumana po absolutní anonymitě, která bránila vtažení státních peněz do projektu. [5; 7; 8]

1.1.2 Bit Gold

Začátkem 21. století se americkému vědci a kryptografovi Nicku Szabovi nelíbilo, že současné finanční systémy kladou až příliš velkou důvěru v centrální autoritu, což může vést k problémům, jako jsou podvody či krádeže. Na základě toho přišel s formou řešení, kterou pojmenoval Bit Gold. Nick Szabo je mimo jiné také považován za tvůrce tzv. smart kontraktů. Smart kontrakt představuje speciální druh smlouvy, na jejíž plnění dohlíží samotná technologie kryptoměn, nikoliv určitá autorita. Detailněji jsou smart kontrakty popsány v další kapitole. [6]

Bit Gold představoval speciální mechanismus pro tvorbu decentralizované měny, jejíž princip byl založen na řešení speciálních kryptografických úloh s následným zapisováním výsledků do veřejného záznamu. Základním kamenem tohoto mechanismu bylo rozdělení celého procesu na malé úlohy, které nesou označení ve formě časového údaje. Stejně jak eCash, i tento projekt se ve své době nedočkal realizace. Realizace myšlenky přišla až o 10 let později, kdy samotný koncept převzal Satoshi Nakamoto. Ten na něm dokázal vyřešit i jeho největší chybu, kterou byl problém s dvojitou útratou tzv. double-spending. To se mu povedlo pomocí technologie zvané blockchain. Blockchain představuje decentralizovanou databázi, která je distribuována po síti a obsahuje záznamy všech dosud provedených transakcí, které jsou neměnné. Díky kompletnosti a transparentnosti databáze je možné dvojí útratě předcházet. Detailněji se blockchainem práce zabývá v další kapitole, kde je popsán samotný princip funkce Bitcoinu. [6; 9]

1.1.3 HashCash

Vznik HashCash sahá až do roku 1997. Tehdy Adam Back popsal systém, díky kterému by bylo možné dosáhnout redukce nevyžádaných emailů za pomocí Proof of Work, neboli protokolu ověřující vykonanou práci. Protokol pracoval tak, že před odesláním emailu

musel uživatel za pomocí výpočetního výkonu svého počítače dojít k řešení systémem vygenerované funkce. Funkce byla zadána tak, aby její řešení zabralo počítači nanejvýš jednu sekundu. Díky toho si byl systém schopen ověřit, že uživatel odesílá pouze pár emailů. V případě, že by došlo k pokusu o odeslání příliš velkého množství zpráv, systém by náročnost hledané funkce zvýšil tak, že by došlo k zahlcení počítače. Zajímavostí je, že princip systému popsali již v roce 1992 ve svojí práci s názvem „Pricing via Processing or Combatting Junk Mail" dva počítačoví odborníci Cynthian Dwork a Moni Naor. [5; 9]

Již výše zmíněný protokol Proof of Work je v dnešní době používán při těžení nových bitcoinů. Princip těžby je popsán v další kapitole. [9]

1.2 Vlastnosti

Kryptoměny v čele s Bitcoinem disponují několika zajímavými vlastnostmi, které je dělají jedinečnými. V některých případech je zásadně odlišují od standardní měny fiat[4], která je lidmi využívána v každodenním životě. Níže jsou zmíněny a vysvětleny typické vlastnosti kryptoměn, díky kterým se z nich stává kvalitní a konkurence schopná měna. [10]

1.2.1 Dělitelnost

Každá měna by měla být do určité míry dělitelná. V případě krypto peněz představuje dělitelnost ten nejmenší problém. V době, kdy začala být cena jednoho BTC[5] už vysoká, začaly se zavádět menší jednotky. Dnes se majitelé bitcoinů setkávají s pojmy jako je centibitcoin, který představuje 0,01 BTC, milibitcoin, což je 0,001 BTC a v neposlední řadě také mikrobitcoin, kdy 1 μBTC je 0,000001. Popularita měny a její vysoká cena si žádala zavedení další, současně nejmenší jednotky, která je pojmenována po jeho zakladateli. Jeden satoshi představuje 10^{-8} BTC. [7; 11]

Pro porovnaní je vhodné uvést další měnu, kterou může být třeba Ethereum, kdy její ether je dělitelný až na 18 desetinných míst. [12]

1.2.2 Volatilita

Vysoká volatilita[6] měny je vlastnost, která je spjata se všemi typy kryptoměn. K rychlým cenovým nárůstům a rovněž pádům může dojít během velice krátké doby. Při zaměření na

[4] Jedná se o peníze s nuceným oběhem, které vydává vláda a reguluje odpovídající orgán - centrální banka. Slovo „fiat" značí v anglickém jazyce „rozkaz".
[5] Zkratka používána pro jednotky bitcoinové měny, lze to přirovnat ke zkratce USD pro americký dolar.
[6] Označuje kolísavost ceny daného aktiva.

nejsilnějšího hráče na trhu, tedy Bitcoin, je kolísání cen prakticky na denním pořádku. Jako jeden z hlavních faktorů způsobujících vysokou volatilitu je uváděná nízká likvidita[7]. Trh kryptoměn je tvořen převážně drobnými investory a chybí mu vyspělost akciového trhu. V případě, že se Bitcoinu povede oslovit větší procento lidí a institucionálních investorů, kteří přinášejí vysokou úroveň likvidity pomocí jejich kapitálu, dojde ke snížení volatility. Celý tento proces však může trvat desítky let. [3; 13; 14; 15]

1.2.3 Bezpečnost

Bezpečnost by měla být u všech typů měn na prvním místě. Je důležité, aby celý systém byl co nejvíc imunní vůči napadení a byl schopen zabránit jakékoliv formě podvádění. I přesto, že je standardní měna centrální bankou zabezpečována pomocí sofistikovaných bezpečnostních mechanismů, stále k podvodům dochází. Velice časté je např. padělání hotovosti. Ve světě kryptoměn žádná centrální banka nebo jiná autorita, která by zajišťovala provoz celého systému, neexistuje. Důvěra je kladena do rukou kryptografie. Tento obor představuje rozsáhlé pole akademického výzkumu využívajících mnoho složitých matematických technik. Některé z nich jsou kryptoměnami využívané. Mezi ty nejznámější patří kryptografická hashovací funkce a digitální podpis. Tyto nástroje jsou využívány například k zabránění neoprávněné manipulace s finančními prostředky. Přístup k nim má pouze jejich majitel, tedy osoba, která disponuje správným klíčem nebo šifrou. Nutno je podotknout, že i přesto, že je systém zabezpečen velice sofistikovaným šifrováním, záleží hlavně na uživatelích, do jaké míry bude jejich majetek v bezpečí. Ztráta či odcizení privátního klíče může mít za následek ztrátu finančních prostředků. [5; 16]

1.2.4 Neměnnost

Při provádění plateb prostřednictvím internetového bankovnictví se může kdykoliv stát, že dojde k mylnému zadání čísla příjemce. V takové situaci každý uživatel neváhá a kontaktuje banku s prosbou o pomoc. Kryptoměny takovou možnost nenabízí, jelikož zde žádná centrální autorita neexistuje. Jakákoliv transakce, která je zaznamenána na blockchain a dostatečněkrát potvrzená, je pak nevratná a neměnná. Ke změně dat na blockchainu může dojít pouze v případě, že výpočetní výkon sítě není dostatečný a je proveden útok na síť tzv. 51% attack, kterému v lednu 2020 čelil Bitcoin Gold. [10; 17]

[7] Ukazatel, který znázorňuje, jak rychle lze proměnit aktiva na hotové peníze s malým dopadem na jejich hodnotu.

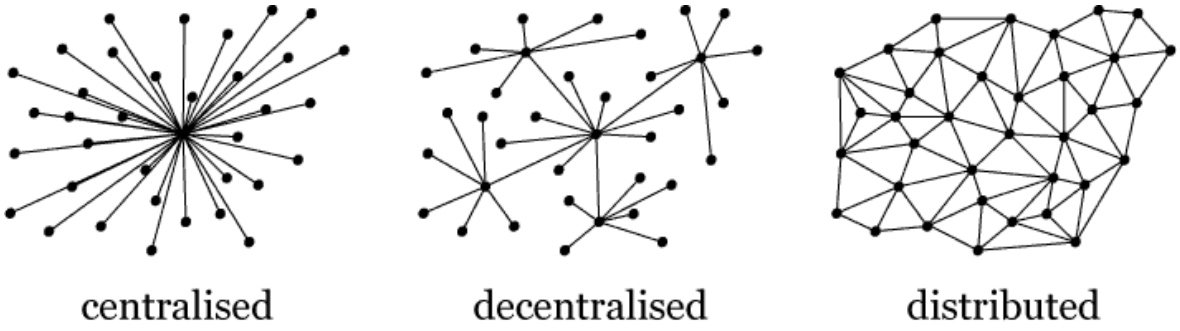
1.2.5 Anonymita / pseudo-anonymita

Lidé si často pod kryptoměnami představí nástroj pro financování trestních činností, praní špinavých peněz a mnoho dalších nelegálních aktivit. Vychází totiž z přesvědčení, že kryptoměny jsou zcela anonymní. Je pravda, že se na trhu vyskytují měny, které byly vytvořené primárně za účelem dokonalé anonymity. Mezi tyto měny se řadí například Monero nebo Zcash. Avšak v případě těch nejpopulárnějších kryptoměn, jako příklad může sloužit Bitcoin, se hovoří spíše o pseudo-anonymitě, jelikož není zcela tak anonymní, jak se může zdát. V běžné praxi se pro provádění finančních transakcí využívá bankovní účet, zřízený bankou na základě poskytnutých identifikačních údajů. Uživatel však může mít svůj „bankovní účet“ také u Bitcoinu. Zřízení takového účtu, který je ve formě bitcoinové adresy, probíhá zdarma a bez nutnosti poskytování jakýchkoliv osobních údajů. Tento fakt přispívá k domnění, že je systém zcela anonymní. Nesmí se však zapomenout na to, že záznamy na blockchainu jsou transparentní a hlavně kompletní. Je tedy možno dohledat kompletní transakční historii bitcoinových adres. Na základě těchto faktorů se o Bitcoinu mluví jako o pseudo-anonymní měně i přes fakt, že uživatel může disponovat libovolným počtem adres. [18; 19; 20]

1.2.6 Decentralizace

Základní vlastností Bitcoinu a většiny kryptoměn je jejich decentralizace do peer to peer[8] (P2P) sítě. U tradičních fiat měn je celý finanční systém kontrolován centrální autoritou a bankami. Decentralizace u kryptoměn znamená, že systém nemá žádný centrální bod. Veškeré transakce jsou zpracovávány distribuovanou sítí, která je tvořena tisíci počítači, kterým se říká uzly (obrázek na další straně demonstruje, v čem se jednotlivé sítě liší). Každý plnohodnotný uzel disponuje kompletní databází všech transakcí (blockchainem), které kdy byly v síti provedeny. Žádný z těchto uzlů nemá kontrolu nad sítí, všichni členové jsou rovnocenní. Pokud dojde k napadení kteréhokoliv z nich, nemá to na fungování sítě žádný vliv. Pro vyřazení sítě z provozu by bylo nutné zneškodnit všechny uzly. Vzhledem k tomu, že přesný počet všech uzlů v síti je v podstatě nezjistitelný, je vyřazení sítě v dosavadních podmínkách téměř nemožné. [9; 21; 22]

[8] Typ sítě, kde jednotlivé uzly komunikují přímo mezi sebou. Nevyskytuje se zde centrální server, který by jednotlivé uzly propojoval a komunikaci mezi nimi zprostředkovával.



Obrázek 1 Typy sítí [23]

1.3 Rozdělení kryptoměn

Nejzákladnější dělení kryptoměn je na Bitcoin a Altcoiny, do kterých spadají všechny ostatní kryptoměny. Poněkud složitější, a ne obecně zcela známé dělení poskytuje stránka coinmarketcap.com, kde se kryptoměny rozlišují podle dalších dvou kategorií, konkrétněji na coiny a tokeny. [3; 24; 25]

1.3.1 Coiny

Coiny jsou kryptoměny, které disponují vlastním blockchainem a fungují nezávisle na jiných kryptoměnách. Dělí se na:

1. Bitcoin
2. Hard forky Bitcoinu
3. Altcoiny vzniklé předěláním zdrojového kódu Bitcoinu
4. Altcoiny s originálním zdrojovým kódem [9; 24]

Dále jsou výše uvedené pojmy vysvětleny.

Hard forky Bitcoinu

Do této kategorie patří měny, které vznikly na základě odlišných představ lidí o fungování Bitcoinu. Podstatou je „tvrdé rozdělení sítě“ na více větví, které nejsou díky nově nadefinovaným pravidlům vzájemně kompatibilní. Mezi nejznámější příklady patří Bitcoin Cash. [9; 26]

Altcoiny vzniklé předěláním zdrojového kódu Bitcoinu

Před nástupem Etherea v roce 2015 vznikaly nové kryptoměny převážně jako klony Bitcoinu. Programátoři naklonovali zdrojový kód Bitcoinu, upravili některé parametry a své dílo prezentovali jako novou kryptoměnu. Ve většině případů docházelo ke změnám

hashovacího algoritmu, rychlosti tvorby bloků a míry inflace. Tímto způsobem došlo k tvorbě stovek nových kryptoměn, z nichž jenom malé procento se „dožilo“ současnosti[9]. Do této kategorie altcoinů lze zařadit např. Litecoin, Dogecoin nebo také Namecoin. [9; 24; 25]

Altcoiny s originálním zdrojovým kódem

Hledání originální koncepce a konkurenceschopné kryptoměny pro Bitcoin ukončil příchod Etherea. Ten disponuje vlastním originálním kódem a přináší velké množství nových funkcionalit ve formě smart kontraktů, decentralizovaných aplikací a možností jednoduchého generování nových tokenů. [9]

Do této kategorie dále patří např. měna XRP, která dle tržní kapitalizace představuje třetí největší kryptoměnu. XRP původně nebyl navržen jako kryptoměna a dle některých fanoušků Bitcoinu se o ní ani nejedná - jsou přesvědčeni, že nesplňuje základní vlastnosti, které by měla typická kryptoměna mít, řeč je převážně o svobodě a decentralizaci. [3; 9; 27]

1.3.2 Tokeny

Výše zmíněné coiny disponují svým vlastním blockchainem, což představuje jejich hlavní rozdíl od tokenů. U tokenů totiž k tvorbě blockchainu nedochází a celá jejich existence je založena na blockchainu jiné kryptoměny, která umožnuje jejich tvorbu. Jako takový token je možné si představit žeton v kasinu. Jde o určitý poukaz, který je používán v daném systému a pro jehož členy má určitou hodnotu. Avšak při použití takového tokenu v jiném systému je jeho hodnota téměř nulová. I když krypto token se v normálních fyzických kasinech nepoužívá, hojné využití najde ve světě kryptoměn. Zde slouží jako uchovatel hodnoty, lze si za něj koupit cloudové úložiště, zafinancovat tvorbu smart kontraktů nebo také obchodovat na speciálních burzách/směnárnách jako je Kraken nebo Coinbase. [9; 25]

Tvorba tokenů probíhá za pomoci smart kontraktů na určité platformě, která poskytuje bezpečnou síť a peněženky. Mezi nejznámější platformy patří již několikrát zmíněné Ethereum. A proč vůbec takové tokeny existují? Jejich tvorba většinou vzniká v rámci ICO[10], kdy firma na výše zmíněné platformě vytvoří tokeny. Ty jsou následně určeny k prodeji investorům, kteří je kupují za své kryptoměny s vidinou zisku. Firma tímto

[9] leden 2019
[10] Initial Coin Offering - jedná se o veřejnou nabídku tokenů. V praxi se ale zažil název ICO obsahující slovo „coin“.

způsobem získá základní kapitál pro financování svého nového projektu, o kterém je přesvědčena, že je revoluční a v budoucnu investorovi přinese výdělek ve formě růstu ceny daného tokenu. Celý tento proces připomíná veřejnou nabídku akcií IPO neboli Initial Public Offering, kterým se ICO inspirovalo. [9; 28]

1.4 Dobrá kryptoměna

Větší zájem společnosti o kryptoměny se neprojevuje pouze prudkými vzrůsty ceny bitcoinu a altcoinů, ale také jejich rostoucím počtem. K růstu počtu kryptoměn napomáhá i již výše zmíněné ICO, které představuje pro firmy novou metodu financování. Dnes se na světě vyskytuje tolik kryptoměn, že se v nich začali ztrácet i odborníci. Jak tedy rozeznat tu dobrou, od té špatné, či dokonce podvodné? [7]

V první řadě je potřeba, aby taková kryptoměna řešila nějaký reálný problém. V případě Bitcoinu se jedná o nahrazení dnešní běžné měny a vrácení plné kontroly nad penězi zpátky do rukou lidí. Dále například Ethereum má v úmyslu vytvořit decentralizovaný počítač světa. Ripple usiluje o nahrazení současného systému SWIFT, který využívají banky pro mezibankovní transakce. [7; 29]

Pro zachování decentralizace je nutné, aby kryptoměna měla dobře vyřešenou distribuci. Distribuce Bitcoinu probíhá na základě předem stanoveného plánu, díky kterému je známo, kdy bude poslední bitcoin vytěžen. Jiným způsobem to má vyřešen Peercoin, který využívá metodu Proof of Stake, která je založena na dodávání nových mincí držitelům jako formu úroku. V poslední době řada nových měn sází na metodu zvanou „Premine“ neboli předtěžení, kdy tvůrci kryptoměny vytěží veškerou měnu hned na začátku a následně ji prodávají investorům. Majoritní část si však nechávají. To jim zajišťuje obrovský vliv na měnu. Předtěžení kryptoměn však přináší i pár výhod, jako jsou nízké poplatky a rychlost transakcí. To vše je ovšem na úkor značné centralizace, na kterou se váže i velká zranitelnost. [7; 30]

Před koupí kryptoměny se investorovi doporučuje provést jednoduchou analýzu, za účelem zjištění základních vlastností o dané kryptoměně. Užitečný je například průzkumu fór, které obsahují názory a recenze ostatních investorů. Zájemci dále můžou zjistit, na kterých burzách se daná kryptoměna obchoduje nebo kdy se v jejich nabídce vyskytne. Také se považuje za vhodné sledovat, jak komunita a tým vývojářů pracují na zlepšení zdrojového kódu, který se obvykle nachází na otevřených softwarových platformách jako je třeba GitHub. [9; 31; 32]

2 BITCOIN

Bitcoin coby otec kryptoměn je měna s aktuálně největší tržní kapitalizací. V lednu 2020 tomu bylo přesně 11 let, kdy byl jeho dosud neznámým zakladatelem Satoshi Nakamotem vytěžen tzv. genesis blok, který na svět přivedl prvních 50 BTC. Historie Bitcoinu však sahá ještě dál než do roku 2009. Již v roce 2008, přesně 18. srpna byla Satoshim zaregistrována doména bitcoin.org, která funguje doposud. O pár měsíců později, tedy 31. října 2008 zveřejnil Satoshi tzv. white paper s názvem „Bitcoin: A Peer-to-Peer Electronic Cash System“, ve kterém popsal podstatu Bitcoinu a účel celého systému. Poté, co došlo k vytvoření Bitcoinu, se Satoshi ještě určitou dobu podílel na účelových fórech, kde uživatelům poskytoval rady. Přelomový se stal rok 2010, kdy předal doménu bitcoin.org fanouškovi a softwarovému vývojáři Gavinu Andresenovi a pro veřejnost „zmizel“. Dodnes se stále vedou polemiky nad tím, zda Satoshi Nakamoto byl jedinec, či skupina lidí. [3; 7; 9; 33]

Jak je zmíněno výše, Bitcoin je zde již 11 let. Za tak krátkou dobu mu bylo dopřáno velké pozornosti. Aktuálně[11] 1 bitcoin stojí v přepočtu na české koruny 222 tisíc Kč a v oběhu je jich něco málo přes 18,2 milionů kusů s tím, že přibližně co 10 minut dochází k vytěžení 12,5 nových[12]. Ovšem maximální počet BTC je fixně nastaven na 21 milionů mincí, což znamená, že k vytěžení posledního BTC dojde v roce 2140. Vhodné je zmínit, že pod slovem Bitcoin se neskrývá pouze kryptoměna, ale celá peer-to-peer síť tvořena tisíci počítači, přinášející revoluční platební systém. Někdy tedy není zcela jasné, o čem se pojednává, proto se v psané podobě zavedly pojmy „bitcoin“ a „Bitcoin“, kdy pojem „Bitcoin“ se využívá pro označení celé bitcoinové sítě a „bitcoin“, kterým je myšlena jednotka měny. [3; 7; 34; 35]

2.1 Princip funkce

Tato podkapitola popisuje základní stavební kameny Bitcoinu a dává si za úkol vysvětlit princip funkce celého systému - například jak fungují transakce, co to vlastně bitcoin je a jak dochází k jeho tvorbě.

[11] 22.2.2020

[12] V polovině května roku 2020 má dojít k tzv. halvingu, což je proces zmenšení odměny z 12.5 BTC na 6.25.

