Univerzita Karlova

Filozofická fakulta

Katedra sociologie

Sociologicko-ekonomická studia

Bakalářská práce

Ondřej Holub

Finanční trhy

Kryptoměna jako prostředek směny

Financial Markets

Cryptocurrency as a Regular Tool for an Exchange

Praha 2020

Vedoucí práce: doc. Ing. Josef Vlček, CSc.

Poděkování:

Chtěl bych poděkovat svým rodičům, kteří mi poskytovali veškerou podporu a zázemí během studia i mimo něj, panu docentovi Ing. Josefu Vlčkovi, CSc., který se mnou podnikl cestu na poli kryptoměn a věnoval mi svůj čas, cenné rady a komentáře i během pandemie, které byly velmi nápomocné a značně pomohly k realizaci této práce. Dále bych také chtěl poděkovat panu docentovi PhDr. Jiřímu Buriánkovi, CSc. a panu Mgr. Martinu Betincovi, Ph.D., kteří mají nemalý podíl na tom, že mohu psát a následně obhajovat svou práci a posléze dostavit se k závěrečným státním zkouškám.

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, řádně citoval všechny použité prameny a literaturu a také deklaruji, že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 2.12.2020 Ondřej Holub

Abstrakt:

Tato práce se zaměřuje na fenomén uplynulého desetiletí, který se nazývá kryptoměna, a na základě historického kontextu formy peněz jej porovnat a posoudit, zda se opravdu jedná o měnu či nikoliv. Nejprve si nadefinuji pojem peníze a jejich podstatu včetně funkcí spolu s tím spjatých a vyobrazení peněz v rámci světové politiky. Následně se rozebere jejich vývoj s vývojem kryptoměn první generace, jejich mechaniky a následné směřování generace druhé a rozbor, zda lze pokládat kryptoměny za měnu a nejedná se pouze o tržní výkyv. Ke konci práce se věnuji nastínění světové kryptoměny, která by plnohodnotně plnila funkci peněz v rámci simulace světové kryptoměny WAT s centrální emitencí prostřednictvím Světové banky v rámci kapacit mých a rozsahu této práce.

Klíčová slova:

Měna, Kryptoměna, Peníze, Euro, Bitcoin, Blockchain, DeFi, Zlato, Komodity, Poplatek za transakci, Altcoiny.

Abstract:

This thesis is focused on the phenomenon of former decade which is called cryptocurrency and compare it on the basis of historical context with a regular currencies that are among us and decide if it is comparatible with a classic kind of money that we usually use in our daily life or not at all. Firstly I will describe the definition of term money and the combination of its features with its functions included and also the view of money as the key instrument in global politics. The following part where is situated a comparation of development of the regular currencies and the first generation cryptocurrencies, their mechanics and the future possible development of cryptocurrencies 2.0 with an answer on the question if the cryptocurrencies are comparatible with the original model of money circulation or if its bubble that will burst. At the end is found possible direction of cryptocurrencies that could lead to the agreement among finacial institutions to consider cryptocurrencies as a regular payment method through a simulation of world cryptocurrency named WAT which would be released by World Bank.

Key Words:

Currency, Cryptocurrency, Money, Euro, Bitcoin, DeFi, Gold, Comodities, Transaction Fee. Altcoins.

Obsah

Úvod **8**
1. Peníze **11**
1.1. Vznik a jejich vývoj **11**
1.2. Měnová soustava a její historie, devizový trh a světové peníze **16**
1.3. Brettonwoodský měnový systém a společná měna **26**
2. Kryptoměny **29**
2.1. Historie alternativ **30**
2.2. Krypta 1.0 ..... **32**
2.3. Mechanika kryptoměn 1.0 ..... **39**
2.4. Kryptoměny 2.0 ..... **45**
3. Kryptoměna WAT **52**
Závěr **54**
Prameny **56**

Seznam tabulek a grafů

Graf č.1: Tržní kapitalizace kryptoměn včetně objemu obsaženého kapitálu. 35
Graf č.2: Tržní kapitalizace kryptoměn mimo BTC. 38
Graf č.3: Tržní podíl kryptoměn na celkové kryptoměnovém trhu. 49

Úvod

V průběhu existence současné měnové soustavy, která zahrnuje centrálu v podobě centrální banky a řady komerčních bank či případně nějakou nadstavbu v podobě nadnárodní centrální banky, se vždy našla skupina lidí, kteří této soustavě nedůvěřovali z racionálních či iracionálních důvodů. Důvěryhodnost finančního systému a příslušných institucí podkopal i fakt, že roku 2008 vyplavala na povrch **hypoteční krize** na americkém trhu, která se přetavila do světové finanční krize v důsledku celosvětového odkrytí toxických aktiv, se kterými manipulovaly finanční instituce a komerční banky. Tím netvrdím, že krize byla důvodem vzniku nového fenoménu jménem kryptoměny, ale rozhodně se na tom znatelně podepsala. Nebyl to jediný důvod, ale rostoucí nedůvěra vůči finančním institucím přispěla k urychlení rozvoje alternativních cest v tomto prostředí. V roce 2008 byl představen **Bitcoin**[1] a platforma na němž běží, tedy blockchain, a o rok později byl tento systém spuštěn anonymním tvůrcem či anonymní skupinou pod pseudonymem Satoshi Nakamoto[2].

Bitcoin měl představovat alternativní měnový systém, který by, za předpokladu všeobecného zájmu, koexistoval s centralizovanou formou. Širšího zájmu se dočkal cca 4 roky po svém uveřejnění, a to v roce 2013, kdy vznikla první kryptoburza Mt.Gox[3] dle údajů Skalického a Stroukala, která dovedla odvážnější investory k této záležitosti kvůli své vysoké volatilitě, která se stále i po téměř 12 letech své existence nestabilizovala. To je také důkazem toho, že Bitcoin nevyužívá dostatečný počet uživatelů a nevzbuzuje důvěru pro širší veřejnost, což je většinová populace mimo investory s dynamickými portfolii a IT pracovníky. A bez účasti širší veřejnosti se tato stabilizace konat nebude.

Navzdory extrémní kolísavosti Bitcoinu vznikly projekty kryptoměn, které byly právě odvozeny od technologie Bitcoinu a to **blockchainu**. Bitcoin byl velkou inspirací pro inovátory, kteří modifikovali platformu pro své účely a v některých případech i pro své vlastní kryptoměny. V letech navazujících od zveřejnění tohoto fenoménu vzniklo mnoho bitcoinových derivátů s tím, že většina si nenašla zájem veřejnosti a jak rychle projekt vznikl, tak rychle zanikl. Za zmínku stojí deriváty jako **Litecoin**, **Ethereum** či **Dash**, kteří využívají technologii blockchainu.

[1] Bitcoin jako systém kryptoměny, BTC jako jednotka „měny“ a zkratka pro název systému.
[2] Dle FreeCoin.cz. Tuto informaci uvádí publikace a weby věnující se kryptoměnám či projektů s nimi spojených, vyjma samotné domovské sítě Bitcoin.org.
[3] První kryptoburza, na níž se začaly obchodovat kryptoměny dle Skalického a Stroukala.

Tento nový segment má v názvu termín měna, ale není to tak úplně jednoznačné, zda se opravdu o měnu jedná. Příkladem může být rozpolcenost jednotlivých států ohledně vnímání kryptoměn. Federální vláda Spojených států amerických postihuje kohokoliv, kdo by chtěl rozvíjet alternativu k dolaru či navázat alternativu přímo na americký dolar. Díky tomu, že zakladatel (či zakladatelé) Bitcoinu je znám pouze pod pseudonymem Satoshi Nakamoto a v reálném světě není dohledatelný díky ochraně svých údajů prostřednictvím blockchainu, tzn. že Federální vláda Spojených států amerických nemá koho stíhat. Autoři centralizovaných projektů takové štěstí neměli a čelili následkům své činnosti, které popisuji v samostatné podkapitole Historie alternativ. Rozpačité přijímání kryptoměn je i mezi evropskými zeměmi jako Německo, které Bitcoin považuje od roku 2013 jako virtuální měnu a s tím příslušné danění dle Holanové, a naopak Finsko dle Lazaroviče považuje kryptoměny za **komodity**. Wolf potvrzuje, že Česká národní banka také nepovažuje Bitcoin a ostatní kryptoměny za **měnu**, ale ani jako **finanční nástroj**. Stroukal se Skalickým dokládá, že zatímco Norsko považuje kryptoměny za měny, tak Švédsko je považuje pouze za aktiva s příslušným přirazením ke komoditám.

Cílem práce skrze výzkumnou otázku je tedy zjistit, zda je možné, aby kryptoměna obsluhovala směnnou interakci ve formě světových peněz a zda se vůbec jedná o směnný prostředek, čímž peníze bezpochyby jsou. Ověření proběhne prostřednictvím definice peněz včetně jejich vývoje a funkcí, kterými disponují. Následuje historický vývoj peněžního prostředí včetně směnných vztahů v jednotlivých strukturách. V navazující kapitole Kryptoměny v souvislosti s předchozí kapitolou toto nové odvětví představím, popíšu jeho mechaniku a uvedu nejnovější směřování tohoto nového segment včetně možného příkladu, kde nastíním možný směr vývoje kryptoměn v případě, že by chtěla proměnit šanci stát se směnným prostředkem.

Všeobecně jsem vnímal nadšení z kryptoměn před psaním samotné práce jako přiměřené a opodstatněné a s vidinou uchopení všech jejich výhod jsem chtěl nastínit možnou mezeru na finančním trhu, která by vyzdvihla veškeré jejich přednosti a naplnila potenciál světových peněz tak, jak to autoři zamýšleli s tím rozdílem, že tyto světové peníze budou decentralizované, ale stále na bázi kryptoměn pod záštitou silné světové organizace. Této modelaci v rámci svých znalostních a mentálních kapacit se věnuji v samostatné kapitole Kryptoměna WAT.

Dle Skalického a Stroukala je hodnota peněz dána užitkem, který mu lidé připisují, což bych interpretoval jako směnitelnost daných peněz či konkrétní měny. Tím více mne

překvapilo, že cena Bitcoinu dosáhla historického maxima 19 300 USD za kus k roku 2017, což odpovídá 424 600 Kč za 1 minci BTC dle tehdejšího kurzu 22 Kč vůči 1 USD dle Kurzy.cz. Navzdory vysoké **volatilitě** si Bitcoin drží svou stálou cenu v několika set tisících českých korunách. Má opravdu takový užitek neboli směnitelnost vzhledem k ceně?

Jelikož tématika kryptoměn byla pro mne neuchopitelná možná stejně tak, jako je nyní možná pro Vás, čtenáře, tak jsem chtěl v této problematice zorientovat a odpovědět si na mnou položené otázky a mezi ty hlavní se řadí, zda kryptoměna může zastávat funkci světových peněz, jak kryptoměny fungují z peněžního hlediska a jaké opodstatnění je za vysokou cenou kryptoměn včetně nástinu jejich možného potenciálu, který zůstal z mého pohledu nevyužit, a jejich dalších možností, které nabízejí.

1. Peníze

1.1. Vznik a jejich vývoj

Peníze jsou spjaty s termínem **hodnota**, která je udávána věcem na základě přirozeného řádu, který některé věci zvýhodňuje a některé naopak znevýhodňuje, kdy hodnota se posuzuje na základě obsahu, ale i odchylku od přirozeného řádu. Všechny věci mají stejnou hodnotu, pouze člověk škatulkuje věci na vzácné a běžné, ale jelikož člověk žije v sebou vytvořeném světě již několik tisíc let, tak hodnoty věcí, reprodukované a vytvořené na základě myšlenek, názorů a objevů, mají odlišnou váhu pro naši společnost. A právě na základě poznatků můžeme přisuzovat věcem odlišnou hodnotu, neboť kvůli poznání detekujeme u věcí odlišné počty vlastností, které jsou využitelné k životu (Simmel,2011).

Přirozeným řádem je zřejmě myšleno množství vlastností daných předmětů a dalších věcí, které je zvýhodňují či nikoliv, což znamená, že vlivem změny způsobu života se tento přirozený řád mění dle našich potřeb, to znamená, že hodnoty věcí budou odlišné ve společnosti využívající ropu, která zajišťuje její chod, a ve společnosti v době páry. To je způsobeno tedy mírou poznatků a informací, které se dědí po předcích a neustále se inovují a rozšiřují a ovlivňují naše preference, a tedy i otázky hodnoty věcí.

Hodnoty jsou pojeny s emocemi, tedy pocitem, který nabudeme při kontaktu s věcí různé hodnoty. Na hodnotu věci tedy mají vliv naše potřeby, na základě, kterých ohodnocujeme věci, které zrovna potřebujeme či po nich toužíme s tím, že se různí druh potřeb, které rozdělujeme na obecnou potřebu, tématický okruh potřeb a konkrétní potřebu (Simmel,2011).

Emoce jsou tedy hybatelem našich potřeb a rozdělujeme je na základě možnosti naplnění. To znamená, že obecné potřeby mají spoustu možností jejich naplnění, tematický okruh potřeb je omezen na užší rozsah možností, například potřeby investice do drahých kovů – zlato, stříbro, palladium či platina, a konkrétní potřeba je víceméně jasná.

Na základě odlišných potřeb vykrystalizovala směna jedné věci za druhou, která pomohla utvořit rovnici hospodářská hodnota statku je rovna ceně statku. Spotřeba je výsledný cíl s pocitem uspokojení či naplnění. Na směně je založeno hospodářství a samotná směna funguje na střetu nabídky a poptávky a dle neoklasické ekonomie by se tím potvrdila skutečnost, že hodnota je totožná s křivkou ceny a zrcadlí její vývoj. Poptávka ztělesňuje žádanost a nabídka moment vzácnosti dle hospodářských hodnot. Tyto hodnoty bylo třeba nějak uchovat, a to dalo vzniknout penězům, které jsou tedy uchovatelem hodnot. Smyslem peněz je uchovávat hodnoty věcí, ale bez směnitelnosti, stability dané měny a možnosti dlouhodobě poskytovat úvěry v dané

měně by to nešlo a měna by nebyla důvěryhodná. Při poklesu či rapidnímu růstu cen u jednoho objektu je potíž s tím, jak určit, zda klesá hodnota peněz a roste cena všeho zboží či naopak. To dalo vzniknout termínu zvýšení cenové hladiny, který popisuje snižující hodnoty peněz. Na penězích se projeví veškeré jevy související s hospodářstvím, změnami ve jeho struktuře, kulturou či mezinárodními vztahy (Simmel,2011).

Jelikož každý jedinec má jiné tužby, tak směna nabízí možnost tyto tužby naplnit za peněžní částku, která by se teoreticky měla rovnat hodnotě dané věci či služby. Vzhledem k rozdílným prostředkům jednotlivců a subjektivní přidané hodnotě dané věci se ovšem ochota zaplatit různí. Toto lze snadno vypozorovat na aukcích, kdy navzdory značnému finančnímu zázemí se ochota zájemců o daný předmět odlišuje a velmi často se najde takový typ zájemce, který by byl schopen dát skoro či celé jmění za daný předmět, neboť v jeho očích je přidaná hodnota nevyčíslitelná. **Směna** a hospodářství, které funguje právě na celoplošném střetu nabídky s poptávkou v rámci geografického celku, lze díky vyčíslit právě díky penězům, které slouží jako uchovatel hodnoty statků na základě, kterého vyměřujeme a hodnotíme vše okolo nás. Funkčnost tohoto systému zajišťuje **směnitelnost**, neboť kdyby dané prostředky směny nikdo neakceptoval, pak by nebyly nic platné. Zároveň by dané peníze neměly smysl, kdyby byly rozkolísané a stabilita by se hledala jen těžko a ani jedna ze směnných stran by neměla přehled o aktuálním vývoji. Od toho se odvíjí možnost věřitelů poskytovat dlouhodobé úvěry, což můžeme si vzít za příklad hypoteční úvěr s fixní úrokovou sazbou, který by ztrácel na smysluplnosti v případě, kdy by dané peníze nebyly stabilizovány. Kdyby dané peníze byly destabilizovány, věřitelovi by daný úvěr postrádal smysluplnost, neboť místo očekávané profitability daného kontraktu by se dostavil do likvidace, neboť těchto uzavřených kontraktů bude mnoho a nebude schopen se domáhat povinností ostatních smluvních stran a sám nebude schopen plnit závazky. Zvýšení cenové hladiny neboli inflace se zjišťuje na základě změny ve spotřebním koši indexu spotřebitelských cen, které zahrnují ceny produktů spotřebované průměrnými domácnostmi a index se vypočítává na základě změny cen těchto produktů.

Před samotnými penězi funkce prostředníka zastávalo různé zboží jako například kožešiny, dobytek či nerostné suroviny a zejména měď či bronz. Prameny dokládají, že méně vzdělané kultury měli větší mince s menší počtem v oběhu. Naopak vzdělanější populace měli větší počet mincí, které byly znatelně menší, a tedy i lépe směnitelné. Obvykle právo na ražbu největších mincí měli nejvyšší mocnáři jako byl král či císař a práva na ražbu menších kusů byly většinou v rukách nižší vrstvy jako byla šlechta, bohatí obchodníci a další. Příkladem může

být ražba velkých mincí velkokrálem, ale satrapové[4] a nižší šlechta vždy razila o jednu čtvrtinu menší mince. Slované v 1. století našeho letopočtu stále využívali lněné plátno jako směnný prostředek, což bylo ekvivalentem 100 slepic či pšenici pro 10 mužů na 1 měsíc. V primitivnějších společnostech se zlatá měna používala jen při směně vzácnějšího a cennějšího zboží, nikoliv zboží každodenní potřeby a na cenu, potažmo hodnotu, se pohlíželo z pohledu míry užitečnosti a výše peněz byla tedy ekvivalentem užitečnosti dané věci, tzn. že palivové dřevo vysoké kvality bude stát více než dřevo ve špatném stavu, které má užitečnost o řád menší. Volby směny peněz jsou takřka neomezené, neboť vše lze pořídit za nějakou sumu a zároveň peníze můžeme ihned, ale nemusíme, protože v budoucnu pro danou sumu taktéž nalezneme využití. Ceny statků jsou citlivé na extrémy a velmi je ovlivňují, ale zejména statky, které můžou být použity nyní, ale ne později či alternativa s nemožností okamžitého uplatnění, ale později ano, jsou velice citlivé na výkyvy. Příkladem můžou být ryby a jejich směna za kožešiny na zimní období, kdy cena ryb vzroste a ceny kožešin klesne, protože se odloží jejich použití a daná prodleva k použití dává prostor k poškození, ztráty či znehodnocení kožešin. Ryby ale poklesnou na ceně, protože zítra by se zkazily, a tak vzroste cena kožešiny, neboť je to záruka odsunutelného užitku (Simmel,2011).