2.1.1 Bitcoinová síť

Základním stavebním kamenem, jenž umožňuje samostatnou existenci bitcoinu, je jeho bitcoinová síť. Jak již je zmíněno v první kapitole, jedná se o decentralizovanou peer-to-peer síť tvořenou tisíci navzájem si rovnými počítači, které jsou připojeny k Internetu a pro síť plní určité funkce. Tyto počítače jsou označovány jako uzly a v Bitcoinu jich existuje několik typů. S tím, že ne všechny plní stejnou úlohu. Společně se však všechny podílí na správě a chodu sítě, což umožňuje tvorbu transakcí, jejich potvrzování, distribuci a v neposlední řadě těžbu nových bitcoinů. Nutné je podotknout, že všechny uzly jsou rovnocenné. Neexistuje žádná hierarchie, která by určovala hlavní, či jinak výjimečný uzel. V případě, že nějaký uzel přestane pracovat, nemá to sebemenší vliv na funkčnost sítě. [5; 9; 36]

Provoz uzlu, který neprovádí těžbu, si může dovolit prakticky každý, kdo užívá rychlý internet, má pár stovek GB volného úložiště, 2 GB RAM a bitconového klienta[13]. V případě těžby je situace poněkud složitější. Pro takový provoz je potřeba instalovat speciální software a hlavně disponovat extrémním výpočetním výkonem, který dnes přesahuje možnosti i kvalitního stolního počítače. V dnešní době se těžba na klasických počítačích neprovádí, je totiž nerentabilní. [9; 37]

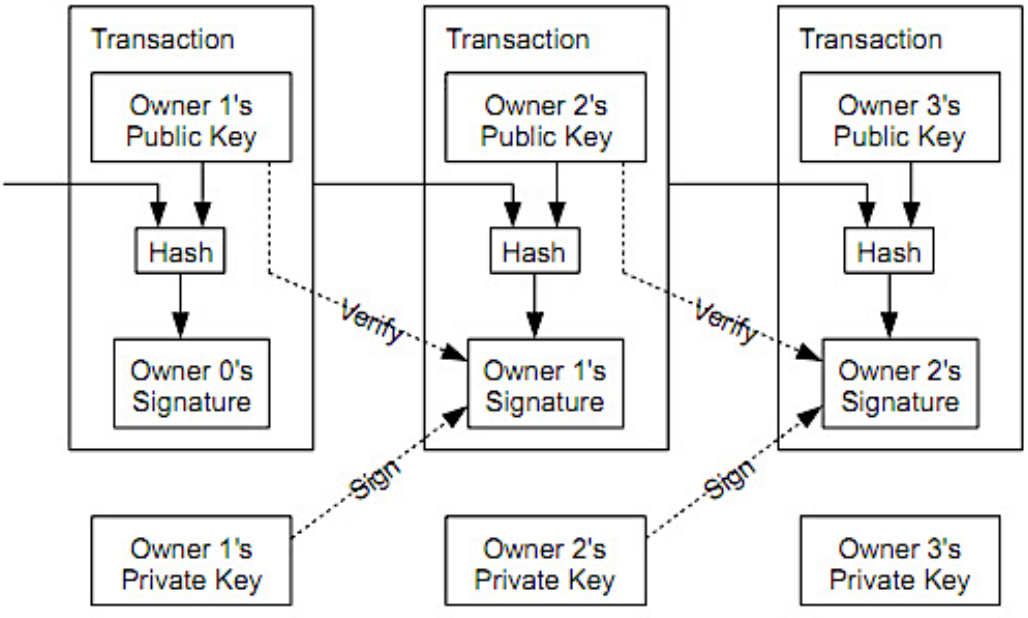
2.1.2 Transakce

Transakce se používají za účelem převodu určitého množství bitcoinů z adresy odesílatele na adresu příjemce. Bitcoin není ve své podstatě nic jiného než řetězec digitálních podpisů, který v sobě nese informaci o předcházejících transakcích. Každá transakce je definovaná vstupy a výstupy. Vstupy odkazují na výstupy nějaké již existující transakce (ty, pomocí kterých uživatel mince nabyl) a výstupy, které jsou tvořeny bitcoinovými adresami, na které jsou mince poslány. Tímto se výrazně odlišuje od tradiční fiat měny a nesplňuje tedy vlastnost zaměnitelnosti - každá mince bitcoinu má totiž svoji transakční historii. V případě, že chce odesílatel poslat svoji minci, potřebuje k tomu znát svůj privátní klíč, díky kterému je schopen s mincí manipulovat a veřejný klíč příjemce. Převod pak funguje tak, že odesílatel digitálně podepíše výstup předchozí transakce (díky které daný bitcoin nabyl) společně s veřejným klíčem příjemce. Tento digitální podpis se přiřadí k minci (čili k řetězci digitálních podpisů) a je odeslán do sítě. Odesílatel tedy provedl transakci, ve které na základě digitálního podpisu veřejného klíče příjemce určuje, kdo je nový vlastník

[13] Např. Bitcoin Core, což je open-source software, který je zdarma ke stažení na bitcoin.org.

mince. S mincí bude moci dále nakládat jenom ten, kdo k onomu veřejnému klíči vlastní i klíč privátní. [7; 33; 38]

Níže, na obrázku se nachází samotné schéma transakce, které Satoshi uveřejnil ve svém white paperu.



Obrázek 2 Schéma transakce v Bitcoinu [33]

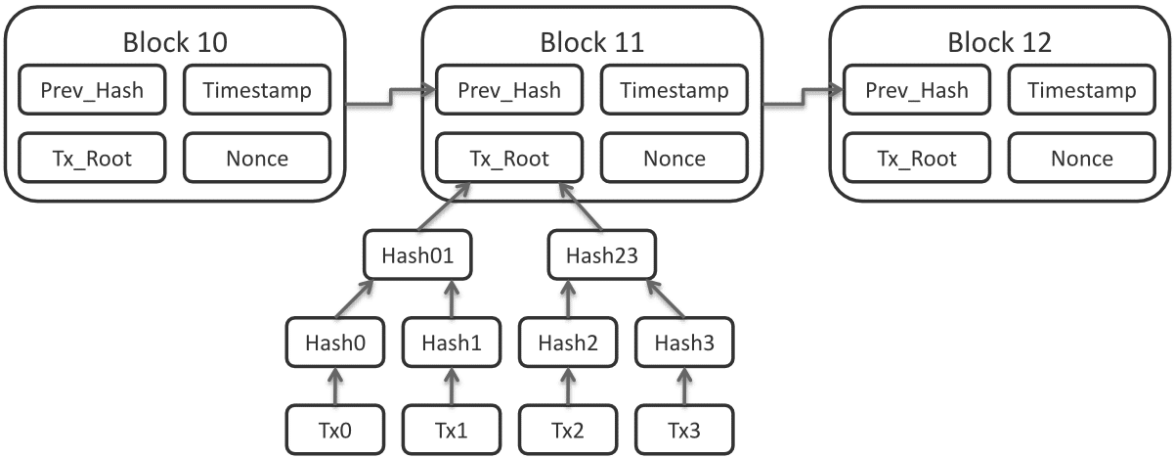
2.1.3 Blockchain

Blockchain představuje decentralizovanou databázi, která je distribuovaná po celé síti a obsahuje záznamy všech transakcí provedených v Bitcoinu od jeho počátku. Jednotlivé transakce jsou uspořádány do bloků, které jsou označeny časovou značkou. Jedná se tedy o řetězec bloků, které jsou navzájem propojené kryptografií, konkrétně hashovací funkcí. Každý blok v sobě skrývá hash bloku předchozího čili jednotlivé bloky na sebe navzájem odkazují. Jakákoliv úprava informace v bloku vede ke změně hashe, což zapříčiní narušení návaznosti bloků. Díky tomu je téměř nemožné jakýmkoliv způsobem upravovat či nahradit data v již existujícím bloku. O blockchainu se tedy mluví jako o neměnné databázi, do které lze jen zapisovat. Zápis je umožněn na základě konsenzu čili vzájemné shodě uzlů v síti, ovšem prohlédnutí databáze je umožněno komukoliv, je totiž veřejně dostupná. [39; 40; 41]

Blok

Veškeré transakce, které proběhly v rámci Bitcoinu, jsou uloženy v blocích, které se řetězí. Bloky disponují maximální kapacitou 1 MB, proto není možné, aby byly všechny

transakce uloženy do jednoho. Pro vytvoření základní představy lze blockchain přirovnat k účetní knize, kdy jeden blok reprezentuje stránku knihy. Pro veškeré bloky je definovaná struktura, která je tvořena ze dvou částí. První část představuje hlavička bloku, která obsahuje hlavně hash předchozího bloku, časovou značkou, náhodné číslo tzv. nonce, kořen Merkleova stromu (viz. obrázek č. 3). Druhou část tvoří tělo, které disponuje veškerými transakcemi, které blok zahrnuje. [9; 38; 42]



Obrázek 3 Struktura hlavičky bloku [43]

Přidání nového bloku

Činnost, při které dochází k hledání nového bloku, který by mohl být přidaný do blockchainu, se nazývá těžba a provádí ji pouze těžaři. Ti poskytují síti svůj výpočetní výkon, který je využíván k potvrzování transakcí, tvorbě nových bitcoinů a zajištění bezpečnosti sítě. Princip těžby je následující: V momentě, kdy uživatel vytvoří transakci, dojde k jejímu odeslání do sítě, kde si ji jednotlivé uzly předávají mezi sebou a ukládají do svého mempoolu. Mempool je virtuální prostor, ve kterém se nachází veškeré nepotvrzené transakce. Aby byla transakce do tohoto poolu zařazena, musí být uzlem ověřena její správnost. Dále přichází na řadu činnost těžařů, kteří si z mempoolu vybírají transakce, ze kterých sestaví blok. Sestavení bloku probíhá tak, že těžař zahashuje mezi sebou dvě transakce a jejich výsledný hash připojí k hashi jiných dvou transakcí a vytvoří hash nový. Tuto činnost provádí těžař tak dlouho, dokud nevznikne pouze jeden hash transakcí, tzv. kořen Merkleova stromu. Ten spolu s dalšími parametry tvoří hlavičku bloku. V posledním kroku se těžař pomocí změny náhodného čísla nonce snaží najít takový hash hlavičky, který splňuje podmínku náročnosti sítě[14]. V momentě nalezení odesílá těžař tento blok do sítě, kde jej uzly ověřují. V případě, že ho uzel shledá jako validní, uloží si jej do

[14] Každých 2016 bloků je náročnost sítě upravována tak, aby vytěžení 1 bloku trvalo přibližně 10 minut.

blockchainu a pošle jej dál. Celý proces je založen na principu zvaném Proof of Work, neboli důkaz o práci. Tedy principu, kdy se těžař snaží objevit kus dat, který je časově náročný na nalezení, avšak jeho správnost lze velice jednoduše ověřit. Těžaři, kterému se povedlo najít správný blok, obdrží odměnu ve výši 12,5 BTC[15], kterou do bloku přináší tzv. coinbase transakce.[16] Dále si ponechá poplatky za transakce, které vytěžením potvrdil. [7; 9; 33; 44; 45; 46]

Otázkou tedy zůstává, jak veliký výpočetní výkon musí těžař poskytnout, aby měl šanci na nalezení bloku. V roce 2009, kdy započala existence Bitcoinu, se prováděla těžba na procesorech (CPU) obyčejných kancelářských počítačů. Jak konstatoval Dominik Stroukal a Jan Skalický [7]: „*Když se snažil sám Satoshi Nakamoto vyřešit „nultý" příklad, stačilo mu prakticky pouze zapnout počítač*". S rostoucím počtem těžařů i přímo úměrně rostla podmínka náročnosti sítě. Již v roce 2010 se objevila metoda těžby na grafické karty, která umožňovala řešit více výpočtů najednou. To proti těžbě na CPU přinášelo značnou výhodu. Vývoj šel nezastavitelně dál a o necelý rok a půl později se na trhu objevil program umožňující těžbu na FPGA[17]. Jedná se o relativně levné zařízení skládající se z programovatelných obvodů umožňující tvorbu procesoru, zaměřeného na určitý druh operací. Zařízení nebylo sice výkonnější než grafická karta, avšak disponovalo velice nízkou spotřebou elektřiny, což při propočtu vycházelo na cenově přijatelnější investici. Vývoj se zastavil v roce 2012, kdy se začalo používat těžební zařízení ASIC, což je speciální druh integrovaného obvodu, který byl vyroben pouze pro určitou činnost. Jedná se tedy o přístroj, který neumí nic jiného než těžit. V současnosti je těžba prováděna výhradně pomocí těchto zařízení a navíc, aby těžaři zvýšili svoji šanci na nalezení validního bloku, seskupují se do tzv. poolu. V případě, že se poolu povede blok vytěžit, je odměna rozdělena mezi jednotlivé členy dle vykonané práce. [7; 9; 44; 47]

2.2 Použití bitcoinu

Cílem této podkapitoly je nastínit základní možnosti získání bitcoinu, formy jeho uložení a možnosti jeho využití.

[15] V polovině května roku 2020 má dojít k tzv. halvingu, což je proces zmenšení odměny z 12.5 BTC na 6.25.
[16] Jedná se o první transakci v bloku, která vytváří nové bitcoiny.
[17] Field Programmable Gate Array neboli programovatelné hradlové pole.

2.2.1 Jak získat bitcoin

Získat bitcoin již nepředstavuje žádný problém. Možností je čím dál více a záleží už jenom na každém, zda zvolí cestu nákupu, prodeje či těžby. [48]

Nákup

Nákup bitcoinů není příliš složitý. Možností je mnoho. Zájemce může zkusit navštívit např. stránku localbitcoins.com, která propojuje prodejce s kupci. Uživatel si na základě cenových nabídek, referencí, podporované banky atd. vybere prodejce, kterého zkontaktuje a domluví se s ním na způsobu platby a předání. Komu tato forma nevyhovuje, může zkusit sice sofistikovanější, za to ale rozšířenější burzy, směnárny či bitcoinové bankomaty. [49; 50]

- **Burzy a směnárny**

  Pořízení bitcoinu na kryptoměnových burzách či směnárnách patří mezi nejpoužívanější formu nákupu. Proti nákupu přes automat nabízí uživateli mnohem větší výběr kryptoměn a zároveň poskytuje i svobodnější volbu, jelikož kryptoměnových směnáren a burz se na světě vyskytuje nemalý počet. Některé z nich demonstruje tabulka č. 1, která se nachází na další straně [7; 51]

  Princip funkce kryptoměnové burzy je prakticky stejný, jako princip jakékoliv jiné burzy. Je to místo, kde se střetává nabídka s poptávkou a dochází zde k uskutečnění obchodů. Burza profituje z poplatků, které uživatelé zaplatili při převodu. Kryptoměnová burza je vhodná pro všechny, kteří chtějí nakupovat bitcoin za nejlepší možný kurz či si vyzkoušet trading. Daní za to je časová náročnost při registraci, kdy uživatel musí poskytnou své osobní údaje a projít zdlouhavými procesy ověřování identity. Alternativou se tedy stává kryptoměnová směnárna, u které si v některých případech uživatel vystačí pouze s peněženkou, emailem a kreditní kartou. Jeden z rozdílů mezi burzou a směnárnou je v tom, že směnárna si kurz určuje sama. Profituje z tzv. spreadů, což je rozdíl mezi nákupní a prodejní cenou. Díky tomu neposkytuje tak výhodně kurz, jak je tomu u burz. Kompenzací ovšem může být její jednoduché a přehledné ovládání. [7; 51; 52]

Tabulka 1 Výčet některých krypto směnáren a burz

Směnárny	**Burzy**
Simplecoin	Kraken
Coinbase	Binance
LocalBitcoins	Coinmate

Zdroj: [52]

- **Bitcoinové bankomaty**

  Představují automatizovanou směnárnu, která svým vzhledem připomíná tradiční bankomat, který ovšem v tomto případě slouží k nákupu či prodeji BTC za hotovost. Existují dva typy bankomatů, jednosměrný a obousměrný. Jednosměrný umožnuje kupci bitcoiny pouze nakoupit, zatímco obousměrný i prodat. Vše, co uživatel potřebuje, je patřičný finanční obnos a bitcoinovou peněženku. Kde se jednotlivé bankomaty nachází, může uživatel zjistit na stránce coinatmradar.com [9; 53]

Prodej

Další variantou představující možnost získání bitcoinu je prodej. Prodej je myšlen ve smyslu nabízení produktů nebo služeb výměnou za bitcoin. V posledních letech roste počet subjektů, nabízejících možnost platit v kryptoměnách, což je ze strany kryptoměnových zastánců vítáno. Mezi světové giganty akceptující úhradu v bitcoinech patří například firma Microsoft, u které si může uživatel pomocí bitcoinu nakoupit hry, filmy a aplikace v obchodech pro Windows a Xbox. Další velice známou je Shopify. Ta svým klientům umožňuje hradit předplatné pomocí bitcoinu, litecoinu a etherea. Za zmínku stojí také všem známá online encyklopedie Wikipedia, která se rozhodla přijímat sponzorské dary i v bitcoinech. [54; 55; 56]

A jak je na tom Česká republika? Možností pro uplatnění bitcoinů je řada. Mezi nejznámější obchodníky akceptující kryptoměny patří e-shop Alza.cz. Ten přijímá platbu v bitcoinech, litecoinech a nově zavedl i možnost nákupu kryptoměn přímo na pobočkách prostřednictvím terminálu Alza. Kromě Alzy nabízí širokou škálu příležitostí, kde utratit bitcoin i hlavní město Praha. Lidé si zde mohou dát například kávu v Paralelní Polis, doplnit nádrž svému autu na čerpací stanici KRYPTO, najíst se v řadě restaurací anebo dokonce zůstat na noc v Apartmánech Siesta. [9; 57; 58]

Nejlepší možnost, jak získat přehled, je navštívit stránku coinmap.org. Tato webová stránka sbírá informace o místech, kde lze uplatnit bitcoin a následně je prezentuje na graficky zpracované mapě světa. V době psaní této práce zobrazuje cca 16 000 míst na celém světě, kde lze bitcoin využít. [59; 60]

Těžba

Další formou jak nabýt bitcoiny je těžba. Těžbou se práce zabývá výše v podkapitole „Blockchain“.

2.2.2 Způsoby uložení

Aby mohl uživatel používat bitcoiny, potřebuje si pořídit kryptoměnovou peněženku. Peněženka představuje softwarovou aplikaci, která umožňuje tvorbu transakcí, zajišťuje generování a správu klíčů i adres. Zároveň poskytuje uživateli přehled, kolik prostředků se na jeho jednotlivých adresách nachází. Uživatel má možnost si vybrat z několika typů peněženek, většina je zdarma, některé varianty jsou však zpoplatněné. Mezi ty nejznámější typy patří peněženky hardwarové, papírové, desktopové, mobilní, webové. Peněženkou může být také i samotný bitcoinový klient. [9; 61]

Mobilní peněženky

Jak už z názvu vypovídá, jde o peněženku ve formě aplikace, instalovanou uživatelem do mobilního telefonu. S rostoucím počtem obchodů, které přijímají bitcoin roste i oblíbenost této formy peněženky. Adresy a klíče má uživatel uložené ve svém telefonu, což mu umožňuje provádět transakce prakticky odkudkoliv, kde má přístup k Internetu. Mezi takové nejznámější peněženky patří Jaxx, Coinomi a Mycelium. Tento typ peněženky je vhodný pro uživatele, kteří za své bitcoiny pravidelně něco kupují. Nutné je ovšem vzít v potaz, že v případě ztráty, odcizení nebo napadení telefonu, může uživatel o své bitcoiny přijít. Nejedná se tedy o nejbezpečnější formu uložení. [61; 62]

Desktopové peněženky

Uživatelé, kteří nedisponují chytrým telefonem nebo preferuji spíše práci na počítači, mohou zvážit umístění peněženky do svého PC. Princip funkce je podobný, jak tomu je u mobilních peněženek. Jako desktopovou peněženku lze využít i bitcoinového klienta, což sice přináší nevýhodu v podobě nutnosti stažení celého blockchainu. To představuje desítky GB, avšak zbavuje uživatele nutnosti důvěřovat vývojářům jiných typů peněženek.

Jak již bylo uvedeno, samotný bitcoinový klient tvoří jeden ze základních kamenů celé sítě. [9; 63]

Webové peněženky

Webové peněženky jsou nejméně doporučovanou formou uložení bitcoinů. Celý princip spočívá v tom, že si uživatel vytvoří peněženku online u některého z poskytovatelů (například coinbase.com) a převede zde své bitcoiny. Veškeré klíče a adresy tedy zpracovává třetí strana, uživatel není přímým vlastníkem bitcoinu. V minulosti došlo k vykradení mnoha webových peněženek, tato krádež je téměř nenávratná. Před vytvořením takové peněženky by měl uživatel zvážit, zda opravdu svěří své peníze třetí straně. [7; 64]

Hardwarové peněženky

O vytvoření prozatím nejbezpečnější formy uložení krypto peněz se postaral český startup SatoshiLabs. Firma představila hardwarovou peněženku, která se jmenuje TREZOR. Jedná se o jednoúčelový počítač o velikosti flash disku, který v sobě uchovává klíče k peněžence, nainstalované na počítači či mobilním telefonu. Každá transakce vytvořená uživatelem, musí být před odesláním podepsána klíčem, který se nachází v hardwarové peněžence. Tedy pro odeslání transakce musí uživatel pomocí USB připojit TREZOR k počítači a stiskem tlačítka nacházejícím se na TREZORU, transakci podepsat. Díky tomu, že privátní klíč nikdy neopouští hardwarovou peněženku, je možné bezpečně odeslat transakci i ze zavirovaného počítače. Dnes se na trhu kromě SatoshiLabs vyskytují i další výrobci poskytující tento typ peněženky. [38; 65; 66]

Papírové peněženky

Hojnou oblibu mají i tzv. papírové peněženky. Název opravdu neklame, jedná se o list papíru, na kterém je vytištěna adresa a privátní klíč. Samotný vzhled peněženky připomíná bankovku. Mezi nesporné výhody patří její hmotné provedení, které zajišťuje, že po vytvoření a vytisknutí peněženky, se nedá nijak vzdáleně napadnout. Avšak stejně jako u klasických bankovek může dojít ke ztrátě, odcizení či zničení. Uživatel si může takovou peněženku vytvořit na stránce bitadrress.org, kde se nachází JavaScriptový generátor, který na základě pohybu myší náhodně vygeneruje adresu a privátní klíč. Samotný generátor funguje i off-line, pro zajištění větší bezpečnosti je doporučováno načíst webovou stránku a před tvorbou peněženky odpojit zařízení od Internetu. [38; 61]

2.3 Výhody a nevýhody

Kromě velikého spektra výhod, ať už ve formě omezeného množství, decentralizace, pseudo-anonymity, vysoké bezpečnosti má Bitcoin i své stinné stránky. Například nenávratnost transakce nebo špatnou škálovatelnost[18]. Těmito vlastnostmi se práce v této podkapitole nezabývá, jelikož mnohé z nich již byly rozebrány. Autor se zde spíše zabývá některými body, které mohou uživatele přivést k zamyšlení a záleží pouze na něm, zda je zařadí mezi výhody či naopak nevýhody. [67]

2.3.1 Zodpovědnost

Kryptoměny včele s Bitcoinem vrací uživatelům plnou kontrolu nad jejich penězi. Uživatelé nejsou limitováni v jeho nakupování, provádění transakcí a nezaleží na tom, zda je den, noc či víkend. Kromě samotného vlastníka zde neexistuje nikdo, kdo například určuje výši transakčních poplatků. Vyřazení prostředníka, tedy banky, z tohoto systému ovšem nemusí vyhovovat všem. Nutnost bezpečného uchování privátního klíče či seedu[19] vyžaduje značnou zodpovědnost. [16; 68]

2.3.2 Vysoká volatilita

Nestabilita ceny kryptoměny může fungovat jako dobrý sluha, ale i zlý pán. Zkušení burzovní obchodníci využívají cenové skoky bitcoinu ve svůj prospěch a uskutečňují spekulativní obchody za účelem výdělku. S tímto je také spjato značné riziko. Bitcoin už několikrát v historii ukázal, že jeho cenový vývoj může být nepředvídatelný. Avšak vysokou volatilitu lze brát i jako bezplatný prostředek propagace. S rostoucí volatilitou roste i počet článků v médiích zabývající se Bitcoinem. [69; 70]

2.3.3 Množství adres

Pro zvýšení anonymity si může uživatel pro každou transakci vygenerovat novou adresu. Tento fakt může vést k přesvědčení, že dochází k plýtvání adres. Je pravda, že počet možných adres je omezený. Avšak i v případě, že by byl člověk schopen vygenerovat 1 bilion klíčů za sekundu, potřeboval by k vypočítání všech adres 3,7 noniliard let[20]. [7; 71]

[18] Této je věnována celá praktická část této práce.
[19] Seznam 12-24 slov, které slouží k obnově peněženky.
[20] 1 noniliarda se prezentuje zápisem 10^{57}.