Dle Skalického a Stroukala existují i prameny dokazujíc o kakaovém bobu zastávající funkci prostředníka směny, takže podoba zboží, které zastávalo funkci **prostředníka směny**, se uzpůsobila daným podnebným podmínkám a lokálnímu georeliéfu. Je zajímavé, že Slované používali na začátku nového tisíciletí specifické zboží, které bylo ekvivalentem směnného prostředku, neboť souběžně existovala měna mocné říše lokalizovaná na Apeninském poloostrově, tedy můžeme uvažovat o lněném plátnu jako o **komunitních penězích** a pro mezinárodní obchod, respektive obchod s Římskou říší se využíval tamní sestercius, který v tehdejším známém světě brán jako světová měna, neboť byla uplatnitelná v celé severní Africe, Blízkém východu, dnešní západní, jižní a jihovýchodní státy Evropy. Jsem toho názoru, že čím vyšší blahobyt společnosti či domácnosti, tím více se vytrácí důležitost pohledu míry užitečnosti při směně a je doplněn jiným úhlem pohledu. Příklad ohledně citlivosti ceny na výkyvy z pohledu užitečnosti reflektuje problematiku jejího stanovení.

Čím více v sobě nějaký objekt, používaný jako směnný prostředek, sjednocuje oba momenty stupňující hodnotu, tím více má peněžní kvality. Svoboda peněz k využití je stejně velká ve vztahu k časovým momentům, v nichž se vydávají, jako k předmětům, za něž se vydávají. Kupec a prodejce, přesněji zákazník a bankéř, kdy pro bankéře jsou peníze pouze

[4] Správce daného území ve jménu panovníka.

zbožím, které je třeba řádně předat zákazníkovi, ale pro klienta jsou to ty peníze, které může, ale nemusí použít a má nespočet voleb k využití těchto prostředků. Bankéř ale nemá jinou volbu než přistupovat k penězům jako ke **zboží**. Navzdory všem možnostem v souvislosti s vlastnictvím peněz a nespočet možností jejich útraty v globálním světě, peníze představují spojující článek, který ale zároveň nás činí zranitelnými a závislými na aktivitě druhých včetně vlivných faktorů jako jsou mezinárodní vztahy a dále. Význam peněz dokládá i možnost v případě spáchání trestného činu prostřednictvím sankce v podobě kauce, což je suma peněz, která se ale neočekává u obžalovaného kvůli své výši, ale po jejím složení je obžalovaný zproštěn obvinění a dalších soudních procesů navazujících na obžalobu ze spáchání daného trestného činu s tím, že výše kauce se odvíjí v souvislosti na závažnosti spáchaného trestného činu. Dříve za vraždu obyčejného občana dostal stejně situovaný viník pokutu, ale v případě, že by se zločin týkal lépe situovaných jedinců, například šlechticů, tak se tato částka násobila na základě důležitosti a váženosti dané osoby, která byla zabita (Simmel,2011).

Neboli čím směnitelnější daná měna či prostředek je, tím více je žádaný a peněžní kvalitou rozumím **důvěryhodnost** směnného prostředku, která pramení ze **stability**. Je nutné rozdělovat odlišné pohledy, kdy pro část obyvatelstva jsou peníze jen a pouze prostředkem, ale pro některé podnikající osoby či právnické osoby ve finančním segmentu, což jsou banky, investiční společnosti a další, vnímají peníze jako zboží. Peníze jsou všeobecným ekvivalentem hodnoty (Simmel,1997). Jejich důležitost je adekvátní, neboť je na nich postaveno hospodářství, které zahrnuje regionální směnu fungující právě na penězích, které vyjadřují hodnotu veškerých statků.

Rakouská škola ekonomie k penězům přistupuje jako k decentralizovanému statku, kde silnější vítězí v tom smyslu, že každá obchodní banka by emitovala svou vlastní měnu, která bude soupeřit s konkurencí a sami spotřebitelé si zvolí. Nepočítá tedy s existencí centrální bankovní autority coby nástroj státu, a naopak označuje intervence centrální bankovní instituce jako škodlivé vůči hospodářství. Cílem je tedy dostat peníze z rukou monopolu centrální banky, tedy státu, a rozdělit jej na několik měn emitovanými jednotlivými bankami (Hanusová,2017).

Svět kryptoměn se rakouskou školou výrazně inspiroval nejen v **decentralizaci**, ale i v konkurenci, kdy výsadní postavení si stále drží s velkým náskokem Bitcoin, ale ostatní měny mezi soupeří právě inovacemi a odlišnostmi, které je od sebe dělí a které cílí na jinou skupinu obyvatel. *„Rakouská škola tvrdí, že jakýkoli zásah do přirozeného plynutí hospodářského cyklu ve výsledku zvyšuje nestabilitu hospodářství..“ (Investičníweb.cz,2014).*

Ammous demonstruje, že představitelé rakouské školy jako Menger, Mises a Rothbard vnímají mezi klasické **atributy peněz** škálovatelnost, prodejnost a stabilitu (Dvořák, 2019). Což je o poznání menší počet atributů, než uvádějí ostatní zdroje s tím, že prodejností se zřejmě myslí poptávka po dané měně, respektive směnitelnost, neboť je třeba mít na paměti, že v teorii rakouské školy se vyskytuje vícero měn vydávaných obchodními bankami, které mezi sebou soupeří o spotřebitele a v případě nulové prodejnosti tato měna spolu s bankou zaniknou. Dvořák taktéž uvádí, že dle Ammouse je dle těchto atributů deklarujících vlastnosti směnných prostředků, že i „*..bitcoin je vynikající formou peněz šetřících hodnotu, protože je na rozdíl od veškerého vzácného zboží (s výjimkou lidského času) „přísně" vzácný a nejen relativně vzácný."* (Dvořák, 2019). Toto tvrzení je podezřelé, neboť Ammous sám shrnuje definici peněz dle rakouské školy, ale následně je sám porušuje, neboť Bitcoin je cokoliv, jen ne stabilní formou peněz.

TU v Liberci definuje **peníze** jako měřítko hodnoty, značení a název měny a dělitelnosti. Skalický a Stroukal uvádějí, že předchůdci peněz ve formě kovu či bankovek byly kakaové boby, kožešiny, plátno, dobytek a další. Většina zmiňovaných statků se váže k barterovému směnnému systému a k atributům, potřebných k plnění peněžních funkcí, nedosahují. Následně se do čela dostal vzácný kov, který byl následně zpracován do formy mincí mincovnou, která podléhala vladaři a zde se rodil monopol vladaře, respektive státu, na měnu a její kontrolu. O několik staletí později přišla na řadu papírová podoba peněz, která nejdříve byla a posléze nebyla směnitelná za vzácný kov, kdy se většinou jednalo o zlato a výjimky tvořilo stříbro. V důsledku hospodářské ho růstu a vývoje bylo třeba papírovou měnovou soustavu spolu s mincemi doplnit o elektronické peníze, které jsou ve formě transakčních dat. Platební kreditní či debetní karty jsou nástrojem, jak okamžitě tyto elektronické peníze využít u prodejce z bankovního účtu, na který jsou dané karty navázány. Peníze obsluhují trh svými atributy, které představují s tím, že někdo je vydává, kontroluje jejich oběh či případné padělky a jako směnný prostředek je všudypřítomný skoro u každé směnné interakce.

1.2. Měnová soustava a její historie, devizový trh a světové peníze

Po vytvoření peněz, které byly stabilní, směnitelné a poskytovaly možnost dlouhodobých úvěrů, bylo zapotřebí vytvořit infrastrukturu pro jejich emitenci[5], kontrolu oběhu, výběr daní a další. Jinými slovy infrastrukturu pro peněžní oběh.

Zprostředkovatelem směny se staly drahé kovy, které nahradily všechny předchůdce díky svým unikátním rysům jako je směnitelnost, dělitelnost a důvěryhodnost a další. Peněžní oběh funguje jako soustava platebních prostředků v určitém objemu a struktuře. **Peněžní soustava** legislativně spravována a využívána na území daného státu se označuje jako **měna**. Součástí soustavy je stanovení základní peněžní jednotky v konkrétním regionu jako měřítko hodnoty, značení a název měny a dělitelnosti. Celý tento soubor stanovení a definice měny se nazývá nominální struktura. Dále se stanovuje forma dané měny a následně způsob vydávání a stahování peněz z oběhu se vznikem příslušných institucí, které budou zodpovědné za průběh těchto funkcí. Je třeba vyřešit i vztah peněžní jednotky územního celku vůči ostatním měnám a v neposlední řadě taktéž definovat ekonomické zásady a pravomoci uplatňované institucemi regulující peněžní oběh včetně stanovení ochranných známek měny, způsoby směny uvnitř domácího státu či mimo něj (Technická univerzita v Liberci).

Peněžní soustavou můžeme rozumět jako základní infrastrukturu pro konkrétní peněžní prostředky, které jsou regulovány pověřenými finančními institucemi zodpovídajícími za kontrolu oběhu včetně ochrany dané měny dostupnými kroky a nástroji. Nejdůležitějším aspektem ohledně mezinárodního obchodu je vztah měny domácí k ostatním zahraničním měnám.

Devizová transakce je nákup či prodej národních peněz za měnu jinou. Tyto transakce se realizují na devizovém trhu, kde se směňují mezinárodní měny za měnu odlišnou. Každá měna má svůj vlastní **devizový trh**, který je ovlivněn několika faktory, a to například mezinárodními vztahy, hospodářskou situací a další. To znamená, že devizový trh dané měny je dostupný kdekoliv na světě, protože finanční centra jsou spojeny v jediný trh. Devizový trh má tři funkce: realizace převodu kupní síly, zajištění úvěru pro zahraniční obchod a vytvoření nástrojů pro zajištění proti devizovým rizikům. Nejdůležitější funkcí je převod kupní síly, který se realizuje směnou peněžních prostředků jedné měny do měny druhé (Kindleberger, 1978).

[5] Výdej oběživa, tj. mincí a bankovek, centrální bankou.

Jinými slovy devizový trh udává za jaký „čistý“ kurz je možno si zakoupit valuty[6] a deviza[7] měny jiné než té národní, s níž uskutečňujeme každodenní směny a jsme s danými penězi stále v kontaktu. „Čistý“ kurzem rozuměno očištěný od marže či případných poplatků za zprostředkování směny peněžních prostředků třetí stranou.

Ještě před uskutečněním transferu se provádí tzv. clearingový proces[8]. Neboť vývozcům dané země vznikají v zahraničí pohledávky a dovozci této země mají uskutečnit platby do zahraničí. Zboží se pohybuje mezi zeměmi, ale platby se realizují uvnitř zemí prostřednictvím clearingového mechanismu s výjimkou vypořádání vzniklých zůstatků. Jinými slovy daná země platí za svůj dovoz vývozem. Vývozci v této zemi obdrží platbu v domácí měně od dovozců konkrétní země, kteří takto platí domácí měnou za své nákupy v cizině. Na devizovém trhu se clearing realizuje pro platební instrumenty při takřka nekonečném počtu různých položek obsažených v mezinárodním obchodu s tím, že značné částky na obou platebních stranách se vzájemně kryjí a k vypořádání zbývají pouze malé zůstatky. V realitě se spíše vyskytuje clearing mezi vícero stranami, což umožňuje, aby země uskutečnily směny zboží, jejichž sjednání by bylo příliš komplikované bez využití mezinárodních platebních prostředků v cizí měně. Tyto mnohostranné platby se obvykle realizují v některé z hlavních světových měn, jež je nosným pilířem v oblasti mezinárodního platebního styku. V případě odlišné velikosti pohledávek dané země, vznikajících ze zahraničních transakcí liší od jejích plateb, se rozdíl nazývá zůstatkem, který vznikl přebytkem poptávky nebo nabídky deviz (národní měny). Tento přebytek může být vyřešen prostřednictvím odstranění skrze spekulanty, pohyby krátkodobého kapitálu, měnovými institucemi či změna ceny (Kindleberger, 1978).

Clearing tedy zjednodušuje uskutečnění mezinárodního obchodu skrze toto vyrovnání vývozu a dovozu. Malý prostor pro různé vlivy vzniká díky přebytkům poptávky či nabídky jedné z obchodujících stran, které se vyřeší výše zmiňovanými aktéry či změnami.

Pro devizový kurs je určující střet poptávky a nabídky po konkrétních národních penězích v rámci určitých mezí daných charakterem devizového systému, do něhož daná země patří, či příslušnost do určité hospodářské organizace anebo podepsání obchodních dohod se závazky, mezi které patří určité devizové omezení. Je několik druhů kursů a prvním druhem je pružný devizový kurs bez zásahu měnových institucí. Cena deviz je podmíněna poptávkou a nabídkou deviz, jež jsou určeny domácími a zahraničními cenami zboží a služeb, informační

[6] Hotovostní forma zahraničních měn.
[7] Bezhotovostní forma zahraničních měn.
[8] Spočívá v tom, že země mezi sebou obchodují v různých měnách zastupující vývoz a dovoz

transparentnosti o příležitostech k obchodu doma i v zahraničí, mezinárodními kapitálovými pohyby, činnost spekulantů v případě budoucího vývoje devizového kursu a dále. Dle některých autorit tento trh bude stabilní, neboť spekulace krátkodobě působí proti vzestupu na trhu, kdy při staré ceně poptávka převyšuje nabídku a při opačných podmínkách působí zase proti poklesu. Dalším druhem systému je pohyb kursu ohraničený. Při zlatém standardu jsou limity dány náklady převodu zlata z jednoho trhu na druhý, přičemž náklady zahrnují dopravu, pojištění a poplatky za manipulaci. Devizový kurs může být ovlivněn v případě potřeby intervencemi ze strany měnových institucí sledující určitý cíl. Pružný devizový kurs bez vládních zásahů je vyrovnáván cenovými změnami. Spekulace u okrajů limitů devizového kursu může taktéž vyrovnat trh anebo příslušné instituce mohou svými nákupy dorovnat přebytek nabídky nebo uspokojit přebytek uspokojit skrze různé nástroje k získání deviz (Kindleberger, 1978).

Kurs domácí měny je tedy ovlivněn zejména tím, zda daná měna je kryta drahým kovem, ať už zlatem či stříbrem. Anebo zda je návaznost zprostředkována jinou stabilní měnou, která má renomé světové měny, která může ale nemusí být i částečně kryta drahým kovem. To ovlivní hranice kursu, které buď existují v podobě intervalového rozpětí s tím, že měnové instituce mohou kdykoliv zasáhnout. **Pružný devizový kurs** tyto hranice nemá a měl by se obejít bez zásahu měnových institucí. Kindleberger taktéž uvádí, že devizový kurs odráží veškeré vnější vlivy, kterými je myšleno dění ve světě v politické či hospodářské rovině.

Peníze jsou dle Technické univerzity v Liberci **uchovatelem hodnot**, **měřítkem hodnot**, **prostředkem směny** a **prostředek úhrady odložených plateb**, čímž se myslí úvěry a dluhy. Světové peníze by potom tyto funkce měli zastávat v globálním měřítku. Nejvíce se tomuto pojmu dle Kindlebergera přibližuje **americký dolar**, který má mnohem širší trh a zároveň působnost než ostatní národní měny, což zajišťuje levné transakční náklady a mnohonásobně větší obchodní příležitosti a dolar se tak stává součástí mnoha transakcí, na nichž se přímo nepodílejí obyvatelé USA. Patria.cz na Kurzy.cz potvrzuje, že navzdory snižujícímu se podílu dolarových světových devizových rezerv se americký dolar používá v 88 % veškerých měnových obchodů a představuje zhruba 62 % devizových rezerv. Proč zrovna americký dolar?

Spojené království a její měna, libra, dominovali světovému trhu nejen díky své geopolitické rozsáhlosti, ale i robustností svého hospodářství. Navzdory 1. světové válce, kdy většina zemí se vzdala zlatého standardu svých měn ve prospěch financování válečného konfliktu, Velká Británie si zlatý standard udržela, ale vlivem toho, že Spojené království bylo ve válce již od samotného počátku, vyvolalo to tendence mezi ostatními zeměmi nakupovat a

půjčovat si od ekonomiky Spojených států, která vstoupila do války až v roce 1917 a stav ekonomiky byl v neporovnatelném stavu s válečnými evropskými ekonomikami. Podobný scénář se opakoval v průběhu a po druhé světové válce. Díky konfliktu se do USA dostala většina světových rezerv zlata, neboť to sloužilo jako úhrada za poskytnuté zboží a dalšího materiálu. Následně se uskutečnila dohoda vyspělých států, tzv. **brettonwoodský měnový systém**, o tom, který vázal národní měny na dolar v rámci pevných směnných kurzů, který jako jediný byl stále plně kryt čerstvě nabytým rezervám zlata v poměru 35 USD za 1 trojskou unci zlata (InvestičníWeb.cz, 2014).

Nezávisle na velikosti britského impéria se libra dostala chtě nechtě válkou do problémů v podobě velkých výdajů na vedení boje ve čtyřletém světovém konfliktu. Oproti USA Spojené království utrpělo materiální i lidské škody mnohonásobně vyšší ztráty v první světovém konfliktu a druhá světová válka stav ekonomiky a financí také nezlepšil. Je zajímavé, že navzdory všemu, tak orientace na zlato ve všeobecné rovině nepolevila a kurz byla daná země ochotna fixovat na cizí měnu, která byla podmíněna zlatým krytím. Mimo rámec této práce by bylo zajímavé zjistit, čím zlato lidstvo tak učarovalo, zda to byly fyzikální vlastnosti tohoto vzácného prvku anebo snad atypická barva, která budí náš neutuchající zájem o tento kov a vše s ním spojené. Spojené státy se posléze staly výsadním věřitelem po první světové válce a tamní ekonomika díky tomuto zájmu rostla do doby Velké deprese koncem 20. let 20. století.

V období, kdy spěla ke svému konci světová válka, se dolar stal přebytkovým zbožím a přebytek se vyřešil nákupem amerických dluhopisů. Snaha o zjištění reálné směnitelnosti amerického dolaru za zlato ohledně dluhového vypořádání vedlo k výpovědi brettonwoodského měnového systému ze strany Spojených států v 70. letech minulého století. Skončily tedy pevné kurzy měn navázaných na dolar a začala doba pohyblivých kurzů. Následně v rámci obav z inflace a ochrany ekonomiky USA se podepsala nová Smithsoniánská dohoda, která měla zpět zafixovat měny na dolar, ale její životnost byla necelá dva roky. Navzdory tomuto faktoru a dalším krizím jako třeba v roce 2008 s toxickými aktivy amerických bank se nic nezměnilo a americký dolar je stále měna (InvestičníWeb.cz, 2014).

„Při běžné arbitráži bude obchodník s devizami současně přijímat i opouštět jednu měnu. To je arbitráž, jež udržuje jednotnost trhu dané měny po celém světě.“ (Kindleberger, 1978). „Arbitražéři nejsou spekulanti. S výjimkou několika momentů nemají žádnou otevřenou pozici v zahraniční měně. Zisk realizují z nákupu a prodeje cizích měn, s touž měnou jako začali. Arbitráž mezi dvěma místy je taková, při níž arbitražér nachází rozpětí v ceně jeho vlastní měny na dvou trzích, zpravidla na vlastním trhu a na některém v zahraničí.“ (Kindleberger, 1978).

Jinými slovy rozdílem mezi arbitražérem a spekulantem je ten, že arbitražér skončí s počáteční měnou obchodu a spekulant končí obchod s tou, která je v dané chvíli nejvýhodnější dle aktuálního kurzu. **Spekulant** je orientován na krátkodobé období a vše s tím spojené včetně zisku, neboť nákupy či prodeje realizuje na základě aktuálních změn cen na trhu daných cenných papírů, komodit a dalších, na kterých spekulant profituje (FXstreet.cz). *„**Arbitráž** je mechanismus, jenž činí ze dvou trhů fyzicky oddělených jediný trh v ekonomickém smyslu. Jeden trh je definován jako místo, kde kupující a prodávající obchodují s daným zbožím za totožnou cenu. Kde trvale existuje shodná cena pro totéž zboží, tam je jeden trh. Kde existují dva trhy a kde jsou náklady nákupu na jednom a prodeje na druhém malé, arbitráž povede v podstatě k jedné ceně a jednomu trhu. Tam, kde se arbitráž z toho či onoho důvodu nemůže realizovat – pro nedostatek znalostí faktů o ostatních cenách, pro neadekvátní spojení nebo v důsledku zákazu – ceny se budou mezi trhy lišit. V posledním případě, když je arbitráž zakázána, budou velké diference v cenách stimulovat skryté obchodování, neboť zisky při postupu proti zákonu jsou velké. “ (Kindleberger, 1978).* Jinými slovy arbitráž je mechanismus globalizující světový trh, který je transparentní pro všechny aktéry za předpokladu, že všichni aktéři na trhu nebudou svázáni informační asymetrií, zákazy, které následně cenu deformují, případně se na uzavřeném trhu cena odlišuje od té světové, což může poškozovat danou národní měnu. Spekulace ve velkém měřítku mohou kromě uměle našponované ceny daného statku, včetně národních měn, mít i dalekosáhlý dopad na obchodovatelnou měnu, kdy masivním prodejům národní měny utrpí i měna samotná a její cena se tomuto masovému prodeji negativně přizpůsobí.

Z původní pozice světového věřitele se USA stalo zemí, která pomalu ale jistě se stává světovým dlužníkem. Otázkou je, co s americkým dolarem udělá koronavirová pandemie a zda se opravdu nejedná o důvěryhodnostní setrvačnost ze strany světových aktérů na poli mezinárodního obchodu či nikoliv. Anebo by čínský juan mohl převzít otěže světové měny navzdory tamnímu socialisticko-kapitalistickému státnímu zřízení?

V dřívějších dobách zastávala peněžní prostředky různorodá skupina věcí jako byl vzácný kov, stříbro či zlato, slitcích či různých předmětech, které byly zmíněny v předešlých kapitolách. Plnily sice částečně funkci peněz, které nahradily barterův obchodní systém[9], ale postrádali většinu funkcí, které peníze mají splňovat, a to bezproblémovou směnitelnost, případně dělitelnost peněžních prostředků, důvěryhodnost a další. Dle Němečka bylo rozhodující pro

[9] Systém, kdy směna sestávala z výměny zboží za zboží bez existence peněz.

vyjádření ekvivalentní hodnoty váhové množství daný prostředků a jejich obsah čistého kovu ve slitku.

První významnou formou peněžních prostředků byly **mince**, které byly raženy mincovnami ze stříbra či zlata, které disponovali rovností mezi nominální a vnitřní hodnotou. Množství mincí v oběhu se upravovalo dle aktuálních potřeb trhu. V případě potřeby se část mincí přetaví do podoby stříbrného či zlatého pokladu, a naopak v situaci, kdy je nedostatek mincí v oběhu, se část pokladu využije k ražení mincí a jejich následné emitenci. Takto se uchovávala rovnováha na trhu, kdy mince představovaly nejen směnný prostředek, ale i dočasného uchovatele hodnoty a zároveň představitel bohatství a jmění. S přibývající potřebou většího množství mincí v oběhu rostla současně potřeba i kontroly, a tak se právo razit mince stalo výsadní pro stát (Technická univerzita v Liberci).

Prezentované množství tedy odpovídalo reálné hodnotě mince. S rostoucím počtem obyvatel rostl i počet uživatelů peněžních prostředků a současně i poptávka rostla a tím se směna pro státní aparát stal nejpřehlednější vzhledem k existenci vícero nestátních mincoven, které zásobovaly trh všelijakými druhy mincí různé kvality.

Dle toho, jaký kov představoval peníze a plnil jejich funkci, nazýváme stříbrný či zlatý standardem neboli monometalismus. V případě, že funkci zastávaly oba kovy, pak se tomu říká bimetalismus, neboť oba kovy byly využity pro tvorbu oběžných mincí a byl dán pevný množstevní poměr mezi jednotlivými kovy (Technická univerzita v Liberci). Tato **metalická měnová soustava** přežila v pozměněné formě dodnes a popularita mincí rozhodně přetrvá a je velká pravděpodobnost, že tu s námi bude i v budoucnu.

Úvěrová měnová soustava umožňuje, že **bankovka** je směnkou emitovanou bankou na určitou peněžní částku se splatností na požádání peněžním kovem. Jinými slovy bezprostřední směnitelnost bankovek za **peněžní kov**. Přechod na oběh bankovek umožnil přizpůsobení aktuální situaci na peněžním trhu bez nutnosti vázání se na růstu těžby vzácných kovů (Bankovnictví-Finance.studentské.eu.).

Užíváním směnek se ulevilo transakčním nákladům a obtížím se samotnou transakcí se vzácným kovem, zejména u velkoobjemových transakcí, které byly logisticky a finančně náročné.

Podhoubím pro vznik úvěrové měnové soustavy byla zpoplatněná služba úschovny (nejen) peněžních mincí ze strany zlatníků, kteří zákazníkovi vystavili potvrzovací listinu, která umožňovala klientovi tuto zástavu kdykoliv vybrat zpět. Dalším vývojem byla emise státovek,

což byl dlužní úpis emitovaný státem, v němž se zavazoval k jeho splacení peněžním kovem. Státovka vznikla ve středověku, kdy státy tímto způsobem sháněly investory na financování válečných konfliktů a jinou neproduktivní spotřebu. Státovky měly oběh podmíněný politickou a právní mocí státu s fixním kursem, který udával stát s tím, že bylo vynuceno přijímání státovek při směnném styku za zboží i služby. Tato možnost se ale zvrhla do nekontrolovatelného tištění nových státovek, což vedlo k zvýšení cenové hladiny, neboť stát měl zájem na zvyšování své kupní síly, ale na splácení dluhu již ne. Dluhová tíseň státu se řešila pomocí měnové reformy, která vyměnila staré státovky za nové s jiným kursem a více zatížila poddané a místní obyvatelstvo novou úrovní zdanění, a nakonec se nedodržovaly ani státní záruky pro vyplácení státovek za měnový kov (Technická univerzita v Liberci).

Středověké obyvatelstvo trpělo nejen častými mezinárodními a vnitrostátními konflikty, morovými epidemiemi, bezprávím, ale i neznalostí státního aparátu ohledně důsledků svého jednání v oblasti správy financí a narážím tím na emitování nových státních směnek, nicméně bez této zkušenosti by trpěli generace pozdější či novodobé nebýt strádání tehdejší společnosti. Nesplácení svých závazků si myslím, že bylo vědomé a po vzoru budoucího francouzského vladaře Ludvíka XIV. se řídili krédem: *Po nás ať přijde potopa.* Což bychom mohli přirovnat k dnešnímu nuznému podílu dluhové služby v rámci veřejných financí nejen v České republice, ve které se splácí státní dluh věřitelům.

Bankovka je ve své podstatě směnkou emitovanou bankou na určitou peněžní částku splatnou na vyžádání peněžním kovem. Pokud se na požádání vymění bankovka za oběžní plnohodnotné kovové mince v odpovídající výši, pak se jedná zlaté či stříbrné krytí bankovek. Oproti předchůdcům měly bankovky větší důvěryhodnost, neboť byla emitována bankou. Emise jednotlivých bankovek bankou či tou centrální se zohledňuje dle aktuální ekonomické situace s tím, aby se urychlil případný hospodářský vývoj daného územního celku. Vzhledem k tomu, že počet bankovek s jejich výši převyšoval reálnou směnitelnost za peněžní kov, tak se tato směnitelnost omezovala a následně úplně zrušena, a to i na mezinárodní úrovni (Technická univerzita v Liberci).

Bankovka tedy dříve v době směnitelnosti za peněžní kov představovala řekněme token či voucher na počet mincí v hodnotě konkrétní bankovky. Důvěryhodnost bankovky byla způsobená zázemím banky, která bankovky emitovali, a nikoliv podnikající osobou, který mohla kdykoliv svou činnost skončit a směnka tak ztrácela stranu, která buď věřila či dlužila. Následně se nové emise bankovek zajišťovali pouze skrze centrální banku, která unifikovala bankovky a ostatní oběživo spolu s příslušnými intervencemi, což ostatně dokládá TU

v Liberci, a v kooperaci s vládou reaguje na hospodářský vývoj země příslušnými reakcemi. Od dob bank vznikl spolu s nimi i bankovní účet, který měl daný klient k dispozici ohledně výběrů dané hotovosti z depozitu daného účtu.

Právě bankovní účty byly dalším krokem k evoluci směnné interakce, neboť byla zde možnost bezhotovostního platebního styku skrze bankovní převody ze zůstatků na bankovních účtech spolu s účetním přepisem a úpravou zůstatku. Takové peníze se nazývají depozitními penězi a umožňují přímou platbu z účtu na účet pomocí zmíněného účetního přepisu s dokladem o provedení převodu na jiný účet. Následně se řada možností plynoucích z vlastnictví bankovního účtu o šek, který umožňuje vypsanému držiteli vyplatit danou částku, která se strhne z bankovního účtu osoby, která vypsala daný šek. Také se upravilo poskytování úvěru přímou cestou bez zprostředkování skrze směnku (Technická univerzita v Liberci).

Papírová měnová soustava je využívána dodnes, akorát je z velké části digitalizována a většina transakcí je realizována v digitálním bankovním prostředí. Každý máme prostřednictvím internetového bankovnictví (za předpokladu, že je dostupné připojení k internetu), kde spravujeme své účty a disponibilní zůstatky svých prostředků, které v dřívějších dobách měli fyzického reprezentanta, ale nyní to jsou pouze digitální a transakční data, které jsou zálohována a zaznamenávána samotnými bankami, ale zároveň centrální národní bankou, případně nadstavbou centrální banky. Navzdory tendenci obecné digitalizace společnosti spolu s užíváním transakcí v digitálním prostředí hotovostní platby mají stále oblibu u veřejnosti a zejména u transakcí za každodenní zboží v maloobjemových částkách dle Ducháčka na webových stránkách České národní banky. Ducháček dále uvádí, že v důsledku koronavirové pandemie se hodnota oběžných mincí a bankovek vzrostla na historické maximum, které činí 687,8 mld. Kč, a dále popisuje, že obliba hotovosti je v důsledku rychlosti transakce, která je okamžitá a anonymní. V případě bankovního převodu je okamžité uskutečnění pouze v případě, že účet, na níž jsou posílané prostředky, se vyskytuje u téže banky jako výchozí účet. V případě odlišné bankovní příslušnosti je čekací doba mezi 2 až 4 pracovními dny pro uskutečnění mezibankovní transakce. Debetní či kreditní karty mají stejnou výhodu jako hotovostní peníze, ale je nutné být navázán na **internetové bankovnictví**.

Oběh řízený centrální bankou má i další důvody mezi které patří kontrola a dohled státu, respektive centrální banky, která spolu vytvořením bankovek a mincí dané národní měny současně i ochraňuje prostřednictvím **ochranných známek** dané bankovky či mince. Ochranné známky typu jako konkrétní druh papíru, styl tisku, unikátní znaky u bankovky či u mince daným poměrem kovů, ze kterých jsou dané mince raženy. Neboť případné padělky mincí či

bankovek mohou infikovat směnnou interakci nedůvěryhodností, která se vztahuje k měně jako takové a informace o padělkách této měny měnu poškodí na poli mezinárodního obchodu, ale i na vnitřním trhu, kdy samotní občané daného územního celku nebudou důvěřovat vlastní národní měně a budou shromažďovat valuty jiných národních měn, případně shromažďovat stříbrné či zlaté rezervy, ke kterým se v krizích lidé obrací. Příkladem nedůvěry občanů vůči vlastní měně může být hyperinflace ve Výmarské republice či měnová reforma v Československu v padesátých letech minulého století.

Kryptoměny mají většinou svou izolovanou decentralizovanou soustavu, která běží tak jak je naprogramována a dle modifikací, které přinášejí vývojáři starající se o ekosystém příslušné kryptoměny. **Kryptoměnová soustava** podléhá také svým vlastním vývojem. Příkladem může být neutuchající vývoj prostřednictvím modifikací a vylepšování verzí platforem, na kterých jednotlivé kryptoměny stojí. Samotná kryptoměna sice až na výjimky nedisponuje zaštiťující institucí, která by oběh mincí kontrolovala, ale bez ochrany transakce nebyly ponechány. Digitální mince nemají ochranu jako u fyzických směnných prostředků jako bankovky či kovové mince, za to ale je chráněná digitálními mincemi uskutečněná transakce prostřednictvím šifrování.

Objem mincí je nastavený v systému konkrétní informace s tím, že takto nastavený systém má deflační tendence, ale naopak systémy, kde není daný konečný počet mincí a je možno kdykoliv doemitovat další počet mincí, podléhají inflačním vlivům. Jako klasické měny podléhají (a možná i více) spekulativním obchodům, které ovlivňují cenu dané kryptoměny. Atraktivita pro kryptoměnové spekulanty zřejmě spočívá v její historicky nevídané kolísavosti, kdy není výjimkou, že denní kolísavost je v řádech procent až několik desítek procent a dává tak prostor pro krátkodobý profit. Na druhou stranu existuje úzká skupina lidí, zejména z oblasti informačních technologií, kteří po celou cestu kryptoměn trpělivě drží daná aktiva v podobě kryptoměn a pokud drží od samého počátku, pak jde o rekordní profit téměř z ničeho (cca 1 až 50 USD za 1 BTC a dnes cca 20 000 USD za 1 BTC).

Takových lidí, zvaných holders či v kryptoměnovém žargonu hodleři[10], je ale velmi málo a nedokáží zklidnit křivku volatility vzhledem k nepoměru spekulantů, kteří se snaží na této volatilitě zbohatnout. Tohle je asi aspekt, které mnohé přivádí k připodobňování Bitcoinu ke zlatu. Zároveň křivka je velmi citlivá na znovuobjevení ztracených mincí u účtů spravovaných třetí stranou. Informace o znovuobjevení „ztracených“ mincí a jejich následný prodej

[10] Ustálený pojem z anglického originálu „hold“ = neprodávat, který vznikl překliknutím.

v dostatečném objemu dokáže znatelně zahýbat s cenou kryptoměn a u takovýchto případů následoval strmý pád i o několik desítek procent po několik dní, což uvádí i Skalický se Stroukalem. A zároveň tento fakt podobnost se vzácnými kovy vyvrací, neboť chybí zde stabilita. Tento spekulativní aspekt zároveň odrazuje od většího přílivu běžných uživatelů, kteří by kryptoměny aktivně využívali ke směně a stabilizovali tak jejich kolísavost dle Skalického a Stroukala, ale místo toho to je ráj investorů s nejasným koncem.