3 ALTCOINY

Alternativou k Bitcoinu jsou Altcoiny. Mezi Altcoiny lze řadit veškeré kryptoměny, které vznikly po Bitcoinu a mají svůj vlastní blockchain. Samotné slovo „altcoin“ vzniklo složením slov „alternative“ a „coin“, což lze volně přeložit jako alternativní měna. [72]

Po spuštění Bitcoinu v roce 2009 netrvalo dlouho a ukázaly se další projekty. Již v roce 2011 byl spuštěn první Altcoin pod názvem Namecoin, který se od Bitcoinu v mnoha věcech neliší. Namecoin disponuje totožným počtem mincí, periodou bloku a také hashovým algoritmem. Velká popularita Altcoinů přišla v letech 2013 a 2014, kdy trh kryptoměn začal zaznamenávat masivní nárůst nových projektů, z nichž velká část byla obchodovatelná proti bitcoinu. [5; 7]

Následuje autorem zpracovaná tabulka, která vychází z dat získaných z různých (níže zmíněných) zdrojů. Tabulka si dává za cíl zobrazit základní charakteristiky Bitcoinu, autorem vybraných Altcoinů a zároveň poskytnout čtenáři přehled o jejich rozdílech.

Tabulka 2 Přehled charakteristik vybraných kryptoměn

Název	**Bitcoin**	**Namecoin**	**Litecoin**	**Monero**	**Cardano**
Zkratka	BTC	NMC	LTC	XMR	ADA
Datum vzniku	3.1.2009	18.4.2011	7.10.2011	18.4.2014	2015
Zakladatel	Satoshi Nakamoto	Vince	Charlie Lee	Skupina vývojářů	Charles Hoskinson
Max. počet mincí	21 000 000	21 000 000	84 000 000	Nekonečně inflační	45 000 000
Perioda bloku	10 min.	10 min.	2,5 min.	2 min.	20 sekund
Těžba	PoW	PoW	PoW	PoW	PoS

Zdroj: [5; 7; 73; 74]

3.1 XRP

Za zmínku stojí dále kryptoměna XRP. Nejde o typický příklad klasické kryptoměny jako je Bitcoin, Litecoin a další. Spíše jde o real-timový platební a zúčtovací systém, jehož

hlavním cílem je dostat se do bankovního sektoru a nahradit současný systém pro mezibankovní transakce (SWIFT). Na rozdíl od Bitcoinu není vývoj vložen do rukou dobrovolných vývojářů nacházejících se napříč celým světem. Za současným vývojem systému stojí firma Ripple Labs Inc[21]. Tento rozdíl vede řadu bitcoinových zastánců k přesvědčení, že XRP nepatří mezi kryptoměny, jelikož zde panuje značná centralizace. [7; 9]

Původním záměrem bylo využívat XRP jako transakční nástroj pro vlastní potřebu Ripple Labs. Rostoucí zájem veřejnosti o kryptoměny přiměl společnost ke změně původního úmyslu a začala svůj produkt propagovat jako kryptoměnu s rychlými transakcemi a nízkými poplatky. Zajímavostí této měny je, že XRP se nedá těžit. Na začátku došlo ke vzniku přesně 100 miliard jednotek s tím, že 20 % této částky si ponechali zakladatelé a 80 % zůstalo ve vlastnictví firmy Ripple Labs. Ta má zbytek uložený v tzv. escrow neboli uzamčené peněžence, která je nastavena na postupné uvolňování měny do oběhu. Dle stránky coinmarketcap.com je aktuálně v oběhu necelých 44 miliard XRP. [3; 7; 9]

Jak tedy dochází k potvrzování transakcí, když ne těžbou? Na rozdíl od Bitcoinu Ripple nevyužívá systém blockchainu, nýbrž sítí putuje decentralizovaná databáze účtů, nazývaná ledger. Každý uzel spravuje svůj vlastní ledger a zároveň udržuje komunikaci s ostatními uzly. Transakci lze chápat jako návrh ke změně dat. V případě, že alespoň 80 % uzlů se shodne na tom, že transakce může být provedena, tak v databázi dojde k aktualizaci dat. Transakce tedy nejsou potvrzovány těžbou, ale vzájemnou shodou důvěryhodných uzlů. Tato metoda se nazývá Proof of Correctness a představuje rychlejší a na výpočetní výkon jednodušší alternativu k Proof of Work. [7; 9; 75]

3.2 Ethereum

V roce 2013 přišel teprve 19letý ruský programátor Vitalik Buterin s myšlenkou, že decentralizovaný blockchain zabezpečený kryptografií, může světu nabídnout mnohem více než jen kryptoměnu. O pouhé 2 roky později zrealizoval a veřejnosti představil něco, co Dominik Stroukal a Jan Skalický [7] označili jako „*virtuální mašinu“.* Jedná se o decentralizovanou platformu složenou z tisíce počítačů, která je prezentována jako nová era Internetu. Je to Internet který:

- má v sobě již zabudovanou vlastní měnu a poskytuje možnost provádění plateb.

[21] Dříve OpenCoin

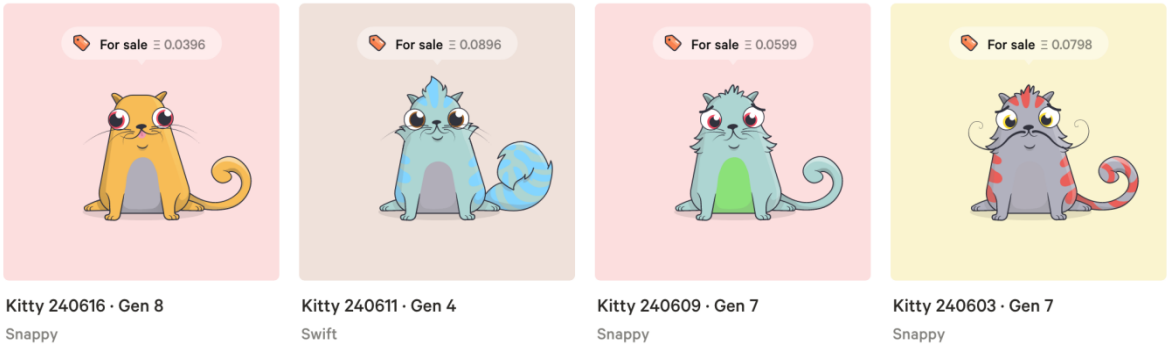
- přináší finanční systém, jenž je určen všem lidem.
- poskytuje bezpečné místo pro uložení dat bez strachu o jejich zcizení.
- stojí na otevřené infrastruktuře, kterou nemá pod kontrolou žádná společnost. [7; 76]

Základ Etherea je ve své podstatě podobný Bitcoinu. Jedná se o síť vzájemně propojených uzlů, které uchovávají blockchain. Samotná měna Etherea se nazývá ether a řadí se mezi měny nekonečně inflační. To znamená, že není stanoven maximální počet etherů, které budou vypuštěny do oběhu. Dle své tržní kapitalizace je Ethereum druhou největší měnou. [3; 7; 76]

V současnosti probíhá těžba kryptoměny za pomocí Proof of Work, ovšem celá síť se připravuje na velký upgrade, který přinese zásadní změnu v protokolu. Tou změnou bude přechod na Proof of Stake. To znamená, že těžaře vystřídají tzv. validátoři, kteří se po složení vratné kauce 32 etherů budou podílet na ověřování transakcí v síti. K této změně mělo dojít již začátkem roku 2020. O důvodech zpoždění se polemizuje. Informace ze strany vývojářů systému uvádějí, že k uskutečnění určitě dojde v průběhu roku 2020. [76; 77]

Hlavní vlastností, která dělá Ethereum výjimečným je jeho programovatelný blockchain. V současné době se nejedná o absolutní unikát, ale jeho příchod v roce 2015 přinesl do světa kryptoměn úplně nové funkce. Nad blockchainovým základem vytvořil Vitalik Buterin programovací jazyk Solidity, který rozšířil možnosti tvorby tzv. smart kontraktů a způsob jejich aplikace. Kombinace Solidity a smart kontraktů umožňuje v rámci Etherea vytvořit plno komplexních programů, ať už ve formě decentralizovaných aplikací, her, burz, cloudových úložišť, tokenů a mnoho dalších. [78; 79]

Mezi nejznámější ethereové programy patří hra Cryptokitties. Jedná se o virtuální kočky (znázorněné na obrázku č. 4), které mohou hráči kupovat za své ethery a vzájemně mezi sebou směňovat. Každá kočka ve hře představuje token, který byl vytvořen dle standardu ERC-721, což znamená že je naprosto unikátní a není zde možná zaměnitelnost. Vznik hry měl primárně demonstrovat potenciál a rozsáhlé možnosti technologie blockchain. Již několik dní po spuštění se hře dostalo velké pozornosti, která vedla k dočasnému zpomalení celé sítě. V historii hry se vyskytuje jistý hráč Rabono, který byl ochoten za jednu crypto kočku zaplatit neuvěřitelných 600 etherů, což v té době představovalo cenu jednoho Porsche 911. [80; 81]



Obrázek 4 Virtuální kočky ze hry Cryptokitties [82]

Smart kontrakty

Představují decentralizovanou smlouvu ve formě software či protokolu, která je uzavřena mezi dvěma stranami. Na její plnění dohlíží samotná technologie sítě nikoliv určitá autorita. Základními předpoklady pro funkci smart kontraktů je neměnnost a distribuovatelnost. V případě, že dojde k vytvoření takové smlouvy, nemělo by být nikomu umožněno s jejím obsahem manipulovat. Pro dosažení těchto vlastností využívají smart kontrakty technologii blockchain. [83; 84]

II. PRAKTICKÁ ČÁST

4 ŠKÁLOVATELNOST BITCOINU

Při pohledu na obecnější definici slova „škálovatelnost“ se jedná o [85]: „*Schopnost systému, sítě nebo procesu zvládnout rostoucí objem práce nebo jeho potenciál rozšířit tak, aby mohl tento nárůst zpracovat*“. V rámci informačních technologií se může jednat o schopnost systému přizpůsobit svůj výkon aktuálnímu zatížení. Avšak nejedná se jen o IT. O škálovatelnosti se diskutuje také v oblastech jako je telekomunikace, ekonomie firem a v neposlední také v oblasti, která bude tvořit samotné jádro této praktické části. Tím jsou kryptoměny, konkrétněji Bitcoin. [85; 86]

V oblasti kryptoměn se škálováním myslí schopnost adaptace sítě na rostoucí počet uživatelů. Kryptoměna se označuje jako dobře škálovatelná, když je schopna zpracovat velké množství transakcí při udržení si přijatelného transakčního poplatku. Mezi takové měny patří například XRP. Koho zde ovšem nelze zařadit je Bitcoin. Sám jeho bývalý vývojář Peter Todd avizoval, že samotný Bitcoin je neškálovatelný. Důkazem se stává i historie, ve které Bitcoin již ukázal, že na to, aby byl využíván širokou veřejností, není připraven. Je příliš pomalý. [87; 88; 89]

První debaty na téma škálování Bitcoinu proběhly již v roce 2013. Komunita si uvědomovala, že za situace, kdy je velikost jednoho bloku omezena na 1 MB a průměrná doba jeho vytěžení se pohybuje okolo 10 minut, může, při stále větším růstu počtu transakcí, vést k zahlcení sítě. Tedy situaci, kdy by potvrzení transakce trvalo mnohem delší dobu. Čtenáře by mohlo napadnout, proč se zde to omezení ve formě 1 MB nachází. V roce 2010 ho v tajnosti sám Satoshi Nakamoto implementoval do zdrojového kódu. Účelem bylo ochránění Bitcoinu před spamovými útoky. Zlepšení ochrany ovšem šlo na úkor škálovatelnosti. V roce 2016 zveřejnil softwarový inženýr Cyle Croman spolu s dalšími spolupracovníky publikaci [90], ve které mimo jiné poukazují na to, že Bitcoin je schopen zpracovat maximálně 3.3 - 7 TPS[22] (transakcí za sekundu). Jak sami hodnotí, je to v porovnání s jednou z největších platebních společností VISA opravdu málo. Ta totiž odbavuje průměrně 2 000 transakcí za sekundu s možností škálovat až do řádů desetitisíců. V počítání maximální propustnosti Bitcoinu se snažil posunout laťku ještě dál Evangelos Georgiadis, který ve svém reportu: How many transactions per second can bitcoin really handle [91] tvrdí, že hranice 7 TPS je pouze přibližná. Zmiňuje zde, že uváděné výpočty

[22] Spodní mez je vypočítána z průměrné velikosti transakce, která činí 500 bajtů. V případě, že by sítí proudily pouze transakce o velikosti 250 bajtů, tedy transakce obsahující pouze jeden vstup a 2 výstupy, byl by Bitcoin schopen zpracovat okolo 7 transakcí za sekundu.

jsou prováděny pomocí přibližné velikosti transakcí. Zároveň se nebere v potaz rozdíl mezi velikosti bloku a skutečným prostorem, který je pro transakce vyhrazen. Georgiadis tedy na to šel z jiné strany a ukázal, že maximální možná propustnost sítě je 27 TPS. Jeho výpočet stojí na teoretických základech, kde od maximální velikosti bloků 1 MB jsou prvně odečteny bajty, které do výpočtu TPS nelze zahrnout - jsou využívány jinými parametry bloku jako je např. hlavička bloku, informace o celkové velikosti bloku apod. Zohledněna je také velikost coinbase transakce, která je součástí každého bloku. Prostor, který může být určen pro uživatelské transakce disponuje přibližně 999848 volnými bajty. Tato hodnota je dále podělena 61 bajty, jenž představují velikost nejmenší transakce, která může být v bitcoinové síti provedena. Pro převedení výsledku do tvaru TPS je potřeba na závěr provést dělení číslem 600 (10 min * 60 sec), které udává čas nutný pro vytěžení bloku.

$$\left[\frac{999848}{61}\right] / 600 = 27\,TPS$$

Tímto způsobem došel Georgiadis k závěru, že maximální propustnost sítě činí přibližně 27 transakcí za sekundu. Nutné je zde podotknout dvě věci. Tou první je, že výše zmíněný výpočet slouží z velké části jenom pro stanovení nových teoretických mezí. Při výpočtu je totiž použita transakce, která je sice velikostně nejmenší, avšak v bitcoinové síti se často nevyskytuje. Jedná se o transakci, která nemá definované omezení určující dalšího vlastníka. To znamená, že výstup této transakce může být utracen kýmkoliv. Přední světový propagátor Bitcoinu Andreas Antonopoulos uvedl, že jediné praktické využití takové transakce je dar síti. Další věc se týká velikosti bloků. Jak Croman, tak Georgiadis kalkulovali s maximální kapacitou bloku 1 MB. V roce 2017 byl totiž proveden upgrade bitcoinového protokolu s názvem SegWit, který dokáže blok opticky zvětšit. Jedná se ovšem o vylepšení, které nelze popsat v několika řádcích, proto o SegWitu a dalších vylepšeních Bitcoinu tato práce pojednává v další části. [7; 90; 91; 92; 93]

Skutečný problém škálovatelnosti Bitcoinu se projevil v roce 2017. V tomto roce nastala spousta situací, které Bitcoinu výrazně pomohly, v jeho propagaci. Začátkem 2017 byla měna japonskou vládou plně zlegalizovaná. V tisku se začala objevovat řada článků na téma kryptoměny. Platbu v BTC začaly přijímat například švýcarské dráhy, platforma Steam, internetový obchod Alza a mnoho dalších. Bitcoinu se začalo dostávat většího povědomí, a ne jen jemu. Popularita rostla i u Altcoinů a trh začal zaznamenávat i velký nárůst Initial Coin Offeringu (ICO). Bitcoin vstupoval do roku 2017 s cenou 1 000 USD.

Tato cena ovšem v průběhu roku raketově vyrostla. V prosinci daného roku Bitcoin nastavil své dosavadní cenové All-Time High (ATH) neboli nejvyšší dosaženou cenu, která jak i obrázek níže znázorňuje, činí necelých 20 000 USD. [7; 94]

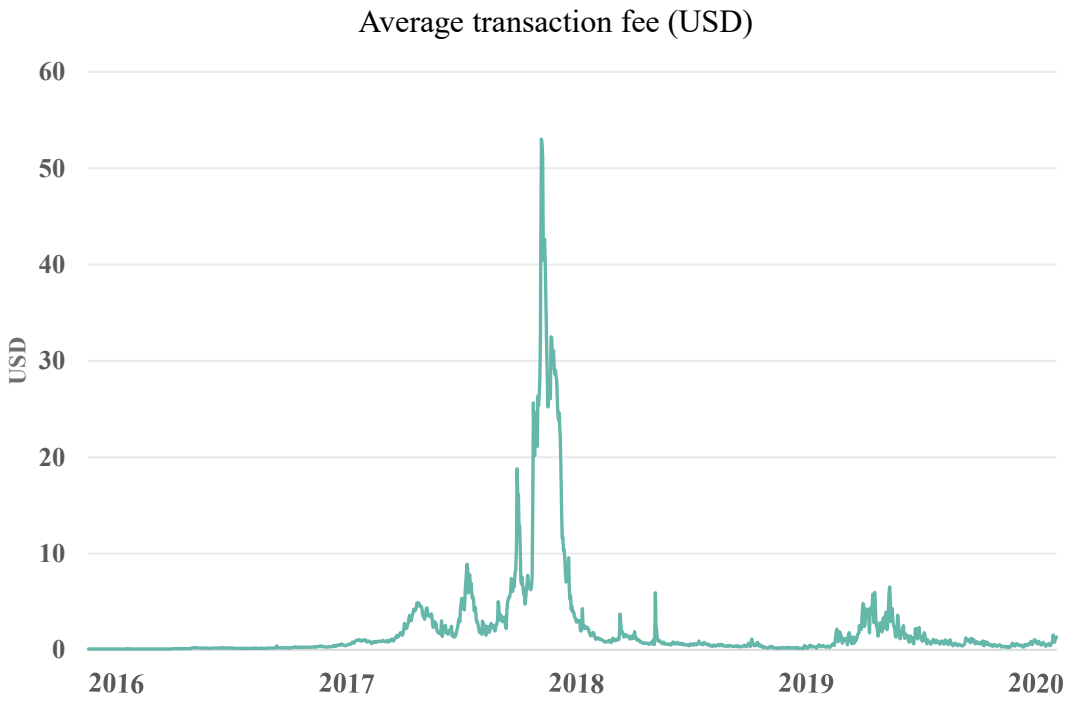
Obrázek 5 Vývoj ceny BTC 2016-2020 [95]

Cenový růst BTC způsobil vznik tzv. FOMO efektu[23]. Počet transakcí v Bitcoinu prudce rostl, burzy ztratily schopnost zajišťovat požadavky nových klientů. Počet nepotvrzených transakcí v mempoolu narůstal - Bitcoin se zahltil. V průběhu prosince 2017 se průměrný počet nepotvrzených transakcí pohyboval okolo 90 tisíc. Samotná velikost mempoolu dosahovala řádů stovek milionů bajtů, což znamenalo, že potvrzení některých transakcí netrvalo minuty, ani hodiny ale dny. Uživatelé se snažili upřednostnit své transakce před ostatními tím, že zvyšovali transakční poplatky. Čím větší poplatek za transakci, tím i větší motivace těžaře danou transakci potvrdit. Díky tomu se poplatek za běžnou transakci vyšplhal do řádů stovek Kč[24]. U transakcí s větším počtem vstupů a výstupů to bylo mnohem víc. Velice zajímavý příklad, kdy poplatek představoval enormní částku, uvedli Dominik Stroukal s Janem Skalickým [7]: *„V bloku 500546 nalezneme transakci o*

[23] Jedná se o situace, která nastává při rapidním cenovém růstu, kdy na trh přichází nezkušení investoři s pocitem strachu, že můžou přijít o zajímavou investici, proto začínají iracionálně nakupovat při vysoké ceně. FOMO efekt většinou končí u nezkušených investorů ztrátou, jelikož při FOMO rapidně roste riziko spuštění masivního výprodeje, což má za následek pokles ceny.

[24] Pro porovnání: průměrný poplatek za transakci provedenou 18.3.2020 činil 1,16 USD. Průměr je ovšem hodně proměnlivý, například 9.3.2020 činil 0,41 USD.

velikosti 73 kB, přesouvající 25 BTC z pěti set adres, s poplatkem jeden celý bitcoin, tehdy 350 tisíc korun!“. Níže přiložený graf znázorňuje, jak se průměrné transakční poplatky měnily v čase, konkrétně od roku 2016 do března 2020. Lze vidět, že v prosinci roku 2017 výše průměrného poplatku za transakci činila až 53 USD. [7; 9; 96; 97]



Obrázek 6 Průměrná cena transakce 2016-2020 [105]

Návrhů na vylepšení škálovatelnosti Bitcoinu, aby se takovým situacím alespoň do jisté míry předcházelo, je několik. Jak je zmíněno výše, první diskuse proběhly již v roce 2013 a s konkrétními nápady přišla komunita hned o 2 roky později. Je velice složité říct, který návrh je nejlepší. Sám Antonopoulos na otázku, které řešení by mělo být adaptováno odpověděl, že všechny. Je přesvědčen, že problém škálovatelnosti není věc, která by někdy byla finálně vyřešena. Jakékoliv implementované řešení narazí časem na svoje limity a síť bude muset projít další optimalizací. Celou situaci přirovnal k vývoji komunikace na Internetu, která probíhala přes systém Usenet, následně prostřednictvím emailu, VoIP[25] atd. Stejně jako Internet, tak i Bitcoin čelí svým limitům a prochází vývojem. [98; 99]

Každý návrh může přispět ke zlepšení škálovatelnosti. Je ovšem otázkou, jaký to bude mít dopad na celou síť. Optimalizace blockchainu je velice složitá záležitost, při jejíž provádění je nutné brát ohled na 3 základní pilíře Bitcoinu, a těmi jsou:

[25] Voice over Internet Protocol – technologie poskytující možnost přenosu hlasu přes Internet.