Vývoj kryptoměn nabírá nečekaný směr, který se začíná velmi podobat s měnovou soustavu FIAT[11] měn, neboť se vytvářejí první deriváty kryptoměnové, které je možno směnit za kryptoměny. Taktéž se experimentuje s poskytováním kryptoměnových úvěrů, které ale nefungují jako úvěry v moderních peněžních soustavách, ale prostřednictvím tzv. **smart kontraktů**, kde se jasně stanovují protistrany či zúčastněné strany, neboť zde není odpovědná centrální autorita.

[11] Národní měny s centralizovanou měnovou soustavou.

1.3. Brettonwoodský měnový systém a společná měna

Brettonwoodský měnový systém měl mimo vzniku **Mezinárodního měnového fondu** (dále MMF), ze kterého by čerpaly v případě trvalých deficitů veřejných financí členské země, také navázat významné národní měny na dolar. MMF je bazén rezerv, ze kterých je možné financovat krátkodobé a přechodné deficity jednotlivých zemí a zároveň do kterého členské státy sami přispívají. Vznik v roce 1944 byl zapříčiněn špatnými předchozími lety, kdy vyspělé země vyčerpaly své rezervy a měli několik let trvalé deficity veřejného rozpočtu. Systém počítá s tím, že se sdruží bazén rezerv ústředních bank a národních měn, jež jsou k dispozici členům za určitých podmínek k financování deficitů, které budou dle předpokladu napraveny automaticky nebo v průběhu času s pomocí uplatněných hospodářských rozhodnutí. Zdroje fondu však nemohly být použity k financování trvalých deficitů, neboť by životaschopnost tohoto fondu byla velmi krátká, to znamená, že využití prostředků je rozhodováno po pečlivém přezkoumání požadavku a historie vývoje daného územního celku (Kindleberger, 1978).

Válkou zničené či poznamenané země jakoukoliv mírou s absencí vlastní kryté měny se schýlily k jediné měně kryté zlatem, a to americkým dolarem, o kterém píši v předešlé podkapitole. Snaha hledat jistotu v pevných kurzech vůči dolaru, který evokoval bezpečný přístav pro ostatní národní měny, je pochopitelná. Z obecného hlediska je příjemnější vědět, že kurz je pevný v tom smyslu, že má nějaké rozpětí, respektive hranice, kursu, kam až může klesnout či vzrůst, ale zároveň to neohrozí stálost hospodářského vývoje či měnové souznění.

Každé členské zemi je přidělena kvóta příspěvku, který je čas od času zvyšován. 25 % kvóty země splácí ve zlatě a 75 % v národní měně, kdy suma takto nahromaděných příspěvků jsou k dispozici pro nákup jednotlivými členskými zeměmi do limitu 200 % národní kvóty. Jelikož se nachází 75 % v národní měně, znamená to, že daná země může nakoupit devizy až do 125 % své kvóty. Prvních 25 % „zlaté tranche[12]“ je k dispozici ihned na požádání. Další komoditní tranche je dána k dispozici tehdy, když klesají ceny komodit méně rozvinutých zemí. Ostatní 25 % tranche se poskytují za vyšších úrokových mírách a za přísnějších podmínek, úměrně tomu, jak se zvyšuje částka národní měny v držení fondu takovým způsobem, aby se zajistilo, že se tyto rezervy používají pro dočasné, a ne permanentní financování deficitu. Limit financování ze strany MMF je určen politikou fondu a kvótou dané země (Kindleberger, 1978).

Jinými slovy je to velmi individuální dle daného rozpočtu dané země s tím, že kvóta příspěvku se může měnit dle aktuální světové či regionální hospodářské situace včetně dopadů

[12] Splátka dluhu, která se po jednotlivých emisích emituje na kapitálový trh, kde je nabízena ke koupi.

na národní měnu. Příspěvkový systém jsem pochopil tak, že daná země nejprve splní svůj závazek zlatým kovem a zbytek následně přispěje v dalších příspěvkových kvótách. Dohromady ze 100 % si lze „vybrat“ až dvojnásobek kvóty s tím, že výběr komoditní tranche je podmíněn cenou komodit spojených s poklesem jejich hodnoty kvůli menší atraktivitě a většímu dání důrazu na promyšlení tohoto nákupu. Tranche národní měny si lze nakoupit za nějakých podmínek s tím, že od nějaké výše s vyšším úrokovou sazbou, která zajišťuje taktéž menší atraktivitu pro dlouhodobější financování deficitu veřejných financí a tyto podmínky by měli sloužit jako výstražné světlo před uskutečněním nákupu pro daný územní celek.

„Moderní ekonomiky současnosti používají tzv. peníze s nuceným oběhem, které nejsou navázané na žádnou komoditu. O vynucení se starají právní normy (zákony), které orgány státu zavádí a řídí konkrétní soustavu peněz a upravují aspekty jejího oběhu a ochrany. Ustanovení měny je vždy právním aktem a měna je jedním z atributů suverenity stát.“ (Kaliský,2018). To znamená, že dnešní měny sice stojí na důvěře, ale každá jednotlivá měna je pod záštitou uzákonění daného státu včetně toho, že důvěrou se myslí spolehlivost a korektnost správy dané měny finančními institucemi a státem. *„Jejich vznik a oběh se řídí zákony, které schvaluje parlament a spravuje je kompetentní úřad – v ČR je to Česká národní banka.“ (Kaliský,2018).*

V souvislosti s **pohyblivými kurzy** mnoha národních měn se vyskytla myšlenka na společnou měnu v rámci hospodářské měnové unie, což je předchůdce Evropské unie. **Hospodářská měnová unie** (dále HMU) měla za cíl dosáhnout ekonomické integrace spolu se sjednocením v politické rovině, neboť mezinárodní ekonomický systém nemůže dlouhodobě existovat bez politické stability. Nelze oddělit mezinárodní ekonomiku a politický systém a vznikla tak myšlenka společné měny včetně centrální jednotné měnové autority s možností dialogu členských států, konzultací a koordinací mezi aktéry, vyrovnáváním různorodých zájmů a aspirací na další rozvoj evropské integrace. Tato integrace a posílení se uskutečňovala již před existencí Evropského společenství, a právě v rámci HMU vykrystalizovala společná potřeba evropských zemí na zúžení fluktuačního pásma kursu národních měn vůči dolaru a omezit toto kolísání. **Basilejské dohody** byly součástí tohoto směru k stabilitě a evropské integraci, které byly podepsány zeměmi severozápadními a severskými zeměmi a konkrétně mezi Irskem, Dánskem, Norskem a Velkou Británií, které zavazovaly ke vzájemné spolupráci centrálních bank, harmonizování devizového kursu vůči státům hlásících se k této dohodě a užší platební styk mezi těmito zeměmi. Tomuto trendu nahrálo i vypovězení brettonwoodský měnový systém ze strany USA, což mělo za následek urychlení této snahy integrace (Sychra, 2009).

V období studené války s východem a kolabujícího pevného vázání národní měny na dolar se jeví jako logické hledání hlubší spolupráce se svými sousedy nejen na ekonomické bázi. Navzdory snahám o ukotvení kurzů zpět k pevným či alespoň zdánlivě připomínajícím fixním kurzům toto období již uplynulo a měny vstoupily do pole pohyblivých kurzů.

Tato snaha dala vzniknout Evropskému společenství a posléze Evropské unii, která zavedla do praxe teorii optimální měnové oblasti, která je definována jako hospodářsky stejnorodý prostor s podobnými ekonomickými strukturami, jehož členové budou reagovat stejným způsobem na ekonomické a politické šoky. Vstupem do této měnové unie ztrácí stát 2 hlavní nástroje, které řeší asymetrické šoky, čímž se rozumí událost s odlišnými dopady na jednotlivé ekonomiky a s odlišnými reakcemi od jednotlivých států ohledně ekonomického růstu, nezaměstnanosti apod., a těmi nástroji jsou měnový kurz a úroková míra. Ale vznikla společná evropská měna euro, které je součástí mezinárodního obchodu a hraje v něm signifikantní roli, což zřejmě značí alespoň částečnou kompenzaci za tyto ztráty skrze mobilitu kapitálu, pracovní síly a mzdovou flexibilitu, které dokládají o ekonomické integraci evropských členských zemí (Sychra, 2009).

Je otázkou, zda se ekonomickou integraci daří nadále rozvíjet v pozitivním slova smyslu, neboť vedoucích států ubývá i vlivem brexitu, kdy se Spojené království definitivně rozhodlo o nesetrvání v Evropské unii. Státy, které měly před koronavirovou pandemií již problémy ve veřejných financí v podobě trvalých deficitů jako například část jihoevropských územních celků a je možné, že budou přibývat a je otázkou, zda se k odtržení Velké Británie se někdo nepřipojí a více rozšíří prasklinu v evropské integraci, která projevuje snahu o vytvoření unifikovaného územního celku, kde společnost i ekonomika reagují téměř totožně navzdory národním aspektům, rozdílné kultuře, historickému kontextu a další.

2. Kryptoměny

Vznik kryptoměn se pojí se vznikem Bitcoinu. „*Bitcoin existuje jako open source projekt. Při tom funguje na dobrovolné bázi, bez zdrojů a bez vymahatelných pravidel. Průběžně ho vyvíjí kolektiv programátorů, kteří jsou velmi volně asociovaní (protože je to zajímá, protože mají zainvestováno do bitcoinu, nebo pracují pro velký těžební pool, směnárnu…) a mají různé zájmy. Tato komunita průběžně navrhuje, audituje navrhovaný kód a implementuje jej do podoby nového protokolu, přičemž se musí dohodnout na jeho parametrech a síť to musí (i nemusí) akceptovat. Tento proces probíhá napříč zeměmi, kulturami a časovými pásmy a zajišťuje hodnotu desítek miliard dolarů.“* (Kaliský, 2018). To znamená, že síť, na které běží Bitcoin je decentralizovaná, neboť ji spravuje skupina programátorů z celého světa s tím, že jakékoliv zásahy se konzultují s komunitou tak, že vývoj směřuje cestou s většinovým souhlasem. Co se pojí s decentralizací je absence pravidel, neboť není zde vydavatel v podobě centrály, která by zodpovídala a kontrolovala dodržování daných pravidel a s tím spojené riziko, že vložené prostředky v případě ztráty nelze získat zpátky, neboť neexistuje žádná garance či pojištění vkladů u centrální správy.

K vytvoření kryptoměn došlo z důvodu ztráty důvěry v centrální měnový systém úzkou skupinou lidí a svým výtvorem, „*který nabízí alternativní oběh digitálních peněz, který je globální, bezpečný a nefiguruje v něm nějaká autoritativní instituce (tj. uživatelé komunikují přímo)..“* (Kaliský, 2018). „*Systém je navržen tak, že nikomu nikdo nedůvěřuje, proto všichni kontrolují všechny bloky a transakce podle jednotných pravidel..“* (Kaliský, 2018). Díky absenci si centrální instituce si tento systém dokázal získat spoustu příznivců, kteří touží nebýt pod drobnohledem autority a počet uživatelů roste spolu s objemem investic, do tohoto systému vložených. S přibývajícím počtem uživatelů roste i počet nápadů na zaplnění mezer v tomto segmentu a automaticky se tím podněcuje vývoj tohoto fenoménu. Kaliský také dodává, že za popularitou mimo jiné stojí i zájem o snižování transakčních nákladů na úplné minimum a vzrůstající nedůvěra v bankovní systém.

2.1. Historie alternativ

Prvním průlomem ve velkém měřítku s digitální měnou **Ecash** byl zaznamenán díky kryptografovi Davidovi Channemu, který vytvořil systém kombinující kryptografii, poskytujíc anonymitu, a digitální transakce, který byl uveden do provozu 1990, ale vznikl již v roce 1982 a neměl dlouhého trvání z důvodu brzkého bankrotu. Způsobila ho přílišná anonymita a následný nezájem, který se také pojil s tím, že systém nebyl substitutem dosavadního peněžního styku. Měl představovat pouze alternativu k tehdejším mikrotransakcím, tedy drobným peněžním převodům, které považoval za příliš složité a málo anonymní, které představovaly zbytečnou zátěž pro dosavadní transakční systém. Zmiňoval zejména nedostatečnou anonymitu u transakcí s platební kartou či prostřednictvím šeku. David Chann byl také autorem myšlenky anonymní decentralizované komunikace typu Tor, což je v podstatě virtuální internet v internetu, který přepojuje komunikaci přes různé počítače kolem celého světa, aby nebyla činnost uživatele vystopovatelná k poskytovateli připojení podobně jako tomu je u PayPal, který to později převzal na začátku nového milénia, nicméně stále šlo o FIAT měny, které byly kódované v elektronické podobě (Skalický & Stroukal,2018).

Dalším zlomový momentem pro alternativní měny z digitálního prostředí byl **E-Gold**, který vytvořil Bernard Von NotHaus z důvodu nulového krytí amerických dolarů a absence limitu peněžní zásoby, tzn. libovolné dotisknutí nových bankovek, což může způsobit libovůle státního aparátu a centrálních finančních institucí. Digitální měna byla kryta zlatem, které společnost nakupovala a skladovala. Zároveň měna 1dmc od stejného zakladatele byla kryta samotnou měnou E-Goldem, což způsobilo problém závislosti jedné měny na měně druhé. Navzdory sníženým nákladům v rámci absence skladování zlatého krytí u provozu druhé měny, společnost a tvůrce E-Goldu byl obviněn federálním úřadem Spojených států z terorismu v rámci snahy zničit měnu vlastní země. Soudní spor firma prohrála a firmy E-Gold i 1dmc a jejich činnost byla ukončena a majetek zabaven federální vládou včetně skladovaného drahého kovu kterým byly měna kryta (Skalický & Stroukal,2018).

Je k neuvěření, že lidské směřování ke směnnému prostředku ekvivalentem bohatství a uchovatelem hodnoty je tak často spojováno se zlatem. Projekt pana Bernarda osobně považuji za pravděpodobně zrealizovatelnější a ryzejší variantu kryptoměn v tom smyslu, že má jasný cíl, východiska a realizaci s výjimkou navázání jednoho projektu na druhý, což jde proti myšlence autora diverzifikace prostředků a rizik od amerického dolaru k E-Goldu, ale sám udělá tutéž chybu.

Podobný osud postihl Arthura Budovského, jehož digitální měna převádějící klasické dolary na peníze tzv. Liberty Reserve dolary či Liberty Reserve eura a z převodu si společnost brala 1 % poplatek. Následně nabízela i možnost investování do zlata a dalších drahých kovů. Federální úřady Spojených států zabavila společnost v rámci prohraného soudního sporu v rámci obvinění z praní špinavých peněz (Skalický & Stroukal,2018).

Je zajímavé, jak moc citlivé jsou federální úřady Spojených států na „dolarové/měnové teroristy“, kteří experimentují s komunitními penězi a je tam snaha je propojit s centralizovanou měnovou soustavou.

2.2. Krypta 1.0

První kryptoměna s názvem Bitcoin vznikla v roce 2009, kdy vývojář (či skupina vývojářů) pod pseudonymem Satoshi Nakamoto vydal(a) průvodní článek na základě kterého se přihlašoval(i) k autorství této kryptoměny. Důvod vytvoření Bitcoinu byl hlavní problém dosavadního měnového systému a to tzv. dvojitá útrata digitálních peněz[13] v rámci transakcí a jejich potvrzování. Tato skupina ale namítá, že centrálu lze zničit či napadnout hackerským útokem či z rozhodnutí vlády. **Blockchain**, platforma, na které běží Bitcoin, je vlastně otevřenou veřejnou účetní knihou provozovanou všemi uživateli Bitcoinu, kteří si vzájemně potvrzují transakce zaslané k ověření tak, jako v centrálním měnovém systému tuto roli plní centrální banka, a zároveň uživatelům jsou viditelné veškeré záznamy již proběhnuvších transakcí za celou historii blockchainu Bitcoinu. Bitcoin je dělitelný podobně jako digitální podoba reálných měn a z tohoto pole pomyslně vytlačují hotovostní peníze a drahé kovy, které mají omezenou dělitelnost. Technologie využívaná v kryptoměnách první generace umožňuje velkou škálu možných forem přenosu této kryptoměny, která je v podstatě digitální informací a tu lze uložit na pevný disk, flashdisk, vytisknout na papír prostřednictvím čárového kódu, nahrání do chytrého telefonu či možnost skladování skrze nahrání na servery třetích stran, které představují investiční společnosti či burzy apod., a následně pro proběhnutí transakce stačí kliknout na tlačítko myši. Sporným bodem většiny prvogeneračních kryptoměn je jejich vnitřní hodnota, která je nulová, tedy v případě, že daná kryptoměna není ničím krytá, a v tomto bodě jsou si dané měny rovny s bezhotovostní formou reálných peněz. Limitace bitcoinových mincí je stanovena na 20 999 999,9769 kusů, která je pevně daná a neměnná. Těžba se postupem zájmu o danou kryptoměnu stává náročnější na výpočetní výkon a až se dosáhne daného počtu vygenerovaných mincí, tak se veškerá těžba zastaví a budou probíhat pouze transakce. Konkrétně v roce 2140 bude dosaženo počtu veškerých vytěžených mincí, ale většina bude uvolněna již v roce 2033, což je v systému nastaveno při tvorbě dané kryptoměny včetně příslušných údajů, a to včetně způsobu získání mincí a dalšího (Skalický & Stroukal,2018).