- Decentralizace
- Škálovatelnost
- Bezpečnost

Jakákoliv změna jednoho pilíře do jisté míry ovlivní i ty zbylé dva. Proto je otázka škálovatelnosti Bitcoinu tak sofistikovaná v porovnání s jinými centralizovanými systémy jako je např. již výše zmíněná VISA. Bitcoinová komunita se snaží najít řešení, které by zlepšilo škálovatelnost bez nutnosti velkého obětování decentralizace nebo bezpečnosti. Jednotlivých návrhů, které se na internetu objevuji ve formě BIP[26] je celá řada. V zásadě je však možné je rozdělit do 2 skupin:

- On-chain
- Off-chain

Návrhy on-chainového typu usilují o uchování všech transakcí uvnitř bloků a jsou realizovány pomoci úprav bitcoinového protokolu, který probíhá prostřednictvím tzv. forku.

Cílem off-chainových návrhů je v blocích uchovat pouze některé transakce, například ty s velkým objemem, a zbylé přesunout mimo hlavní řetězec do sekundárního blockchainu tzv. sidechainu nebo do platebních kanálů umožňující vysokorychlostní a levné transakce. [7; 98; 100; 101]

4.1 Fork

Jde o pojmenování situace, která nastává v bitcoinové síti v momentě, kdy těžaři vytěží 2 či více bloků ve stejný čas a aniž by o sobě navzájem věděli, tak je distribuují v síti. Najednou v síti putuje více bloků, které se napojují na stejný blok a způsobují rozvětvení blockchainu. Toto rozvětvení je označované jako vidlička (v angličtině „fork“) - více napojených bloků na jeden blok připomíná vzhledem hroty vidličky. Takto vzniklou situaci je potřeba vyřešit, jelikož zde hrozí riziko dvojí útraty mince. I přesto, že se tato situace může jevit jako velice problematická, Bitcoin ji dokáže vyřešit vcelku jednoduše. Síť se totiž řídí pravidlem, že platná větev je ta, na jejíž vytěžení bylo vynaloženo více práce. Dojde tedy k tomu, že těžba pokračuje pouze nad jednou větví a bloky té druhé se označí

[26] Bitcoin Improvement Proposal neboli návrh na vylepšení Bitcoinu. Jedná se o dokument, představující nápad na zlepšení bitcoinového protokolu. Samotnými BIP se práce zabývá v podkapitole níže.

jako tzv. orphan bloky. Veškeré transakce, které skončily v oprhan blocích jsou vráceny zpátky do mempoolu a čekají, až je těžaři potvrdí v bloku jiném. [7; 102; 103]

K forkování nedochází pouze náhodně, ale taky úmyslně za účelem aktualizace protokolu (úpravy chyb či implementace nové funkcionality), jelikož Bitcoin je síť, která se neustále vyvíjí. Jakákoliv úprava protokolu se následně do sítě distribuuje vydáním nové verze bitcoinového klienta a záleží už na každém, zda na novou verzi přejde či nikoliv. Hlavní otázkou většinou je, zda je nová verze s tou starou zpětně kompatibilní, tzn. jestli bloky vytěžené podle nového protokolu budou validní i v protokolu starším. Na základě toho se rozlišuje, zda byla změna implementována jako soft fork nebo hard fork. [103; 104]

4.1.1 Soft fork

K soft forku dochází v momentě, kdy je vydána nová verze softwaru, která je zpětně kompatibilní s verzí starou. Znamená to, že bloky vytěžené podle nových pravidel jsou validní i ve starší verzi. Toto tvrzení ovšem nemusí platit opačně. Nová verze nenahlíží na všechny dříve vytěžené bloky jako na platné. V případě, že v síti zůstanou těžaři se starší verzí softwaru, může se stát, že bude docházet k těžbě bloků neplatných. Jako příklad lze uvést soft fork, který provedl Satoshi Nakamoto v roce 2010, kdy omezil velikost bloku na 1 MB. Těžaři, kteří přešli na novou verzi, začali těžit bloky, které byly validní i pro zbytek sítě. Starší software, který neměl velikostní omezení, dokázal přijmout blok o velikosti 1 MB, avšak nový software blok větší než 1 MB přijmout nedokázal. Těžaři se tedy vyplatí těžit podle aktuálních pravidel, aby nedocházelo k tvorbě neplatných bloků.

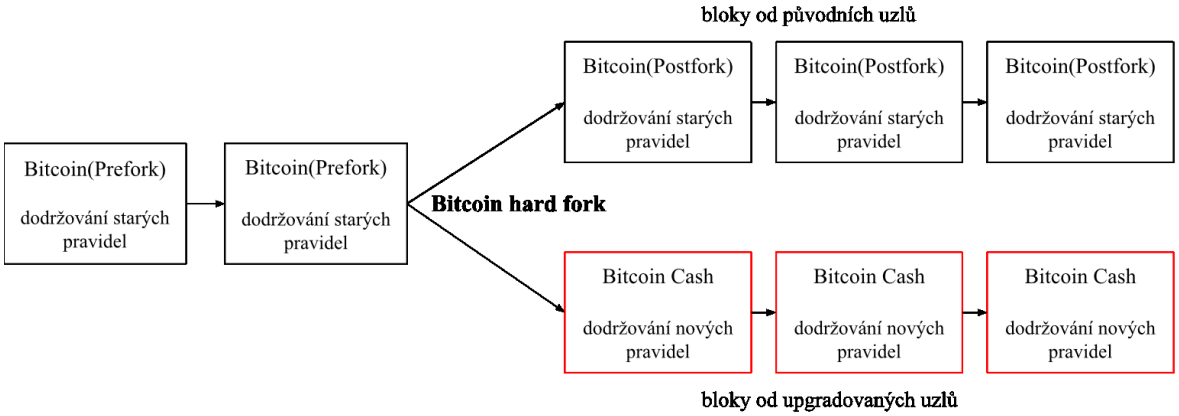
Aby byla zaručena zpětná kompatibilita, dochází při soft forku k zpřísňování pravidel, které definují platný blok a ne k jejich rozvolňování, jak to dělá hard fork. Je nutné si uvědomit, že zpřísňování nemusí mít vždy jenom negativní dopad. Jak je již výše zmíněno, Satoshi omezil velikost bloku za účelem zvýšení bezpečnosti Bitcoinu proti spamového útoku. [7; 105; 106]

4.1.2 Hard fork

Při hard forku dochází naopak ke změně pravidel, které nezajistí zpětnou kompatibilitu se starší verzí protokolu. Je tedy zapotřebí, aby upgrade softwaru provedli jak těžaři, tak i uživatelé. V případě, že by obyčejný uzel zůstal u staré verze softwaru, jeho existence v síti

by prakticky skončila. Nenacházel by se zde žádný těžař, který by pro uzel vytvořil validní blok. V situaci, že by u starší verze setrval i těžař a nadále tvořil bloky dle starých pravidel, došlo by k rozdělení blockchainu tzv. trvalým forkem. To znamená, že blockchain by se v daném bloku, kde byl proveden hard fork, rozdělil na 2 větve, které jsou vzájemně nekompatibilní. Takovéto rozdělení vede i ke vzniku nové kryptoměny, jelikož se zde nachází 2 odlišné větve, které propagují svoje pravidla a tím pádem i svojí měnu. Mezi nejznámější hard forky Bitcoinu patří Bitcoin Cash, který vznikl na základě nesouladu názorů vývojářů ohledně škálovatelnosti Bitcoinu. Proto dne 1.8.2017 provedla určitá část komunity úpravu pravidel v bitcoinovém protokolu a začala těžit bloky o velikosti 8 MB. Došlo tedy k vytvoření zpětně nekompatibilní verze a tedy k rozdělení blockchainu trvalým forkem. [104; 107; 108]

Níže se nachází nákres znázorňující hard fork Bitcoinu. Nákres vznikl přepracováním obrázku autorky Julie Bang [109] a dále byl doplněn o data z obrázku „Schematische Darstellung der Hard Fork“ který zpracovala autorka Paulina Würth [110].



Obrázek 7 Hard fork Bitcoinu [109; 110]

4.2 BIP

Jedná se o standard, který byl v roce 2011 vytvořen vývojářem Amirem Taaki. Ten umožňuje komukoliv navrhnout změnu bitcoinové sítě či protokolu nebo poskytnout komunitě nějakou důležitou informaci ohledně Bitcoinu. Zavedení tohoto standardu bylo nutností, jelikož zde neexistoval žádný prostředek usnadňující vývojářům vzájemnou spolupráci. BIP představuje dokument, který by měl obsahovat popis navrhované funkce, zdůvodnění, proč by měla být implementována a zároveň technickou specifikaci. Tento dokument je odeslán správci BIP repozitáře, který ověří, zda dokument obsahuje požadované náležitosti. V případě, že ano, přiřadí mu sériové číslo a zveřejní ho na stránku

github.com/bitcoin/bips obsahující již provedené či navrhované změny v Bitcoinu. Například BIP s číslem 1 byl navrhnut Amirem Taaki a obsahuje specifikaci toho, co vlastně Bitcoin Improvement Proposal (BIP) je a k čemu slouží. O tom, zda jednotlivý návrh bude implementován, závisí na komunitě, která o jednotlivých změnách pravidelně diskutuje a snaží se Bitcoin vyvíjet neustále k lepšímu. Stále však platí, že každý se může svobodně rozhodnout. V případě, že někdo se změnou nesouhlasí, stačí mu pouze neupgradovat software na novější verzi. Aby byla implementace jednotlivých změn pomocí soft forku či hard forku úspěšná, je nutné získat podporu těžařů. Ti mohou pomocí rezervovaných bitů v hlavičce bloku (který vytěží) signalizovat, zda se změnou souhlasí. Proces dále probíhá tak, že z posledních 1000 vytěžených bloků se zjišťuje, kolik procent těžařů je připraveno změnu akceptovat. V případě, že jejich počet dosahuje předem stanoveného požadavku, dojde ke schválení změny a následně její implementaci. Procentuální požadavek se stanovuje na základě míry změny pravidel, může to být 75 % procent, či dokonce i 95 %. Na první pohled to vypadá, že o změnách v síti rozhodují pouze těžaři, avšak není tomu tak. V případě, že by se rozešel zájem těžařů a uzlů, došlo by k vytváření bloků, které by uzly nepřijímaly. Důsledkem by mohlo být rozdělení blockchainu. Proto je v zájmu každého provádět pouze změny, které mají značnou podporu v komunitě, aby byla zajištěna co největší míra interoperability. Vhodné je ještě dodat, že bitcoinový klient Bitcoin Core je open-source software. To znamená, že každý je schopen nahlédnout do zdrojového kódu a provádět v něm změny dle libosti. Otázkou už jen je, do jaké míry budou změny kompatibilní se softwarem, který používá zbytek sítě. [7; 111; 112; 113]

5 NÁVRHY NA VYLEPŠENÍ

Návrhů na vylepšení škálovatelnosti Bitcoinu se v BIP repozitáři nachází celá řada. Z pravidla lze návrhy rozdělit do dvou skupin, na návrhy typu on-chain a off-chain. Obě skupiny přistupují k dané problematice jinak. Jednotlivé návrhy mají kromě svých zastánců i své odpůrce - nikdy nelze vymyslet něco, co by vyhovovalo všem. Faktem zůstává, že neexistuje jedno magické řešení, které by dokázalo problém škálovatelnosti nadobro vyřešit. Nikdo neví, kým a jak bude síť využívaná v budoucnu. Proto jednotlivé návrhy představují spíše řešení dočasné. Ve chvíli, kdy Bitcoin znovu narazí na své limity, začne komunita otázku škálovatelnosti řešit opět. [98; 100] Jak tvrdí Andreas Antonopoulos [98]: „*Scale is not a goal to achieve, it is the definition of what can you do with the network today. And the moment you increase the capacity, the very definition of what can you do with the network today changes.*“[27]

Tato kapitola má za cíl ukázat rozdíl mezi řešeními typu on-chain a off-chain. Představit vybrané zástupce z obou skupin, popsat princip jejich funkce a také analyzovat výhody a nevýhody jednotlivých vylepšení.

5.1 On-chain

První skupinu tvoří tzv. on-chain řešení. Podstatou je uchovat veškeré transakce on-chain neboli „na řetězci“. To znamená, že je kladen důraz na to, aby byly všechny transakce zpracovávány hlavním blockchainem a nedocházelo by k jejich přesouvání mimo řetězec (jak to řeší off-chain). Hlavní motivací je dosáhnout zlepšení bezpečnosti, decentralizace a škálovatelnosti na hlavním blockchainu. Ovšem v současnosti zatím neexistuje návrh, který by dokázal provést zlepšení všech těchto tří parametrů. Jak již bylo zmíněno, optimalizace blockchainu je velice náročná. Při snaze dosáhnout větší škálovatelnosti se některé návrhy potýkají s problémem obětování decentralizace a ty zbylé zase s bezpečností. Dle Petra Todda (bývalého vývojáře bitcoinového klienta Bitcoin Core) neexistuje z pohledu škálování žádné efektivní on-chain řešení, budoucnost vidí spíše v off-chainech. [89; 114; 115]

Návrhy spadající do skupiny on-chain jsou realizovány pomocí úpravy samotného zdrojového kódu Bitcoinu a následně jsou do sítě distribuovány prostřednictvím soft nebo

[27] Volně lze text přeložit jako: Škálování/Škála není cíl, kterého dosáhneme, je to definice toho, co se sítí můžeme dnes dělat. Ve chvíli, kdy dojde k navýšení kapacity, se samotná definice toho, co se sítí dnes můžeme dělat, změní.

hard forků. Níže jsou popsány dva ze zástupců on-chainového řešení společně i s jejich hlavními výhodami a nevýhodami. Konkrétně jde o řešení pomocí zvýšení kapacity bloku, kdy pomocí hard forku by došlo k navýšení současného limitu, který činí 1 MB. Dále je zde řešení s názvem SegWit. Ten byl již v roce 2017 implementován a dokázal transakční propustnost Bitcoinu v určitém obhledu zlepšit. I přesto, že nepřináší takové navýšení TPS (transactions per second), představuje obrovský krok pro zlepšení škálovatelnosti. Jeho zavedení umožnuje realizaci dalších návrhů, které samotné TPS navyšují znatelně. [115; 116]

5.1.1 Zvětšení bloku

V BIP repozitáři se nachází spousta příspěvků, které navrhují zlepšení škálovatelnosti Bitcoinu pomocí zvětšení samotné kapacity bloků. Každý návrh přistupuje ke zvětšení trochu jinak. Ovšem i přes rozdílnost představ mají obecně všechny návrhy společné to, že jejich realizace by musela být provedena pomocí rozvolňování pravidel protokolu - síť by se tedy nevyhnula hard forku. Tato možnost byla hodně diskutována v minulých letech. Po nástupu SegWitu a vzniku Bitcoinu Cash se pozornost komunity začala upínat spíše k off-chain řešením, jenž nevyžadují hard fork a mohou přinést revoluční změny. Ovšem vyskytují se názory, že pokud má být Bitcoin dlouhodobě perspektivní měnou, měly by změny ke zlepšení škálování nejprve přijít v úpravě samotného základu Bitcoinu čili jeho zdrojového kódu. Takovou úpravu by mohla představovat již zmíněná změna velikosti bloku. [117; 118; 119]

Pro představu lze uvést následující příklad: V případě, že by se velikost bloku stanovila na 8 MB a ostatní parametry by byly zachovány, byl by Bitcoin schopen zpracovat přibližně 25-53 transakcí za sekundu. Pro výpočet rozmezí byla využita metoda, kterou použil Kyle Croman a spol. [90], kde spodní mez počítá s průměrnou velikostí transakce (500 bajtů) a vrchní kalkuluje s transakcemi tvořené 1 vstupem a 2 výstupy (250 bajtů).

Příklady BIP navrhující změnu velikosti

- **BIP 100**

  Jedná se o první BIP navrhující změnu velikosti bloku. BIP 100 byl vytvořen roku 2015 Bitcoin Core vývojářem Jeffem Garzikem. Hlavní myšlenkou návrhu je, zbavit vývojáře pravomocí stanovit velikost bloku a předat rozhodnutí do rukou těm, kteří ty bloky vytvářejí. Velikost bloku by byla dynamická a stanovila by se vždy pro následujících 2016 bloků na základě hlasování prováděné těžaři. Těžaři by

byli pouze omezeni maximální možnou velikostí bloků, která by představovala 32 MB. [120]

- **BIP 101**

  BIP který v roce 2015 navrhl Gavin Andresen. Podstatou návrhu je změnit fixní hodnotu 1 MB na 8 MB s tím, že vždy po 2 letech by docházelo k dvojnásobení velikosti. V momentě, že by velikost bloku dosáhla 8 GB, byl by proces zvětšování ukončen. [119; 121]

- **BIP 103**

  Jedná se o návrh Pietera Wuille spočívající ve zvětšování kapacity bloku každých 97 dní o 4,4 % až do července roku 2063. Wuille v návrhu zmiňuje, že hard fork by nemusel vést k rozdělení blockchainu trvalým forkem, jelikož pravidelný nárůst je jen o pouhé 4,4 procenta. [122]

- **BIP 107**

  BIP s číslem 107 navrhuje zvětšování bloku, které by probíhalo ve 2 fázích. V 1. fázi by blok narůstal až do velikosti 6 MB. Dále by započala 2. fáze, ve které by se vždy po 4 týdnech zjišťovala průměrná zaplněnost posledních 3025 bloků. V případě, že průměr by představoval více než 60 % aktuální velikosti bloku, došlo by ke zvětšení maximální kapacity o 10 %. [123]

Klady a zápory

Níže vytvořená tabulka přináší přehled hlavních kladů a záporů řešení pomocí zvětšení bloku. Následuje vysvětlení, proč se jedná o pozitivum či negativum.

Tabulka 3 Klady a zápory větších bloků

Klady	**Zápory**
+ Větší propustnost samotného Bitcoinu	- Hard fork
+ Uchování transakcí na blockchainu	- Velikosti blockchainu
	- Snížení decentralizace
	- Malý nárůst TPS
	- Pomalejší propagace bloků

Zdroj: [89; 115; 124; 125]

Klady

+ **Větší propustnost samotného Bitcoinu**

  Bitcoin by se snažil řešit škálovatelnost na své základní vrstvě a nemusel by spoléhat na řešení off-chain. [115]

+ **Uchování transakcí na blockchainu**

  Bitcoin by zůstal u své základní koncepce, kterou Satoshi vytvořil, tedy že Bitcoin funguje na principu jednoho blockchainu, ve kterém jsou zaznamenány všechny transakce. Při řešení problému škálovatelnosti, se uživatelé odvolávají, že toto přesně bylo podstatou „Satoshi's Vision" neboli Satoshiho vize jak škálovat Bitcoin. Ovšem např. Andreas Antonopoulos toto tvrzení zpochybnil. [33; 100; 115]

Zápory

- **Hard fork**

  Hard fork je situace, které se chce většina komunity vyhnout, proto se vývojáři snaží veškeré změny provést pomocí soft forku. [7; 124]

- **Velikost blockchainu**

  Provoz uzlů v Bitcoinu je dobrovolná záležitost. Zvětšení velikostí bloků vede i k růstu nákladů na provoz samotného uzlu. Tento fakt může vést majitelé uzlů k rozhodnutí o ukončení provozu, což vede k snížení bezpečnosti sítě. V momentě, kdyby náklady byly tak obrovské, že provoz uzlů by si již nemohl dovolit obyčejný uživatel ale jen určitá skupina lidí – korporace, těžební pooly apod., došlo by k značnému snížení decentralizace sítě. [125]

- **Malý nárůst TPS**

  Toto on-chain řešení není schopné dosáhnout takové propustnosti jako např. Lightning Network (off-chain). Při porovnání s VISOU by i po razantním zvětšení bloků byla hodnota TPS malá. Dalším faktorem je rychlost potvrzení transakce, která stále trvá nejméně 10 minut. [89; 124]

  Pomalejší propagace bloků a snížení decentralizace

  S většími bloky se prodlouží i čas pro jejich propagaci, což znamená nárůst forků neboli více orphan bloků. Z této situace nejvíc profitují velké těžařské pooly. Je u

nich největší pravděpodobnost, že nový blok těží nad správným koncem blockchainu, s čímž souvisí i větší náchylnost k centralizaci těžby. [125; 126]

5.1.2 SegWit

Segregated Witness[28] (SegWit) představuje upgrade bitconového protokolu, který byl představen v roce 2015 trojicí vývojářů jako možné řešení problému škálovatelnosti pomocí soft forku. Dva roky na to, konkrétně v srpnu 2017, byl SegWit implementován do protokolu. SegWit je změna provedena v architektuře transakce, díky které je možné oddělit digitální podpis od samotné transakce a umístit ho do jiné datové sktruktury, která není využívána pro výpočet transakčního ID. Díky tomu vznikl název Segregated Witness. Dochází totiž k oddělení svědka (digitálního podpisu) od samotné transakce. Svědci neboli digitální podpisy zaberou až 65% kapacity bloku, čili jejich separace umožní, aby více transakcí bylo umístěno do bloku. [127; 128; 129]

Kromě škálovatelnosti se SegWit zabývá problémem označovaným jako transaction malleability. Když útočník napadne transakci, která ještě nebyla potvrzena, pozmění u ní digitální podpis a distribuuje ji do sítě. Najednou v síti putují 2 skoro totožné transakce, které se liší pouze v jedinečném identifikátoru (ID). Je to způsobeno tím, že podepisovací skript je přímou součástí samotné transakce a v případě, že dojde k jeho modifikaci, způsobí to změnu ID. I přesto, že útočník nemůže nijak změnit hlavní parametry transakce, jako je množství posílaných peněž, příjemce apod., dokáže zmást některé systémy, které klasifikují transakce na základě ID. SegWit tento problém vyřešil tak, že dokázal oddělit digitální podpis od samotné transakce. V případě, že dojde k jeho pozměnění, nebude výsledné ID nijak ovlivněno. [7; 128; 130]

Struktura transakce

Mezi parametry, které definují transakci patří vstup a výstup. Každý vstup transakce obsahuje podepisující skript (scriptSig). Ten je tvořen digitálním podpisem a dalšími informacemi nutnými pro manipulaci se vstupem. Digitální podpis transakce může zabírat až 65 % její velikosti. SegWit tento podepisující skript ze vstupu vyjímá a umísťuje ho do jiné datové struktury, která je někdy označována jako svědek. Prostor, který byl ve vstupu pro podepisující skript vyhrazen, se definuje jako OP_TRUE. V případě, že dojde k odstranění svědka, je transakce uzlem vnímána jako „anyone-can-spend“ neboli, že její obsah může být dále kýmkoliv utracen. Rozdíl mezi klasickou a SegWit transakcí