Spekulace a dohady, zda tento fenomén může vůbec fungovat jako měna, vzrostly po uskutečnění první transakce, kterou bylo směnění 10 000 BTC (Bitcoinů) za dvojici pizz programátorem Laszlym Hanyeczem 18. května v roce 2010, což v té době představovalo 41 amerických dolarů, ale nyní (k datu psaní této práce) tato transakce 10 000 BTC (dále jen BTC) má hodnotu přibližně 154 milionům USD (amerických dolarů), 130 milionům eur, a to je

[13] Znamená dvojitou útratu peněz v systému a tento problém byl vyřešen centrální autoritou, která zabraňuje duplicitnímu zalistování transakce v bankovním systému a následné dvojité útratě peněžních prostředků z bankovního účtu.

ekvivalentem pro 2,5 tisíc tun investičního zlata či 188 tun investičního stříbra dle webu Bitcoin Pizza Index, který je denně aktualizován.

Tato směnná interakce byla hybným krokem k myšlence, že kryptoměna se může stát měnou či se za ní vydávat. Bez této transakce by projekt Bitcoin zůstal ve skupině s omezenou působností.

V roce 2011 se uskutečnily první velké krádeže na poli kryptoměn, kdy uživatelský účet s 25 tisíci BTC byl odcizen a vykraden, kdy tyto případy způsobily propad ceny BTC o 70 % z 31,91 USD na 10 USD. Zmíněné události předcházely napadení kryptoburzy Mt. Gox, kde byly ukradeny data a obsah desítky tisíc uživatelských účtů hackery, kteří prolomili jejich příliš jednoduché zašifrování včetně údajům k účtu administrátora burzy, díky kterým mohl být obsah účtů odcizen pomocí příkazu k prodeji stovek tisíc BTC, což negativně ovlivnilo cenu BTC, která se znovu propadla ze 18 USD téměř k nule a nepomohla tomu i skutečnost, že se tehdy jednalo o jedinou burzu obchodujíc s kryptoměnami a burzu tento útok vyřadil z provozu na sedm dní, načež až s jistou setrvačností vytvořená nová nabídka BTC (a to kvůli velkému objemu, který vyžaduje vysoký počet potvrzení) snížila cenu. Cena se vrátila na původních předkrizových 32 USD za 1 BTC až po roce a půl, kdy k této nejistotě přispěly i zprávy o dalších desetitisících ukradených BTC v roce 2012. V pozadí těchto událostí zároveň rostl tzv. Silk Road, neboli hedvábná stezka, což byl server pro nákup a prodej nelegálního zboží různého druhu, nejčastěji zbraně a drogy, kde bylo možno nakupovat právě prostřednictvím BTC. Takové okolnosti zastínily vývoj likvidity Bitcoinu v legálním prostředí, a to prostřednictvím možné směny u obchodů s elektronikou, u vybraných taxislužeb, právníků, lékařů, restaurací, hazardu či ojediněle požadavky na výplaty mezd pouze v BTC díky rozrůstajícímu se kryptoměnovému podhoubí a jeho uplatnitelnosti. Snahou o stabilizaci a nápravu v minulosti vzniklých škod byl vznik aplikace BitPay, což představilo platby v BTC dle aktuálního kurzu v daném okamžiku zadání platby a obratem na účet získáte americké dolary v rámci internetových plateb (Skalický & Stroukal,2018).

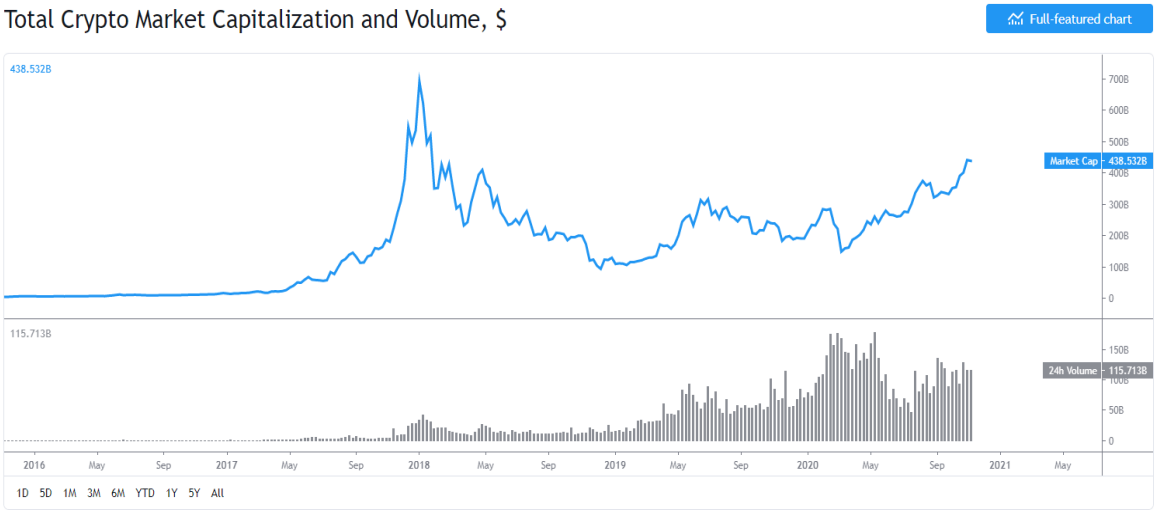
Stinné stránky kryptoměn v podobě krádeží obsahu účtů či odcizení přístupových údajů do daného účtu mi evokují, že navzdory rafinovanosti tvůrců ohledně zabezpečení platforem kryptoměn je tato vysoká úroveň rafinovanosti i u osob, které mají stejné či podobně kvalitní znalosti s tím, že je využívají proti tvůrcům a řadovým uživatelům. Zdá se, že poměr mezi rafinovanými krádežemi je v neprospěch v oblasti tohoto kryptoměnového prostředí, kde jsou více časté, než je tomu u klasického peněžního prostředí. Pohled jsem si tvořil na základě krátkodobé historii kryptoměn a reprezentativní to rozhodně tvrzení není, neboť oficiální

výzkumy ani data potvrzující odcizení neexistují, neboť platforma blockchain je pseudoanonymní. To znamená, že pro směnnou interakci je nutné znát číslo účtu protistrany a na základě toho je možné si spojit fyzickou osobu s daným číslem účtu, ale na obecné úrovni je toto nerealizovatelné, neboť žádné osobní údaje nejsou vidět ani nejsou zaznamenávány, a tak nelze ani určit, zda daná transakce veřejně probíhající a viditelná ostatními uživateli není momentální krádež.

Na přelomu roku 2013 a 2014 se tržní kapitalizace BTC prolomila hranici 14 mld. USD, zároveň Silk Road [14]a jeho tvůrce byli zablokováni a tvůrce odsouzen na doživotí a zabavené BTC byly ve státní aukci prodány, nicméně to podnítilo vznik podobných ilegálních serverů, které předčily své předchůdce včetně jejich zabezpečení. V roce 2014 zkrachovala, již dříve vykradená, kryptoměnová burza Mt. Gox, která vlivem soudních sporů a zabavení 5 milionů USD federální vládou USA nezvládla ustát tyto rány včetně skutečnosti, že odliv uživatelů a klientů si způsobila vlastní chybou, když nezaregistrovala odcizení 744 408 BTC během provozu činnosti. V té době již existovala vícero kryptoměnových burz, takže struktura tím tak neutrpěla jako v minulých letech. Díky velkému zájmu veřejnosti a přílivu nových uživatelů nastal neočekávaný stav, a to nedostatek kapacity sítě Bitcoinu, což vedlo k modifikaci, která by toto zahlcení odstranila, ale tím by část těžařů přišla o 20 % bonusový součet k výpočetnímu výkonu a vedlo tedy k odtržení, tzv. hard forku, a založení vlastní kryptoměny **Bitcoin Cash**. V témže roce vzniklo bezpočet investiční společností orientujících se na kryptoměny a také vznikly první kryptomaty, kde lze dle kurzu a obchodní marže směnit papírové peníze za kryptoměnu, a naopak či rozvoj kryptoměnových směnáren a vznik kryptoměnových bank. Navzdory tomuto příznivému vývoji byl Bitcoin a ostatní kryptoměny silně volatilní a tato volatilita odrazovala potencionální uživatelé, kterým se nelíbí představa denní kolísavosti v řádech desítek procent. To ale tvoří smyčku, neboť pouze noví uživatelé stabilizují kurs kryptoměn, neboť pouze masovou směnou lze zvýšit důvěryhodnost kryptoměny a přilákat i firmy, které budou přijímat platby v Bitcoinech za své služby či výrobky a umožnění tak přiblížení Bitcoinu ke světovému prostředku směny (Skalický & Stroukal,2018).

[14] Darknet kryptoměn.

Čím větší pozornost bude u veřejnosti mít kryptoměna tohoto typu, který nemá hlubší smysl než nabízet danou soustavu jako alternativní vůči té klasické, tím stejně vzroste zájem osob s odlišnými úmysly a vzhledem k četnosti podobných příkladů v publikacích a pramenů, ze kterých čerpám, znovu narážíme na to, že nemáme jak zjistit dané riziko, alespoň tak se mi to jeví, vzhledem k decetralizovanému autonomnímu ekosystému jménem blockchain, který neobsahuje nějakou centralizovanou databázi o zločinnosti v systému, neboť v systému nelze definovat nějakou transakci jako špatnou v případě, že je potvrzena osobním, třeba odcizeným, klíčem, který se potvrzuje transakce k odeslání.



Graf č.1: Tržní kapitalizace kryptoměn včetně objemu obsaženého kapitálu.

Dostupné zde: https://www.tradingview.com/markets/cryptocurrencies/global-charts/

Svou vlastní kryptoměnu stvořila i firma Facebook, kdy 16. června 2019 oznámila vznik své kryptoměny Libra fungující na decentralizovaném blockchainu, kdy správcem je nezisková asociace Libra Association tvořená desítkami firem a institucí – například společností Visa, MasterCard, PayPal,Uber,eBay či Vodafone. Od ostatních altcoinů se Libra liší kurzem, který je vázán přímo na koš FIAT měn, a proto bude více stabilní a méně vyhovující pro spekulace ovlivňujíc strmé vzestupy i hluboké propady. Množství vydaných Liber bude záviset na zájmu lidí a počtu mincí dané kryptoměny, což je odlišné od ostatních kryptoměn, že nebude omezeno (ccco.cz).

Měna by byla vázána na americký dolar, ale vzhledem k tomu, že federální úřady nepovolili spuštění této kryptoměny, tak byl vydán pouze zdrojový kód, na kterém se stále pracuje a jeho podoba není finální v případě změnění rozsudku a možné vydání je v nedohlednu (Klofáč, 2020).

Přijde mi nemyslitelné, aby soukromá společnost si vytvořila komunitní měnu, čímž by získala nově přehled i o vašich transakčních datech, které by se přidaly k tzv. velkým datům, které konkrétně firma Facebook shromažďuje a nastává otázka, zda je i přeprodává třetím stranám či nikoliv.

Bitcoin Cash není derivátem Bitcoinu, ale víceméně klonem, který se odlišuje zejména v technických záležitostech dané sítě, neboť ke vzniku díky tzv. hard forku došlo teprve v polovině roku 2017 a většina struktura sítě je totožná se zmiňovaným Bitcoinem. Taktéž využívá těžaře k potvrzování transakcí, ostatně samotní činští těžaři vytvořili Bitcoin Cash (dále jen BCH), a také se vyznačuje vysokou volatilitou, tím spíše, když tato kryptoměna je poměrně novou záležitostí a nemá takovou uživatelskou základnu jako jeho původce, trpí více na tržní výkyvy v řádcích několika desítek procent za týden či dokonce za jediný den. Také využívá stejný mechanismus jako Bitcoin včetně zabezpečení. Vzhledem k jeho menší základně, a tedy i nižší tržní kapitalizací, je BCH dělitelný „pouze" na 8 desetinných míst, neboť cena za jednu minci je mnohonásobně nižší, ale v případě, že by dosáhla strmé hranice, kde by byla vyžadována vyšší dělitelnost, lze síť modifikovat. Emitence mincí je stejná jako v případě Bitcoinu, kdy tempo uvolňování se přizpůsobuje snaze těžařů, tzn. nyní se uvolňuje 12,5 BCH za 10 minut a každé 4 roky se odměna za těžbu půlí. Finální počet mincí je necelých 21 milionů s tím, že už nyní je v oběhu 17 milionů mincí (FreeCoin.cz).

BCH akceptuje pouze 5000 kamenných prodejen, restaurací či kaváren a nadnárodní e-shop prodejci celosvětově, zároveň ale má levnější transakční poplatky než jeho původce, plynulejší chod systému v rámci rychlosti i objemu potvrzovaných transakcí, ale i lepší zabezpečení díky největší robustnosti řetězců, které je nutné prolomit k tomu, aby transakce byla narušena či k odcizení mincí z peněženky (BitcoinCash.org).

Dash je dalším altcoinem[15]. Síť je založena na blockchainu, tzn. že využívá služeb těžařů, kteří zde hrají podobnou roli jako u Bitcoin a zajišťují chod sítě. Specifikem sítě jsou tzv. Masternodes neboli master uzly, které se zpřístupní po držení 1000 mincí Dashe jako základní ochranu uzlu před nekalými pokusy ho napadnout či pozměnit, ale provozovatelé jsou odměněni za provozování sítě skrze master uzly tím, že 45 % nově uvolněných mincí jde právě do jejich peněženek. Dalších 45 % nově emitovaných mincí jde regulérním těžařům a zbylých 10 % mincí je určeno k financování vylepšování ekosystému a putují do pokladnice, o jejímž využití právě master uzly a formou hlasování se upíná další vývoj infrastruktury Dashe. Master

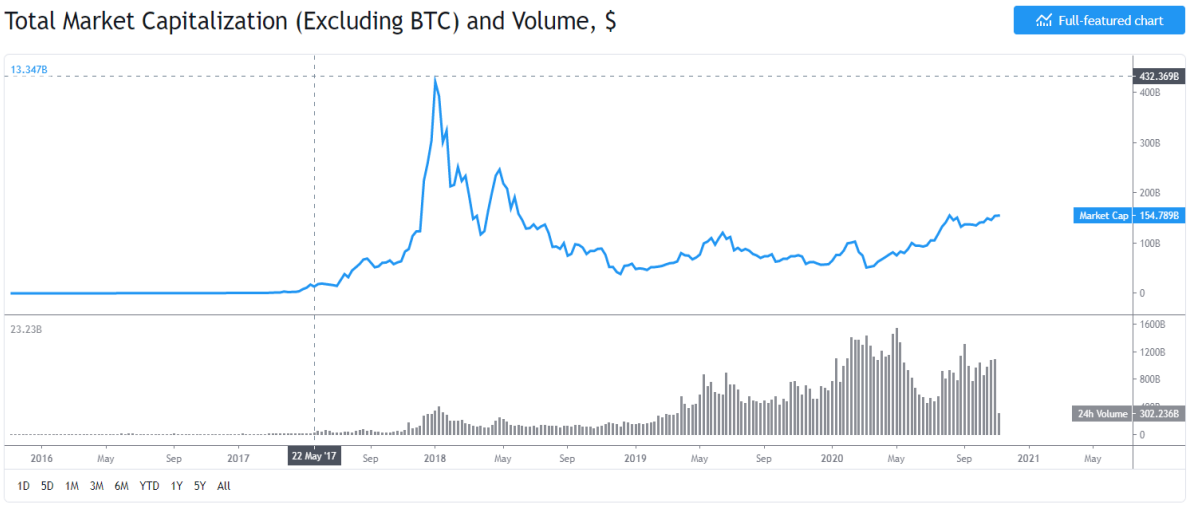
[15] Alternativní kryptoměna mimo BTC.

uzly dávají uživatelům zásadní výhodu ohledně rychlých či instantních plateb, které se považují za věrohodné už jen z konsensu ostatních master uzlů, tzn. zpřístupnění plné anonymity, ale pokud shody není dosaženo, poté transakce čeká na klasické potvrzení od těžařů (Skalický & Stroukal,2018).

Cílem Dashe je stát se platformou, která bude disponovat co možná nejrychlejším systémem a nejvíce anonymní platební bránou na světě s tím, že má osminásobně větší kapacitu sítě než BTC a transakční plynulostí předčí také jiné kryptoměny. Dělitelnost je stejná jako u většiny krypt a to na 8 desetinných míst. Emitence této měny se každý rok sníží o jednu třináctinu s tím, že konečný počet mincí je 19 milionů kusů, z toho cca 9 milionů už je v oběhu. Zároveň taktéž trpí vysokou volatilitou, která je pro většinu kryptoměn typická (FreeCoin.cz).

Nejznámější derivát je **Litecoin** (dále LTC), který byl představen nedlouho po prvních dvou úspěšných letech BTC vyvinutý programátorem Google.org. Oproti své předloze je mnohem agilnější včetně toho, že celkový počet mincí je nastaven na 84 milionů a těžba kryptoměny je vhodná i pro méně výkonnější hardware (procesory či grafické karty). Mnohem nižší transakční poplatky než u BTC, kdy poplatek u BTC se u větších pohybuje i 400 Kč v přepočtu za transakci (Skalický & Stroukal,2018).

Opravdu velký rozdíl nabízí decentralizovaná kryptoměnová soustava, kde vlivem stále ještě nového fenoménu jsou deriváty či klony podobné měny pro uživatele a investory stejně zajímavý objekty, obzvlášť pokud se jedná o klon prvotního BTC. Narážím na to, že kdyby se někdo rozhodl vytvořit klon české koruny, tak může oslovit pár jedinců, ale následně promyslet vlastní měnovou soustavu s velikou pravděpodobností centralizovanou a tak dále. A než by se tak událo, je velmi pravděpodobné, že tento klon bude v propadlišti dějin derivátů české koruny. Chci tím říct, že v tomto novém poli je snadnější se zviditelnit vzhledem k neprobádanosti



Graf č.2: Tržní kapitalizace kryptoměn mimo BTC.

Dostupné zde: https://www.tradingview.com/markets/cryptocurrencies/global-charts/

segmentu, ale i vzhledem k té neprobádanosti je segment velmi kolísavou lodí, která sem tam narazí do většího či menšího ledovce a velmi mnoho projektů začne, ale ještě více projektů nedopadne a zmizí, což ostatně dokládají i sami autoři Skalický a Stroukal.