[28] V překladu – oddělený svědek

demonstruje obrázek níže, kde pomocí červené barvy jsou znázorněny hlavní odlišnosti. [128; 131; 132]

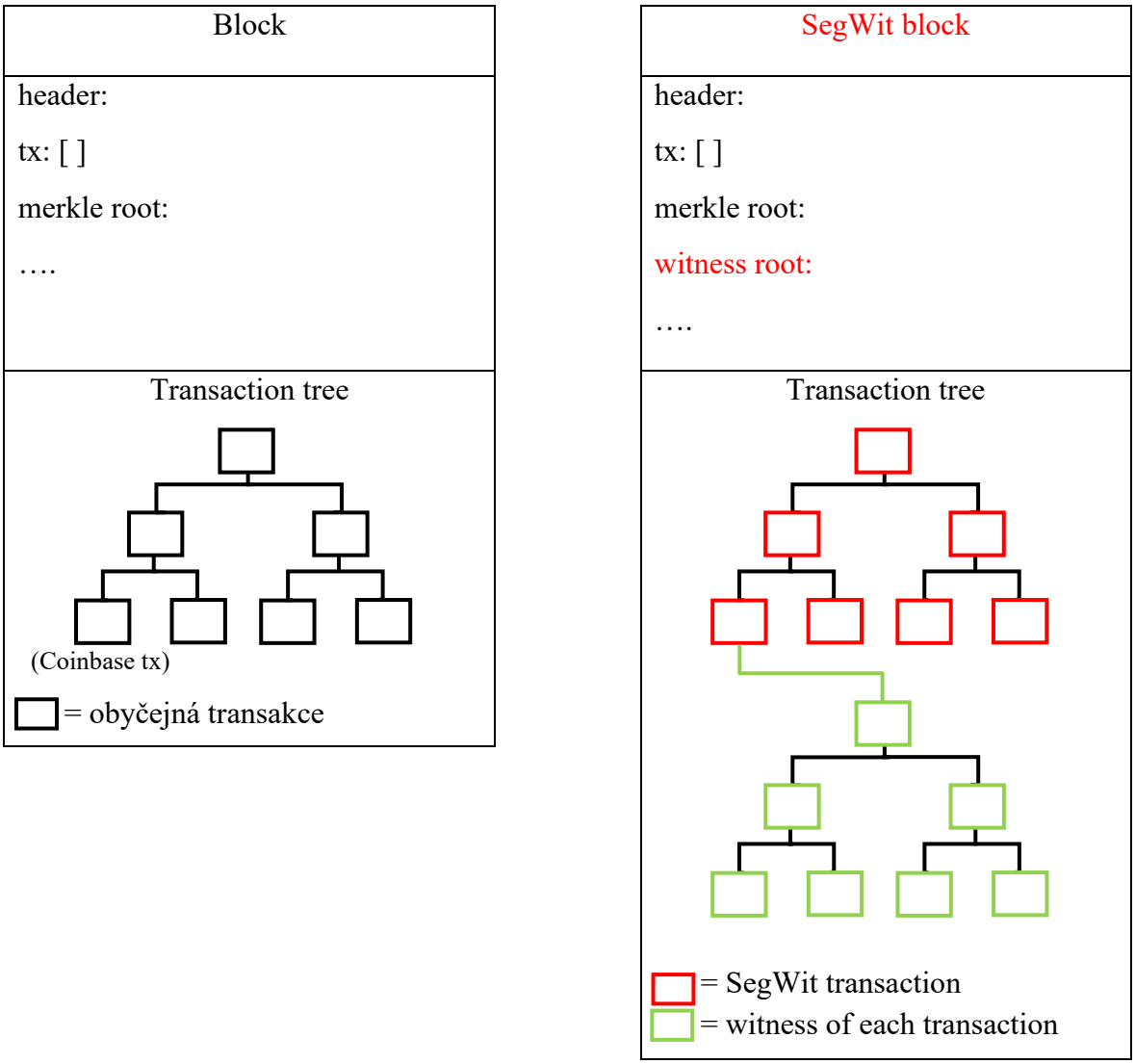
Ordinary transaction
tx: inputs: [{ scriptSig : "_" }] output: [{…….}] …

SegWit transaction
tx: inputs: [{ scriptSig : OP_TRUE }] output: [{…….}] …
witness: [{ scriptSig : "_" }]

Obrázek 8 Schéma normální a SegWit transakce [133]

Struktura bloku

Na Internetu lze dohledat řadu článků, které uvádí, že witness data nejsou přímou součástí bloku, ale jsou k němu nějakým způsobem připojeny. Pravdou ovšem je, že v případě, kdy svědci nejsou uzlem odstraněni, jsou obsaženi ve stejném bloku jako transakce. Rozdíl je v tom, že witness data nejsou promíchaná s transakcemi. Leží v jiné datové struktuře, kde tvoří svůj vlastní Merkleův strom, jehož kořen je následně začlení do coinbase transakce. Tyto rozdíly jsou vyobrazeny na níže přiloženém obrázku. [128; 132]



Obrázek 9 Schéma normálního a SegWit bloku [134]

Princip funkce

SegWit je také někdy označován jako převlečený hard fork, jelikož umožňuje upgradovaným uzlům přijímat bloky větší než 1 MB. Pomocí implementačních triků dokázali vývojáři zajistit zpětnou kompatibilitu se starými uzly (které přijmou pouze 1 MB bloky) a tak implementovat SegWit jako soft fork. Princip spočívá v tom, že SegWit

rozděluje transakci na část SegWitovou a non-SegWitovou. Do SegWitové části transakce spadají pouze svědci. Do non-SegWitové patří všechna ostatní transakční data. Následně při těžbě bloků musí těžaři dodržet podmínku, že blok se může skládat maximálně z 1 MB non-SegWitových dat a 3 MB dat SegWitových. Když se blok dostane ke starému uzlu, ten SegWitovou část čili svědky odstraní a ponechá si pouze blok, jehož kapacita dosahuje maximálně velikosti 1 MB. Díky tomuto triku byla zajištěna zpětná kompatibilita. Odhaduje se, že implementace SegWitu dokázala propustnost Bitcoinu zvýšit až na 7-14 transakcí za sekundu. Jedná se ovšem o odhad, protože ne všichni uživatelé Bitcoinu SegWit využívají. [127; 128; 135]

Nutné je dodat, že SegWit sice je zpětně kompatibilní, avšak přináší neupgradovaným uzlům určitá omezení. V momentě, co dojde k odstranění svědků, staré uzly vidí všechny SegWitové transakce jako „anyone-can-spend“. Na základě toho se již staré uzly nemohou považovat za polnohodnotné, jelikož nemohou validovat veškeré transakce. Validace SegWitových bloků probíhá tak, že uzel prvně zkontroluje witness a transakční merkleův strom a následně ověřuje podpisy vůči transakcím. V případě, že uzel podpisy nemá, tak pouze předpokládá, že veškeré „anyone-can-spend“ transakce jsou validní. Níže vytvořená tabulka přináší jednoduchý přehled hlavních kladů a záporů řešení SegWit. [128; 136]

Tabulka 4 Klady a zápory SegWitu

Klady	**Zápory**
+ Soft fork	- Podpora uživatelů
+ Vyřešení transaction malleability	- Tvorba nové adresy
+ Více transakcí v bloku	- Závislost starých uzlů
+ Rychlejší transakce	- Menší odměna za potvrzení transakce
+ Levnější transakce	

Zdroj: [127; 128; 129; 137]

Klady

+ **Soft fork**

  Upgrade protokolu je zpětně kompatibilní, čili i přes určitá omezení, mohou staré uzly stále přijímat nové bloky. [127]

+ **Vyřešení transaction malleability**

Vyřešení problému se změnou ID umožňuje Bitcoinu provádět další inovace, ať už ve formě off-chain řešení nebo třeba smart kontraktů. [127]

+ **Více transakcí v bloku, rychlejší transakce**

  Díky SegWitu se do bloků vejde více transakcí, jelikož jsou velikostně úspornější. S tím souvisí i jejich zrychlení, jelikož s vytěžením 1 bloku dojde k potvrzení více transakcí. [127; 137]

+ **Levnější transakce**

  Oddělení svědka (witness) od transakce vede k snížení velikosti transakce, to znamená, že uživatel zaplatí menší poplatek za provedení transakce. [137]

Zápory

- **Podpora uživatelů**

  Dle aktuálního přehledu, který poskytuje stránka transactionfee.info, v síti probíhá průměrně 60 % transakcí využívající SegWit. [138]

- **Tvorba nové adresy**

  V případě, že chce uživatel využívat výhody tohoto upgradu, potřebuje mít peněženku, která SegWit podporuje, a v ní mít vytvořenou SegWit adresu. Tato adresa začíná číslem 3 nebo zkratkou „bc1“. [128]

- **Závislost starých uzlů**

  V momentě, kdy dojde k oddělení svědka, jsou všechny transakce starými uzly brány jako "anyone-can-spend". Díky toho již nemůžou plnit funkci plnohodnotného uzlu. [136]

- **Menší odměna za potvrzení transakce**

  Těžaři obdrží menší odměnu za potvrzení jedné transakce, kompenzací může ovšem být fakt, že blok těchto transakcí pojme více. [128]

5.2 Off-chain

Druhou skupinu představuje řešení off-chain, kterému se také říká „řešení druhé vrstvy“. To díky tomu, že změny pro zlepšení škálovatelnosti neprobíhají na samotném blockchainu, ale mimo něj. Hlavním cílem tohoto řešení je přemístit většinu transakcí mimo řetězec a tímto ulehčit hlavnímu blockchainu. I přes svoji míru zabezpečení a

decentralizace není prozatím Bitcoin schopen poskytnout takové platební prostřední, které by se mohlo vyrovnat současným velikánům jako je VISA nebo MasterCard. Nutno podotknout, že díky SegWitu je Bitcoin schopen zpracovat přibližně 7-12 transakcí. Ovšem při porovnání s výše zmíněnými platebními společnostmi je to poněkud malé číslo. I když příchod SegWitu nepřinesl tak značné navýšení propustnosti, upoutal pozornost komunity vyřešením transaction malleability. Díky tohoto byla překážka před implementací off-chain řešení překonána. [7; 89; 139]

Níže je popsáno řešení Lightning Network, kterému se v poslední době dostává velké pozornosti. Stává se z něho nejvíc diskutované řešení, které by mohlo výrazně zlepšit škálovatelnost Bitcoinu. I přes určité nevýhody, které toto řešení má, klade v něj komunita velké naděje. [7; 89]

5.2.1 Lightning Network

Lightning Network přináší alternativu ke standardním on-chain transakcím ve formě protokolu podporujícího instantní transakce za velice nízké poplatky. Uživatelé se mohou dobrovolně rozhodnout, zda Lightning Network a jeho funkce využívat či nikoliv. V žádném případě se nejedná o jakoukoliv náhradu Bitcoinu (jak bývá někdy špatně pochopeno), nýbrž o peer-to-peer síť platebních kanálů, jenž je implementována jako jeho nadstavba. Bitcoin je pro funkcionalitu Lightning Network klíčový. Lightning Network je navržen tak, aby si jeho uživatelé nemuseli vzájemně důvěřovat. V případě, že dojde mezi nimi k nesrovnalostem, slouží Bitcoin jako soudce, který konflikt vyřeší podle předem stanovených pravidel. [140; 141]

Tyto pravidla určují smart kontrakty, jejichž základem jsou 3 technologie:

- ***Multisignature Technology***

  Jedná se o technologii vyžadující více podpisů pro provedení validní transakce. Jako příklad lze uvést uživatele Alici a Boba, kteří mají vytvořenou společnou 2-of-2 multisignature[29] (neboli více podpisovou) adresu, na které mají uložený 1 bitcoin. Pro uskutečnění převodu onoho bitcoinu na jinou adresu je potřeba, aby transakce byla podepsána jak Bobem, tak Alicí. Jedná se o určitou možnost zajištění - Bob není schopen utratit prostředky bez Alice a naopak.

[29] Číslo 2-of-2 znázorňuje kolik podpisů je potřeba z kolika. Tedy v případě 2-of-3 jsou potřeba 2 podpisy, z celkově 3 možných.

- ***Check Sequence Verify (CSV)***

  CSV definuje, jak dlouho musí být výstup transakce součástí blockchainu, než může být další transakcí utracen.

- ***Hash TimeLock Contract (HTLC)***

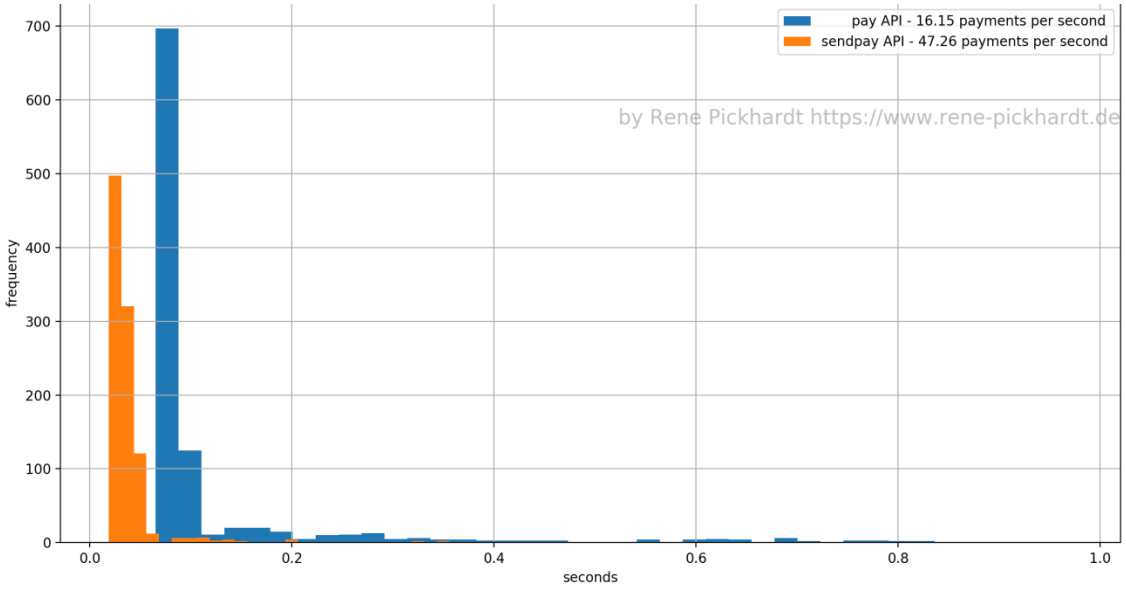
  Jedná se o třídu platby, která vyžaduje, aby její příjemce před stanoveným termínem poskytl doklad o jejím přijetí nebo se přijatá částka vrací odesílateli.

[142; 143; 144]

Lightning Network funguje pomocí platebních kanálů, které si mezi sebou uživatelé otevírají. Tyto kanály umožnují provádět vysokorychlostní transakce s velice nízkými poplatky. Jak již bylo vícekrát zmíněno, jedná se o řešení off-chain, kdy transakce neprobíhají na hlavním řetězci, nýbrž mimo něj. Do bitcoinového blockchainu jsou vždy zaznamenány jenom 2 transakce – První kanál otevírá a druhá, pomocí které se kanál zavírá. Tedy o transakcích, které proběhly v platebních kanálech, nejsou v blockchainu žádné zmínky. Uvádí se, že díky Lightning Network může být Bitcoin schopen odbavit nespočetně mnoho transakcí za sekundu. Neexistuje zde totiž žádné omezení ve formě block size (velikosti bloku) nebo block time (času nutného pro vytěžení bloku). [7; 139]

Jak uvedl Andreas Antonopoulos [139]: „*The Lightning Network completely changes the scaling game. It changes it because now we can start talking about millions and millions of transactions per second, which you can't even conceive of with a block size increase.*"[30] V roce 2018 provedl René Pickhardt [31] test, ve kterém se zabýval problémem, kolik transakcí za sekundu je možné provést pomocí jednoho platebního kanálu mezi dvěma lokálními klienty využívající Lightning Network implementaci c-lightning. Výsledky, které jsou zobrazeny na obrázku na další straně ukázaly, že pomocí jednoho platebního kanálu je možné provést přibližně 47 transakcí za sekundu. Pro představu je vhodné zmínit, že podle aktuálních statistik se v síti Lightning Network nachází přibližně 37 tisíc platebních kanálů. [145; 146]

[30] Text lze volně přeložit jako: Lightning Network kompletně změnil škálovací hru. Změnil ji, protože teď se můžeme začít bavit o milionech a milionech transakcí za sekundu, což v případě zvětšování kapacity bloku je nepředstavitelné.
[31] Spoluautor připravované knihy Mastering the Lightning Network.



Obrázek 10 Počet TPS provedených v jednom platebním kanále [147]

Implementace

V roce 2015 byl Josephem Poon a Thaddeusem Dryja zveřejněn white paper, který jako první popisoval protokol Lightning Network. Tohoto návrhu se ujaly tři společnosti – Blockstream, Lightning Labs a ACINQ, které na vývoji Lightning Network odvedli nejvíc práce. Každá společnost vytvořila svou vlastní implementaci protokolu napsanou v jiném programovacím jazyce. V případě společnosti Blockstream se jedná o implementaci s názvem c-lightning, která je napsána v jazyce C. Lightning Labs napsal v Golang implementaci LND (Lightning Network Daemon) a společnost ACINQ využila programovací jazyk Scala pro vytvoření Eclair. V současnosti existuje mnoho dalších implementací, ovšem dle testů je plná interoperabilita zatím zajištěna u třech výše zmíněných, tzn. že tyto implementace mohou spolu bez problémů spolupracovat. [148; 149]

V případě, že chce uživatel začít používat Lightning Network, stačí mu pouze použít kompatibilní software. Pokud chce provozovat svůj vlastní uzel, může si stáhnout jednu z výše zmíněných implementací. Pro ty, kterým stačí jen lightning peněženka, je zde například mobilní aplikace Breez, která je dostupná pro Android i iOS. [141; 150]

Otevírání kanálů

Otevření platebního kanálu mezi dvěma uživateli začíná odesláním on-chain transakce, kdy uživatel odešle libovolný počet BTC na jejich společnou multisignature adresu. Tato transakce je nazývána jako „financující“ a její objem stanovuje maximální kapacitu kanálu

po celou dobu jeho životnosti – kanál zatím nelze zpětně doplnit. Platební kanál tedy není nic jiného, než 2-of-2 multisignature adresa v bitcoinové síti. Kanály jsou obousměrné, tedy oba účastníci mohou přijímat a odesílat platby. Ovšem v současnosti může být kanál naplněn pouze jedním uživatelem. To přináší určité omezení. V případě, že Alice otevře s Bobem kanál odesláním 1 BTC na společnou adresu, může prostřednictvím kanálu poslat transakci až do výše 1 BTC, avšak není prozatím schopna jakoukoliv platbu přijmout. Za takové situace může Bob přijmout od Alice až 1 BTC, ale nemůže jí žádné prostředky poslat. Kanál byl totiž otevřen Alicí a Bob v něm zatím žádné BTC nemá. Situace se změní v momentě, kdy Alice pošle Bobovi např. 0.5 BTC. V takovém případě Alice i Bob disponují určitými prostředky, což jim umožňuje přijímat a odesílat platby v rámci kanálu. Možnost oboustranného naplnění jednoho kanálu je sice zmíněna ve white paperu, avšak je stále ve vývoji. [141; 151; 152]

Nabízí se zde otázka, co se stane v případě, že Alice převede BTC na multisignature adresu a Bob s ní přestane komunikovat. Za normální situace by to znamenalo ztrátu BTC. Alice totiž není schopna bez digitálního podpisu od Boba s prostředky jakkoliv nakládat. Ovšem otevírání kanálů je mnohem sofistikovanější a s takovou situací Lightning Network počítá. Při detailnější pohledu probíhá otevírání kanálu tak, že:

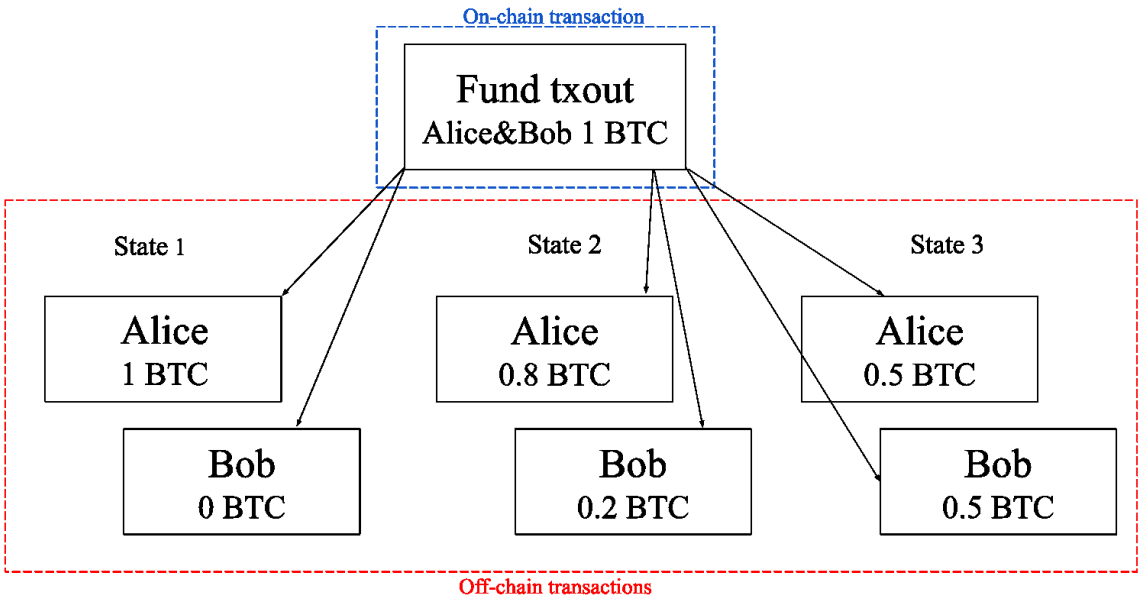
- Alice si vygeneruje nový veřejný a privátní klíč a odešle Bobovi **open_channel** zprávu, ve které ho informuje, že by ráda otevřela kanál.
- V případě, že Bob souhlasí, vygeneruje si také nový pár klíčů a pomocí **accept_channel** zprávy pošle svůj veřejný klíč Alici.
- Alice vytvoří financující transakci, která převádí např. 1 BTC na multisignature adresu. Ovšem před odesláním této transakce do sítě, si Alice vytváří tzv. „závazkovou“ transakci, která převádí BTC ze společné adresy zpátky na adresu její a posílá ji Bobovi.
- V momentě, co Bob podepíše Alici její závazkovou transakci pomocí **funding_signed** zprávy, může Alice odeslat financující transakci do sítě, a tím otevřít platební kanál.