2.3. Mechanika kryptoměn 1.0

Svým směrováním projekt alternativních peněz, neboli předchůdců kryptoměn, narazil na velmi vzácné pokrytí světa internetem, neboť bez internetu by tato měna fungovat nemohla spolu s faktem, že bez osobního počítače taktéž ne a v dřívějších dobách se to nesetkalo s potřebnou odezvou, neboť dané technologie nebyly tak hojně rozšířeny jako je tomu dnes spolu s tím, že projekty měly koexistovat s hotovostí většinou u maloobjemových transakcí, ale hotovost byla okamžitě likvidní, dostupná, taktéž anonymní a je snadné ji využívat a hlavně akceptovat. Proto po dlouhé odmlce vznikla nová platforma ve formě blockchainu.

Většina prvogeneračních kryptoměn běží přímo na blockchainu či je od něj odvozeno, tedy řetězci bloků, který byl prvně vydán společně s dalším příslušenstvím infrastruktury Bitcoinu v roce 2009. Bitcoin je decentralizovaná Peer-to-Peer síť v internetu spravující historii platebních transakcí mezi svými uzly (toky šifrovaných číselných kombinací), základní jednotkou je BTC a síť má omezený počet mincí na již zmíněných necelých 21 milionů. Vznik nových mincí zajišťuje těžba těžařů, kteří zároveň i verifikují odeslané transakce uvnitř sítě prostřednictvím potvrzení. Síť funguje na souboru pravidel, které každý jednotlivý uzel vyhodnocuje dle výchozího nastavení sítě a pokud jsou daná pravidla splněna, která jsou očekávána, pak se daný uzel akceptuje jako věrohodný. Tato kontrola je prováděna samostatně každým uzlem, neboť neexistuje žádná centrální autorita. Všechny transakce jsou spravované „účetní knihou“, tzv. ledgerem, který je uložen v blockchainu a lze, po stažení blockchainu do našeho počítače, v něm volně prohlížet od vzniku až po aktuálně potvrzující transakce, tzn. že transakční data jsou viditelná pro všechny uživatele se stáhnutým blockchainem. Ostatně typ počítačové sítě Peer-to-Peer zrovnopravňuje všechny uzly, které jsou si rovnocenné a jednotlivý klienti spolu komunikují přímo bez existence centrálního uzlu či serveru. Na rozdíl od modelu klient-server, zde s rostoucím množstvím uživatelů roste i přenosová kapacita sítě, ale naopak nevýhodou je velká obtížnost navázání komunikace, a tedy uskutečnění transakce (Skalický & Stroukal,2018).

Blok, nejvýznamnější datová struktura **bitcoinového protokolu**, kóduje množinu transakcí, které svým zahrnutím potvrzuje. Pouze jedna z transakcí je generující a pouze jejím prostřednictvím vznikají nové BTC. Validní blok musí mít určitou kryptografickou vlastnost, jejíž splnění je náročné na výpočetní výkon, kde náročnost je proměnná v čase, což umožňuje zpětnovazebnou regulaci k dosažení stability průměrné rychlosti generování nových bloků, a tím i ovlivnění inflace měny. Nalezení validního bloku je důkazem o vynaloženém úsilí a tento

koncept je nazýván jako „proof of work“ a právě vynaložené úsilí na odměně v podobě množství nově uvolněných mincí je využíváno v bitcoinovém protokolu (Lánský, 2018).

Řetězec bloků je spojový seznam bloků s odkazem na předcházející blok, kdy spojení je dosaženo obsažením hashe předchozího bloku v datech bloku následujícího. Každý blok má jednoznačně určený předcházející blok s výjimkou úplně prvního bloku, tzv. genesis bloku, kde místo hashe předešlého bloku je nula. Vazba bloků je pouze jedna a má podobu stromového obrazu vazeb, které nejsou cyklické. K větvení neboli forku, ke kterému dochází velmi zřídka a „strom“ bloků vypadá spíše místy jako dlouhá rovina s odbočkami, kdy se pracuje vždy s nejdelší historií, což znamená, že bloky by bylo nejtěžší spočítat, a právě tomuto řetězci se říká blockchain, neboť již nejde o strom ale o lineární řetězec. Tak vzniká ochrana proti hackerům či nahodilým chybám systému. Bloky zbylé v nepokračujících větvích se ignorují. Relevantní jsou naopak bloky v blockchainu a transakce v nich zahrnuté jsou považovány za potvrzené a věrohodné, přičemž tímto způsobem se koncept zabezpečuje ukládáním nepřepisovatelné historie, neboť modifikace bloku uprostřed řetězu by vyžadovalo přepočítávání všech následujících bloků, které obsahují hash předcházejících, který se při modifikaci dat změní, což mimo jiné znamená, že by se při přepočítávání nepracovalo s nejdelším řetězcem, neboť nejdelší zůstává původní řetězec, který navíc může být obsažen ve všech ostatních bočních řetězcích sítě (Lánský,2018).

Asymetrická kryptografie je v této síti využita v rámci šifrovacích a dešifrovacích klíčů, které představují dlouhou kombinaci čísel a znaků, které jsou náhodně vygenerované sítí a využívají se k bezpečnému fungování prostřednictvím tzv. hashovací funkce, což je pokrytí jednotlivých obrazů příslušnými vzory s vysokou nelinearitou, což znamená, že malá změna vzoru způsobí velkou změnu obrazu a díky asymetrické složitosti výpočtu lze snadno dopočítat přímý obraz na vzor, ale výpočet nejednoznačného zobrazení obrazu na vzor je extrémně obtížné. Veřejný klíč slouží k zašifrování zprávy pro majitele soukromého klíče nebo k ověření jeho podpisu, kdy v bitcoinové síti má veřejný klíč význam adresy příjemce platby, kde adresa se vypočítá z veřejného klíče. Soukromý klíč je tajný klíč pouze pro majitele jednoho či více účtů, který se používá k dešifrování jemu určené zprávy nebo podepisování jím ověřované zprávy, tím se tedy liší od klasické kryptografie, kde slouží pouze jeden klíč k šifrování i dešifrování. Digitálním podpisem se myslí zadání soukromého klíče se zprávou či informací, kdo bude novým majitelem BTC patřících majiteli klíče, kdy ke každé adrese je právě jeden klíč privátní, který je uložen v BTC peněžence (Skalický & Stroukal,2018).

Adresa je jednoznačná identifikace příjemce platby, která je ekvivalentem čísla bankovního účtu, ve formě dlouhého kódu čísel a písmen s různými vlastnostmi, kdy délka je většinou 27 až 34 znaků, ale u některých protokolů se můžeme setkat i s intervalem od 14 do 74 znaků, rozlišují se velká a malá písmena, neobsahuje typograficky zaměnitelné znaky jako ‚0' a ‚O' či ‚I' a ‚1' a v poslední řadě poslední znaky obsahují kontrolní součet, což slouží k zabezpečení proti špatnému opsání či okopírování. **Adresu** lze vygenerovat i mimo síť, neboť je pouze **veřejným klíčem**, který nutný ke správné komunikaci prostřednictvím transakcí. Vygenerování veřejného klíče je levné a lze generovat novou adresu pro každou nesouvisející transakci, což znesnadňuje jejich stopování. Adresy uživatele a k nim příslušné klíče jsou zpracovány a spravovány **peněženkou**, která může mít podobu aplikace na chytrém telefonu či formu programu v počítači. Zásadní je, kde jsou data peněženky uložena, neboť existují peněženky mimo síť, které ukládají data na pevný disk, následně peněženky spravovány třetími stranami, ať už se jedná o burzu, směnárnu či investiční společnost anebo data peněženky mohou být ukládána do síťových úložišť v serverech, které jsou neznámo kde na planetě. Nebezpečí a odcizení a rizikovost jsou vzestupné dle pořadí uváděných možných formách peněženky. Funkce peněženky je správa **soukromých klíčů** příslušejících k adresám uživatele a stará se o vedení účtu, odesílání plateb, archivace transakcí včetně evidence známých adres. Uživatel prokáže vlastnictví konkrétní adresy tím, že podepíše soukromým klíčem určitou zprávu příslušející k dané adrese. Nejdůležitější je tedy neztratit přístupy do peněženky, kde jsou uchovávána citlivá data (Skalický & Stroukal,2018).

Převod kryptoměny v BTC protokolu z adresy na adresu je interní datová struktura obsahující vstupy a výstupy, kde vstup odkazuje na výstup v nějaké již existující transakci. Vlastností výstupu je množství BTC, které z něho lze uvolnit a celkový objem hodnot všech již existujících výstupů, na které jsou vstupem nové transakce odkazovány. Celkový objem lze mezi výstupy nové transakce rozdělit libovolně, pokud součet hodnot není větší. Pokud je menší, rozdíl je chápán jako **poplatek za transakci**. Speciální transakce obsahující pouze výstupy je generující transakce, která je obsažena v genesis bloku, tedy úplně prvnímu bloku, který umožní uvolnění prvních BTC a spustí de facto provoz sítě Bitcoinu. Při použití výstupu dochází k jeho konzumaci v celé výši, tzn. není dělitelný a použitelný je pouze jednou. Pokud převáděná hodnota má být menší než hodnota výstupu či výstupů, nová transakce bude obsahovat i výstupy pro rozměnění, kterými si majitel vrátí rozdíl na jakoukoliv svou adresu. K uvolnění výstupu je potřeba, respektive jeho použití na vstupu nové transakce, podepsat data transakce soukromým klíčem patřícím k jeho adrese, což má právo k výstupu pouze majitel účtu svým soukromým klíčem. Systém nárokování výstupu umožňuje vytvářet složité

podmínky, které musí být pro jeho použití splněny, například uvolnění výstupu více podpisy, heslem, postdatováním či jinými způsoby. Složitějším a kombinovaným podmínkám k uvolnění výstupu se říká **kontrakty** (Skalický & Stroukal,2018).

Snahou uživatelů je vyhnout se tzv. maleabilitě transakce[16]. Když se do blockchainu dostane místo původní transakce její pozměněná verze (obě verze být potvrzeny nemohou, protože uvolňují stejné vstupy) může si nevhodně navržený software (software potvrzující transakci na základě hashe a nikoliv obsahu) myslet, že k transakci nedošlo a může se pokusit transakci zopakovat uvolněním jiných BTC, čímž provede platbu vícekrát, což může vést k mylnému domnění, že výstupy použité v pozměněné transakci má stále k dispozici a to způsobí problém při pokusu o jejich opětovné uvolnění v rámci jiné transakce v budoucnu (Skalický & Stroukal,2018).

Potvrzená transakce je taková, která je obsažena v blockchainu a čím hlouběji je obsažena, tím je bezpečnější a hůře zpětně prolomitelná. Hloubka je počet bloků mezi blokem zahrnujícím transakci ve svých datech a blokem aktuálně těženým a bezpečnost se pozná dle počtu potvrzení, neboť s rostoucím počtem potvrzení se snižuje riziko zvrácení transakce a zároveň platí, že u velkoobjemových transakcí se využívá alespoň 6 potvrzení (Lánský,2018).

[16] Jedná se o pozměnění ještě nepotvrzené transakce, kde se ve formátu podpisu změní její hash – pokrytí jednotlivých obrazů nelineárními vzorci.

Generující transakce, díky níž vznikají nové mince kryptoměny, nemá žádné reálné vstupy, obsahují libovolná data a její objem je roven součtu nově vygenerovaných mincí a poplatků za ostatní transakce v bloku obsažené (Skalický & Stroukal,2018).

Poplatek za transakci je rozdíl mezi hodnotou výstupů a vstupů transakce, který stanoví odesílatel platby a mince dané kryptoměny ve výši rozdílu připadnou v rámci generující transakce tomu, kdo vytěží blok transakce potvrzující. Poplatek za transakci je motivací k jejímu zahrnutí do těženého bloku a po vytěžení všech možných mincí dané kryptoměny bude přetrvávající motivací k pokračování v těžbě (Lánský,2018).

Výše poplatku se odvíjí od různých parametrů a nejčastěji dle požadované rychlosti převodu (ccco.cz).

Těžba je proces, který pomocí strojově náročného výpočtu hledá další blok pro napojení do blokového řetězce (blockchainu). Blok je nalezen, pokud splní podmínku, že jeho hash je nižší než určitý cíl. Cíl se odvozuje z momentální obtížnosti, která se mění každých 2016 bloků v závislosti na rychlosti jejich nalezení tak, aby průměrná rychlost generování nových bloků činila 1 blok za 10 minut. Prostřednictvím výpočetního výkonu se celý těžební proces dává do pohybu a mezi nosiče výpočetního výkonu řadíme procesory, které ale už nestačily s přibývající obtížnosti na nalezení bloku a tak se přešlo na grafické karty a následně na zákaznické hardwarové obvody. Časem ale i to nestačilo, a tak se těžaři rozhodli shlukovat do tzv. těžařských poolů (sdružení), kde se vlastní výpočetní výkon přidá k celku a odměna se rozděluje dle přidaného výkonu do poolu. To znamená, že odměny nejdou přímo těžařům, ale nejprve správci daného „bazénu“, kde mohou ale nemusí být se členstvím spojeny nějaké poplatky, a následně správce rozdělí odměnu dle výpočetního výkonu, což znamená jistotu výdělku pro těžaře v rámci těchto uskupení (Skalický & Stroukal,2018).

Situace, kdy by kryptoměny ztratili veškerou důvěryhodnost, by nastala v případě vlastnění 51 % podílu veškerého výpočetního výkonu sítě kryptoměny. V ten moment vlastník tohoto nadpolovičního podílu sítě má možnost zaútočit na síť stylem, kdy útočník se snaží použít, respektive využít, stejný výstup již existující transakce vícekrát neboli na vstupech více než jedné transakce. Tento útok se realizuje snáze, pokud příjemce platby nepožaduje potvrzování transakce, tzn. že každému příjemci stačí rozeslat pouze jemu určenou transakci. Čím přibývající počet potvrzení vyžadovaných od příjemce platby, které mají zajistit důvěryhodnost transakce, tím hůře se útok realizuje, neboť útočník je nucen rychle vytěžit alternativní bloky a tím obětovat svůj výpočetní výkon k útoku, jehož nejistota úspěchu roste

s počtem potvrzení, která musí svojí alternativní větví blockchainu „obejít“ (Skalický & Stroukal,2018).

Signifikantní změny v blockchainu se označují jako tzv. fork[17]. Fork může být dvojího druhu, a to dle dopadů vzniklých změn – softfork a **hardfork**. Softfork je změna kryptoměnového protokolu, kde platí, že datové struktury, tzn. bloky a transakce, vytvořené dle nových pravidel jsou vždy platné i dle pravidel starých. Jinými slovy je zajištěna zpětná kompatibilita softwaru a není tedy potřeba aktualizovat či vylepšovat stávající, pokud nechceme dané nové funkce v nové verzi. Softfork se taktéž vyznačuje snižováním počtu bloků za jednotku času, tedy restriktivní tendence ohledně objemu měny, která proteče za jednotku času, a tedy zmenšení kapacity transakcí, což v případě Bitcoin Cash byl kámen úrazu, kdy jedna část komunity chtěla vyšší rychlost sítě s přibývajícím objemem transakcí ve frontě díky rostoucímu počtu uživatelů, ale druhá část se obávala, že by to narušilo bezpečnost sítě. Změny v datových strukturách, které nedisponují zpětnou kompatibilitou, se označují jako tzv. hardfork. Navzdory naší vůli, zda chceme či nechceme využívat nové funkce vylepšené infrastruktury sítě, je nutné aktualizovat na novou verzi v případě, že chceme nadále využívat danou službu. Důsledkem hardforku může být rozdělení blockchainu trvalou změnou, viz. Bitcoin Cash. Mince původní měny mi v případě BCH zůstaly, a navíc jsem obdržel mince měny nové a pokud uživatel má své prostředky v online peněžence či na burze, pak je odkázán na akce jejich provozovatelů, zda mu bude přiznáno vlastnictví mincí i druhé měny. Je pravděpodobné, že hodnota mincí po hardforku klesne a že ani v součtu s těmi novými nebude na předešlých hodnotách a vše tedy záleží na tržním vyhodnocení. Hardfork se naopak vyznačuje expanzivní tendencí v podobě zvyšování počtu bloků transakce za jednotku času, což znamená vyšší kapacita transakcí (Skalický & Stroukal,2018).

[17] Proces zapojování více bloků za stejný předchozí při vytěžení bloku a jeho propagací do sítě došlo k vytěžení jiného bloku anebo v publikacích se spíše o forku ve spojitosti s významnými změnami řetězce.