Závazková transakce slouží Alici jako pojistka v případě, že by Bob přestal komunikovat. V momentě odeslání této transakce do sítě by Alice dostala svůj 1 bitcoin zpátky. Závazková transakce je vytvořena pokaždé, kdy dojde v platebním kanále k pohybu. [153; 154]

Transakce

V momentě, kdy je úspěšně otevřen platební kanál, může docházet k převodům prostředků. To, co v platebním kanálu probíhá, je prakticky výměna podepsaných závazkových transakcí, které definují, jak mají být prostředky, které jsou na multisignature adrese rozděleny mezi účastníky kanálu. Při každé transakci si vždy obě strany vygenerují svoji verzi závazkové transakce (níže je vysvětleno proč), kterou si následně nechají protějškem podepsat. Poslední proběhlá transakce definuje aktuální balanc, čili kolika prostředky disponuje každý uživatel kanálu. Princip spočívá v tom, že tyto transakce uživatelé nezveřejňují, avšak si je ponechávají. Díky tomu je platební kanál schopen odbavit mnohem více transakcí než Bitcoin samotný - probíhá zde pouze výměna podpisů. Zveřejňování probíhá až v momentě, kdy dochází k uzavírání kanálů, nebo když vznikne mezi účastníky spor. [140; 155; 156]

V předchozím příkladu si Alice otevřela s Bobem kanál, do kterého nahrála 1 BTC. Nyní chce Bobovi poslat 0.2 BTC. Dojde tedy k vytvoření závazkové transakce, která převádí z multisignature adresy prostředky na adresy účastníků v poměru 0.8 BTC Alici a 0.2 BTC Bobovi. V průběhu doby dojde ještě k další transakci, kdy Alice dále posílá Bobovi 0.3 BTC. Jak je znázorněno na obrázku, vzniká tedy situace, kdy oba účastníci kanálu disponují 0.5 BTC.



Obrázek 11 Transakce v platebním kanále [157]

Jak je zmíněno dříve, při každém pohybu prostředků dochází ke vzniku nové závazkové transakce. Každý z účastníků drží svoji verzi, které jsou poněkud odlišné. Alice i Bob se

tedy nyní dostali do situace, kdy disponují 3 závazkovými transakcemi. Jelikož tyto transakce nejsou zaznamenány na blockchainu, neexistuje žádný záznam o tom, v jakém pořadí transakce proběhly a zda vůbec proběhly. Alice může tedy Boba podvést a zapsat na blockchain transakci, která jí převádí 0.8 BTC a Bobovi místo konečných 0.5 BTC pouze 0.2 BTC. Aby k těmto podvodům nedocházelo, je výstup každé transakce zajištěn pomocí CSV neboli Check Sequence Verify a Revocable keys. CSV v transakci specifikuje, jak dlouho musí být transakce součástí blockchainu, aby mohla být utracena. Revocable key představuje pojistný klíč, i pomocí kterého může být transakce utracena. Klíč je společně s CSV zaznamenán ve výstupu transakce. Pokaždé, když dojde k vytvoření nové závazkové transakce, účastníci kanálu si mezi sebou odhalí Revocable keys, které jsou spojené vždy s předchozí závazkovou transakcí. Tímto odhalením zabrání sami sobě v podvádění. Na otázku „Jak?“ odpoví příklad níže. [155; 156]

Alice se pokusí o podvod a zveřejní v bitcoinové síti závazkovou transakci, která jí připisuje více prostředků než poslední transakce, která v platebním kanálu proběhla. Jelikož se nejedná o poslední transakci v kanále, Alice již svůj Revocable key Bobovi odhalila. Struktura této transakce vypadá následovně:

<table>
<tr><td colspan="2">Commit Tx (held by Alice)</td></tr>
<tr><td>input</td><td>output</td></tr>
<tr><td rowspan="2">fund txid
Bob’s signature</td><td>Alice key & 100 blocks
or AliceRevocable & Bob key

0.8 BTC</td></tr>
<tr><td>Bob address

0.2 BTC</td></tr>
</table>

Obrázek 12 Struktura transakce v síti Lightning Network [158]

V momentě, kdy dojde k zapsání této transakce do blockchainu, je na adresu Boba převedeno 0.2 BTC. Ovšem výstup převádějící 0.8 BTC je zajištěn pomocí CSV a Revocable key. V tomto případě to znamená, že Alice (jelikož vyslala svou verzi transakce) bude moct 0.8 BTC utratit až v momentě, kdy nad blokem obsahující tuto transakci, bude vytěženo dalších 100 bloků. Tento časový interval dává Bobovi možnost prokázat, že Alice podvádí. Jelikož transakce dále definuje, že výstup může být utracen i hned Bobem, když ukáže, že zná AliceRevocable key. Jelikož se nejedná o poslední transakci, která v platebním kanále proběhla, Bob klíč zná. Bob má tedy 100 bloků čas na

to, aby Alici potrestal tím, že ji vezme veškeré prostředky, které v kanále měla. Podvádět v síti Lightning Network se tedy nevyplácí. [155]

V případě, kdy by se Bob pokusil podvádět (i když by neměl důvod, jelikož poslední transakce v kanále mu připisuje více prostředků, než transakce předtím), zveřejnil by svoji verzi transakce, která vypadá podobně jako ta od Alice, pouze podmínky pro utracení výstupu by byly stanovené přesně opačně. Struktura transakce by vypadala následovně:

<table>
<tr><td colspan="2">Commit Tx (held by Bob)</td></tr>
<tr><td>input</td><td>output</td></tr>
<tr><td rowspan="2">fund txid
Alice’s signature</td><td>Alice address
0.8 BTC</td></tr>
<tr><td>Bob key & 100 blocks
or BobRevocable & Alice key
0.2 BTC</td></tr>
</table>

Obrázek 13 Struktura transakce v síti Lightning Network [159]

Zveřejněním této transakce by se Bob sám okradl, jelikož by na adresu Alice převedl 0.8 BTC a ještě by jí dal možnost získat 0.2 BTC. Alici by stačilo jenom prokázat, že zná BobRevocable key a zbylých 0.2 BTC by byly její. [155]

Uzavírání kanálů

Uzavřít kanál v síti Lightning Network lze třemi níže zmíněnými způsoby. Hlavním cílem Lightning Network je, aby uživatelé drželi kanály otevřené co nejdéle. Každé uzavření a otevření kanálu vyžaduje on-chain transakci, což vede k nutnosti platit poplatky těžařům a nárůstu velikosti blockchainu. Uzavřít kanál lze tedy pomocí:

- **Cooperative Close**

  Jedná se o možnost, kdy se oba uživatelé dohodnou na tom, že platební kanál bude uzavřen. Dojde k vygenerování tzv. "uzavírací" transakce, která je téměř totožná s poslední závazkovou transakcí, ovšem s tou odlišností, že ihned po zapsání do blockchainu uvolňuje prostředky oběma stranám.

- **Force Close**

  Force close neboli uzavření silou se provádí většinou v situaci, kdy druhý uživatel kanálu přestal odpovídat a není tedy možné provést cooperative close. Uzavření

probíhá zveřejněním poslední verze závazkové transakce. Jelikož se jedná o poslední verzi, nedošlo ještě k odhalení Revocable keys a transakce může být tedy bezpečně zveřejněna. Omezující pouze je, že uživatel musí na své prostředky čekat po dobu stanovenou v CSV (v minulém příkladu to bylo 100 bloků).

- **Fraudulent Force Close**

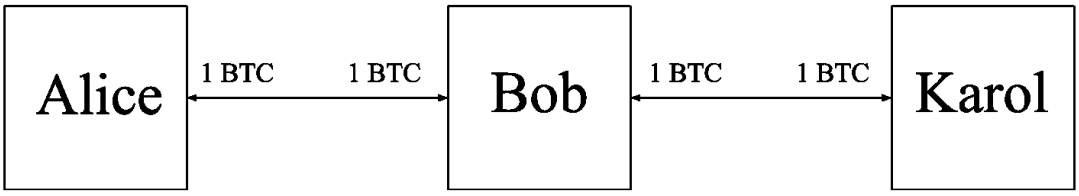
  Jedná se o podvodné uzavření kanálu, kdy jeden z uživatelů zveřejní jinou, než poslední závazkovou transakci. V takovém případě nastává situace, kdy podvedený uživatel má určitou časovou dobu na to, aby prokázal, že se nejedná o poslední transakci – ukáže, že zná Revocable key od této transakce. (příklad Alice a Boba v podkapitole „Transakce“)

[160; 161]

Směrování plateb

Jednou z mnoha unikátních vlastností Lightning Network je schopnost provádění plateb mezi uživateli, kteří mezi sebou nemají otevřený kanál. Není tedy potřeba otevírat platební kanál pokaždé, kdy uživatel chce s někým novým provést transakci. Stačí pouze, aby mezi nimi vedla cesta skrz jiné uživatele. [7]

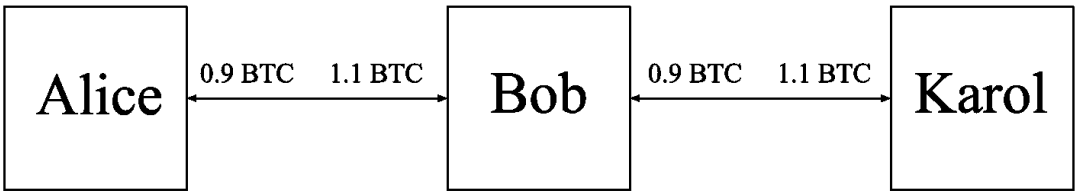
Pro lepší pochopení lze uvést příklad s Alicí, Bobem a Karol. Jak je znázorněno na obrázku níže, Alice má otevřený kanál s Bobem a on zase s Karol. (Jedná se o jednoduchý příklad. V praxi se může mezi Alicí a Karol nacházet mnohem více jedinců.)



Obrázek 14 Cesta mezi Alicí a Karol [155; 162]

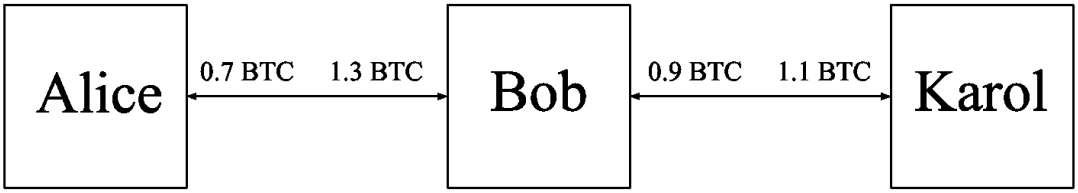
V případě, že chce Alice poslat Karol peníze, nemusí si s ní otevírat nový kanál. Postačí jí využít kanál, který má otevřený s Bobem. Podmínkou je, aby Bob měl v kanále s Karol dostatek prostředků na to, aby uspokojil požadavek Alice. Tedy v případě, že Alice chce poslat Karol 0.1 BTC, je potřeba, aby Bobův zůstatek v kanále s Karol nebyl menší. Alice odešle Bobovi 0.1 BTC s prosbou, zda by stejnou částku nemohl poslat Karol prostřednictvím kanálu, který mají mezi sebou otevřený.

Jednotlivé zůstatky v kanálech by po převodu 0.1 BTC vypadaly následovně:



Obrázek 15 Převod mezi Alicí a Karol prostřednictvím Boba [155; 162]

Za to, že Bob přesměroval platbu, může Alici požádat o poplatek. V případě, že by si Bob řekl o 0.2 BTC za zprostředkování této transakce, musela by Alice Bobovi poslat 0.3 BTC, aby Karol obdržela 0.1 BTC. Pohyb by vypadal následovně:



Obrázek 16 Převod s poplatkem [155; 162]

Ilustrace výše vyobrazené představují vlastní zpracování autora, který vycházel z obrázků prezentované na přednášce Tadga Dryji [155] s názvem „13. Payment Channels and Lightning Network“ a videa Reného Pickhardta [162].

Na závěr je nutné zmínit, že aby přeposílání prostředků bylo bezpečné, je využívaná technologie Hash Time Locked Contract (HTLC). Jak je zmíněno na začátku kapitoly, jedná se o třídu platby, která vyžaduje, aby její příjemce před stanoveným termínem poskytl doklad o jejím přijetí nebo přijatá částka bude vrácená plátci. V praxi to funguje následovně: před provedením platby si Alice s Karol stanoví tajnou informaci, která bude značit, že platba úspěšně proběhla. Transakce začne tím, že si Alice v kanále s Bobem definuje HTLC. V něm stanoví dobu, do které jí musí Bob dokázat, že peníze Karol poslal, jinak se Alici peníze vrací zpátky. Bob to může dokázat sdělením dané tajné informace. K této informaci se dostane tak, že si v kanále s Karol sestaví HTLC, ve kterém vyžaduje, aby mu jí Karol poskytla před stanoveným termínem. Jinak se mu odeslaná částka zpátky vrátí. V případě, že Karol prostředky obdrží, sdělí Bobovi tajnou informaci, pomocí které on Alici dokáže, že platba úspěšně proběhla. K vrácení prostředků tedy nedochází. [155; 162]

Klady a zápory

Níže je uvedena tabulka shrnující hlavní klady a zápory projektu Lightning Network. Jednotlivé pozitiva a negativa jsou pak dále detailněji rozvedeny.

Tabulka 5 Klady a zápory Lightning Network

Klady	**Zápory**
+ Nízké nebo žádné poplatky	- Prostředky jsou uzamčeny v kanále
+ Instantní transakce	- Uložení mincí v tzv. hot wallet
+ Posílání transakci s malým objemem	- Nutnost být on-line
+ Lepší soukromí	- Zálohování
+ Atomic swaps	

Zdroj: [141; 149; 163; 164; 165]

Klady

+ **Nízké nebo žádné poplatky**

  Lightning Network se pyšní tím, že dokáže provádět bezpoplatkové transakce. K účtování poplatků dochází pouze tehdy, kdy je platba směřována přes další uzly. [164; 165]

+ **Instantní transakce umožňující posílat malé částky**

  Nejmenší možná částka, která může být poslána bitcoinovou transakcí představuje přibližně 0.00000546 BTC (546 satoshi). Jedná se o relativně malou částku, která při současném kurzu činí přibližně 1,19 Kč. Avšak Lightning Network posunuje hranice ještě dál a dovoluje posílat částky mnohem nižší. Nejmenší částka, kterou lze odeslat je 0.00000001 BTC (1 satoshi = 0,0022 Kč). [165]

+ **Lepší soukromí**

  Transakce proběhlé v Lightning Network se nikde nezaznamenávají. To vede k výraznému zvýšení soukromí oproti standardním on-chain transakcím, kdy každý pohyb je zapsán do blockchainu. [164]

+ **Atomic swaps**

Lightning Network připravuje možnost provádění tzv. atomic swaps. Jedná se smart kontart technologii, která umožňuje uživateli převádět mince mezi jednotlivými blockchainy. Uživatel tedy nebude potřebovat zprostředkovatele např. burzu, aby si své bitcoiny směnil za litecoiny apod. [149]

Zápory

- **Prostředky jsou uzamčeny v kanále**

  Jak bylo zmíněno v úvodu kapitoly, pro otevření kanálu je nutné odeslat prostředky na 2-of-2 multisignature adresu. Mince jsou tedy na této adresy uzamčeny. V případě, že je uživatel nutně potřebuje k provedení on-chain platby, musí dojít k uzavření kanálu. To může v závislosti na rychlosti vytěžení bloku trvat nejméně 10 minut. [164]

- **Nutnost být on-line a riziko spojené s uložením mincí v hot wallet**

  Lightning Network nepodporuje off-line platby. Při otevírání kanálů nebo provádění transakcí si uživatelé posílají zprávy, které obsahují důležité informace či nutné digitální podpisy. Toto lze provádět pouze za předpokladu, že oba uživatelé jsou připojení k Internetu. V momentě, kdy je peněženka neustále připojena k Internetu, hovoří se o ní jako o tzv. hot wallet. V takovéto peněžence se doporučuje držet jen malý počet mincí, jelikož v případě napadení zařízení může dojít k jejich odcizení. [141; 163]

- **Zálohování**

  Jelikož nejsou off-chain transakce zapsány na blockchainu, je nutné provádět zálohu kanálu. V momentě, kdy uživatel přijde o svá data, je schopen si ze zálohy zjistit poslední závazkovou transakci, a tím si své peníze vyvést z kanálu na svou bitcoinovou adresu. [141]

6 JAK ŠKÁLUJÍ ALTCOINY

Tato kapitola nastiňuje řešení, které využívají vybrané Altcoiny za účelem zlepšení škálovatelnosti. Pro popis si autor vybral kryptoměny Bitcoin Cash, XRP a Ethereum.

6.1 Bitcoin Cash

Ke vzniku Bitcoin Cash došlo 1.8.2017, kdy se část komunity oddělila od Bitcoinu trvalým forkem. Hlavními důvody byl nesoulad názorů na budoucnost řešení škálovatelnosti a neobliba vývojářů Bitcoin Core čínskými těžaři. Bitcoin Cash se tedy vydal cestou zvětšování bloků. Po splitu blockchainu začali těžaři Bitcoinu Cash těžit bloky o velikosti 8 MB. Již rok po rozdělení byl úspěšně proveden upgrade protokolu s názvem Milestone, který stanovil novou velikost bloků na 32 MB. Bitcoin Cash v současné době dokáže zpracovat cca. 100 transakcí za sekundu, ovšem netají se, že propustnost sítě hodlá dále navýšit. Na svých oficiálních stránkách uvádí, že do budoucna plánuje zavést bloky, jejichž velikost se bude adaptovat na růst trhu. Maximální kapacita takových bloků by mohla být až 1 TB. [7; 166; 167]

6.2 XRP

Uvádí se, že platební systém Ripple se svou měnou XRP je schopen konkurovat platební společnosti VISA. Aktuální propustnost sítě činí přibližně 1500 transakcí za sekundu, ovšem s možností škálovat až na 50 tisíc TPS. Těchto rychlostí dosahuje díky technologii, na které je systém postaven. Ripple na rozdíl od jiných tradičních kryptoměn nevyužívá blockchain, avšak spoléhá na decentralizovanou databázi účtů, kterou nazývá ledger. Zápis do ledgeru probíhá na základě vzájemné shody důvěryhodných uzlů. Jedná se o rychlejší alternativu k Proof of Work (kterou využívá Bitcoin), díky které je Ripple schopen potvrdit transakci již do 4 sekund. [168; 169]

6.3 Ethereum

I přesto, že Ethereum se zdá být jako revoluční projekt, který uživateli nabízí široké možnosti, ať už ve formě decentralizovaných aplikací, her, burz, cloudových úložišť, potýká se se stejným problémem jako má Bitcoin. Uvádí se, že síť dokáže zpracovat pouze cca 15 transakcí za sekundu. Vývojářský tým v čele s Vitalikem Buterinem si je vědom, že propustnost Etherea je potřeba navýšit. V teoretické části bylo již zmíněno, že Ethereum plánuje uskutečnit velký upgrade sítě s názvem ETH 2.0. Tento upgrade by měl kromě

přechodu na metodu Proof of Stake přinést i technologii Sharding, která by měla škálovatelnost vylepšit. Princip Shardingu spočívá v tom, že každý uzel již nebude validovat každou transakci, ale dojde k vytvoření skupin tzv. shardu neboli střepů. Každá skupina disponuje jinou částí blockchainu a validuje pouze transakce, které s danou částí souvisí. Jako příklad lze uvést síť, která má 10 000 uzlů a je schopna zpracovat pouze 15 transakcí za sekundu. V případě, že by se uzly rozdělily do 10 skupin, byla by síť najednou schopna zpracovat 150 TPS. Nutností je, aby každá skupina měla dostatečný počet členů a nemohlo tak docházet k manipulaci zápisů. [9; 168; 170]

ZÁVĚR

Cílem práce bylo uvést čtenáře do světa kryptoměn, popsat největší kryptoměnu světa Bitcoin a detailněji se zaměřit na problematiku jeho škálovatelnosti.

V úvodu teoretické části je čtenář seznámen s historií kryptoměn. Historie sahá až do osmdesátých let minulého století, kdy se odehrála řada událostí, která se stala pro zakladatele Bitcoinu Satoshi Nakamota inspirací. Bitcoin tedy nepředstavuje první digitální měnu světa, nýbrž se o něm hovoří jako o první plně decentralizované kryptoměně, která se prosadila na globálním trhu. Úvodní kapitola dále pojednává o základních vlastnostech, které kryptoměny dělají výjimečné. Za zmínku stojí například jejich decentralizace a vysoká míra bezpečnosti, která je zajištěná pomocí kryptografie. V této části se čtenář také dozví, že ne všechny kryptoměny disponují svým vlastním blockchainem. Díky toho jsou také děleny na coiny a tokeny.

Druhá kapitola teoretické části se věnuje samotnému Bitcoinu. Autor zde popisuje jeho základní stavební kameny, princip funkce a jakým způsobem probíhají transakce v síti. Nastíněn je zde i princip a účel těžby, se kterým souvisí i vznik nových bitcoinů. Součástí je také výčet možností, jak Bitcoin získat, uschovat či utratit. K nabytí může dojít např. přes face-to-face obchody, burzy nebo také bitcoinové automaty, z nichž jeden se nachází i ve Zlíně.

V závěru této části rozebírá autor kryptoměny, které jsou dle jeho názoru zajímavé. Místo je zde vyčleněno pro virtuální mašinu s názvem Ethereum a ne všemi uznávanou kryptoměnu XRP.

Praktická část práce uvádí čtenáře do problematiky škálovatelnosti Bitcoinu. Hned v úvodu je definováno, že v případě kryptoměn, se škálováním myslí schopnost zpracovat velké množství transakcí, při udržení si přijatelného transakčního poplatku. Na příkladu z historie je ukázáno, že Bitcoin sám o sobě tuto schopnost nemá a je příliš pomalý. Před komunitou tedy stála otázka, jaké kroky pro jeho vylepšení provést. Optimalizace blockchainu je totiž složitá záležitost a při jejím řešení je nutné brát ohled na základní pilíře Bitcoinu, kterými jsou decentralizace, škálovatelnost a bezpečnost.

Návrhů na vylepšení škálovatelnosti je mnoho. Hovoří o tom i poslední kapitola praktické části, kde autor popisuje odlišné přístupy Altcoinů k této problematice. V případě Bitcoinu si autor vybral ty návrhy řešení, o kterých se vedou největší diskuse. Analýza tedy proběhla u 3 typů řešení, z nichž některé jsou již implementované.

Nejdříve se čtenář může seznámit s řešením pomocí zvětšení kapacity bloků. Jedná se o on-chain řešení, jehož principem je navýšení velikosti ze současných 1 MB. Možností navýšení je několik, buď blok zvětšit na předem stanovenou fixní hodnotu nebo jeho kapacitu ponechat dynamickou, která by se vždy přizpůsobovala aktuálnímu zatížení sítě. Po zhodnocení všech kladů a záporů, které toto řešení má, se dá konstatovat, že v dlouhodobém hledisku se nejedná o perspektivní možnost.

V další části došlo k analýze řešení SegWit, které se dočkalo svojí implementace již v roce 2017. Princip SegWitu spočívá v oddělení digitálních podpisů od transakcí. To vede k úspoře místa v bloku, do kterého se tím pádem vejde více transakcí. I přesto, že samotný SegWit škálovatelnost Bitcoinu ve velké míře nezlepšil, sklidil úspěch v důsledku vyřešení problému „transaction malleability“, díky čemuž se mohlo začít uvažovat nad implementací Lightning Network.

Poslední analyzované řešení je Lightning Network, kterému se v poslední době dostává velké pozornosti. Jedná se o řešení typu off-chain, jehož cílem je ulehčit pomalému bitcoinovému blockchainu, pomocí převedení většiny transakcí mimo řetězec do platebních kanálů, které umožnují provádět instantní transakce. Díky této nadstavbě by byl Bitcoin schopen zpracovat až miliony transakcí za sekundu. I přes svoje nedostatky, které jsou v práci popsány, představuje Lightning Network revoluční řešení, které by mohlo výrazně zlepšit škálovatelnost Bitcoinu.

Co se týče pohledu autora, je jeho důvěra kladena v řešení Lightning Network, které je stále ve svých začátcích a má pořád co nabídnout. Ať už ve formě atomic swaps, možností oboustranného naplnění kanálů apod. Jako největší nevýhodu Lightning Network považuje nutnost využívání tzv. hot wallet.

V obecném pohledu na problém škálovatelnosti Bitcoinu se autor ztotožňuje s názorem Andrease Antonopoulose, který tvrdí, že se nejedná o problém, který by někdy byl vyřešen s konečnou platností. V momentě, co Lightning Network či ostatní řešení narazí na své limity, začne komunita tento problém řešit znovu.

SEZNAM POUŽITÉ LITERATURY

[1] BAJER, Matěj, Johana NÁDVORNÍKOVÁ a Jakub MONÍK. Kryptoměny: Vše, co jste o nich potřebovali vědět, ale nenapadlo vás se zeptat. *Kvalitní internet* [online]. Eurosignal, 2019 [cit. 2019-12-16]. Dostupné z: https://www.kvalitni-internet.cz/kryptomeny-vse-co-jste-o-nich-potrebovali-vedet-ale-nenapadlo-vas-se-zeptat

[2] Co je kryptoměna. *Kurzy.cz* [online]. Praha: Kurzy.cz, c2000-2020 [cit. 2019-12-16]. Dostupné z: https://www.kurzy.cz/kryptomeny/co-je-kryptomena

[3] Top 100 Cryptocurrencies by Market Capitalization. *CoinMarketCap* [online]. CoinMarketCap, 2020 [cit. 2020-02-16]. Dostupné z: https://coinmarketcap.com/

[4] KARMA, . Vzděláváme se: Jak kryptoměny používají kryptografii. *Kryptoportal.cz* [online]. Kryptoportal.cz, 2019 [cit. 2019-12-16]. Dostupné z: https://kryptoportal.cz/vzdelavame-se-jak-kryptomeny-pouzivaji-kryptografii/

[5] NARAYANAN, Arvind, Edward FELTEN, Joseph BONNEAU, Steven GOLDFEDER a Andrew MILLER. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016. ISBN 978-0-691-17169-2.

[6] LAI, Victor. The History of Digital Currency. *Crush Crypto* [online]. Crush Crypto, 2018 [cit. 2019-12-18]. Dostupné z: https://crushcrypto.com/digital-currency-history/

[7] 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.

[8] EXTANCE, Andy. The future of cryptocurrencies: Bitcoin and beyond. *Nature* [online]. Nature News, 2015 [cit. 2020-03-03]. Dostupné z: https://www.nature.com/news/the-future-of-cryptocurrencies-bitcoin-and-beyond-1.18447

[9] KALISKÝ, Boris. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing, 2018. ISBN 978-80-87383-71-1.

[10] Properties Of Cryptocurrencies. *Cryptocurrency Army* [online]. Cryptocurrency Army, 2020 [cit. 2020-02-05]. Dostupné z: https://www.cryptocurrencyarmy.com/properties-of-cryptocurrencies/

[11] KINGDOM, Crypto. Je bitcoin dělitelný jako koruna na haléře?. *Kurzy.cz* [online]. Praha: Kurzy.cz, 2019 [cit. 2020-02-05]. Dostupné z: https://www.kurzy.cz/tema/5772447.html

[12] Wei. *Binance Academy* [online]. Binance, c2017-2019 [cit. 2020-02-05]. Dostupné z: https://www.binance.vision/glossary/wei

[13] AJIBOYE, Timi, Luis BUENAVENTURA, Alex GLADSTEIN, Lili LIU, Alexander LLOYD, Alejandro MACHADO, Jimmy SONG a Alena VRÁNOVÁ. *The little bitcoin book: why bitcoin matters for your freedom, finances, and future*. Redwood City, CA: 21 Million Books, 2019. ISBN 978-1641990509.

[14] M., Michaela. What are the Properties of a Cryptocurrency Asset. *Cryptimi* [online]. 2019 [cit. 2020-02-05]. Dostupné z: https://www.cryptimi.com/guides/what-are-the-properties-of-a-cryptocurrency-asset

[15] REIFF, Nathan. Why Bitcoin Has a Volatile Value. *Investopedia* [online].

Invesopedia, 2020 [cit. 2020-02-05]. Dostupné z: https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp

[16] Some things you need to know. *Bitcoin* [online]. c2009-2020 [cit. 2020-02-05]. Dostupné z: https://bitcoin.org/en/you-need-to-know

[17] CANELLIS, David. Bitcoin Gold hit by 51% attacks, $72K in cryptocurrency double-spent. *The Next Web* [online]. 2020 [cit. 2020-02-05]. Dostupné z: https://thenextweb.com/hardfork/2020/02/05/love-is-a-myth-tinder-earned-1-2-billion-revenue-in-2019/

[18] KONEČNÝ, Lukáš. Co je to kryptoměna a jak funguje Bitcoin. *Power of Doing* [online]. 2018 [cit. 2020-02-05]. Dostupné z: https://powerofdoing.blog/co-je-bitcoin

[19] Jak funguje anonymita bitcoinu?. *Bitcoin v kapse* [online]. Králův Dvůr: bitcoin v kapse, 2018 [cit. 2020-02-05]. Dostupné z: https://bitcoinvkapse.cz/jak-funguje-anonymita-bitcoinu/

[20] Bitcoin Anonymity - Is Bitcoin Anonymous?. *Buy Bitcoin Worldwide* [online]. 2020 [cit. 2020-02-05]. Dostupné z: https://www.buybitcoinworldwide.com/anonymity/

[21] KHATWANI, Sudhir. Can Bitcoin Be Shutdown? Let's See…. *The Money Mongers* [online]. 2019 [cit. 2020-02-05]. Dostupné z: https://themoneymongers.com/can-bitcoin-shutdown/

[22] SHAVINN, . Four key features of Cryptocurrency & what makes it special?. *Coinut* [online]. 2018 [cit. 2020-02-05]. Dostupné z: https://coinut.com/blog/features-cryptocurrency-bitcoin/

[23] KONEČNÝ, Lukáš. Centralizace. In: *Proof of Doing* [online]. Power of Doing, 2018 [cit. 2020-02-27]. Dostupné z: https://powerofdoing.blog/wp-content/uploads/2017/10/centralised-decentralised-distributed.png

[24] PETRÁŠ, Radek. [Pro začátečníky] Coin a token. Jaký je mezi nimi rozdíl?. *Kryptomagazin.cz* [online]. Praha, 2019 [cit. 2020-02-05]. Dostupné z: https://kryptomagazin.cz/pro-zacatecniky-coin-a-token-jaky-je-mezi-nimi-rozdil/

[25] KYTKA, . Rozdělení kryptoměn – čím se liší coin a token. *Kryptomagazin.cz* [online]. Praha, 2019 [cit. 2020-02-05]. Dostupné z: https://kryptomagazin.cz/rozdeleni-kryptomen-rozdil-mezi-coinem-a-tokenem/

[26] DIAN, Mario. Bitcoin: co je hard fork a kdo o něm rozhoduje. In: *Btctip* [online]. 2017 [cit. 2020-02-05]. Dostupné z: https://btctip.cz/bitcoin-co-je-hard-fork-a-kdo-o-nem-rozhoduje/

[27] Co je to Ripple - Jak Obchodovat CFD Ripple a jak Investovat do Ripple CFD. *Admiral Markets* [online]. Admiral Markets Group, 2020 [cit. 2020-02-05]. Dostupné z: https://admiralmarkets.cz/education/articles/cryptocurrencies/co-je-to-ripple

[28] JP, . Kryptoměny: Co je ICO (Initial Coin Offering). *A1Finance.cz* [online]. 2017 [cit. 2020-02-05]. Dostupné z: https://a1finance.cz/investice/forex/digitalni-meny/kryptomeny-ico-initial-coin-offering

[29] SAXENA, Sagar. Ripple Beating Swift with Significantly High Speed & Minimal Cost. *CoinGape* [online]. 2018 [cit. 2020-02-05]. Dostupné z: https://coingape.com/ripple-beating-swift-with-high-speed/

[30] Premine. *Decryptionary* [online]. Decryptionary.com, 2017 [cit. 2020-02-05]. Dostupné z: https://decryptionary.com/dictionary/premine/

[31] REIFF, Nathan. How to Identify Cryptocurrency and ICO Scams. *Investopedia*

[online]. Investopedia, 2019 [cit. 2020-02-05]. Dostupné z: https://www.investopedia.com/tech/how-identify-cryptocurrency-and-ico-scams/

[32] 7 základních pravidel, jak poznat podvodnou kryptoměnu. *Kurzy.cz* [online]. Praha: Kurzy.cz, 2019 [cit. 2020-02-05]. Dostupné z: https://www.kurzy.cz/zpravy/516247-7-zakladnich-pravidel-jak-poznat-podvodnou-kryptomenu/

[33] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin* [online]. 2008 [cit. 2019-12-18]. Dostupné z: https://bitcoin.org/bitcoin.pdf

[34] BITCOIN - Kurz BTC/Bitcoin. *Kurzy.cz* [online]. Praha: Kurzy.cz, 2020 [cit. 2020-02-24]. Dostupné z: https://www.kurzy.cz/bitcoin/

[35] How to Invest in Bitcoin. *Buy Bitcoin Worlwide* [online]. 2020 [cit. 2020-02-24]. Dostupné z: https://www.buybitcoinworldwide.com/kb/investing-in-bitcoin/

[36] Co je to bitcoin. *Kurzy.cz* [online]. Praha: Kurzy.cz, 2020 [cit. 2020-02-25]. Dostupné z: https://www.kurzy.cz/bitcoin/co-je-to-bitcoin

[37] Running A Full Node. *Bitcoin Core* [online]. Bitcoin Project, c2009-2020 [cit. 2020-02-25]. Dostupné z: https://bitcoin.org/en/full-node

[38] ANTONOPOULOS, Andreas. *Mastering Bitcoin: Unlocking digital cryptocurrencies*. Second release. Sebastopol, CA: O'Reilly, 2015. ISBN 978-1-449-37404-4.

[39] REIFF, Nathan. Blockchain Explained. *Investopedia* [online]. Investopedia, 2020 [cit. 2020-02-26]. Dostupné z: https://www.investopedia.com/terms/b/blockchain.asp

[40] Blockchain. *Bitcoin* [online]. c2009-2020 [cit. 2020-02-26]. Dostupné z: https://bitcoin.org/en/blockchain-guide#introduction

[41] WOLF, Karel. Co je to vlastně ten blockchain?. *Alza.cz* [online]. Praha: Alza.cz, 2019 [cit. 2020-02-26]. Dostupné z: https://www.alza.cz/co-je-blockchain

[42] VIDRIH, Marko. What Is a Block in the Blockchain?. *Medium* [online]. 2018 [cit. 2020-02-27]. Dostupné z: https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

[43] WHITTLE, Ben. Block Structure. In: *CoinCentral* [online]. CoinCentral, 2018 [cit. 2020-02-27]. Dostupné z: https://coincentral.com/wp-content/uploads/2018/12/Bitcoin_Block_Data.png

[44] TUWINER, Jordan. What is Bitcoin Mining and How Does it Work?. *Buy Bitcoin Worldwide* [online]. 2019 [cit. 2020-03-02]. Dostupné z: https://www.buybitcoinworldwide.com/mining/

[45] DENEUVILLE, Marion. An in-depth guide into how the mempool works. *Medium* [online]. 2016 [cit. 2020-03-02]. Dostupné z: https://blog.kaiko.com/an-in-depth-guide-into-how-the-mempool-works-c758b781c608

[46] HUSKANOVIć, Alen. Proof of Work – What it Is and How Does it Work?. *Async Labs* [online]. Croatia: Async Labs, 2020 [cit. 2020-03-02]. Dostupné z: https://www.asynclabs.co/blog/proof-of-work-what-it-is-and-how-does-it-work/

[47] FRANKENFIELD, Jake. Mining Pool. *Investopedia* [online]. Investopedia, 2019 [cit. 2020-03-02]. Dostupné z: https://www.investopedia.com/terms/m/mining-pool.asp

[48] MICHELSON, Brad. How to Earn Bitcoin: 5 Simple Ways to Earn More BTC. *Hackernoon* [online]. 2019 [cit. 2020-02-24]. Dostupné z: https://hackernoon.com/how-to-earn-bitcoin-5-simple-ways-to-earn-more-btc-40ecfd1480c4

[49] BAJPAI, Prableen. How to Buy Bitcoin. *Investopedia* [online]. Investopedia, 2019 [cit. 2020-02-24]. Dostupné z: https://www.investopedia.com/tech/how-to-buy-bitcoin/

[50] LocalBitcoins – Směna kryptoměn mezi lidmi. *Finex.cz* [online]. 2020 [cit. 2020-02-24]. Dostupné z: https://finex.cz/recenze/localbitcoins/

[51] TOMAS, . FAQ: Jaký je rozdíl mezi bitcoinovou směnárnou a burzou?. *Bitcoin v kapse* [online]. Králův Dvůr, 2019 [cit. 2020-02-24]. Dostupné z: https://bitcoinvkapse.cz/faq-jaky-je-rozdil-mezi-bitcoinovou-smenarnou-a-burzou/

[52] JAK KOUPIT KRYPTOMĚNY – kde provést nákup, burzy a směnárny, návod. *InvestPlus* [online]. 2020 [cit. 2020-02-24]. Dostupné z: https://investplus.cz/investice/jak-koupit-kryptomeny-kde-provest-nakup-burzy-a-smenarny-navod/

[53] FINEX, Magazín. Jak nakoupit nebo prodat bitcoin v automatu. *Finex.cz* [online]. 2018 [cit. 2020-02-24]. Dostupné z: https://finex.cz/jak-nakoupit-nebo-prodat-bitcoin-v-automatu/

[54] BEIGEL, Ofir. Who Accepts Bitcoin as Payment?. *99Bitcoins* [online]. 99 Coins International PTE. LTD, 2020 [cit. 2020-02-24]. Dostupné z: https://99bitcoins.com/bitcoin/who-accepts/

[55] Jak si přidat peníze na svůj účet Microsoft pomocí Bitcoinu. *Microsoft.com* [online]. Microsoft, 2018 [cit. 2020-02-24]. Dostupné z: https://support.microsoft.com/cs-cz/help/13942/microsoft-account-how-to-use-bitcoin-to-add-money-to-your-account

[56] RAJIB, Md. Top 10 Companies That Accept Bitcoin Payment. *Cryptooa* [online]. 2019 [cit. 2020-02-24]. Dostupné z: https://cryptooa.com/companies-accept-bitcoin-payment/

[57] BĚLKA, . Kde všude můžeme platit Bitcoinem. *IKrypto.cz* [online]. 2019 [cit. 2020-02-24]. Dostupné z: https://www.ikrypto.cz/kde-vsude-muzeme-platit-bitcoinem/

[58] Přehled možností platby. *Alza.cz* [online]. Praha: Alza.cz, 2020 [cit. 2020-02-24]. Dostupné z: https://www.alza.cz/article/112.htm

[59] Kde platit Bitcoinem. *Bitcoin-info.cz* [online]. Bitcoin-info.cz, 2020 [cit. 2020-02-24]. Dostupné z: https://www.bitcoin-info.cz/kde-platit-bitcoinem

[60] All the cryptocurrency merchants and ATMs of the world in one map. *Coinmap* [online]. Invity.io, 2020 [cit. 2020-02-24]. Dostupné z: https://coinmap.org/

[61] PLACHÝ, Rosťa. Co je to Bitcoinová peněženka? A jejich porovnání. *Jak Na Krypto* [online]. 2020 [cit. 2020-02-24]. Dostupné z: https://jaknakrypto.cz/co-je-to-bitcoinova-penezenka-a-jejich-porovnani

[62] FILIM, . Nejlepší mobilní krypto peněženky na kryptoměny. *CryptoSvět* [online]. 2017 [cit. 2020-02-24]. Dostupné z: https://cryptosvet.cz/nejlepsi-mobilni-krypto-penezenky-na-kryptomeny/

[63] Kryptoměnové peněženky - Jak vybrat tu správnou?. *Finex.cz* [online]. 2020 [cit. 2020-02-24]. Dostupné z: https://finex.cz/rubrika/kryptomeny/penezenky/

[64] Peněženky pro kryptoměny, kde uchovat virtuální měny, co je TREZOR?. *InvestPlus* [online]. 2020 [cit. 2020-02-24]. Dostupné z: https://investplus.cz/investice/penezenky-pro-kryptomeny-kde-uchovat-virtualni-meny-co-je-trezor/

[65] SATOSHILABS, . 7 Years of Hardware Wallets: The Success Story of Czech Crypto Enthusiasts Creating a Brand New Industry. *Trezor Blog* [online]. 2018 [cit. 2020-02-24]. Dostupné z: https://blog.trezor.io/7-years-of-hardware-wallets-the-

success-story-of-czech-crypto-enthusiasts-creating-a-brand-new-6648769d373a

[66] TUWINER, Jordan. TREZOR One Review. *Buy Bitcoin Worldwide* [online]. 2020 [cit. 2020-02-24]. Dostupné z: https://www.buybitcoinworldwide.com/wallets/trezor/

[67] Bitcoin Pros and Cons. *Cryptonews* [online]. Cryptonews.com, 2020 [cit. 2020-02-24]. Dostupné z: https://cryptonews.com/guides/bitcoin-pros-and-cons.htm

[68] SAUREL, Sylvain. Bitcoin Gives You Back Control Over Your Wealth but There Is a Price to Pay. *Medium* [online]. 2020 [cit. 2020-02-24]. Dostupné z: https://medium.com/in-bitcoin-we-trust/bitcoin-gives-you-back-control-over-your-wealth-but-there-is-a-price-to-pay-1e065b1e4534

[69] SERRANO, Michael. How to take advantage of volatility in Bitcoin Value. *Wikicrypto* [online]. 2020 [cit. 2020-02-24]. Dostupné z: http://wikicrypto.com/take-advantage-bitcoin-value-volatility

[70] MOLLEN, Felix. Bitcoin's Recent Raging Volatility: The Good and the Bad. *CryptoPotato* [online]. 2019 [cit. 2020-02-24]. Dostupné z: https://cryptopotato.com/the-recent-bitcoin-raging-volatility-the-good-and-the-bad/

[71] What if my wallet generated an existing Bitcoin address?. *CoinHouse* [online]. Coinhouse SAS, 2020 [cit. 2020-02-24]. Dostupné z: https://www.coinhouse.com/what-if-my-wallet-generated-an-existing-bitcoin-address/

[72] AZIZ, . Altcoins vs. Tokens: What's the Difference?. *Master The Crypto* [online]. 2020 [cit. 2020-02-14]. Dostupné z: https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/

[73] What is Cardano (ADA)?. *CoinSwitch* [online]. 2020 [cit. 2020-02-14]. Dostupné z: https://coinswitch.co/info/cardano/what-is-cardano

[74] Ada Blockchain Explorer. *Seiza: Cardano Blockchain Ada Explorer* [online]. MURGO PTE. Ltd, 2020 [cit. 2020-02-14]. Dostupné z: https://www.seiza.com/

[75] Introduction to Consensus. *XRP Ledger* [online]. XRP Ledger Project, 2020 [cit. 2020-02-14]. Dostupné z: https://xrpl.org/intro-to-consensus.html

[76] What is Ethereum?. *Ethereum* [online]. Switzerland: Stiftung Ethereum, 2020 [cit. 2020-02-14]. Dostupné z: https://ethereum.org/what-is-ethereum/

[77] CZEPCZOR, Pavel. Ethereum 2.0 se spustí 3. ledna 2020, co přinese přechod na PoS?. *Investree* [online]. Olomouc: Investree s. r. o., 2019 [cit. 2020-02-14]. Dostupné z: https://investree.cz/ethereum-2-0-se-spusti-3-ledna/

[78] STAFF, Editorial. Ethereum Cryptocurrency: Everything A Beginner Needs To Know. *CoinSutra* [online]. 2019 [cit. 2020-02-14]. Dostupné z: https://coinsutra.com/ethereum-beginners-guide/

[79] Ethereum (VŠE, CO CHCETE VĚDĚT). *Alza.cz* [online]. Praha: Alza.cz a.s., 2018 [cit. 2020-02-14]. Dostupné z: https://www.alza.cz/ethereum

[80] V, Michal. CryptoKitties: Virtuální kočka za cenu nového Porsche. *Kryptomagazin.cz* [online]. Praha, 2018 [cit. 2020-02-14]. Dostupné z: https://kryptomagazin.cz/krypto-kocka-drazsi-nez-luxusni-auto/

[81] MCMULLEN, Grag. Do You Really Own Your CryptoKitties?. *Medium* [online]. 2017 [cit. 2020-02-14]. Dostupné z: https://medium.com/@gmcmullen/do-you-really-own-your-cryptokitties-d2731d3491a9

[82] MCMULLEN, Greg. The CryptoKitties marketplace. Prices are listed in ether (approx. $700 USD / eth). In: *Medium* [online]. 2017 [cit. 2020-02-27]. Dostupné z:

https://miro.medium.com/max/2130/1*080QNkW_lItjCr135MkNzg.png

[83] KUDLÁČEK, Patrik. Smart contracts (Chytré kontrakty) – Co jsou a jak fungují?. *Finex.cz* [online]. 2019 [cit. 2020-02-14]. Dostupné z: https://finex.cz/chytre-kontrakty-smart-contracts-co-jsou-a-jak-funguji/

[84] F, Pavel. Smart kontrakty a jejich revoluční potenciál. *Kryptomagazin.cz* [online]. Praha, 2018 [cit. 2020-02-14]. Dostupné z: https://kryptomagazin.cz/smart-kontrakty-a-jejich-revolucni-potencial/

[85] Škálovatelnost. *IT SLOVNÍK.cz* [online]. IT-Slovnik.cz team, c2008-2020 [cit. 2020-03-23]. Dostupné z: https://it-slovnik.cz/pojem/skalovatelnost

[86] HAYES, Adam. Scalability. *Investopedia* [online]. Investopedia, 2020 [cit. 2020-03-23]. Dostupné z: https://www.investopedia.com/terms/s/scalability.asp

[87] ETFBITCOIN, . Re: Bitcoin Scalability. In: *Bitcointalk.org: Bitcoin Forum* [online]. 2019 [cit. 2020-03-23]. Dostupné z: https://bitcointalk.org/index.php?topic=5209865.msg53356427#msg53356427

[88] O'NEAL, Stephen. Who Scales It Best? Inside Blockchains' Ongoing Transactions-Per-Second Race. *CoinTelegraph* [online]. 2019 [cit. 2020-03-23]. Dostupné z: https://cointelegraph.com/news/who-scales-it-best-inside-blockchains-ongoing-transactions-per-second-race

[89] WOLF, Karel. Peter Todd: Bitcoin je absolutně neškálovatelný, to ale není velký problém. *Lupa.cz* [online]. 2019 [cit. 2020-03-23]. Dostupné z: https://www.lupa.cz/clanky/peter-todd-bitcoin-je-absolutne-neskalovatelny-to-ale-neni-velky-problem/

[90] CROMAN, Kyle, Christian DECKER, Ittay EYAL et al. On Scaling Decentralized Blockchains. *Financial Cryptography and Data Security*. FC2016. Lecture Notes in Computer Science Vol. 9604. Berlin: Heidelberg: Springer, 2016, s. 106-125. ISBN 978-3-662-53357-4.