2.4. Kryptoměny 2.0

Mezi kryptoměny druhé generace se označují veškeré alternativní kryptoměny, které sledují i jiný cíl než jen svou existencí nabízet alternativu k centrální měnové soustavě. Jinými slovy přidaná hodnota těchto krypt je účel, díky kterému byla daná kryptoměna stvořena. Kryptoměna **Ripple**, která byla ve vývoji již od roku 2004, je decentralizovaný systém, ve kterém si uživatelé mohou vytvářet a vyměňovat vlastní peníze a dluhy, což jsou v podstatě elektronické směnky. Transakce Ripplu se nepotvrzují těžbou, ale důvěryhodností uzlů, které jsou uživatelem vybrané, což je rychlejší včetně menší náročnosti podmínek na výpočetní výkon. Další ojedinělou funkcí je databáze Ripple účtů, která kromě vlastní měny obsahuje i nabídku a poptávku jiných aktiv, tedy taková decentralizovaná burza. Pro uznání důvěryhodnosti uzlu je nutno dosáhnout alespoň osmdesátiprocentní shody ostatních námi vybraných uzlů. Transakce je návrh na změnu uzlu, a pokud se uzly neshodnou na všech transakcích, sporné se vyřadí a cyklus shody se opakuje do okamžiku, než se na novém obsahu shodne potřebná většina. Původní uzel založený společností Ripple obsahuje od svého vzniku pevně daný počet mincí a to 100 miliard s označením XRP. 20 procent z celkového počtu si ponechali zakladatelé a zbylých 80 procent získala dceřiná společnost Ripple Labs. Část se rozdala různým neziskovým organizacím a jednotlivcům v rámci propagaci systému. Dělitelnost 1 XRP lze rozložit až na 1 milion kousků s tím, že každý uživatel Ripple účtu musí splnit podmínku v podobě pasivního držení alespoň 20 XRP. Kromě kryptoměny XRP síť obsahuje i tokeny na další druhy aktiv, ať už se jedná o FIAT měny, jiné kryptoměny či komodity. Při převodu XRP na jiné aktivum se do sítě ukládá podepsaný uživatelem „dlužní úpis“, takže reálné vypořádání vyžaduje důvěryhodnost stran dle nastavení protokolu společností Ripple a pokud se nenajde přímá důvěra mezi obchodujícími subjekty, hledá se v síti cesta, která důvěryhodnost zprostředkuje. Na konkrétní nalezené cestě pak závisí výše transakčních poplatků, případně i možnost převodu měn (Skalický & Stroukal,2018).

Líbivá myšlenka je zde ohledně souznění kryptoměnového světa a světa klasických měn, kde Ripple v podstatě nabízí tokeny či směnky na reálné peníze pro mezibankovní obchod, který bude rychlejší, bezpečnější díky kryptografii a menší transakční poplatky. Vzhledem k zájmu bank, které se řadí mezi ty nejkonzervativnější investory, by volatilita nemusela být v budoucnu tak vysoká jako tomu je u kryptoměn. Potíž může být znovu u kontroly, neboť anonymita či pseudoanonymita ji buď kompletně znemožňuje či velmi ztěžuje. Chápu, že byl prvotní účel se odstřihnout od centralizovaného systému, který sbírá o každém účastníkovi v podobě transakčních dat a dalších, ale je mi trochu podezřelé, že jsou tací, kteří si přejí být

v téměř či kompletní anonymitě a nechtějí být nalezeni. To u mezibankovních transakcí by nevzbuzovalo velkou důvěru důvěryhodných bank. Takže se to zřejmě bude týkat zase jenom částečného mezibankovního obchodu, pokud se systém neoptimalizuje a nezmění do přehlednější podoby, která vzbudí důvěru i u ostatních bankovních hráčů.

Databáze Ripplu není odvozena ani postavena na blockchainu, tedy transakce nejsou uspořádány do bloků, ale účetní kniha volně dostupná na síti je aktualizovaná každých pár sekund a není tedy náročná na energetickou spotřebu, neboť je zde absence výpočetního výkonu, který zařazuje transakce do bloků. Cílem společnosti je vytvoření platformy pro finanční instituce, banky a jiné zprostředkovatele plateb, kterým by nabízela efektivnější a rychlejší transakční podmínky než ty dosavadní na mezinárodním poli. XRP má fungovat jako tzv. měnový most, kdy finanční instituce nejdříve smění svoji měnu na XRP a poté skrze síť prostředky přepošle na účet adresáta u příslušné banky, a nakonec se XRP převede na lokální měnu. Druhou možností je nakoupit tokeny příslušného aktiva, které jsou elektronickou formou směnky. XRP se sice netěží a je rovnou emitován v plné výši, ale v roce 2017 se 55 miliard XRP uložilo do speciálního kontraktu, který definuje to, že každý měsíc se z této sumy emituje 1 miliarda mincí, tzn. že není tedy decentralizovaný z pohledu řízení a vývoje infrastruktury, ale síť samotná je decentralizovaná fungujíc na základě důvěryhodnosti uzlů. Zajímavý způsob, jak odrazovat od zbytečného spamování systému maloobjemovými transakcemi, je kombinace povinného držení 20 XRP pro umožnění přijmutí menších transakcí, než je právě 20 XRP, a transakční poplatky, které jsou ničeny po strhnutí daného podílu z transakce a slouží jako bariéra pro bezmyšlenkovité transakce s cílem zahlcení transakční kapacity sítě, ale tato deflační tendence nemá svým podílem valný vliv na objem dostupné kryptoměny. Navzdory značné centralizaci, XRP je stále velmi kolísavou záležitostí. Robustnost sítě, co kapacity týče, je představena v podobě 1500 transakcí za sekundu, které jsou potvrzené po 5 vteřinách. Pro srovnání v Bitcoinové síti je maximum transakcí za sekundu 7 a desetiminutová prodleva do vzniku nových bloků (FreeCoin.cz).

Dle Ripple.com rychlost odesílání včetně potvrzení transakcí dosahuje od 3 sekund.

Posledním významným hybatelem ve světě kryptoměn je **Ethereum**. Ethereum je virtuální stroj, respektive spíše globální decentralizovaný virtuální počítač pro obecné výpočty, tedy k využití i mimo převody digitálních kryptoměn mezi jednotlivými adresami uživatelů. Aplikace vytvořené pro fungování na Ethereu běží nad blockchainem, ze kterého si vzala infrastrukturu a jsou dle blockchainového protokolu naprogramovány, a využívají ho jako úložiště dat včetně uloženého kódu programu aplikací běžících na Ethereu. Mimo aplikace na

Ethereu nalezneme i vlastní kryptoměnu jménem **Ether** (ETH), jejímž prostřednictvím platí uživatelé těžařům za běh aplikací, kdy těžaři realizují výpočty sítě a jejich výsledky zapisují do samotného blockchainu. Nevýhodou sítě je, že výpočet se nedeleguje a všechny těžební uzly počítají totéž a rychlost výpočtu je v porovnání s distribuovaným výpočtem velmi nízká, ale zároveň síť se tím chrání a garantuje vysokou míru zabezpečení (Skalický & Stroukal,2018).

Síť Etherea je transparentní a pseudoanonymní jako BTC, která umožňuje vytvářet a zároveň ukládat tzv. smart kontrakty, které jsou elektronickou verzí smluv s nadefinováním podmínek a zároveň jejich vymáhání. Transakční poplatky se odvíjejí od velikosti transakce a její náročnosti zpracovat. Odměny z těžení se každé 4 roky půlí, ale finální počet mincí Etheru není stanoven a má tedy inflační tendence. Dělitelnost ETH je na 18 desetinných míst a vysoká kolísavost se této kryptoměně taktéž nevyhnula. Nejčastěji využívané smart kontrakty v síti jsou tzv. ICO, které v překladu znamenají prvotní nabídku mincí, což je veřejná sbírka, kde se vybírají příspěvky od přispívajících, kteří na oplátku získají tokeny projektu, kterého se sbírka týká, ve stanoveném poměru za poslané Ethery. Větší přešlap pro Ethereum byl projekt The DAO, který ztělesňoval pokus o decentralizovanou autonomní organizaci, který však skončil zneužitím chyby v kódu aplikace, čímž umožnil útočníkovi získat třetinu ze 11 milionů Etherů, což v tehdejším kurzu bylo 2,5 miliardy Kč, vybraných ve veřejné sbírce, která byla zdrojem financování projektu. Rozhodnutí společnosti Ethereum bylo ukradené peníze vrátit prostřednictvím hard forku, tedy nevratné modifikaci sítě, která nebude zpětně kompatibilní s původní verzí a oddělí se. Veškeré ukradené Ethery tak byly útočníkovi vzaty a uloženy do smart kontraktu se speciální adresou, kde se darované Ethery investorům vrátily za dané DAO tokeny. Nicméně část komunity Etherea byla proti a vytvořili druhou větev Etherea s názvem Ethereum Classic, která běží na původním blockchainu, kde útočník má svůj lup v podobě 3,6 milionů Etherů k dispozici (FreeCoin.cz).

Ethereum je unikátní jev, který má za cíl být cílem ostatních, to znamená býti platformou, která je otevřena všem návrhům prostřednictvím zmiňovaných smart kontraktů, které jsou zjednodušenou verzí smluv reálného světa, kdy strana A po akci strany B bude reagovat dle požadovaných podmínek stanovených v tomto kontraktu. Za poplatek v tomto prostředí můžete uzavřít tento kontrakt a pak stačí nalákat potencionální uživatele. Ethereum nabízí nejen svou technologii v osekané podobě svým kupcům, ale i provoz sítě smart kontraktu, který je v podstatě projektem, kdy strana A nabízí něco straně B a naprogramují se jednoduché interakce mezi těmito stranami, že když A udělá to, tak B reaguje takto. Provoz sítě je zajištěn těžaři,

kteří zajišťují plynulou existenci platformy a zároveň jsou odměňováni Etherem, což je kryptoměna Etherea, která se používá jako komunitní peníze.

Dalším příkladem může být článek Novotného, který se zaměřuje na kryptoměnový počin zakladetele energetické skupiny Amper Holdingu Jana Palasčáka a jeho ideu vytvoření virtuální měnu s emisními povolenkami CO2IN, která je založena na obchodu s emisními povolenkami bez zprostředkovatele přímo pro koncové uživatele. Dle slov Palasčáka by tato virtuální měna podnikům v kombinaci s úsporami energií či instalací bezuhlíkových zdrojů snížit svoji bilanci produkce CO2 na čistou nulu a města mohou pomocí placení CO2IN integrovat do svých aplikací (Novotný, 2020). Tato virtuální měna, která se dostupná prostřednictvím aplikace s funkcí prodeje či nákupu, je kryta reálnou hodnotou v poměru 100 CO2IN za 1 emisní povolenku a zároveň platí, že čím více se tyto virtuální tokeny budou používat, tím více emisních povolenek bude staženo z trhu a urychlí to modernizaci směrem nízkoemisní ekonomice včetně vedlejšího efektu, a to navyšování a udržování hodnoty těchto tokenů (Novotný, 2020).

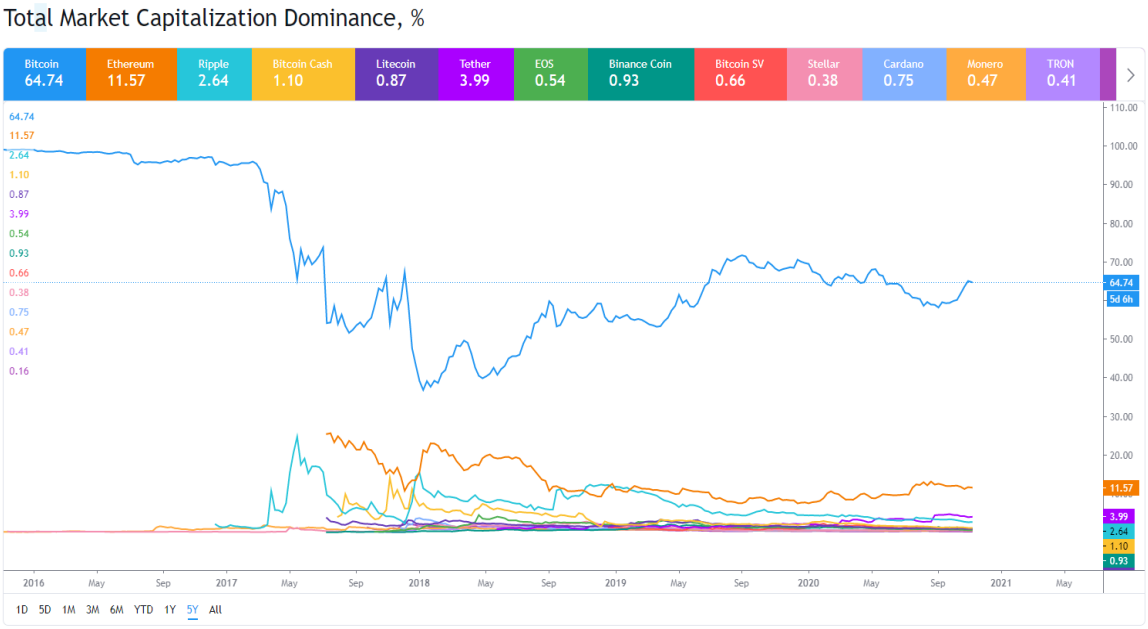
Prostřednictvím tzv. věštby, v angličtině oracle, je umožněn vznik tzv. smart contractů v daném prostředí a je to taková nadstavba nad blockchainem, která zprostředkovává interakce mezi blockchainem a reálným světem, tedy takový most. (ccco.cz).

Projekty běžící na tzv. oraclu, kde je základní popis vzniklého či vznikajícího smart kontraktu zajišťující nějakou službu, lze sledovat na stránkách defipulse.com. Tyto projekty dle DeFiPulse.com většinou běží, vyjma **Lightning Networku** fungujícím na blockchainu Bitcoinového protokolu, na oraclu Etherea, které prodává svou volnou kapacitu sítě blockchainu a umožňuje do sítě ukládat právě tyto projekty vzniklé veřejnými sbírkami, které vytvářejí smart kontrakty mezi investory a daným projektem (FreeCoin.cz).

DeFiPulse.com uvádí celkovou tržní kapitalizaci těchto smart kontraktů, která dosahuje výše 14,55 miliard USD, včetně dynamiky **DeFi** trhu a konkrétních projektů včetně kategorizace v podobě oblasti činnosti zaměřující se na kryptoměnové deriváty, platební platformy, směna projektových tokenů za konkrétní prostředky či na poskytování kryptoměnových půjček.

Jednou z takových stálých platforem s významnou aktuálně třetí největší tržní kapitalizací je Compound, která zprostředkovává uživatelům podílet na obchodu s kryptopůjčkami v různých kryptoměnách či tokenech (app.compound.finance). Compound je trh s půjčkami tokenů a kryptoměn, kde lákadlem pro investory je zúročení vložených

prostředků, které je aktualizované a viditelné v úvodní stránce a vložené kryptoměny či reálné prostředky, které si uživatel smění za dané tokeny či kryptoměnu, slouží jako zástava s tím, že si lze půjčovat jiné kryptoměny, ale v hodnotě menší, než je daná zástava, kdy daná výše je odvozena od volatility dané kryptoměny či tokenů (Dapp University, 2019).



Graf č.3: Tržní podíl kryptoměn na celkové kryptoměnovém trhu.

Dostupné zde: https://www.tradingview.com/markets/cryptocurrencies/global-charts/

Ether funguje jako komunitní měna v rámci platformy Ethereum, kdy tvůrce projektu (smart kontraktu) zakoupí za reálné peníze (většinou americké dolary či eura) v aktuálním kurzu Ethery, které umožní zaplacení za vytvoření projektu v prostředí Etherea a následné naprogramování projektu, kde stanovíme, co chceme, aby se dělo, když uživatel se účastní daného projektu. Aby nebyl projekt pro nic za nic, vytvoří se veřejná sbírka, kam může zájemce přispět na vytvoření daného projektu reálnými penězi či Ethery a tím tvůrce projektu zjistí potencionální poptávku po daném projektu a v případě nezájmu či nevybrání požadované částky ve veřejné sbírce se prostředky vrátí na odchozí účet potencionálních zájemců o kontrakt. Po vybrání a spuštění projektu se platí za provoz těžařům sítě prostřednictvím Etherů. Vše je nadefinováno. Výše uvedené příklady jsou jen výčtem mnoha projektů, které jsou v činnosti, ale více než u kryptoměn samotných zde platí, že kolísavost životaschopnosti projektů je mnohonásobně větší než u kryptoměn samotných, neboť ty aspoň existují, protože existují z recese či z jiného důvodu: decentralizace a další, ale zde je velký počet podvodných projektů, které mají za úkol ze zájemců vysát peníze a následně se uvrhnout do tiché neaktivity.

Dění na platformě Ethereum lze připodobnit k divokému západu v období zlaté horečky, neboť kontrakt něčím osloví zájemce – například jako vize pana Palasčáka s uhlíkovými

poukázkami či tokeny. Člověk si nakoupí za Ethereum dané poukázky s tím, že je bude chtít využít směnit za emisní povolenky, které by měli mít autorizovanou certifikaci a tak dále. Jenomže právě zde je kámen úrazu, kdy spousta projektů je aktivních do doby uvedení do provozu a nakoupení těchto poukázek/tokenů či derivátů (sub)komunitních peněz a následně se projekt odmlčí ve smyslu, že zmizí z nabídky, kontrakt je vadný a dále. O těchto úskalích tzv. DeFi neboli decentralizovaných financí je právě video (videa) Dapp University, kde alespoň je přítomna kritická stránka těchto projektů, sice v malém měřítku, ale navzdory všudypřítomnému entuziasmu rozptýleném v celém segmentu kryptoměn či decentralizovaných financí se i toto malé množství reflexe počítá.

Kryptoměnový svět a jeho směnná interakce funguje vesměs pouze v elektronickém světě díky internetu, který spojuje jednotlivé aktéry napříč celým světem. Kdokoliv, kdo má účet a je tím pádem vidět v ekosystému dané kryptoměny, která má pseudoanonymní transparentnost, je schopen přijímat a odesílat platby v kryptoměnách. Každý systém se liší v menším či větší míře, ale princip zůstává stejný. Těžba se zároveň podílí na směně a směna na těžbě. Těžaři v případě decentralizovaného systému ověřují transakce k potvrzení s tím, že čím větší počet potvrzení daná transakce vyžaduje, tím je bezpečnější a zároveň uvolní nové mince z naprogramovaného protokolu, který je danými mincemi obdaruje přímo či si jej těžaři rozdělí ve sdružení těžařů nazývající se poolem. Tímto způsobem se uskutečňuje emitence nových mincí v decentralizovaném systému blockchain.

Směna krypt je skrze klasický převod jako v případě toho bankovního, kdy aktéři pouze musejí znát název účtu toho druhého pro uskutečnění transakce, ale taktéž je možné pomocí QR kódu. Ten je schopen uskutečnit okamžitou transakci pomocí obrazce na digitálním přístroji jako je například tablet, chytrý mobilní telefon, chytré hodinky či prostřednictvím vytisknutí QR obrazce na papír obsahující kód, který obsahuje určitou informaci či jejich soubor a prostřednictvím daného souboru obsahující data je možné převést kryptoměnové mince z účtu na účet (Kaliský, 2018). Na co kryptoměny naráží je složitá směnitelnost, kdy například BTC je uplatnitelný vzhledem k nejdelší historii nejvíce a obchody přijímají tuto kryptoměnu nejvíce, ale stále se nejedná o bezproblémovou, a tedy okamžitou likviditu. Odpadlík od Bitcoinu Bitcoin Cash je celosvětově směnitelný pouze u 5000 obchodních prodejců, což vůči celkovému poměru, který uvádí Datapo, je zanedbatelné, neboť ten čítá na 200 milionů podniků celosvětově.

Taktéž u některých kryptoměn se nejedná o stabilní projekty, které mají reálný cíl nabízet alternativu ke klasické měnové soustavě. To samozřejmě poškozuje reputaci celého segmentu

včetně toho, že vzhledem k neexistující autoritě neexistuje domáhání se pojištění svých vkladů v dané peněžence spravující několik Vámi vlastněných účtů a v případě odcizení těchto prostředků a následné jejich využití pachatelem již nelze tyto prostředky získat zpět, ovšem za předpokladu, že peněženka se nachází na Vámi spravovaných platformách. Pokud se peněženka ovšem nachází na platformách spravujících třetí stranou, to znamená například investiční společnost, burza či různé platformy, které se zálohují na servery kdekoliv po světě jako je tomu například u cloudových služeb, které nevyžadují fyzickou instalaci aplikace či souboru přes který se uživatel dostane do správy svých prostředků kdekoliv a kdykoliv na světě s dostupným internetovým připojením. V případě fyzické instalace má reálně větší kontrolu nad uložením dat a jejich správou, tzn. že je i menší šance vystavení se většího rizika, ale zase na druhou stranu následně není po kom vymáhat odcizené či ztracené prostředky v případě ztráty hlavního klíče do peněženky.

Důvěryhodnost nepřidává ani fakt, že dle DiscoverDash.com, což je domovská webová stránka kryptoměny Dash, která se zasazuje o to, aby byla co možná nejvíce anonymní kryptoměnou na kryptoměnovém trhu, udává, že možné uplatnění této kryptoměny je zejména ve Venezuele, která předčila Spojené státy, a následují Kolumbie, Rakousko a Nigérie, která má více uplatnění v hlavním městě Niger než celé Německo a Velká Británie dohromady.

3. Kryptoměna WAT

Aby se kryptoměna mohla stát světovou, je třeba aby obstarávala stejné funkce jako světové peníze, které dokáží obsloužit směnnou interakci kdekoliv na světě. Světové peníze mají stejné funkce jako funkce národních měn, ale s tím rozdílem, že jsou toho schopny na globální úrovni. Peníze jsou dle Technické univerzity v Liberci uchovatelem hodnot, měřítkem hodnot, prostředkem směny a prostředek úhrady odložených plateb, čímž se myslí úvěry a dluhy. Světové peníze by měli mít své výsadní postavení na globálním trhu buď díky své dlouhodobé pozitivní historii, ve které se vložená důvěra více či méně nevymstila a zachovala si svou dominantní pozici anebo prostřednictvím směnitelnosti za vzácný kov, a to se tedy bavíme o standardu v návaznosti na vybraný vzácný kov. Jelikož kryptoměna dlouhodobou a důvěryhodnou historii nemá, alespoň pro všeobecnou veřejnost, tak cesta skrze, v tomto případě zlatý, standard by byla vhodnější volbou pro získání důvěryhodnosti a částečnou evokací reálného obrazu měny jako digitální zlato. Nadstavbou důvěry by byla centralizace pod záštitu Světové banky, která by emitovala a kontrolovala oběh kryptoměny WAT.

Zlato by bylo shromažďováno Světovou bankou centralizovaným způsobem tak jako tomu bylo u podobného návrhu s názvem E-Gold v publikaci Skalického a Stroukala, kdy zlaté devizy jsou fyzicky drženy. V tomto případě by bylo možné nakoupit WAT v jakékoliv měně danou částkou, která odpovídá trojské unci zlata čili lehce přes 31 gramů tohoto zlatého kovu. Zároveň je nutné zdůraznit, že manipulaci a nákup pouze skrze lokace s dostupností internetového připojení, což digitální prostředí tohoto rázu bez návaznosti na internetu prozatím není veřejně dostupná či neexistuje. Emitence „zlatých mincí“ kryptoměny WAT bude mít deflační tendenci, neboť bude dán určitý počet mincí, který bude konečný a emitence se bude uvolňovat dle zájmu s tím, že dostatečná dělitelnost daných mincí zajistí hladký průběh ve směnné transakci v případě nedostatku mincí v důsledku enormního zájmu. Počet mincí by zahrnoval 1 bilion kusů, které by mohly být dělitelné až na svou šedesátičtyřtinu. Teoreticky by tedy bylo zapotřebí 31,33 bilionu gramů investičního zlata, což odpovídá 313,3 milionů tun zlata, které na planetě zatím nejsou k dispozici, ale připomínám, že toto je pouze nástin toho, jak by mohla kryptoměna fungovat ve stylu, aby zastávala funkci světových peněz. Kryptoměnu bude možné nakoupit pouze skrze online směnárnu, která bude provozována Světovou bankou. Transakce by byly šifrovány, ale samotný účet by byl sumou rodného čísla a státní příslušnosti, tzn. že by byl pseudoanonymní a uživatel dohledatelný s jistou dávkou úsilí. Bezpečnost transakce by zajišťovalo potvrzování na důvěryhodnosti uzlů, tzn. nejednalo

by se o blockchain a klíčové uzly potvrzující transakce by byly představovány samotnou Světovou bankou.

Stabilita a důvěryhodnost by teoreticky byla tímto zajištěna a tím by se mohlo usnadnit zastání funkce uchovatele hodnot a funkci směnného prostředku, což by připoutalo osoby a firmy nabízející produkty a služby, které by umožnili akceptování této kryptoměny. Tím by se tato kryptoměna měla vyhnout tomu, že by byla vnímána jako komodita, neboť její přijímání bude jednoduché skrze internetové bankovnictví, které bude dostupné na chytrých hodinkách, telefonech, tabletech a obecně na všech zařízeních, které jsou připojeny k internetu a umožňují verifikaci uživatele pro potvrzení uživatele. Uživatel by tedy měl bankovní účet vyhrazenou pouze na kryptoměnu WAT registrovaný přímo u Světové banky, ze kterého by bylo možné utrácet danou kryptoměnu u příjemců této platby s tím, že v ideálním případě by se odstranila potřeba směnáren do cizích měn, neboť by existovala jedna světová měna, která by dokázala obsloužit po celém světě jakoukoliv směnnou interakci. Samozřejmě by se to odvíjelo od dostupnosti internetu a přívětivému uživatelskému prostředí internetového bankovnictví a samotnému uskutečnění plateb.

Závěr

Zdá se, že první generace kryptoměn dosahuje povahy komodity, která jistým způsobem likvidní je, ale ne natolik, aby se mohla nazývat měnou, spíše komunitními kvazipenězi s tržní kapitalizací přes půl bilionu amerických dolarů k 12.12. 2020 ve 2:00 dle CoinMarketCap.com a s extrémně vysokou volatilitou, a tedy i velkou predispozicí podléhat spekulacím. Dále je nutno vnímat riziko decentralizace a autonomie ekosystému jménem blockchain, kdy se není na koho odvolat v případě ztráty přístupových údajů k účtu či rovnou ztráta přístupu do peněženky. Tato ztráta je nevratná a s penězi již nikdo nebude manipulovat, pokud daný účet či peněženka nebudou vykradeny.

Druhá generace je o poznání propracovanější, co se cíle dané kryptoměny týče, neboť zde jsou výstižné projekty Ripple a Ethereum. Ripple se snaží zefektivnit mezibankovní přesuny kapitálu a je určená výhradně na mezibankovní transfery s tím, že reaguje na požadavky bank a úzce s nimi spolupracuje na zefektivňování této služby. Ethereum je naopak skvělý business plán poskytující platformu za příslušné poplatky pro ostatní projekty skrze smart kontrakty, kde se využívá ethereová kryptoměna Ether, která slouží jako komunitní peníze zejména uvnitř tohoto systému. Decentralizované finance vázané až na pár výjimek na síť Etherea mají navzdory velkým ambicím i velkou nevýhodu, a to fixování na soukromou firmu, která může kdykoliv skončit a její platforma s ní. Dále, dle mého názoru, je problematické i případné realizování styku mezi státními či nadnárodními institucemi a samotných projektů, které by umožňovaly nákupy daných tokenů či poukázek na danou službu či produkt nabízenou konkrétním projektem. Problém vidím v tom, že tento trh je i oproti kryptoměnám velice mladý a přitahuje podvodné projekty, které okrádají potencionální zájemce o peněžní prostředky, čímž se snižuje důvěryhodnost nejen projektu samotného, ale vzhledem k době existence a nestálého počtu projektů s nejistým výsledkem, důvěryhodnost klesá. Dále vidím problém v monopolizaci poskytování platformy pro projekty decentralizovaných financí, což je pochopitelné vzhledem k nízkému stáří tohoto systému, ale zároveň to taky nevybízí k vyšší důvěryhodnosti, čemuž odpovídá pouze 13 miliardová tržní kapitalizace dle DeFiPulse.com.

Skalický a Stroukal uvádějí, že státní peníze jsou vytvořené ze vzduchu komerčními bankami včetně toho, že vnitřní hodnoty národních měn jsou nula. Jsou tedy kryptoměny na tom lépe? Vše nasvědčuje tomu, že ne a přesvědčuje o opaku, neboť u národních měn je záštita státního aparátu a finančních institucí, které nějakým způsobem spravují danou měnu. Národní měny lze použít i mimo internet v hotovostní podobě a v případě ztráty přístupových údajů je možno na základě identifikace totožnosti ke svým prostředkům se dostat a nadále je využívat.

Paradoxně mi připadají ze vzduchu kryptoměny, které mají v lidské historii nevídanou kolísavost měnící se každých 5 sekund s tím, že lze očekávat růst či propad v procentech, ale také i o několik desítek procent, což není žádnou výjimkou. Vytvořené jsou komunitou či soukromou firmou a buď tedy síť je spravována danou firmou vlastnící většinu sítě či její celek anebo správci, kteří jsou nějakým způsobem vybráni. Netvrdím, že tento fenomén nemá potenciál, má a velký, ale spíše mne zaráží, že i odborná část komunity mluví o kryptoměnách jako o konkurenci národním měnám, což rozhodně není pravda. Vzhledem i k tomu, jak jsou národní měny lehce směnitelné a jednoduché oproti světu kryptoměn či decentralizovaných financí. Je nutno být realistický a přiznat si, že o kryptoměnách by se jako o měně nikdy nikdo nezmínil nebýt jedné transakce za 2 pizzy. Vnímám to jako nafukovanou iluzi, která se rozplyne až velcí investoři budou chtít vybrat své vklady a dominový efekt způsobí, že většina investorů bude hledat přijatelnou hranici ztráty svých investic. Kryptoměny se tedy prozatím nezdají penězi, natož světovým směnným prostředkem. Budoucnost vidím ve fúzi centrálního systému s kryptoměnovým světem tak, aby si ideálně z obou světů vzal největší část toho dobrého.

Prameny

Bankovnictví-Finance.studentské.eu. *Bankovnictví, finance – studium: 2. Měna a měnová soustava.* Dostupné zde: http://bankovnictvi-finance.studentske.eu/2010/03/2-mena-menove-soustavy.html

BitcoinCash.org (2020). *„Where can I spend Bitcoin Cash?“.* Dostupné z: https://www.bitcoincash.org/spend-bitcoin-cash/

BitCoinPizzaIndex.net (2020). *„Homepage“.* Dostupné z: https://bitcoinpizzaindex.net/

Compound (2020). *„Homepage“.* Dostupné z: https://app.compound.finance/

CoinMarketCap (2020). *CoinMarketCap: Charts*. Dostupné z: https://coinmarketcap.com/charts/

CzechCryptoCompany.cz (2020). *„Slovníček kryptoměnových pojmů.“*. Dostupné z: https://www.ccco.cz/slovnicek-kryptomenovych-pojmu/

Dapp University (2019). *„What is decentralized finance (DeFi)?“*. Dostupné z: https://www.youtube.com/watch?v=Nkx0r9R0Krk

Datapo.com (2020). *Datapo: News: How many companies are there in the world?.* Dostupné z: https://datapo.com/news/how-many-companies-are-there-in-the-world/

DeFiPulse.com (2020). *„Homepage“.* Dostupné z: https://defipulse.com/

Ducháček, J. (3.8.2020). *Čnb.cz: Jak je to s hotovostí aneb Česko s bankovkami a mincemi.* Dostupné zde: https://www.cnb.cz/cs/o_cnb/cnblog/Jak-je-to-s-hotovosti-aneb-Cesko-s-bankovkami-a-mincemi/

Dvořák, M. (29.10.2019). *Kurzy.cz: Bitcoin prohnaný rakouskou školou.* Dostupné zde: https://www.kurzy.cz/zpravy/517686-bitcoin-prohnany-rakouskou-skolou/

FreeCoin.cz (2020). *„O kryptoměnách“.* Dostupné z: https://www.freecoin.cz/okryptomenach#

FXstreet.cz (2020). *FXstreet.cz: Forex slovník pojmů: Spekulant.* Dostupné zde: https://www.fxstreet.cz/forex-slovnik-pojmu+spekulant.html

Hanusová, J. (6.1.2017). *Roklen24.cz: Rakouská škola: Centrální banka, vrchol finanční moudrosti?.* Dostupné zde: https://roklen24.cz/rakouska-skola-centralni-banka-vrchol-financni-moudrosti/

Holanová, T. (19.8.2013). *Zprávy.Aktuálně.cz: Bitcoin jsou peníze, rozhodlo Německo o virtuální měně.* Dostupné zde: https://zpravy.aktualne.cz/ekonomika/svetova-ekonomika/bitcoin-jsou-penize-rozhodlo-nemecko-o-virtualni-mene/r~45b1943008d411e3a6c60025900fea04/

Kaliský, B. (2018). *Bitcoin a ti druzí: Nepostradatelný průvodce světem kryptoměn.* IFP Publishing, s.r.o.

Kurzy.cz (2020). *Kurzy.cz. Bitcoin – Kurz BTC/Bitcoin.* Dostupné zde: https://www.kurzy.cz/bitcoin/

InvesticniWeb.cz (25.11.2014). *Investicniweb.cz: Proč je dolar nejmocnější měnou na světě.* Dostupné zde: https://www.investicniweb.cz/2014-11-25-proc-je-dolar-nejmocnejsi-menou-na-svete/

InvesticniWeb.cz (4.11.2014). *Investicniweb.cz: Keynesiánci vs. rakouská škola: Kdo má pravdu?*. Dostupné zde: https://www.investicniweb.cz/2014-11-4-kdo-ma-pravdu-keynesianci-nebo-rakouska-skola/

Skalický, J. & Stroukal, D. (2018). *Bitcoin a jiné kryptopeníze budoucnosti*. Praha: Grada Publishing.

Kindleberger, Ch. P. (1978). *Světová ekonomika.* Praha: Academia.

Klofáč, O. (10.9.2020). *"Konzultace u kryptospecialisty"*. Praha: 2020.

Lánský, J. (2018). *Kryptoměny.* Praha: C.H.Beck.

Lazarevič, A. (20.1.2014). *Měšec.cz: Finsko: Bitcoin není měna, ale komodita.* Dostupné zde: https://www.mesec.cz/aktuality/finsko-bitcoin-neni-mena-ale-komodita/

Němeček, E. (1967). *Teorie měnových kursů v kapitalistické měnové soustavě.* Praha: Československá akademie věd – Academia.

Novotný, J. (17.9.2020). *UHLÍKOVÉ MINCE. PALAŠČÁK SPUSTIL KRYPTOMĚNU KRYTOU EMISNÍMI POVOLENKAMI. Euro.cz.* Dostupné z: https://www.euro.cz/kryptomeny/uhlikove-mince-palascak-spustil-kryptomenu-krytou-emisnimi-povolenkami

Patria.cz. (31.7.2020). *Kurzy.cz: Goldman Sachs: Dolar by mohl přijít o status světové rezervní měny.* Dostupné zde: https://www.kurzy.cz/zpravy/552849-goldman-sachs-dolar-by-mohl-prijit-o-status-svetove-rezervni-meny/

Ripple.com (2020). *„RippleNet“.* Dostupné z: https://ripple.com/ripplenet/

Roklen24.cz (

Simmel, G. (1997). *Peníze v moderní kultuře a jiné eseje*. Praha:SLON.

Simmel, G. (2011). *Filosofie peněz.* Praha: Academia.

Sychra, Z. (2009). *Jednotná evropská měna: Realizace hospodářské a měnové unie v EU.* Brno: MU: Mezinárodní politický ústav.

Technický ústav v Liberci. *TU v Liberci. 1 Základní pojmy peněžní ekonomie.* Liberec: Technický ústav v Liberci. Dostupné zde: https://turbo.cdv.tul.cz/file.php/5/data/texty/kap_01.pdf

Wolf, V. (20.11.2016). *Lidovky.cz: Místo bankovek digitální ekrona? Švédsko chce do dvou let zavést elektronické peníze.* Dostupné zde: https://www.lidovky.cz/byznys/moje-penize/svedsko-jako-prvni-zeme-na-svete-zvazuje-zavedeni-digitalni-meny-v-cesku-se-nic-takoveho-nechysta.A161119_135515_moje-penize_ELE