[91] GEORGIADIS, Evangelos. *How many transactions per second can bitcoin really handle ? Theoretically* [online]. Cryptology ePrint Archive: Report 2019/416 [cit. 2020-03-23]. Dostupné z: https://eprint.iacr.org/2019/416

[92] DINKINS, David. Satoshi's Best Kept Secret: Why is There a 1 MB Limit to Bitcoin Block Size. *CoinTelegraph* [online]. 2017 [cit. 2020-03-23]. Dostupné z: https://cointelegraph.com/news/satoshis-best-kept-secret-why-is-there-a-1-mb-limit-to-bitcoin-block-size

[93] SONG, Jimmy. Understanding Segwit Block Size. *Medium* [online]. 2017 [cit. 2020-03-23]. Dostupné z: https://medium.com/@jimmysong/understanding-segwit-block-size-fd901b87c9d4

[94] Bitcoin All Time High (ATH). *99Bitcoins* [online]. 99 Coins International PTE. LTD., 2020 [cit. 2020-03-23]. Dostupné z: https://99bitcoins.com/bitcoin/historical-price/all-time-high/

[95] Market Price (USD): Average USD market price across major bitcoin exchanges. In: *Blockchain.com* [online]. Luxembourg: BLOCKCHAIN LUXEMBOURG S.A, 2020 [cit. 2020-03-23]. Dostupné z: https://www.blockchain.com/charts/market-price?timespan=all

[96] THORSRUD, Erlend. *Long-term Bitcoin Scalability*. Norsko, 2018.. Master of Science in Communication Technology. Norwegian University of Science and Technology. Vedoucí práce Colin Alexander Boyd, IIK.

[97] NOVÁK, Ondřej. Kurz bitcoinu – analýza. FOMO může udělat divy. *Btctip* [online].

2016 [cit. 2020-03-23]. Dostupné z: https://btctip.cz/kurz-bitcoinu-analyza-fomo-muze-udelat-divy/

[98] PARALELNÍ POLIS. Bitcoin scaling with Andreas Antonopoulos. In: *Youtube* [online]. 2016 [cit. 2020-03-23]. Dostupné z: https://www.youtube.com/watch?v=Ul-WFb9MHR8

[99] AANTONOP. Bitcoin Q&A: How Bitcoin will scale gracefully, over and over again - Scaling Options. In: *Youtube* [online]. 2016 [cit. 2020-03-23]. Dostupné z: https://www.youtube.com/watch?v=NMzBatr4mMk

[100] AANTONOP. Bitcoin Q&A: Scaling and "Satoshi's vision". In: *Youtube* [online]. 2018 [cit. 2020-03-23]. Dostupné z: https://youtu.be/Ub2LoTcYV54

[101] GERSHUNI, Stepan. Second Layer Blockchain Scaling: Off-Chain Solutions. *Masterthecrypto* [online]. 2020 [cit. 2020-03-23]. Dostupné z: https://masterthecrypto.com/second-layer-blockchain-scaling-off-chain-solutions/

[102] Orphan Block. *Investopedia* [online]. Investopedia, 2019 [cit. 2020-03-25]. Dostupné z: https://www.investopedia.com/terms/o/orphan-block-cryptocurrency.asp

[103] AZIZ, . Guide to Forks: Everything You Need to Know About Forks, Hard Fork and Soft Fork. *Master The Crypto* [online]. 2020 [cit. 2020-03-25]. Dostupné z: http://masterthecrypto.com/guide-to-forks-hard-fork-soft-fork/

[104] TĚTEK, Josef. Kryptoměnové forky (VŠE, CO CHCETE VĚDĚT). *Alza.cz* [online]. Praha: Alza.cz a.s, 2019 [cit. 2020-03-25]. Dostupné z: https://www.alza.cz/kryptomenove-forky#co-je-to

[105] SOBOTKA, Petr. SegWit jako soft fork je špinavé řešení. *Petr Sobotka* [online]. 2017 [cit. 2020-03-25]. Dostupné z: https://www.petrsobotka.cz/blog/segwit-soft-fork.html

[106] FILIM, . Nejen Bitcoin fork: co je hard fork nebo soft fork. *CryptoSvět* [online]. 2018 [cit. 2020-03-25]. Dostupné z: https://cryptosvet.cz/nejen-bitcoin-fork-o-co-jde-kdyz-se-rekne-hard-fork-nebo-soft-fork/

[107] DIAN, Mario. Bitcoin: co je hard fork a kdo o něm rozhoduje. *Btctip* [online]. 2017 [cit. 2020-03-25]. Dostupné z: https://btctip.cz/bitcoin-co-je-hard-fork-a-kdo-o-nem-rozhoduje/

[108] OGURCAKOVA, Denisa. Bitcoin Cash (BCH). *Kryptomagazin.cz* [online]. Praha, 2018 [cit. 2020-03-25]. Dostupné z: https://kryptomagazin.cz/polopate-bitcoin-cash/

[109] BANG, Julie. A Hard Fork: Non-upgraded nodes Reject The New Rules, Diverging The Chain. *Investopedia* [online]. Invesopedia, 2019 [cit. 2020-02-05]. Dostupné z: https://www.investopedia.com/thmb/OWkAaU3VGhqo3JYMNDjemLJJ5fY=/5751x0/filters:no_upscale():max_bytes(150000):strip_icc():format(webp)/HardForkBlockchain3-6f5d8ce52f8a4dcba1137264e0d6c2d6.png

[110] WÜRTH, Paulina. Schematische Darstellung der Hard Fork. Das Logo für Bitcoin Cash wurde nocht nicht vergeben. *Elektronik* [online]. 2017 [cit. 2020-02-06]. Dostupné z: https://cdn.weka-fachmedien.de/thumbs/media_uploads/images/1501581174-312-worotijgk.png.950x534.jpg

[111] HAVEL, Mário. BIP – Technologická vylepšení Bitcoinu. *Alza.cz* [online]. Praha: Alza.cz a.s, 2019 [cit. 2020-03-31]. Dostupné z: https://www.alza.cz/bip-technologicka-vylepseni-bitcoinu

[112] WIRDUM, Aaron. Why Some Changes to Bitcoin Require Consensus: Bitcoin's 4 Layers. *Bitcoin Magazine* [online]. 2016 [cit. 2020-03-31]. Dostupné z:

https://bitcoinmagazine.com/articles/why-some-changes-to-bitcoin-require-consensus-bitcoin-s-layers-1456512578

[113] TAAKI, Amir. BIP Purpose and Guidelines. *GitHub* [online]. 2011 [cit. 2020-03-31]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki

[114] VANČURA, Tadeáš. Co je škálovatelnost u kryptoměn a bitcoinu. *TradeArena.cz* [online]. GTO Solutions, 2018 [cit. 2020-03-31]. Dostupné z: https://www.tradearena.cz/rubriky/bitcoin/co-je-skalovatelnost-u-kryptomen-a-bitcoinu_509.html

[115] NODE, Blockchain. The Case for Scaling Bitcoin On-chain: Version 1.5. *Nodeblockchain.io* [online]. 2018 [cit. 2020-03-31]. Dostupné z: https://drive.google.com/file/d/1BX4BebYFgG1S8HsXGyak46H_rwEHnTsM/view

[116] AZIZ, . Blockchain Scalability Solutions: Overview of Crypto Scaling Solutions. *Master The Crypto* [online]. 2020 [cit. 2020-03-31]. Dostupné z: https://masterthecrypto.com/blockchain-scalability-solutions-crypto-scaling-solutions/

[117] BASHIR, Imran. *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Second Edition. Birmingham: Packt Publishing Ltd, 2018. ISBN 978-1-78883-904-4.

[118] TORPEY, Kyle. 7 Bitcoin Leaders Speak Up On The Bitcoin Block Size Limit Debate. *CoinGecko* [online]. CoinGecko, 2015 [cit. 2020-03-31]. Dostupné z: https://www.coingecko.com/buzz/bitcoin-leaders-speak-up-block-size

[119] GÖBEL, Johannes a Anthony KRZESINSKI. Increased block size and Bitcoin blockchain dynamics. *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*. Melbourne, 2017, , 1-6.

[120] GARZIK, Jeff, Tom HARDING a Dagur JOHANNSSON. Dynamic maximum block size by miner vote. *GitHub* [online]. 2015 [cit. 2020-03-31]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip-0100.mediawiki

[121] ANDRESEN, Gavin. Increase maximum block size. *GitHub* [online]. 2015 [cit. 2020-03-31]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki

[122] WUILLE, Pieter. Block size following technological growth. *GitHub* [online]. 2015 [cit. 2020-03-31]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip-0103.mediawiki

[123] SANCHEZ, Washington. Dynamic limit on the block size. *GitHub* [online]. 2015 [cit. 2020-03-31]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip-0107.mediawiki

[124] BUZZ, Coin. Gavin Andresen Proposes 20 MB Block Size: Pros and Cons. *CoinBuzz* [online]. 2015 [cit. 2020-04-07]. Dostupné z: https://www.coinbuzz.com/2015/05/12/gavin-proposes-20-mb-block-size/

[125] What Is the Bitcoin Block Size Limit?. *Bitcoin Magazine* [online]. 2020 [cit. 2020-04-07]. Dostupné z: https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit

[126] NETWORK, Conflux. Technical comments on the debate of the block size in BCH fork: is increasing the block size the right approach for throughput improvement?. *Medium* [online]. 2019 [cit. 2020-04-07]. Dostupné z: https://medium.com/@ConfluxNetwork/technical-comments-on-the-debate-of-the-block-size-in-bch-fork-is-increasing-the-block-size-the-748b999d6091

[127] A Beginner's Guide to Segregated Witness (SegWit). *Binance Academy* [online]. Binance.com, c2017-2020 [cit. 2020-04-07]. Dostupné z: https://www.binance.vision/blockchain/a-beginners-guide-to-segretated-witness-segwit

[128] AANTONOP, . Bitcoin Q&A: What is Segregated Witness?. In: *Youtube* [online]. 2018 [cit. 2020-04-07]. Dostupné z: https://youtu.be/dtOjjB4mD8k

[129] MUKHOPADHYAY, Anujit. Bitcoin SegWit implementation: key lessons for blockchain developers. *101 Blockchains* [online]. 2018 [cit. 2020-04-07]. Dostupné z: https://101blockchains.com/bitcoin-segwit-implementation/

[130] BRADBURY, Danny. What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability. *Coindesk* [online]. 2014 [cit. 2020-04-07]. Dostupné z: https://www.coindesk.com/bitcoin-bug-guide-transaction-malleability

[131] ScriptSig. *Trezor Wiki* [online]. SatoshiLabs, 2020 [cit. 2020-04-07]. Dostupné z: https://wiki.trezor.io/ScriptSig

[132] MEHER, Akshay. Segwit Block Size and Block Weights. *Medium* [online]. 2019 [cit. 2020-04-07]. Dostupné z: https://medium.com/@akshay_111meher/segwit-block-size-and-block-weights-f5864a6133fc

[133] MEHER, Akshay. Legacy and Segwit Transaction. In: *Medium* [online]. 2019 [cit. 2020-04-07]. Dostupné z: https://medium.com/@akshay_111meher/segwit-block-size-and-block-weights-f5864a6133fc

[134] MEHER, Akshay. Witness trie is appended at the end of the coinbase transaction. In: *Medium* [online]. 2019 [cit. 2020-04-07]. Dostupné z: https://medium.com/@akshay_111meher/segwit-block-size-and-block-weights-f5864a6133fc

[135] TUWINER, Jordan. What is Segregated Witness (Segwit)?. *Buy Bitcoin Worldwide* [online]. 2019 [cit. 2020-04-07]. Dostupné z: https://www.buybitcoinworldwide.com/segwit

[136] BLOCKTALKCHAIN, . How Does non-SegWit (Legacy) Node Verify SegWit Transaction?. *Medium* [online]. 2018 [cit. 2020-04-07]. Dostupné z: https://medium.com/@BlockTalkChain/how-does-non-segwit-legacy-node-verify-segwit-transaction-c3bc0872842b

[137] BITDEGREE, . What is SegWit and How it Works Explained. *BitDegree* [online]. 2020 [cit. 2020-04-07]. Dostupné z: https://www.bitdegree.org/tutorials/what-is-segwit/#What_is_SegWit_The_Pros

[138] SegWit spending Payments: Shows the percentage of payments spending SegWit per day. *Transactionfee: Bitcoin Protocol Layer Statistics* [online]. 2020 [cit. 2020-04-07]. Dostupné z: https://transactionfee.info/charts/payments-spending-segwit/

[139] AANTONOP, . Bitcoin Q&A: Lightning Network scaling. In: *Youtube* [online]. 2018 [cit. 2020-04-08]. Dostupné z: https://youtu.be/4KiWkwo48k0

[140] BITCOINOVEJ KANÁL, . #35 - Bitcoin Lightning Network. In: *Youtube* [online]. 2019 [cit. 2020-07-06]. Dostupné z: https://www.youtube.com/watch?v=pZdRxi-zi1Y&t=579s

[141] BITCRYPTEX, . Basics of the Lightning Network. In: *Bitcointalk.org: Bitcoin Forum* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://bitcointalk.org/index.php?topic=4940536.msg44524521#msg44524521

[142] RICHARD, . Multisignature Technology Explained. *Mycryptopedia* [online]. mycryptopedia.com, 2018 [cit. 2020-07-06]. Dostupné z:

https://www.mycryptopedia.com/multisignature-technology-explained/

[143] AANTONOP, . Bitcoin Q&A: The Lightning Network. In: *Youtube* [online]. 2017 [cit. 2020-07-06]. Dostupné z: https://www.youtube.com/watch?v=vPnO9ExJ50A

[144] FRIEDENBACH, Mark, BTCDRAK, Nicolas DORIER a KINOSHITAJONA. Relative lock-time using consensus-enforced sequence numbers: BIP: 68. *GitHub* [online]. 2015 [cit. 2020-07-06]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip-0068.mediawiki

[145] PICKHARDT, René. How many Transactions per Second are possible in one Payment Channel of Bitcoins Lightning Network?. In: *Youtube* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://www.youtube.com/watch?v=txcjxSRDvqQ

[146] Real-Time Lightning Network Statistics. *1ML.com* [online]. 1ML.com, 2020 [cit. 2020-07-06]. Dostupné z: https://1ml.com/statistics

[147] PICKHARDT, René. Times for complete round trip payments on the lightning network usinf two local c-lightning clients. In: *GitHub* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://github.com/renepickhardt/HackALapp/blob/master/HackABechmarkLAPP/data/HistogramPayVsSendPayAPI.png

[148] AANTONOP, . Bitcoin Q&A: Lightning and onion routing. In: *Youtube* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://www.youtube.com/watch?v=D-nKuInDq6g&t=112s

[149] What Is Lightning Network And How It Works. *CoinTelegraph* [online]. 2020 [cit. 2020-07-06]. Dostupné z: https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works

[150] Lightning Fast Bitcoin Payments: Send and receive instantaneous Bitcoin payments with Breez mobile app. *Breez* [online]. 2020 [cit. 2020-07-06]. Dostupné z: https://breez.technology/

[151] SHEA, Ryan. Channel Capacity. *ION Lightning Network Wiki* [online]. 2019 [cit. 2020-07-06]. Dostupné z: https://wiki.ion.radar.tech/tech/channels/channel-capacity

[152] SHEA, Ryan. Opening A Channel. *ION Lightning Network Wiki* [online]. 2019 [cit. 2020-07-06]. Dostupné z: https://wiki.ion.radar.tech/tech/channels/channel-opening

[153] THORSRUD, Erlend. *Long-term Bitcoin Scalability*. Norway, 2018.. Norwegian University of Science and Technology. Vedoucí práce Colin Alexander Boyd, IIK.

[154] BOND, Federico. A Deep Dive into LND: Overview and Channel Funding Process. *Muun.com* [online]. 2019 [cit. 2020-07-06]. Dostupné z: https://blog.muun.com/a-deep-dive-into-lnd-overview-and-channel-funding-process/v

[155] MIT OPENCOURSEWARE, . 13. Payment Channels and Lightning Network: Instructor - Tadge Dryja. *Youtube* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://www.youtube.com/watch?v=Hzv9WuqIzA0&t=3785s

[156] HARDING, David. What is a hash pre-image as it is used for the breach remedy?. In: *StackExchange* [online]. 2016 [cit. 2020-07-06]. Dostupné z: https://bitcoin.stackexchange.com/questions/48053/what-is-a-hash-pre-image-as-it-is-used-for-the-breach-remedy

[157] DRYJA, Tadge. Add and delete states (image in the video). In: *Youtube* [online]. 2018 [cit. 2020-07-06]. Dostupné z: 13. Payment Channels and Lightning Network

[158] DRYJA, Tadge. Revocable tx: Commit Tx held by Alice (image in the video). In: *Youtube* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://www.youtube.com/watch?v=Hzv9WuqIzA0&t=3785s

[159] DRYJA, Tadge. Revocable tx: Commit Tx held by Bob (image in the video). In: *Youtube* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://www.youtube.com/watch?v=Hzv9WuqIzA0&t=3785s

[160] SHEA, Ryan. Closing A Channel. *ION Lightning Network Wiki* [online]. 2019 [cit. 2020-07-06]. Dostupné z: https://wiki.ion.radar.tech/tech/channels/channel-closing

[161] CDECKER, . Closing a channel in Lightning Network. In: *StackExchange* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://bitcoin.stackexchange.com/questions/80394/closing-a-channel-in-lightning-network

[162] PICKHARDT, René. Onion Routing with HTLCs on the Lightning Network explained! - Beginner / Experts. In: *Youtube* [online]. 2019 [cit. 2020-07-06]. Dostupné z: https://www.youtube.com/watch?v=toarjBSPFqI&t

[163] BOSE, Sumedha. Pros and Cons Of Lightning Network. *BtcWires* [online]. 2018 [cit. 2020-07-06]. Dostupné z: https://www.btcwires.com/block-o-pedia/pros-and-cons-of-lightning-network/

[164] JANNES, . What are the trade-offs between transacting on Lightning Network and Bitcoin mainchain?. In: *StackExchange* [online]. 2016 [cit. 2020-07-06]. Dostupné z: https://bitcoin.stackexchange.com/questions/42639/what-are-the-trade-offs-between-transacting-on-lightning-network-and-bitcoin-mai

[165] A Beginner's Guide to Bitcoin's Lightning Network. *Binance Academy* [online]. Binance.com, c2017-2020 [cit. 2020-07-06]. Dostupné z: https://academy.binance.com/blockchain/what-is-lightning-network

[166] The Bitcoin Cash Roadmap. *Bitcoin Cash* [online]. bitcoincash.org, 2020 [cit. 2020-04-08]. Dostupné z: https://www.bitcoincash.org/roadmap.html

[167] REDMAN, Jamie. Bitcoin Cash Upgrade Milestone Complete: 32MB and New Features. *Bitcoin.com* [online]. Saint Bitts LLC, 2018 [cit. 2020-04-08]. Dostupné z: https://news.bitcoin.com/bitcoin-cash-upgrade-milestone-complete-32mb-and-new-features/

[168] TAYGUNDOGAN, . Who Scales It Best? Blockchains' TPS Analysis. *Hackernoon* [online]. 2020 [cit. 2020-04-08]. Dostupné z: https://hackernoon.com/who-scales-it-best-blockchains-tps-analysis-pv39g25mg

[169] FEBRERO, Pedro. What is Ripple?: Our guide explains everything you need to know about Ripple. *Coin Rivet* [online]. 2018 [cit. 2020-04-08]. Dostupné z: https://coinrivet.com/guides/what-is-ripple/what-is-ripple/

[170] JAIN, Siddharth. Understanding Ethereum Scaling — Categorizing projects by approach adopted. *Medium* [online]. 2019 [cit. 2020-04-08]. Dostupné z: https://medium.com/matic-network/understanding-ethereum-scaling-categorizing-projects-by-approach-adopted-97c79b25eb55

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BIP	Bitcoin Improvement Proposals
BTC	Bitcoin
CPU	Central Processing Unit
CSV	Check Sequence Verify
ETH	Ethereum
FOMO	Fear of Missing Out
FPGA	Field Programmable Gate Array
HTLC	Hash Time Locked Contract
ICO	Initial Coin Offering
ID	Identification
LND	Lightning Network Daemon
LTC	Litecoin
MB	Megabyte
PoS	Proof of Stake
PoW	Proof of Work
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TPS	Transactions Per Second
Tx	Transaction
USD	United States Dollar
VISA	Visa International Service Association
VoIP	Voice over Internet Protocol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK