Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra ekonomických teorii

Bakalářská práce

Kryptoměny: porovnání výkonu a faktory úspěchu Bitcoinu a Etherea

Marek MACH

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Marek Mach

Podnikání a administrativa

Název práce

Kryptoměny: porovnání výkonu a faktory úspěchu Bitcoinu a Etherea

Název anglicky

Cryptocurrencies: performance comparison and factors of success of Bitcoin and Ethereum

---

Cíle práce

Na základě výzkumu vývoje poptávky a nabídky po kryptoměnách, názoru veřejnosti a medializace, posouzení vlivu politických změn na vývoj, změn vládních regulací kryptoměn, a změny pravidel samotných těžařů a následnému "forku" a studia odborné literatury zhodnotit vývoj a faktory úspěchu Bitcoinu a Etherea, formulace vývoje trendové funkce v období od vzniku až po současnost BTC a ETH – trendová složka, periodická složka a náhodná složka, rizika a příležitosti investic do kryptoměn, posouzení rizik a bezpečnosti, posouzení investičního a technologického potencionálu na základě analýzy statistických dat a určení vlivu nezávislých proměnných na kryptoměny.

Metodika

Průzkum a názor populace pomocí dotazníkového šetření. Analýza vývoje Bitcoinu a Etherea statistickými metodami pomocí indukce, jejich komparace, analogie, měření výkonu a následné zobrazení výsledků do grafů a tabulek. Generalizace Bitcoinu a Etherea a komparace jejich vlastností s jinými kryptoměnami. Studium odborné literatury a definice pojmů. Pozorování vývoje poptávky a nabídky po kryptoměnách, vlivu politických změn na vývoj a změn vládních regulací a investice do kryptoměn. Posouzení rizik, bezpečnosti, příležitostí a investičního potencionálu kryptoměn na základě analýzy statistický dat. Na základě výzkumu určení vlivu nezávislých proměnných na kryptoměny. Abstrakce vlastností Bitcoinu a Etherea a následná konkretizace vlastností.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

Aktiva, Bitcoin, Blockchain, Budoucnost, Decentralizace, Ethereum, Investice, Kryptoměna, Výkonnost, Vývoj

---

Doporučené zdroje informací

HARTMAN, O. – FXSTREET (FIRMA). *Začínáme na burze : jak uspět při obchodování na finančních trzích: akcie, komodity, forex a kryptoměny.* Brno: BizBooks, 2018. ISBN 978-80-265-0780-2.

HOSP, J. Kryptomeny Bitcoin, Ethereum, Blockchain, ICO and Co. jednoducho a zrozumiteľne, 2018. ISBN 978-80-222-0945-8

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

LÁNSKÝ, J. *Kryptoměny.* V Praze: C.H. Beck, 2018. ISBN 978-80-7400-722-4.

MUNOZ, J M. – FRENKEL, M. The Economics of Cryptocurrencies, 2021. ISBN 978-0-367-1910-0

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

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. David Křížek

Garantující pracoviště

Katedra ekonomických teorií

Elektronicky schváleno dne 29. 12. 2021

doc. PhDr. Ing. Lucie Severová, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 8. 2. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 15. 03. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Kryptoměny: porovnání výkonu a faktory úspěchu Bitcoinu a Ethereu" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2022 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu bakalářské práce panu Ing. Davidovi Křížkovi za jeho ochotu a trpělivost. Také bych rád poděkoval všem svým přátelům, kteří mě podporovali a motivovali k napsání mé bakalářské práce.

Kryptoměny: porovnání výkonu a faktory úspěchu Bitcoinu a Etherea

Abstrakt

Tématem bakalářské práce je analýza dat a cenového vývoje Bitcoinu a Etherea, porovnat jejich vlastnosti, využití a rizika. Dílčím cílem je zhodnocení vývoj a faktory úspěchu těchto kryptoměn, a to na základě výzkumu vývoje poptávky a nabídky. Dále zhodnocení vývoje podle názoru veřejnosti a medializace. Bude posuzován i vliv politických změn na vývoj, změn vládních regulací kryptoměn, a změny pravidel samotných těžařů.

Dalším dílčím cílem bude i zhodnocení následného "forku" a studium odborné literatury. V praktické části bylo vysvětlen a v grafech a tabulkách popsán cenový vývoj kryptoměn Bitcoin a Ethereum. Nejdříve byl popsán cenový vývoj Bitcoinu, poté Etherea. Byly zde popsány nejdůležitější události, které stály za změnou ceny těchto kryptoměn. Tyto cenové výkyvy byly v řádu několika procent, ale také byly popsány změny, kde se cena změnila např. o 10 000 %.

Bylo zjištěno, že na cenu měla vliv především medializace a regulace ze strany úřadů a vlád jednotlivých kontinentů a států, jako např. Evropa, Spojené státy americké nebo Čína. Vliv na cenu měly ale také forky, kterých proběhlo za vývoj kryptoměn hned několik.

Klíčová slova aktiva, bitcoin, blockchain, budoucnost, decentralizace, ethereum, investice, kryptoměna, výkonnost, vývoj

Cryptocurrencies: performance comparison and factors of success of Bitcoin and Ethereum

Abstract

The topic of the bachelor thesis is the analysis of data and price development of Bitcoin and Ethereum, to compare their features, use and risks. A partial goal is to evaluate the development and success factors of these cryptocurrencies, based on research into the development of demand and supply. Furthermore, evaluation of development according to public opinion and media coverage. The impact of political changes on development, changes in government regulations for cryptocurrencies, and changes in the rules of the miners themselves will also be assessed.

Another partial goal will be the evaluation of the subsequent "fork" and the study of professional literature. In the practical part, the price development of the cryptocurrencies Bitcoin and Ethereum was explained and described in graphs and tables. The price development of Bitcoin was described first, then Etherea. The most important events behind the change in the price of these cryptocurrencies were described here. These price fluctuations were in the order of several percent, but changes were also described where the price changed, for example, by 10,000%.

It was found that the price was mainly influenced by media coverage and regulation by the authorities and governments of individual continents and states, such as Europe, the United States or China. However, the price was also influenced by the forks, which took place during the development of several cryptocurrencies.

Keywords: assets, bitcoin, blockchain, future, decentralization, ethereum, investment, cryptocurrency, performance, development

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

Dolar – Americký dolar (USD)
P2P – Peer to Peer
BTC – Bitcoin
BCH – Bitcoin Cash
ETH – Ethereum
NFT – Non-fungible token
ETF – Exchange Traded Fund (Veřejně obchodovaný fond)
ICO – Initial Coin Offering
FOMO – Fear of Missing Out
FUD – fear, uncertainity and doubt
ATH – all time high
DAPPS – Decentralized Applications
MB – Megabyte

1. Úvod

Tato práce se věnuje investicím, jejich historii a následné navázání na nejaktuálnější formu investice – kryptoměny, přesněji Bitcoin a Ethereum. Pozornost se bude ubírat k počátkům kryptoměn, jejich vlastnostem, využití, faktorům, které stály za jejich úspěchem, efektivnosti, dopadům na finanční trh a také jejich historické a současné výkonnosti. Budou zde popisovány vlastnosti Bitcoinu a Etherea, které budou následně porovnávány mezi sebou a z toho budou vyvozeny specifické funkce, kterými se od sebe tyto dvě kryptoměny liší. Bude zde popsána mechanika kryptoměn a celkový způsob, jakým fungují, cestu, kterou se dají pořídit a také různé druhy vlastnictví kryptoměn.

Budou zde znázorněny výkonnostní grafy obou kryptoměn od jejich vzniku až po současnost a tabulky porovnávající Bitcoin a Ethereum, jejich ceny v průběhu let a změny, kterými si prošly nebo aktuálně prochází. Popsány budou i rizika spojené s investováním do kryptoměn, které jsou často výraznější než jakékoliv jiné investice. Budou zde formulovány výrazy a terminologie týkající se kryptoměn a zároveň i finančního trhu. Práce se bude zabývat i bezpečností kryptoměn při jejich nákupu a prodeji, riziku při jejich uschování na různých platformách a jakým způsobem se dá proti rizikům bránit a využití při platbách zboží a služeb, anebo transakcí mezi osobami, které jsou navzájem úplně neznámé, oproti platbám mezi zákazníkem a obchodníkem, kdy zákazník ví základní informace o obchodníkovi.

Budou zde popsány výhody a nevýhody decentralizovaného světa a tím pádem i decentralizované sítě, ve které se kryptoměny nachází, a čím se odlišuje od dnešního centralizovaného světa. Popsána bude i budoucnost Bitcoinu a Etherea, které je stále nejasná, jejich technologický vývoj, který nadále pokračuje, důvod vzniku kryptoměn a jejich smysl. Práce se bude věnovat i okolí Bitcoinu a Etherea, a to firmám, bankám a skupinám lidí, kteří nejsou jen fanoušky kryptoměn, ale i průkopníky v této oblasti nebo analytiky, kteří zkoumají jejich vývoj, případně jsou sami zapojeni do jejich samotného vývoje.

S tím jsou spojena již zmíněná rizika, která jsou bez důkladné a dlouhodobé analýzy významná, a mohou tak být pro mnoho investorů odrazující. I přes to se může s rezervou říct, že se jedná o možnost, jak zhodnotit své finanční prostředky, byť velmi rizikovou. Nicméně je obtížnější investovat do určité „věci“, která i přes to, že má hodnotu několika milionů dolarů, má krátkou historii na finančním trhu a zatím tak nebudí dojem, že by měla nahradit již dlouhodobě zavedené finanční nástroje, které tuto historii mají.

2. Cíl práce a metodika

2.1 Cíl práce

Hlavní cíl práce je definovat kryptoměnu Bitcoin a Ethereum, porovnat jejich vlastnosti, využití a rizika. Dílčím cílem je zhodnocení vývoj a faktory úspěchu těchto kryptoměn, a to na základě výzkumu vývoje poptávky a nabídky. Dále zhodnocení vývoje podle názoru veřejnosti a medializace. Bude posuzován i vliv politických změn na vývoj, změn vládních regulací kryptoměn, a změny pravidel samotných těžařů. Dílčím cílem bude i zhodnocení následného "forku" a studium odborné literatury.

Bude zde formulace vývoje trendové funkce v období od vzniku až po současnost BTC a ETH. Ta obsahuje trendovou, periodickou a náhodnou složku. Bude zde zhodnocena rizika a příležitosti investic do kryptoměn a bezpečnosti. Bude zde posouzen investiční a technologický potencionál kryptoměn. Na základě analýzy statistických dat následné určení vlivu nezávislých proměnných.

2.2 Metodika

Průzkum a názor populace bude proveden pomocí dotazníkového šetření, kde bude zjišťováno povědomí o kryptoměnách, jejich účelu a použití. Analýza vývoje Bitcoinu a Etherea statistickými metodami pomocí indukce, jejich komparace, analogie, měření výkonu a následné zobrazení výsledků do grafů a tabulek. Generalizace Bitcoinu a Etherea a komparace jejich vlastností s ostatními kryptoměnami. Bude využito studium odborné literatury a definovány pojmy spojené s touto problematikou.

Bude provedeno pozorování vývoje poptávky a nabídky po kryptoměnách, vlivu politických změn na vývoj a změny vládních regulací a investice do kryptoměn. Dále bude posouzena rizika, bezpečnost, příležitosti a investiční potencionál kryptoměn na základě analýzy statistický dat. Na základě výzkumu bude určen vliv nezávislých proměnných na kryptoměny. Poté bude provedena abstrakce vlastností Bitcoinu a Etherea a následná konkretizace vlastností.

3. Teoretická východiska

Úvodní kapitola je věnována definici kryptoměnám, blockchainu a investicím. V rámci podkapitol se práce zabývá porovnáním Bitcoinu a Etherea. Dále se zaobírá faktorem úspěchu daných kryptoměn a porovnává jejich výkonnost.

3.1 Kryptoměny

„Kryptoměna je typ virtuální měny využívající ke své výrobě i k platebním transakcím síť počítačů individuálních uživatelů, kteří dávají k dispozici část výkonu svého počítače připojeného k internetu.“ (Kurz.cz)

Kryptoměny nejsou zhmotněné, nemůžeme je fyzicky vlastnit, oproti mincím nebo bankovkám, které nesou určitou hodnotu některé z měn, jako je euro nebo dolar. Je to systém, který nepotřebuje centrální autoritu a dosahuje distribuované shody o jeho stavu, ukládá se v něm přehled o jednotkách a vlastnictví daných kryptoměn. *„Vlastnictví jednotek kryptoměny se prokazuje výhradně kryptograficky“* (Kaliský, 2018, s. 3)

Tento systém také definuje, zda mohou vznikat nové jednotky kryptoměny a pokud ano, systém definuje podmínky jejich vzniku a způsob, jakým se určí vlastnictví nových jednotek. Díky tomuto systému je možné provádět transakce, *„ve kterých dochází ke změně vlastnictví jednotek kryptoměny“* (Stroukal, 2021, s. 3) a pokyn k transakci může provést pouze objekt, který se prokáže aktuálním vlastnictvím těchto jednotek. V případě, že jsou současně zadány dva odlišné pokyny ke změně vlastnictví stejných jednotek kryptoměn, tak systém vybere nejvýše jeden z těchto dvou pokynů.

Kryptoměny mají tu nevýhodu, že je jejich hodnota se odvíjí od reputace, kterou mezi lidmi mají, což znamená, že by při snaze o centralizaci nebo znehodnocení významné kryptoměny mohl být ohrožen finanční trh. Pro kryptoměny platí, že čím více je systém decentralizovaný, tím je bezpečnější, protože se sníží míra rizika, *„že se nějaké entitě podaří porušit některou z ostatních podmínek“* (Lánský, 2018, s. 4), které kryptoměny mají. *„V současné době je na známých webových stránkách uvedeno přes 5 000 "kryptoměn"“* (Munoz, 2020)

3.1.1 Blok a blockchain

Jakýkoliv systém má svoji strukturu, a tak je tomu i u bitcoinu. Systém bitcoinu se skládá z jednotlivých bloků (blocků), které jsou spojené v soustavu těchto bloků a tím je blockchain. Blok je základní jednotkou blockchainu – ten označuje více věcí.

Může to být veřejný zápis bitcoinových transakcí, datová struktura, kterou používají i jiné kryptoměny a databáze, systém, jenž ukládá data do veřejné i neveřejné databáze s různou úrovní decentralizace a svobodnému postoji k danému systému.

Avšak blockchain bitcoinu je *„speciální druh distribuované, decentralizované databáze“* (Kaliský, 2018, s. 39), uchovávající záznamy, které se neustále rozšiřují a jsou chráněny proti neoprávněným zásahům z vnější strany. Údaje v blockchainu nelze mazat ani měnit, taktéž samotný blockchain je extrémně obtížné změnit nebo manipulovat. Proto je vhodný na specifické úkoly (evidenci vlastnictví, transakcí, smluv), kde je bezpečnost nadřazená rychlosti, energetické náročnosti a pružnosti.

Čím více uzlů je pod správou blockchainu, tím je blockchain bezpečnější. S větší bezpečností se však zvyšují energetické nároky pro chod sítě, protože všechny uzly dělají tu stejnou činnost, i když to není zrovna potřebné. Její rychlost se tím však nezvyšuje. Je možné *„si blockchain stáhnout a přepsat v něm údaje“* (Kaliský, 2018, s. 39), avšak je nutné přesvědčit další tisíce uzlů, aby přepsanou verzi uznaly. Uzly přepsanou verzi srovnají se svou, zjistí, že se verze neshodují a odmítnou ji přijmout. Chráněny jsou i samotné uzly peer-to-peer sítě. Blockchain je vlastně „kniha“ a blok jedna strana této „knihy“. Nelze určit přesný počet uzlů v bitcoinové síti, protože je majitelé mohou schovat.

Transakce je *„informace o převodu bitcoinů z určité adresy na adresu jinou.“* (Stroukal, 2021, s. 49). Taktéž je to datová struktura, která obsahuje vstupy a výstupy. Výstup zde znamená množství bitcoinů, které lze z výstupu uvolnit. Celkový objem transakce se rovná součtu hodnot veškerých jejich vstupů – jsou to hodnoty všech existujících výstupů, které jsou poté referencovány vstupy nové transakce. Nová transakce umožňuje, aby se mezi její vstupy rozdělil celkový objem libovolně, pokud ale není větší součet jejich hodnot. Pokud je však menší, rozdíl je brán jako poplatek za transakci. *„Při použití výstupu (jeho referencování vstupem nové transakce) dochází k jeho konzumaci v celé výši – výstup není dělitelný (a je použitelný pouze jednou).“* (Stroukal, 2021, s. 49)

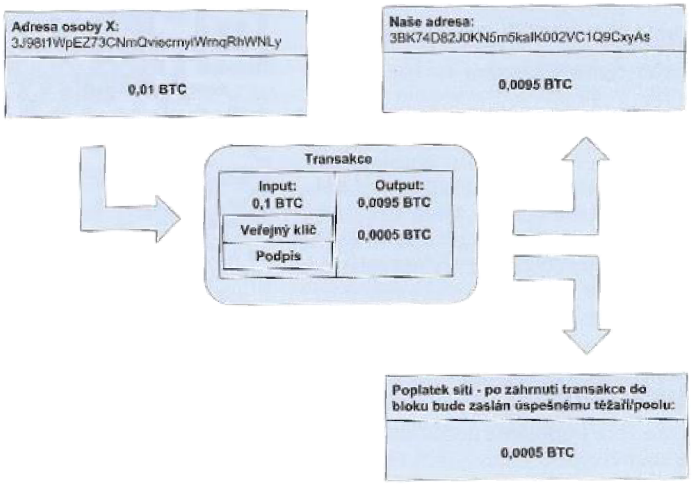
Pokud má být převáděná hodnota nižší než hodnota výstupů, tak bude nová transakce obsahovat i výstupy pro možnost „rozměnění“, jejichž majitel si rozdíl vrátí na vlastní

adresu. K uvolnění je zapotřebí podpisu dat transakce pomocí soukromého klíče patřící k jeho adrese. K výstupu má dispoziční právo pouze její majitel.

Složitější podmínky mají kontrakty, které se programují ve skriptovacím jazyce a větou je i regulérní podmínka podpisu klíčem přiřazeným k dané adrese. *„Právě jedna z transakcí v bloku je "generující" a pouze jejím prostřednictvím vznikají nové bitcoiny.“* (Stroukal, 2021, s. 41)

Od normální transakce se liší tím, že u ní neexistují reálné vstupy (místo toho je zde parametr coinbase přenášející libovolná data) a její objem se rovná součtu poplatků za jiné transakce v bloku a nově vytvořených bitcoinů. Množství nových bitcoinů je 50 BTC v bloku 0 a každých 210 tisíc bloků (odpovídající 4 rokům) se sníží na polovinu. V jednom bloku může být zapsáno několik tisíc transakcí. Praxe ukázala, že maximum bylo okolo 2 700 transakcí/blok. U transakce je možné, aby byla poskládána ze vstupů z několika adres. Tato transakce přenese více dat než ta, která je zaslána z jediné adresy. *„V praxi se do bloku dostanou vždy různě velké transakce a podle toho se mění jejich celkový počet v bloku.“* (Kaliský, 2018, s. 39). Blok má velikost přibližně 1 MB a jsou v něm obsaženy údaje o odeslaných transakcích. V bitcoinovém protokolu je nejvýznamnější datovou strukturou. Zahrnutím zakódované množiny transakcí blok transakce potvrzuje.

Obrázek 1 - Schéma transakce



Zdroj: Kaliský, 2018

„Bloky jsou propojeny hashy – pokud použijeme analogii bloku jako stránky knihy, tak číslem této stránky je hash bloku.“ (Kaliský, 2018, s. 39). Hash bloku je proces, kdy

hashovací funkcí projdou data o transakcích. Na konci hashe bloku bude soubor náhodných čísel a písmen např. v této formě: „00000000015e88a29f4784b5d6469b15575“.

Hash bloku předchozího bude v hlavičce bloku, aby bylo zřetelné, na který navazuje blok. Obsahuje údaj o čase, kdy blok vznikl, a ještě několik jiných údajů.

Hash má obecný požadavek – obrazy musí být uniformně pokryty, což znamená, že jednotlivé obrazy by měli příslušet téměř shodnému počtu vzorů. *„Požadavkem na kryptografickou hashovací funkci je navíc vysoká nelinearita“* (Stroukal, 2021, s. 92) (jakkoliv malá změna způsobí, jakkoliv velkou změnu obrazů, ale hlavně musí být zajištěna nesymetrická výpočetní složitost). Výpočet přímého zobrazení vzorů na obrazy není obtížné, ale výpočet obecně nejednoznačně inverzního zobrazení obrazů na vzory je téměř nemožné.

3.2 Investice

„Investice jsou finanční prostředky, které byly investorem vloženy do konkrétního projektu za účelem jejich zhodnocení a výnosu.“ (Moneta.cz). Investor podstupuje při investici míru rizika, která je daná rizikovostí dané investice. Toto riziko by mělo odpovídat požadované výši výnosu investice.

3.2.1 Historie investic

Ve finančním světě panovala vždy jistota – měna. Libra, dolar, frank, marka či rakouská koruna *„obsahovaly fixní množství zlata nebo stříbra“* (Kohout, 2018, s. 14). Tyto měny se daly přímo směnit za stříbro nebo zlato. Mezi měnami také fungovali stabilní převodní poměry. *„Bankovní systémy v tomto období – které zhruba trvalo od poloviny 19. století až do počátku první světové války v roce 1914 – byly převážně neregulované a postrádaly státní garance.“* (Kohout, 2018, s. 14). Výhoda této „neregulace“ byl růst v době konjunktury, nevýhoda naopak byly řetězové krachy bank v době krize.

Dluhopisy byly od 19. století až do roku 1914 pro vlastníky státních dluhopisů radostné období. Měli tak zaručené příjmy a dlouhodobě trvající všeobecný pokles cen zapříčinil růst kupní síly výnosů z dluhopisových kuponů, i přes to, že byly sazby stabilní.

Burzy akciových trhů v minulosti byly odlišné od těch současných. *„První moderní burza otevřená počátkem 17. století v Amsterdamu měla zpočátku jediný úkol: obchodovat s akciemi holandské Východoindické společnosti“* (Kohout, 2018, s. 24). V Evropě dominovaly dlouhodobě obchodní společnosti. Britská Východoindická společnost, která vlastnila část Indie a měla vlastní armádu, která bojovala ve válkách, ovlivnila i část

britských dějin. *„Kromě obchodních společností během první poloviny 19. století patřily burzy vlastně jen dvěma odvětvím: bankám a železničním společnostem.* (Kohout, 2018, s. 30). Banky patřily z hlediska kapitálu k nejsilnějším společnostem a železnice byly v 19. století stejně důležité, jako v současné době automobilky, počítače a telekomunikace dohromady.

Kryptoměny, jako digitální fiat měny, vznikly z několika jiných projektů, které řešily úskalí digitálních nestátních peněz. Již v roce 1989 Američan David Chaun představil systém firmy DigiCash, který měl pod správou měnu eCash. *„Chau se věnoval šifrování s použitím veřejných a soukromých klíčů, které jsou dodneška jednou ze základních technologií kryptoměn.“* (Kaliský, 2018, s. 8)

3.2.2 Současné investování

V současné době je stále možné investovat do dluhopisů, drahých kovů nebo cenných papírů, avšak jsou tu i jiné prostředky, díky kterým investovat a vstoupit tak na finanční trh.

Indexové certifikáty jsou jednou z možností. Jsou to *„dluhové cenné papíry s pevnou, předem stanovenou dobu trvání nebo bez pevně stanoveného termínu splatnosti (tzv. open end certifikáty)“* (Málek, 2010, s. 82).

Dále jsou tu cenné papíry kolektivního investování. Nejde o nákup jednotlivých akcií, ale o *„shromažďování peněžních prostředků upisováním akcií investičního fondu nebo vydáváním podílových listů podílového fondu, investování na principu rozložení rizika a další obhospodařování tohoto majetku“* (Málek, 2010, s. 83). Sem patří investiční a podílové fondy.

Indexové fondy a ETF jsou také variantou, jak investovat. Indexové fondy kopírují co nejpřesněji hodnotu vybraného tržního indexu. ETF znamenají indexové akcie, které jsou strukturou podobné fondům indexovým, *„neboť i v tomto případě jsou finanční prostředky investorů investovány do aktiv vybraného indexu“* (Málek, 2010, s. 87).

Investování do kryptoměn je nejnovější způsob investice. Vše začalo 18. srpna 2008, kdy *„byla registrována doména bitcoin.org.“* (Kaliský, 2018, s. 14). V následujících letech byla umožněna těžba kryptoměn a následná investice přes směnárny a burzy, které využívali i velké společnosti schopné utratit miliony korun za vlastnictví kryptoměn. Investování do kryptoměn je rozšířené jako nikdy před tím, i přes to, že je stále mnohonásobně rizikovější než jakákoliv jiná investice.

3.3 Bitcoin

Bitcoin je měnová jednotka bitcoinového systému a označuje se zkráceně BTC. Dělí se menší jednotky, satoshi. 100 milionů satoshi je jeden bitcoin. Satoshi Nakamoto, zakladatel bitcoinu, v srpnu roku 2008 poslal e-mail s popisem toho, jak by měl vypadat bitcoinový systém Adamu Backovi. Odstartoval tak maraton událostí, které zahýbali celým světem a hýbou jím dodnes. Doména bitcoin.org, která dodnes slouží jako rozcestník k informacím o bitcoinu, byla založena 18. srpna 2008. 31. října byl uveřejněn Satoshi Nakamotem článek *„Bitcoin: A Peer-to-Peer Electronic Cash System“* (Kaliský, 2018, s. 14), kde popsal, proč je peer-to-peer systém důležitý (aby mezi dvě obchodující strany nevstupovala třetí osoba, která bude garantovat danou transakci).

Bitcoin je program – konkrétně se jedná o evidenční a komunikační protokol. Na začátku ledna 2009 zaslal Satoshi Nakamoto finální verzi C++ zdrojových kódů do kryptografické e-mailové konference, přitom *„zveřejnil bitcoinového klienta, tj. program, který umožňuje zapojení do bitcoinové sítě, těžbu bitcoinu a transakce.“* (Kaliský, 2018, s. 14) a zároveň začal těžit bitcoin na několika svých počítačích, kde jich na začátku vytěžil 50.

3.3.1 Proof of work

Bitcoinový systém dosahuje díky decentralizaci konsenzu. Jedná se o konsenzus vlastního stavu a rozšíření tohoto stavu o nový blok transakcí. *„Tvůrce nového bloku musí zbytku sítě předložit důkaz (proof), že tento blok byl vytvořen v souladu s pravidly dané kryptoměny.“* (Lánský, 2018, s. 20). Vytvořit důkaz je namáhavé, naopak ověřit platnost důkazu je snadné. Algoritmus pro konsenzus v bitcoinové síti se nazývá *proof of work* (důkaz prací). V tomto systému je používána těžba bloku neboli mining, což je název shodný s fyzickou těžbou zlata. Těžba bloku vyžaduje značné úsilí a mnoho práce, v tomto smyslu výpočetní, stejně jako těžba drahých kovů. Vykonání této pracuje však nezaručuje, že bude pracující strana odměněna, úspěšně vytěžený blok je dílem náhody, podobně jako nalezení malého kusu zlata.

Po podařeném vytěžení bloku se měnová zásoba bitcoinu zvýší o další jednotky, které náleží těžaři, opět jako analogie při zvyšování zlata v oběhu. Stejně jako se vyčerpávají ložiska zlata, tak se také snižuje odměna za vytěžení bloku. Proof of work je *„nejstarším*

typem algoritmů tvorby bloků" (Lánský, 2018, s. 23). Autor Back tento algoritmus navrhl v roce 2002 a *„je používán v nejstarší kryptoměně Bitcoin"* (Lánský, 2018, s. 23)

3.3.2 Soukromé a veřejné klíče

Jednotlivé uzly sítě používají tzv. úplného klienta, program, jenž používají jednotlivé uzly v síti, a který zvládne plnit veškeré funkce (nejčastěji program Bitcoin core). Kryptoměny využívají kryptografii k tomu, aby zabezpečili transakce. U bitcoinu se využívá konkrétně asymetrické kryptografie, která je *„základem zabezpečení původu transakcí – slouží k tomu, aby bitcoiny mohl poslat jedině vlastník soukromého klíče"* (Kaliský, 2018, s. 40), kterým „odemkne" bitcoiny na klíčem chráněné adrese. Operace s bitcoiny jsou zajištěny programy čili klienty – tou částí klienta fungující jako peněženka. Existují dva typy klientů. Plní klienti přijímají a posílají transakce, uchovávají kompletní historii transakcí bitcoinu, vytváří nové transakce a slouží i jako peněženka.

Odlehčení klienti naopak kompletní historii neuchovávají, jen její omezenou podobu/hlavičky bloků. S plným klientem přichází do kontaktu jen velmi málo uživatelů. Plný klient je záležitostí fanoušků a nadšenců, kteří chtějí zlepšit bezpečnost bitcoinu a zvýšit bezpečnost vlastních transakcí pomocí provozování plnohodnotného uzlu. Plného klienta využívají samozřejmě různí poskytovatelé služeb – burz, webových peněženek, těžebních poolů, směnáren, obchodníků. Běžný uživatel využívá nejčastěji odlehčeného klienta při používání mobilní aplikace v chytrém telefonu, která se v případě potřeby spojí s plným klientem.

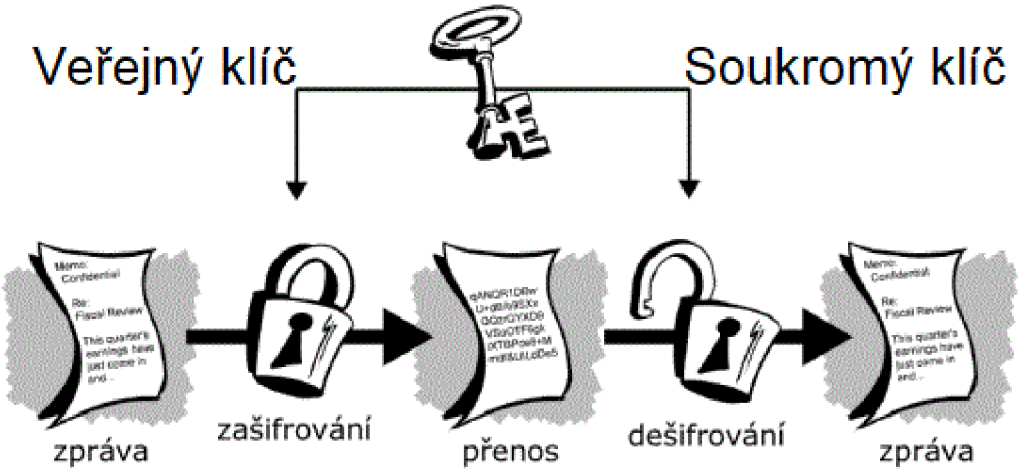
„Soukromý klíč je z hlediska bezpečnosti nejcennější" (Kaliský, 2018, s. 40). Znalost soukromého klíče znamená přístup k bitcoinovému účtu. Soukromý klíč je generován peněženkou ze seedu – sada anglických slov. Pomocí eliptické křivky je ze soukromého klíče odvozen klíč veřejný. Operace, kdy se ze soukromého klíče odvodí ten veřejný, je jednosměrná, a proto není možné, aby se z veřejného klíče vypočítal ten soukromý. Zároveň je podstatné, že jakmile majitel provede transakci, a použije k tomu soukromý klíč, tak je možné, aby použil k jeho ověření veřejný klíč.

Z veřejného klíče, který je vidět na obrázku 1 (Obrázek 1 - Schéma transakce) a obrázku 2 (*Obrázek 2 - Schéma asymetrického šifrování pomocí veřejného a soukromého klíče*) se poté vytvoří bitcoinová adresa kombinací hashovacích funkcí *„konkrétně se jedná o Secure Hash Algorithm, verze SHA 256 a RACE Integrity Primitives Evaluation Message Digest – RIPMED160"* (Kaliský, 2018, s. 40). Bitcoinovou adresu je možné převést do QR

kódu. QR kód (anglicky *Quick response*) je vylepšená verze regulérního čárového kódu. Informace, které jsou v něm uloženy jsou standardizovány podle ISO normy, aby byl strojově snadno čitelný i potom, co by byl poškozen nebo znečištěn. U kryptoměn se používá k zobrazení klíčů a adres, protože lze jednoduše načíst kamerou mobilu. To umožní, aby transakce rychle proběhly, protože přepis adresy nebo okopírování a posílání jinými kanály komunikace je obtížné, nepraktické a náchylné na chyby.

„Soukromý a veřejný klíč spolu s bitcoinovou adresou jsou základní data, která potřebujeme, abychom mohli přijmout, uchovávat a posílat bitcoiny“ (Kaliský, 2018, s. 41). Pro uživatele je nejjednodušší, když si stáhnou peněženku jako aplikaci do mobilního telefonu, která vytvoří adresu a klíče během několika sekund.

Obrázek 2 - Schéma asymetrického šifrování pomocí veřejného a soukromého klíče



Zdroj: PCTuning.cz

Transakce lze provést, jakmile má uživatel k dispozici klíče a adresu. Poté může přijímat bitcoiny od někoho, kdo je vydělal, vytěžil nebo koupil. Postup je takový, že osoba, která posílá bitcoiny, si nejdříve naskenuje QR kód příjemcovi adresy, kterou příjemcova peněženka zobrazí v mobilní aplikaci, zadá do peněženky částku, kterou chce zaslat a stiskne poslat. Mobilní peněženka odesílatele vytvoří vstup (tzv. input), což je nová transakce, kde bude zadaná částka. Následně vytvoří dva outputy (výstupy). První výstup je částka, které se zašle příjemcovi.

Druhý výstup je poplatek těžařům za to, že transakci zpracovali. Tato částka (poplatek) je výrazně nižší než samotná odeslaná částka, a to v řádu jednotek procent. Tyto dva použité údaje (vstup a výstup) jsou doplněny veřejným klíčem, podpisem soukromého

klíče a několika dalšími údaji, které jsou formálně vyžadovány protokolem na zpracování dané transakce. *„Tyto všechny údaje jsou jedna bitcoinová transakce“* (Kaliský, 2018, s. 41). Jakmile je transakce zaslána (Munoz, 2020, s. 18) do sítě, tak mohou uzly ověřit, že bitcoiny byly opravdu na adrese odesílatele, a že byly podepsány správně soukromým klíčem. Správnost podpisu lze ověřit veřejným klíčem.

Aby bylo možné ukrást bitcoiny, čili vytvořit transakci na základě znalosti veřejného klíče a částky, je nutná znalost soukromého klíče. Soukromých klíčů je odhadem 2^{256}. Je tak téměř nemožné, aby člověk našel soukromý klíč, který je zrovna používán a k němu příslušnou adresu s nějakými uchovanými bitcoiny.

3.3.3 Rizika Bitcoinu

Každý systém nebo technologie jsou vyvíjeny tak, aby byly chráněny před útoky zvenčí nebo jejich zneužitím. Bitcoin je také chráněn algoritmy, a také díky své decentralizaci (Obrázek 3 a 4 - Porovnání decentralizované (vlevo) a centralizované sítě) a systémem peer-2-peer sítě. I přes to, jako u většiny systémů, má své slabiny a dává možnost útočníkům poškodit jak samotnou síť, tak i uživatele bitcoinové sítě. Systém bitcoinu je *„navržen tak, že nikdo nikomu nedůvěřuje, proto všichni kontrolují všechny bloky a transakce podle jednotlivých pravidel, a zároveň je odměňována poctivá práce čili správný zápis transakcí do bloků“* (Kaliský, 2018, s. 44). Problém je v tzv. dvojité útratě. Ta je základním problémem u všech kryptoměn – je-li možné, aby se v digitálním světě dalo vše okopírovat, jak lze zabránit tomu, aby kdokoliv nemohl zkopírovat bitcoinovou transakci a zaplatit jí na více místech?

Race attack je jedna z možností, jak podvodem získat, respektive neutratit žádné bitcoiny. Pokud obchodník při přijímání transakcí čeká pouze na ověření platnosti transakce, nikoliv na potvrzení, že je transakce zapsána do bloku, je zde riziko, že bude okraden. Zápis do bloku trvá 10 minut, a proto není praktické, aby obchodník nechal zákazníka čekat příliš dlouho. *„Útočník to může využít a poslat jednu transakci přímo peněžence kavárny“* (Kaliský, 2018, s. 44) a jinou transakci s identickým vstupem na vlastní adresu, která se nachází v síti. Peněženka obchodníka zaznamená transakci, avšak za pár minut se zapíše transakce poslaná do sítě do blockchainu a bitcoiny zůstanou ve vlastnictví útočníka. Obranou pro obchodníka může být zabezpečení terminálu proti posílání přímých plateb a přijímání jen transakcí ze sítě od ověřených uzlů.

Dalším způsobem, jak je možné bitcoin utratit dvakrát z jedné adresy, je tzv. *„útok alternativní historií“* (Kaliský, 2018, s. 44), který počítá na rozdíl od race attacku s tím, že se transakce zapíše i do blockchainu. Pokud by útočník chtěl bitcoin utratit dvakrát, a ještě k tomu ho zapsat do blockchainu, musel by také najít unikátní kód a dodat do sítě blok, který obsahuje správný hash. V případě, že by byl útočník dost odvážný, tak zašle jednu transakci např. do směnárny kryptoměn v síti, a zároveň bude těžit blok, ve kterém by transakce byla zaslána na útočníkovu sledovanou adresu. *„V této chvíli se snaží o tzv. fork nebo rozštěpení blockchainu.“* (Kaliský, 2018, s. 45). V nejlepším případě se mu podaří potají vytěžit několik bloků za sebou. V poctivé síti jeho transakce získá dost potvrzení na to, aby útočníkovi zaslala koupenou kryptoměnu. V tuto chvíli do sítě pošle své vytvořené bloky (adresa, kam je poslána transakce) a doufá v to, že nalezne dostatečně bloků na to, aby síť uznala jeho verzi blockchainu za legitimní.

V praxi je tato technika nesmírně nerentabilní. *„Současný úzus je považovat transakci za potvrzenou v okamžiku, kdy má 6 potvrzení.“* (Kaliský, 2018, s. 45). Útočník by musel disponovat několika procenty celkového výkonu sítě, což je velmi investičně náročné z hlediska nákupu zařízení a platby energií. Musel by vytěžit dost bloků na to, aby předstihl ostatní poctivé těžaři v síti. Má 8% šanci na úspěch při prvním potvrzení, při pátém jen 0,002 % a při šestém potvrzení je šance téměř nulová. Pro útočníka by tak bylo výhodnější těžit poctivou cestou a mít tak zaručené stabilní zisky.

Útok 51 % je spíše spekulativní možnost zneužití bitcoinu. Tato možnost předpokládá, že *„útočník ovládá 51 % (a více) výkonu těžby.“* (Kaliský, 2018, s. 45). Mohlo by se tak stát v případě, že by čínská vláda přinutila těžaře a pooly nacházející na čínském území pracovat podle jejích příkazů. Pokud by tím získala 51 % a více těžebního výkon, byla by zde vyšší pravděpodobnost, že vytěží bloky rychleji než svobodní těžaři, bude blokovat transakce, vytvářet dvojité útraty a celkově podlomí důvěru v bitcoinový systém. Z praktického hlediska je to opět velmi náročné na realizaci a situace by vyústila v obrovské finanční, energetické a hardwarové ztráty pro čínskou vládu. V roce 2014 dosáhl pool Ghash.io na 51 % kapacity sítě. Pool přestal přijímat nové těžaře, někteří přešli k jiným poolům, a poté, co kapacita v poolu klesla, prohlásil Ghash.io, že se nepřekročí 39, 99 % kapacity. Tento postup byl lepší možnost, než ztráta důvěry v bitcoin a jeho bezpečnost.

V roce 2012 byl bitcoin na ceně 5 USD/BTC. V březnu napadl hacker poskytovatele služeb pro internetové firmy Linode, kde byly cílem útoku směnárny Bitcoinica. Ukradl přes 46 000 bitcoinů. Ve většině případů se jedná o *„krádeže soukromých klíčů“* (Kaliský, 2018,

s. 16), které se musí skladovat na zabezpečeném místě. Zloději se dostali také k uživatelským účtům Slushpoolu a v reakci na to se začala vyvíjet první hardwarová peněženka Trezor.

3.3.4 Peněženky

V roce 2014 na trh přišel Trezor – produkt od firmy Satoshi Labs, na jehož vývoji se podílel Marek Palatinus a Pavel Rusnák. *„Doposud bylo možné skladovat bitcoinové adresy v "peněženkách", v programech pro počítače a telefony, které generovaly přístupové klíče a bitcoinové adresy“* (Kaliský, 2018, s. 18), a také spravovaly a vysílaly transakce. Byly však náchylné na útoky hackerů, kteří využili toho, že v adresách byly chyby v kódu, zabezpečení samotných počítačů a mobilů nebylo dostatečné, nebo zneužili lidský faktor, což se stalo firmě Canadian Bitcoins, kdy se hacker dostal k bitcoinům tím způsobem, že zavolal na podporu datacentra, spravující firmě IT a řekl, že je ředitel společnosti. Zaměstnanec podpory mu poté vytvořil nové heslo. Trezor, tzv. hardwarová peněženka, byl *„alternativou "mobilním a počítačovým peněženkám"“* (Kaliský, 2018, s. 18). Místo toho se bitcoinová adresa uložila na obyčejný papír nebo na jiný druh analogového média, které bylo schopné zapsat třicet a více čísel a písmen.

Podstata hardwarových peněženek spočívala v tom, že se soukromé klíče bitcoinu uložily na zařízení, které bylo možné připojit rovnou k telefonu, počítači či tabletu.

Zařízení nikdy nepošle klíče dál a transakce jsou potvrzovány, takže je možné, aby posílalo a přijímalo transakce i na počítači, který je sledován nebo kompromitován.

3.3.5 Fork a jeho formy

Fork je nějaké rozštěpení, rozdělení nebo také rozvětvení blockchainu. Fork, v překladu znamená vidlička, a přesně to se při forku blockchainu děje. Při forku se konsenzus v blockchainu na základě větší či menší radikální změny základního protokolu rozdělí na dva či více konsenzů. Vždy, když někdo navrhne aktualizaci původního blockchainového kódu, musí být použit soft nebo hard fork, aby změny měly nějaký účinek. K forku dochází opětovně. Např. tehdy, *„když se v síti v rychlém sledu objeví dva bloky, neboť dva těžaři našli nonce a vytěžili blok těsně po sobě“* (Kaliský, 2018, s. 45). Oba bloky jsou legitimní a záleží, na který z bloků síť naváže – *„hash kterého bloku bude zahrnut do dalšího bloku“* (Kaliský, 2018, s. 45). Síť poté zohlední dané bloky a přidá bloky na delší

větev. Z druhého bloku se stane slepý výhonek blockchainu. Síť se pak rozdělí na dvě, ale každá s jinou verzí záznamu, nicméně podle stejných pravidel.

„Soft fork funguje jako aktualizace již vytvořeného protokolu“ (Hosp, 2018, s. 96). Starší verze jsou stále akceptovány. Soft fork lze přirovnat k aplikaci, která se neaktualizuje. Aplikace půjde stále používat, ale uživatel, který nebude mít nejaktuálnější software, nebude mít možnost používat některé z funkcí.

Hard fork je výsledkem nesourodých představ o tom, jak by měl bitcoin nebo jiná kryptoměna fungovat. V případě bitcoinu se těžaři rozhodli, že použijí hard fork, čili *„tvrdé rozdělení sítě“* (Kaliský, 2018, s. 72). Při hard forku je zapotřebí upravit současného klienta podle nových priorit pro nově vytvořenou síť a funkci měny, obstarat uzly či uživatele, kteří budou jevit zájem o provoz nových uzlů a těžaře s dostačujícím výkonem pro těžbu (aby byla síť dostatečně ochráněna proti útokům). Poté, v příslušný blok, začnou těžaři nové sítě a uzly s aktualizovaným klientem vytvářet bloky do nové větvě a podle nových pravidel. Při tomto hard forku získali majitelé bitcoinu i nový bitcoin cash/BCH. Roger Ver je hlavní tváří Bitcoin cash. Byl také jeden z prvních, kteří investovali do bitcoinu a také jeho popularizace. Tato aktivita mu vynesla přezdívku bitcoinový Ježíš.

3.3.6 Halving

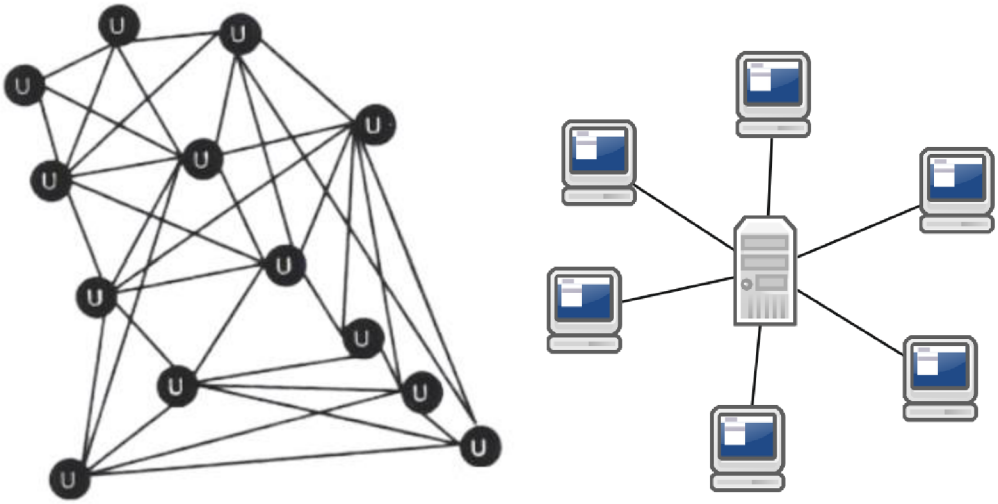
„V roce 2012 nastal první tzv. halving, tedy snížení odměny za těžbu bitcoinu“ (Kaliský, 2018, s. 16). Do tohoto roku byl každý, kdo využil algoritmus proof of work a našel blok bitcoinu, odměněn 50 bitcoiny. Nakamoto zavedl do protokolu pravidlo, že se každé 4 roky sníží odměna na polovinu. V listopadu 2012 se snížila odměna na 25 BTC.

Toto snižování bude ukončeno v roce 2140, kdy budou vytěženy zbylé bitcoiny z celkových 21 milionů. Toto opatření – zastropování celkových měnových zásob způsobuje, že je bitcoin deflační. Fiat peníze ztrácejí v průběhu let vlivem inflace svou hodnotu a bitcoin přichází s tím, že jeho hodnota bude s postupným klesáním emise růst.

3.3.7 Peer-to-peer

Bitcoin funguje na principu peer-to-peer (P2P) – typ počítačové sítě, kde jsou si všechny uzly rovnocenné a jednotliví klienti spolu mohou komunikovat bez nutnosti využívat centrální uzel – server. *„Na rozdíl od asymetrického modelu klient-sever, v P2P s rostoucím množstvím uživatelů roste i přenosová kapacita sítě“* (Stroukal, 2021, s. 28). Nesymetrie P2P má však jednu nevýhodu – je obtížné počáteční navázání komunikace.

Obrázek 3 a 4 - Porovnání decentralizované (vlevo) a centralizované sítě



Zdroj: Kaliský, 2018, Napočítači.cz

3.3.8 Počáteční bloky

Tyto první bitcoiny vznikly společně s tzv. „*blokem genesis*“ (Kaliský, 2018, s. 14) - prvním blokem blockchainu (účetní knihou) s pořadovým číslem 0. Uvnitř tohoto bloku se nacházel název článku *„Chancellor on brink of second bailout for banks“* (Lánský, 2018, s. 5), jenž byl vydán deníkem Times 3.1.2009. Odkaz na článek prokazuje, že základní blok nebyl vytvořen dříve, než byl vydán článek a píše se zde o další finanční pomoci bankám, které byly zasaženy finanční krizí. *„Kromě důkazu o datu vzniku Bitcoinu poukazuje tato zpráva na finanční marasmus, pro který by mohl být bitcoin alternativou.“* (Kaliský, 2018, s. 14).

Druhý blok s pořadovým číslem 1 byl vytvořen 3.1.2009. Jednotlivé bloky si může každý dohledat na internetu. První transakce se uskutečnila 12. 1. 2009 v bloku 170. Satoshi odeslal 10 bitcoinů Hal Finneymu. V květnu roku 2009 nabídl Satoshi Nakamotu pomoc student Martti Malmi. Přepracoval webové stránky bitcoin.org tak, aby je pochopila i široká veřejnost. Do té doby se zabývali technickými parametry bitcoinu a byly užitečné pro kryptografiky. Z Martti Malmiho se stal třetí provozovatel uzlu v bitcoinovém systému. Společně s Nakamotem vymysleli název kryptoměna *„cryptocurrency“* (Lánský, 2018, s. 5)

3.3.9 ICO

Rok 2017 znamenal skokový nárůst *„tzv. ICO´s (Initial Coing Offering nebo prvotní nabídka digitální měny)“* (Kaliský, 2018, s. 23). Jde o proces, při kterém se financuje projekt pomocí veřejné nabídky a nabízí se veřejnosti. Na počátku je firmou nebo týmem vývojářů představena technologie v takzvaném white paperu – popis toho, pro koho a proč je nová technologie užitečná, jak má fungovat a jak se technologií dají vydělat peníze. Dále se vybudují základní kanály pro komunikaci jako je webová stránka, sociální sítě, představí se tým, který na technologii spolupracuje a nejlépe se představí i základní verze kódu produktu. *„Na ní demonstruje jeho funkcionality, otestuje ji a nabídne k odzkoušení jako open source“* (Kaliský, 2018, s. 23). Dále si vytvoří na určité platformě (Bitcoin, Ethereum) token, který nabídne výměnou za danou kryptoměnu. Kryptoměnu, kterou získal při směně prodá, získá peníze a začne vytvářet verzi, které bude použitelná již jako plnohodnotná. ICO tokeny se nabízejí na burzách, kde s nimi lze obchodovat, respektive divoce spekulovat. Cena tokenů bývá často mimořádně volatilní a nekoresponduje s kvalitou produktu, projektu nebo týmu, který projekt vyvíjí.

„Výhodou ICO je rychlost, s jakou lze projekt zafinancovat a vytvořit podmínky pro jeho vývoj“ (Kaliský, 2018, s. 23). Zakladatelé tak nemusí shánět finanční zdroje od bank nebo jiných forem investic a také se jim nemusejí zodpovídat ani podřizovat jejich kontrolám. Riziko se tímto způsobem přenáší na investora. Nevýhodou je, že crowdfundingové portály jsou omezeny v ověřování, zda-li je autor schopný projekt zrealizovat, a pokud se tak nestane, portál obvykle vrátí peníze investorům. Veřejnost takto posuzuje kvalitu projektu svými penězi. Když se ale vybere dostatečná částka, tak se riziko za další vývoj přenáší právě na skupinu podporovatelů tohoto projektu. Většinou jde o projekty v řádech stovek až tisíců korun jako jsou knihy, hudební alba, festivaly nebo třeba rukavice. Výjimečně projekty dosahují hodnoty statisíců nebo milionů dolarů.

„Pomocí ICO vzniklo mnoho zajímavých, technologicky inovativních projektů“ (Kaliský, 2018, s. 24), ale také jich mnoho skončilo, i přes to, že byly vytvořeny pro něco užitečného. Někteří ovšem zneužili tento boom a za zanedbatelné částky nechali naprogramovat token (většinou v standardu ERC20), vytvořit white paper, vytvořit prezentaci na webových stránkách s vymyšlenými lidmi, zaplatili reklamu na Google

a Facebooku, poté předstírali, že jsou aktivní na sociálních sítích a jakmile ICO skončilo, zmizeli neznámo kam.

Byli zde i odvážnější, kteří zalistovali své tokeny na malou burzu v Jižní Koreji, zaplatili za FOMO na Facebooku a jakmile začala cena kulminovat, prodali velké množství tokenů, které drželi právě za účelem pozdějšího prodeje. Tento postup se nazývá Pump and Dump. Pump – *„pumpování ceny koordinovaným nákupem a intenzivní propagací“* (Kaliský, 2018, s. 24). Tato strategie navýší cenu a zapojí se do ní mnoho dalších investorů. Dump – *„prodej velkého množství tokenů“* (Kaliský, 2018, s. 24), na kterém má zisk jen několik aktérů, cena tokenu spadne, a ti, kteří zainvestovali příliš pozdě, mají jen nepoužitelný token.

3.3.10 Futures kontrakty

„Jeden z korků směrem k začlenění kryptoměn mezi legitimní finanční nástroje bylo spuštění tzv. "Futures kontraktů"“ (Kaliský, 2018, s. 26). Ve světě kryptoměn se kontrakty staly prvními investičními produkty, které jsou zaměřené na institucionální investory. Ti se liší od malých investorů investující individuálně tím, že na rozdíl od svých peněz investují peníze cizí. Tyto peníze vkládají do produktů, které mají dostatečnou likviditu a dlouholetou historii, je u nich známa míra rizika a jsou definovány jasnými regulačními pravidly. Doposud byly kryptoměny pro tyto investory *„okrajovou záležitostí s nejasnou regulací, a také nízkou kapitalizací“* (Kaliský, 2018, s. 26), kde je v porovnání s komoditami nebo akciovými trhy stále málo peněz a velký investor může zásadně ovlivnit cenu kryptoměny. U Futures kontraktů se obchoduje s cenou bitcoinu, ale v dolarech a zároveň musí obchodník splnit požadavky úřadu, který dohlíží na obchodování kryptoměn. Dá se říct, že to není obchodování s bitcoinem, ale spíše obchodování s budoucí cenou bitcoinu.

3.4 Ethereum

Druhá nejznámější a nejrozšířenější kryptoměna Ethereum má společné s Bitcoinem to, že je to kryptoměna založená na decentralizaci, díky které chrání a uchovává záznamy, jejichž počet se neustále zvyšuje. Jeho vnitřní struktura a smysl samotný se však od bitcoinu liší.

Ethereum je open-source platforma, ve které viděl rakousko-kanadský programátor Vitalik Buterin nevyužitý potenciál, a díky jehož myšlence Ethereum v roce 2015 vzniklo.

Buterin se mimo jiné podílel na vývoji bitcoinu. Cílem vývojářů Etherea nebylo vytvořit novou kryptoměnu, ale spíše vznik sdílené výpočetní platfromy, která by umožňovala využít blockchain k provozování decentralizovaných aplikací. *„Celý vývoj byl financován formou crowdfundingu a vybralo se necelých 450 milionů korun. Síť Etherea byla následně spuštěna 30. července 2015“* (Parke, 2021, s. 20). Ethereum svým charakterem spadá do tzv. další generace kryptoměn, které se označují jako Bitcoin 2.0.

Kryptoměna Ethereum je označována jako smart chain. Pro své fungování využívá stejně jako bitcoin blockchain, který Ethereu umožňuje nadstavby. Tyto nadstavby se nazývají smart contracts, v překladu *„chytré dohody“* (Parke, 2021, s. 12), což jsou dohody více stran, následně vložené do kódu s přesně danými podmínkami a již napořád zamknuté do blockchainu. Ethereum se od Bitcoinu liší tím, že Bitcoin umí uchovat záznamy o pohybech bitcoinu na účtech, podporuje skripty a if podmínky, avšak nelze na něm vytvořit např. cykly. Díky tomu lze na platformě Etherea vytvářet zajímavější a univerzálnější kód.

Každý programátor na blockchainu Etherea může vytvořit své vlastní výtvory. Obvykle se na blockchainu Etherea staví chytré kontraky, tzv. smart contracts, *„decentralizované aplikace (DAPPS), DAPPs často mají svoji vlastní“měnu” ERC20 tokeny. ERC20 tokeny mohou existovat i bez DAPPs“* (Parke, 2021, s. 12). Vše míří do systémů pro decentralizované finance (DeFi). Ethereum má i vlastní platidlo, jímž je ether (ETH). Rozdíl mezi Ethereem a Bitcoinem je i v tom, kolik mincí je v oběhu.

Zatímco počet mincí Bitcoin je omezen, Ethereum jich má neomezené množství. Hovoříme tak o inflační kryptoměně. Cena za transakci se nazývá Gas – ten se počítá v jednotkách Gwei (jedna miliardtina etheru). I přes to, že je Ethereum díky své technologii těžby ekologičtější než Bitcoin, dá se dodnes těžit výpočetním výkonem založením na principu proof of work, ke kterému jsou potřeba grafické karty. V brzké budoucnosti se však plánuje přejít na princip těžby jménem proof of stake. Při tomto principu těžby již není potřeba dedikovaný výpočetní výkon, avšak jen vlastnění určitého množství Etherea, díky čemuž lze potvrzovat transakce, a není zapotřebí tolik výpočetního výkonu, s čímž jsou spojeny nižší náklady na energie.

3.4.1 Smart Contract

Tato chytrá smlouva nebo také chytrý kontrakt, jiným slovem nadstavby *„jsou v překladu chytré dohody (dohody více stran vložené do kódu s jasně danými podmínkami*

a navždy veřejně zamknuté do blockchainu)" (Parke, 2021, s. 12). Tento kontrakt (dohoda) se následně zapisuje a uchovává v blockchainu, takže je možné ji zpětně dohledat a je zároveň všem přístupná. U smart contractu jsou podmínky přesně dané a neměnné, takže pokud vznikne jen malá odchylka nebo nedodržení dohody z jedné strany kontraktu, kód vyhodnotí, zda byli splněny zadané podmínky a jestli dohoda proběhne či nikoli. Programovací jazyk Solidity je využíván při psaní smart contractů.

„Pokud je smart contract naprogramovaný správně, je nesrovnatelně méně chybový než lidský úsudek a nabízí spoustu výhod" (Parke, 2021, s. 40), jako je např. důvěra a transparentnost, díky čemuž není nutné, aby si strany navzájem věřili a není zde žádná instituce, která by měla větší pravomoci. Nabízí také lokaci a jazyk – obě nebo všechny strany dohody nemusí být přítomny na jednom specifickém místě, nemusí ani žít ve stejném státě či na stejné polokouli, ani nemusí hovořit stejnou řečí. K uskutečnění smart contractu tak stačí jen jazyk Solidity a připojení k internetu.

3.4.2 Ethereum 2.0

Další naplánovaná verze Etherea nese název Ethereum 2.0. U staré verze již není možné, aby byla přebudována/změněna v takovém rozsahu. V komunitě se o nové verzi mluví jako o *„nutné evoluci"* (Parke, 2021, s. 18). Hlavní důvody k přechodu na Ethereum 2.0 jsou:

- Zachování bezpečnosti a decentralizace – bezpečnost narušují tzv. Asic mineři, stroje specializované na těžbu, které svým velkým výkonem zvyšují obtížnost těžby běžným těžařům.

- Škálování – Ethereum 1.0, což je v podstatě jen prototyp smart contractového chainu, který se posouvá dál, zpracuje okolo 15 transakcí za sekundu, což je srovnatelné s pomalým bitcoinem. Nová verze (Kaliský, 2018, s. 14) bude fungovat na principu proof of stake a liší se také tím, že používá sharding, což je spojení více (i tisíce) blockchainů dohromady.

- Na novou verzi se bude postupně přecházet ve třech fázích – 0, 1 a 2. V lednu 2021 došlo ve fázi 0 ke spuštění beacon chainu (proof of stake blockchain). Následující bude fáze 1, kde se vylepší technologie shard chain (vícefázové

vylepšení škálovatelnosti a celkové kapacity Etherea) a poté fáze 2, která spojí Ethereum 1.0 s Ethereem 2.0.

Také samotný shard (Ethereum 1.0 a jeho všechny transakce) poté přejde na PoS. Než se dokončí fáze 2, tak poběží Ethereum 1.0 a 2.0 paralelně vedle sebe a na konci se spojí v jeden chain. *„Odhady míří na dokončení za 2 roky, ale například i za 6 let“* (Parke, 2021, s. 18). Ve fázi 0 bude možné uzamknout nenávratně 32 ETH díky tzv. stakingu, které bude možné vyjmout pouze po zapojení Etherea 2.0.

Přes tuto komplikaci se však díky měnové inflaci Etherea slibuje výnos až 18 % ročně. Lidé na sociálních sítích a v článcích se ve většině shodují, že ethery ze staré verze zůstanou vlastníkům i po přechodu na verzi 2.0.

3.4.3 DAO Fork

Po neshodách v komunitě Etherea došlo k rozdělení na nový řetězec Etherea – ETH a Ethereum Classic (starý řetězec) – ETC. *„Mnozí se domnívají, že Ethereum Classic (ETC) vzniklo jako hardfork z měny Ethereum (ETH), ale opak je pravdou“* (Parke, 2021, s. 29). Ethereum vzniklo z kryptoměny Ethereum Classic, když společnost Slock.it vydala převratný vynález DAO na Ethereum. DAO byla decentralizovaná společnost, která se vyznačovala čistě demokratickým způsobem fungování. Akcionáři dávali návrhy na projekty, které byly následně schvalovány a pomocí smart kontraktů se uvolňovali peníze.

Před spuštěním nasbíral po pár týdnech zveřejnění 150 milionů USD. Když se po spuštění hlasovalo o použití peněz pro větší bezpečnost, tak byla nalezena bezpečnostní chyba, která zapříčinila přesun asi 60 milionů USD na nezabezpečený účet. Po zveřejnění se snížila cena Etherea o polovinu a mezi lidmi zavládla panika. Po rychlém hlasování byla bezpečnostní chyba vymazána a byla naplánován hard fork. Pro hard fork hlasovalo okolo 6 % komunity a *„ve dvanáctidenním hlasování bylo rozhodnuto, že se bude forkovat. 20. července“* (Parke, 2021, s. 29). Vznikl tak nový blockchain s cenzurovanou a vymazanou historií. Nový blockchain se tedy jmenuje Ethereum, starý Ethereum Classic.

3.4.4 Ethereum Classic

Tato starší kryptoměna oproti velmi známému Ethereu má na vlastním webu Grayscale fond, který vlastní největší množství bitcoinu. Během roku 2020 bylo ukradeno

3,6 milionů ETH. *„Ethereum classic má omezené množství coinů (210 mil. podle CMC) a také snižující se odměny za těžbu, bude tedy jednou na rozdíl od ETH neinflační“* (Parke, 2021, s. 30). Kdyby ETC přešlo na princip PoS, znamenalo by to pro Ethereum foundation veliké zisky. To samé by platilo pro hackera, který vlastní 3,3 milionu ETC.

3.4.5 Rozdíly mezi Bitcoinem a Ethereem

Tyto dvě kryptoměny mají společné to, že jsou založeny na decentralizované veřejné databázi jménem blockchain. Rozdíly jsou ovšem značné, jak technicky, tak v tom, za jakým účelem vznikly.

Nejvýznamnější rozdíl, který je rozlišuje, je z pohledu kryptoměny jako platidla. Ani jedna z kryptoměn nebyla až do současné doby přijímána jako oficiální platidlo, ve smyslu měny státu. To se ale změnilo 7. září 2021, kdy *„Salvador jako první na světě zavedl bitcoin coby oficiální platidlo“* (Dvořák, 2021) a to i přes kritiku Světové banky. Důvod by nestabilní salvadorský colón, který vystřídal roku 2001 americký dolar. Politici si od toho kroku *„slibují především příliv zahraničních investorů“* (Dvořák, 2021), kteří by rozproudili tamní ekonomiku. Riziko bitcoinu jako oficiálního platidla je jeho extrémní volatilita. Problém je to také pro centrální banku, která se *„musí vzdát role tvůrce měnové politiky“* (Dvořák, 2021) protože nemůže regulovat počet bitcoinů v oběhu. Příkladem volatility může být pouhý jeden tweet nejbohatšího muže planety, Elona Muska, který *„si změnil popisek u svého jména na Twitteru jen na logo Bitcoinu a hashtag #bitcoin“* (Stroukal, 2021, s. 72).

Společnost Genesis zaznamenala ve 3. čtvrtletí roku 2021 klesla poptávka po Bitcoinu z důvodu relativního nedostatku obchodních příležitostí. Společnost uvádí, že došlo ke *„snížení páky maloobchodních burz“* (Zima, 2021) a *„v kombinaci s čínským zásahem proti kryptoměnám“* (Zima, 2021) se odvětví posunulo k institucionalizaci a pro některé oportunistické obchodníky se tak Bitcoin stal méně atraktivním. Mezi roky 2020 a 2021 vzrostla poptávka po Bitcoinech pětinásobně. V lednu 2021 byl objem nakoupených kryptoměn více jak půl miliardy korun, *„což je o polovinu více než ve stejném měsíci“* (ČTK, 2021) předešlého roku. V roce 2020 se v České republice v průběhu roku prodaly kryptoměny za čtyři miliardy korun. V minulém roce se podíl tržní kapitalizace Bitcoinu dotkl 70 % z celkového trhu s kryptoměnami.

Na počátku většího růstu hodnoty Bitcoinu *„stálo zapojení větších společností jako Paypal a budování pozic u větších investorů“* (ČTK, 2021). Investice do bitcoinu oznámila i Tesla, Mastercard nebo JPMorgan Chase & Co. *„Je evidentní, že nejen menších investorů, ale také velkých korporací se zmocnil 'FOMO' efekt“* (ČTK, 2021), což je strach z toho, že přijdou o dobrou příležitost investovat. Placení bitcoinem v ČR zavedl na jaře roku 2017 internetový obchod Alza.cz, poté se přidávali další, jako např. *„zprostředkovatelé realitních služeb, konkrétně HOME Hunters“* (Dvořák, 2021), která zprostředkovává pronájmy a prodeje nemovitostí, začala *„jako první v České republice akceptovat kryptoměny jako bitcoin, litecoin a ethereum k platbě provizí“* (Dvořák, 2021, s. 1)

Možností pořízení Bitcoinu je poněkud více než u Etherea. Jednou z možností je online směnárna Simplecoin.eu, která je v Čechách od roku 2013*„Umožňuje nákup a prodej bitcoinu, litecoinu a bcash (neboli bitcoin cash) za české koruny“*. (Kaliský, 2018, s. 92). LocalBitcoin je další možnost pořízení, kde jsou propojeni prodejci a zájemci o kryptoměny a jsou zde nastaveny *„mechanismy důvěry a bezpečnosti“* (Kaliský, 2018, s. 92). Coinbase je velký hráč na trhu s kryptoměnami. Díky jednoduchému rozhraní a propagace společnosti lze obchodovat s desítkami kryptoměn za poplatek za transakci a *„spread – kurzový rozdíl mezi cenou nákupu a prodeje“* (Kaliský, 2018, s. 93). Coinbase, jako i jiné služby, které u sebe drží klíče ke kryptoměně zákazníků, mají jednu závažnou slabinu. Zákazník totiž není vlastníkem soukromého klíče – *„jeho kryptoměna je na účtu služby, a tím majitel přichází o zásadní vlastnost a výhodu kryptoměn – jistotu vlastnictví“* (Kaliský, 2018, s. 93).

Druhá v pořadí nejpopulárnější kryptoměna Ethereum zatím nebyla uznána jako oficiální měna žádného státu, avšak také sklízí úspěchy ve finančním světě. Podíl na trhu s kryptoměnami tvořilo v roce 2021 16,5 % a společně s Bitcoinem tak *„tvořily prakticky veškerou tržní kapitalizaci na celém kryptoměnovém trhu“* (Stroukal, 2021, s. 71). Hodnota Etherea se ale také v průběhu let měnila, a to razantně. Cena se v únoru 2021 na okamžik dotkla 2 000 dolarů, v dubnu už tuto hranici překonala *„Kryptoměna tak letos vzrostla již o 183,2 %“* (Capital.com, 2021).

Philip Gradwell, hlavní ekonom v Chainalysis *„uvedl, že nad úrovní podpory 1850 $ bylo koupeno jen velmi malé množství etherea a ještě menší poptávka je nad hranicí 2000 $“* (Capital.com, 2021). Z dlouhodobého hlediska se očekává, že kurz etherea poroste. Investor Mark Cuban tvrdí, že *„po vylepšení nechá ethereum bitcoin za sebou“* (Capital.com, 2021) *„Předpověď ceny etherea od Digitalcoin předpovídá, že se jeho hodnota do roku 2023 zdvojnásobí“* (Capital.com, 2021), což znamená, že může být

ethereum vhodný investiční prostředek stejně jako bitcoin. Ethereum se stejně jako Bitcoinu dá obchodovat na burzách nebo ve směnárnách jako již zmíněný Coinbase.

4. Porovnání výkonu Bitcoinu a Etherea

Tato část bakalářské práce se bude věnovat porovnání výkonu Bitcoinu a Etherea od jejich vzniku, respektive od doby, kdy byly přístupné k obchodování až po současnost. Bude zde popsán vývoj Bitcoinu a následně Etherea. Ačkoli jsou to obě kryptoměny, v mnoha ohledech se liší a také plní odlišný účel a mají i jiné vlastnosti.

Bude zde popsán cenový vývoj Bitcoinu a Etherea a vysvětleny důvody cenových výkyvů v průběhu vývoje. Ceny v jednotlivých letech budou psány v dolarech.

Vývoj kryptoměn záleží, jako u každé měny, na důvěře, kterou do ní lidé vloží. U vývoje Bitcoinu a Etherea je tato důležitá vlastnost poznat na vývoji, kdy je jejich hodnota extrémně volatilní a téměř nepředvídatelná.

Tabulky vývoje cen Bitcoinu a Etherea budou počítány vždy v lednu jednotlivého roku při jejich nejvyšší hodnotě daného měsíce. V grafech pak budou následně zobrazeny vývoje cen daných kryptoměn v období u Bitcoinu od roku 2010 do roku 2021. U Etherea bude popsán vývoj ceny od roku 2015 až do roku 2021. A následně bude v kombinovaném grafu popsán vývoj Bitcoinu společně s etherem od roku 2015 až do roku 2021. Ceny budou uváděny vždy v amerických dolarech. Údaje do grafů a tabulek budou brány z více webových stránek, které sledují vývoj Bitcoinu a Etherea, především pak stránka bitinfocharts.com, která zobrazuje cenu kryptoměn, od doby, kterou jiné stránky nedokážou poskytnout.

4.1 Cenový vývoj Bitcoinu

Tato kapitola se bude věnovat cenovému vývoji Bitcoinu od roku 2010, kdy byla založena burza Mt. Gox až po současnost. „*První bitcoiny byly vytěženy 3. ledna 2009 v 18:15 a pět sekund*“ (Stroukal, 2021, s. 41), avšak „*zlom přišel až 21. května 2010, kdy se na fóru bitcointalk.org objevila nabídka: "Zaplatím 10 000 bitcoinů za pár pizz*“ (Stroukal, 2021, s. 43), což byla první objednávka od muže jménem Laszlo Hanyecz, která byla zaplacena v bitcoinech. Ten jí koupil v přepočtu za 0,01 dolaru za bitcoin.

V roce 2010 byly zakládány různé burzy, směnné obchody, kupovalo se zboží a služby za bitcoiny a už tehdy byli lidé, kteří vlastnili Bitcoiny. Bitcoin v tomto roce však ještě neměl přesně specifikovanou hodnotu vůči měně (americkému dolaru).

Situace se změnila až v roce 2011, kdy měl Bitcoin hodnotu 1 dolaru. Avšak stále není nikde evidován k obchodování. V této době také vznikly dvě další kryptoměny, Litecoin a Namecoin. Litecoin se dal těžit 4krát rychleji než bitcoin.

V roce 2012 byl bitcoin za 5 USD. V tomto roce nastal první halving, což snížilo odměnu za vytěžení bitcoiny. Bitcoiny už začalo přijímat větší množství obchodníků.

Cena bitcoinu se však začala více vyvíjet až v roce 2013, kdy jeho hodnota začala stoupat.

Tabulka 1- Vývoj ceny bitcoinu 2010-2021

Rok	Cena (v dolarech)	Procento růstu
2010	0,01	-
2011	1	100 %
2012	5,49	449 %
2013	19,7	258,8 %
2014	829,92	4112,8 %
2015	217,46	-73,8 %
2016	368,76	69,6 %
2017	907,40	146 %
2018	10221,1	1026,4 %
2019	3450,11	-66,2 %
2020	9357,21	171,2 %
2021	33053,68	253,2 %

Zdroj: vlastní zpracování podle Finex.cz

Cena se od roku 2010 začal vyvíjet a exponenciálně rostla. V roce 2010 to bylo způsobeno založením burzy Mt. Gox. Přesun do roku 2011 znamenal 100% narůst oproti roku 2010. Tržní kapitalizace přesáhla milion amerických dolarů a bylo dosaženo parity s dolarem. V lednu 2011 byl kurz 1 dolar za bitcoin (*Tabulka 1- Vývoj ceny bitcoinu 2010-2021*), avšak do července vystoupala až na 31 dolarů za bitcoin, pak ovšem spadla zpět na 2 dolary. Leden 2012 měl bitcoin hodnotu vyšší o téměř 450 % oproti stejnému měsíci minulého roku.

Mezi březnem a červencem 2012 byla cena v rozmezí 4-7 dolarů za bitcoin, i přes to, že došlo ke krádeži soukromých klíčů ve směnárně Bitcoinica. V reakci na to byla vytvořena

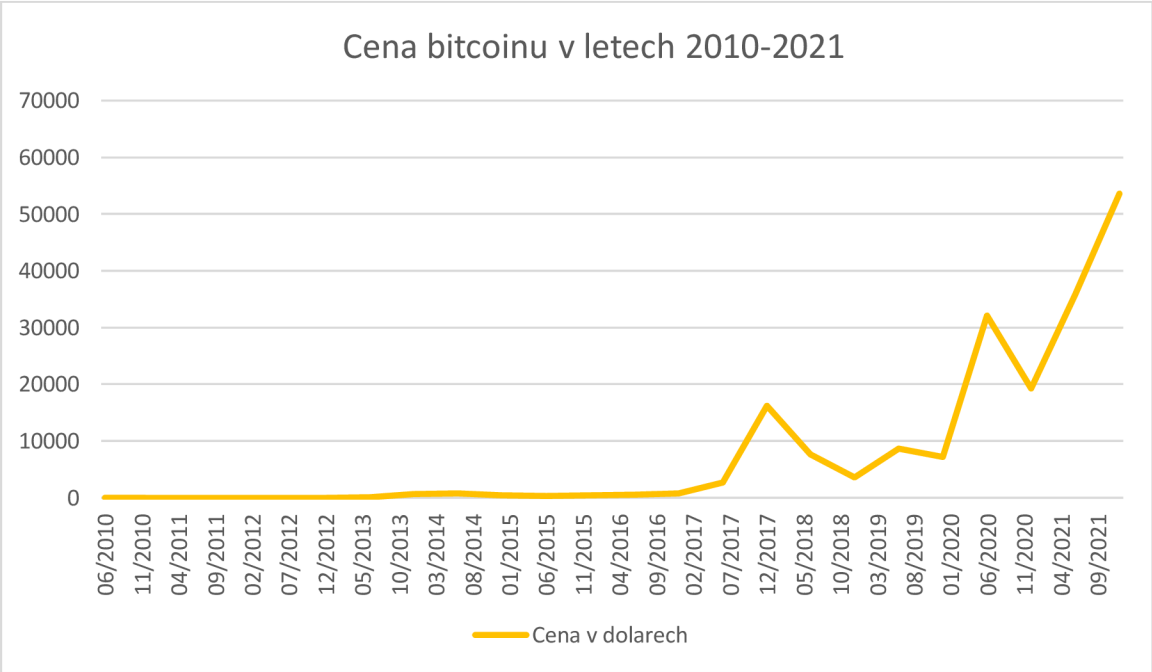
hardwarová peněženka Trezor k ochraně soukromých klíčů. Lidé se začali ve větších počtech přihlašovat na burzy. V roce 2012 nastal první halving, což snížilo odměnu za těžbu.

Tržní kapitalizace vzrostla v tuto dobu na jednu miliardu, poté se zvýšila na 10 miliard a v roce 2014 už to bylo 14 miliard dolarů. To bylo způsobeno velkým nárůstem zájmu o Bitcoin, jeho obchodování na burzách a také díky medializaci. O bitcoinu bylo vysíláno v televizi, psalo se o něm v novinách a začala i výuka na vysokých školách.

Mezi lednem 2013 a 2014 byl enormní rozdíl v hodnotě o více jak 4 000 %. V dubnu 2013 byl bitcoin poprvé na 100 dolarech, do dubna byl na vrcholu na 266 dolarech. I přes to, že hodnota následně spadla, meziroční růst byl 2 000 %. Roku 2013 byl zavřen SilkRoad[1], který vlastnil 9,5 milionů bitcoinů (takový objem byl vytěžen až v roce 2012). Tato událost snížila hodnotu bitcoinu, avšak na konci roku vyšplhala až na 1000 USD/BTC.

V roce 2014 byl zatím nejstrmější pád bitcoinu. Bylo to způsobeno krádeží bitcoinů na burze Mt. Gox, který zapříčinil pokles o více jak 144 %. I přes to, že se od ledna 2014 do ledna 2015 a ledna 2018-2019 snížila, bitcoin zaznamenal obrovské růsty a také navýšení kapitalizace, které překročilo v roce 2021 bilión dolarů.

Graf 1 Vývoj ceny bitcoinu v letech 2010-2021



Zdroj: vlastní zpracování podle Coindesk.com

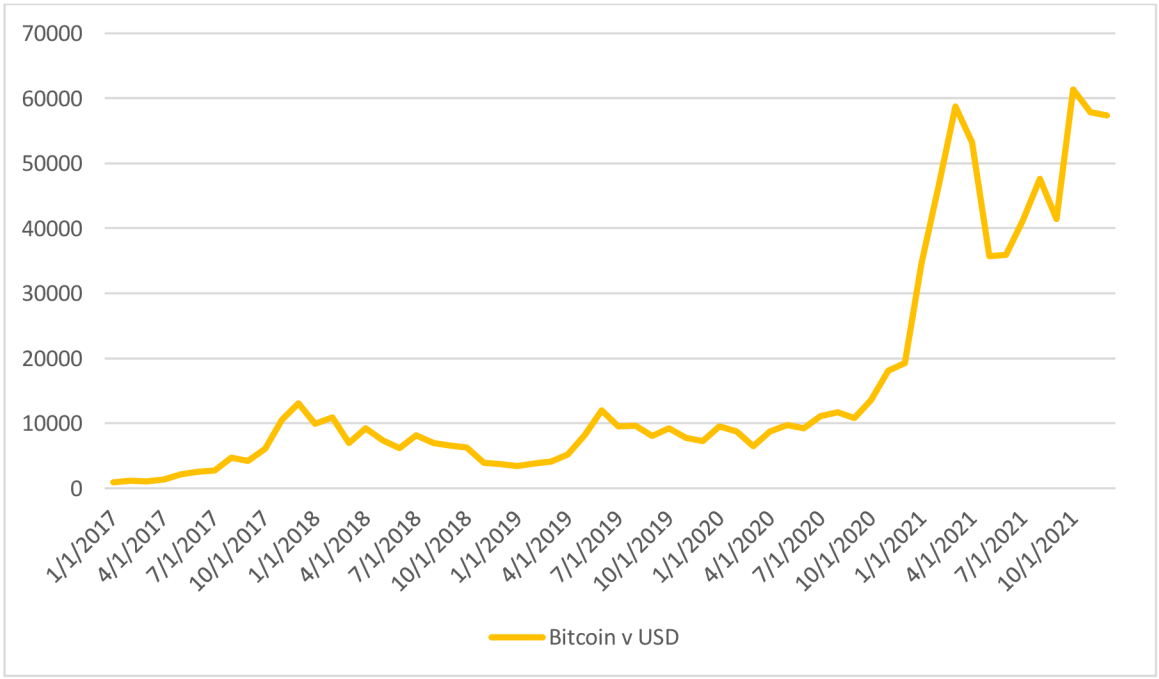
[1] Ilegální online tržiště

Na grafu 1 (Graf 1 Vývoj ceny bitcoinu v letech 2010-2021) lze vidět, že kromě rozdílu ledna 2013 a 2014 nebyly změny až tak drastické prakticky do roku 2017, kdy bitcoin atakoval hranici 20 000 dolarů (Graf 2 Vývoj ceny bitcoinu 2017-2021 v *USD*). S bitcoinem rostly i ostatní kryptoměny a další tokeny. Bitcoin opět vzbudil pozornost médií a poptávka po něm rostla, investory pohltilo FOMO (Fear of Missing Out) (3.3.9) a začali zběsile nakupovat.

Počet obchodů se od roku 2016 ztrojnásobil. V roce 2017 začal přijímat bitcoiny český e-shop Alza.cz. Počet bankomatů na bitcoiny se zdvojnásobil oproti minulým létům na téměř 800.

Poptávka byla zvýšena také nárůstem projektů ICO (3.3.9). Od roku 2017 následně hodnota bitcoinu klesala, až do počátku roku 2019, kdy jeho cena opět začala růst z důvodu zvýšeného zájmu z firemního sektoru. V roce 2020 pak jeho cena začala růst téměř exponenciálně, což bylo způsobeno uvolněnou měnovou politikou centrálních bank a politikou vlád a s nimi spojenými zvýšenými financemi mezi investory, kteří se snažili své finance chránit a rozšiřovat pomocí investic právě do kryptoměn a pokračujícími investicemi ze strany firem. V první polovině roku 2021 pak nastala korekce, způsobena částečným výprodejem ze strany investorů, nicméně v druhé polovině roku cena opět začala růst.

Graf 2 Vývoj ceny bitcoinu 2017-2021 v USD



Zdroj: vlastní zpracování podle Statista.com

Pro lepší zobrazení vývoje jsou v Grafu 2 popsány hodnoty od roku 2017 v každém měsíci daného roku až do prosince 2021. Bitcoin měl na začátku roku 2017 hodnotu 1000 USD/BTC. Po pádu burzy Mt. Gox se bitcoin obnovila důvěra.

S náporem uživatelů začala být síť přehlcována. Čínští těžaři okolo společnosti Bitmain zatěžovali síť tzv. AsicBoostem („*algoritmická optimalizace výpočetní smyčky těžby*“) (Stroukal, 2021, s. 69), která umožnila zvýšit těžbu bitcoinu až o 20 %. V reakci na to vznikla nová kryptoměna Bitcoin Cash, jako odštěpení od Bitcoinu. Panika zajistila Bitcoin Cashi na konci 2017 hodnotu okolo 2 000 dolarů, což byla okolo poloviny hodnoty bitcoinu v té době. Majitelé bitcoinu si však kryptoměnu nechali a hodnota Bitcoin Cashe spadla na šestinu ceny bitcoinu.

Tržní kapitalizace byla v roce 2018 u bitcoinu pouze třetinová z celkové tržní kapitalizace, v srpnu to byla již polovina a hodnota se již nesnížila. Bitcoin byl v červnu 2019 nad hranicí 12 000 dolarů, postupně však v průběhu roku začal klesat.

12. března 2020 začala panika kvůli Covidu-19 a tím i výprodej bitcoinu, který se propadl během dne o třetinu. Za 5 dnů od této paniky ztratil o více jak 50 % své hodnoty před covidem až na hodnotu 4 400 dolarů. V květnu 2020 se však vrátil až na hodnotu 10 000 dolarů, o prázdninách vyšplhal na 12 000 USD/BTC.

Počátek roku 2021 byl pro bitcoin úspěšný. Hodnota 30 000 USD/BTC a tržní kapitalizace 70 % všech kryptoměn na trhu z něj udělali nejvíce rostoucí kryptoměnu. Společně s Ethereem tvořili okolo 90 % celkové tržní kapitalizace všech kryptoměn. Svou hodnotou zaujmul i investiční společnosti, kde např. Fond Grayscale získal více jak 3 % celkovou zásobu bitcoinu (650 000 bitcoinů). Tyto velké instituce nakoupili do roku 2021 skoro 7 % všech bitcoinů. Náhodná složka u bitcoinu je fork. Bitcoin zažil za svůj vývoj jeden hard fork a dva halvingy. Hard fork cenu zvýšili až o 2 000 dolarů, první halving změnil cenu o pár desítek dolarů, protože bitcoin v roce 2017 neměl ještě takovou hodnotu. Po druhém halvingu cena stoupla o téměř 600 dolarů v průběhu 6 dnů.

4.2 Cenový vývoj Etherea

Ethereum je druhá nejznámější kryptoměna, jejíž síť byla úspěšně spuštěna 30. července 2015 – 2 roky od popisu konceptu Etherea a o 6 a půl roku později od první zmínky i Bitcoinu. Na vývoj se pomocí crowdfundingu vybralo téměř 450 milionů korun. Ethereum je charakterizováno jako kryptoměna další generace, často označováno jako Bitcoin 2.0.

Účel Etherea je „*zdokonalení chytrých kontaktů*“ (Parke, 2021, s. 20) (3.4.1), které by decentralizovali všechny klasické dohody a smlouvy. Tímto způsobem se zásadně liší od Bitcoinu.

Tabulka 2 - Cena etherea 2015-2021

Rok	Cena v dolarech	Procento růstu
2015	1	-
2016	2,4	140 %
2017	10,46	335,83 %
2018	1 100	10 416 %
2019	108	-90,18 %
2020	177,4	64,26 %
2021	1338	654,23 %

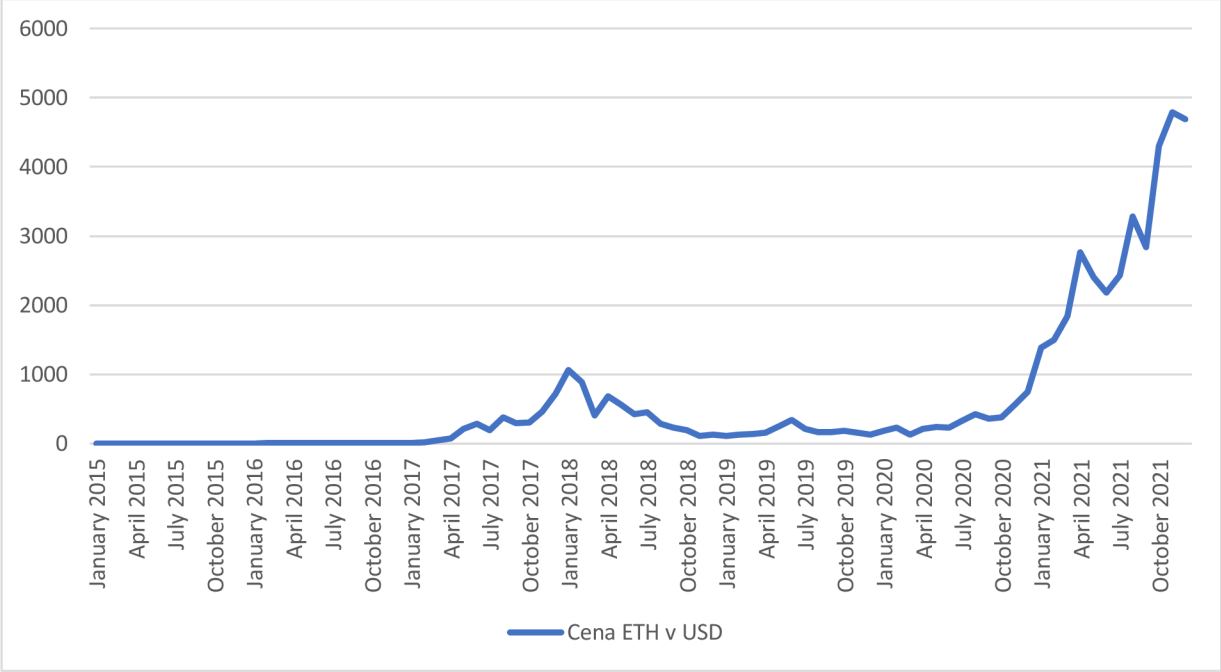
Zdroj: vlastní zpracování podle bitinfocharts.com

Ethereum začínalo s cenovkou 1 dolar, což bylo 100násobek hodnoty bitcoinu při jeho počátku. Ethereu se dostavila pozornost velmi brzy. Už v roce 2016, kdy začínal na 2,4 dolarech (Tabulka 2 - Cena etherea 2015-2021) se začal využívat potenciál smart kontraktu, kterého se ujmul projekt The DAO (3.4.3.). Cena v roce 2016 dokázala vzrůst až na 14 dolarů, skončila však 8 dolarech. Po krádeži 50 milionů dolarů v etherech cena klesla ze 17 dolarů až na 10 USD/ETH. Po tomto incidentu se rozvětvilo Ethereeum hard forkem (3.3.5) na Ethereum Classic a standardní Ethereum. Tento fork je stejně jako u bitcoinu součástí náhodné složky, protože se neopakuje v periodách, tudíž není obsažen v periodické složce.

Na začátku ledna 2017 se cena během čtyř dnů dostala z 8 na 10 dolarů. Tuto cenu si až na výkyvy pod 10 dolarů v průběhu ledna Ethereum udrželo, poté už jen stoupalo. 13. ledna 2018 byla hodnota 1 356 USD/BTC. To je meziroční nárůst 14 051 %. Tomuto růstu předcházel v říjnu 2017 hard fork v bloku 4 370 000. Meziročním růstem Ethereeum překonalo i nejoblíbenější a nejznámější bitcoin (Tabulka 1- Vývoj ceny bitcoinu 2010-2021). V lednu 2019 se snížila cena o 10 500 % Následoval opět hard fork v únoru 2019. Leden 2020 byl pro ethereum úspěšný a cena začala opět stoupat až k hranici 278 USD/ETH, a to po hard forku z 1. 1. 2020. Po 19. únoru začala cena rapidně klesat až ke 112 USD/ETH. To znamenalo pokles o 148 %.

V lednu 2021 začala cena na 737 dolarech. Cena se zvyšovala až překročila částku 1 400 USD/ETH. Tento nárůst byl opět značný. Meziroční nárůst 654 % a jen v měsíci lednu nárůst o 90 %. 12. května se Ethereum dostalo až na cenu 4 215 dolarů, což bylo až do 9. listopadu nejvyšší cena. Dalo by se říct, že tak Ethereum dosáhlo dvakrát tzv. ATH (All time high), a to v lednu 2018 a listopadu 2021. Ethereum si při vývoji prošlo celkem čtyřmi forky, které jeho cenu ovlivnili v řádu desítek dolarů v průběhu několika dnů.

Graf 3 Vývoj ceny etherea 2015-2021 v USD



Zdroj: vlastní zpracování dle Statista.com, Bitinfocharts.com

Pro zpřesnění a zlepšení přehlednosti vývoje etherea byl opět vytvořen graf (*Graf 3 Vývoj ceny etherea 2015-2021 v USD*), který ukazuje, že stejně jako u bitcoinu cena začala výrazněji stoupat až počátkem roku 2017. Na grafu je vidět, že v lednu 2018 cena překročila hranici 1 000 dolarů, což bylo historicky nejvíce a mnohonásobně více než za poslední 3 roky vývoje kryptoměny. Tomuto vzestupu předcházel Byzantium Fork v roce 2017, od kterého se ethereum dosatlo na 1000 USD/ETH za necelé tři měsíce. I přes tuto překonanou hranici je vidět, že Ethereum postupně ztrácelo na hodnotě a hranici 1 000 dolarů znovu překročilo až v lednu 2021.

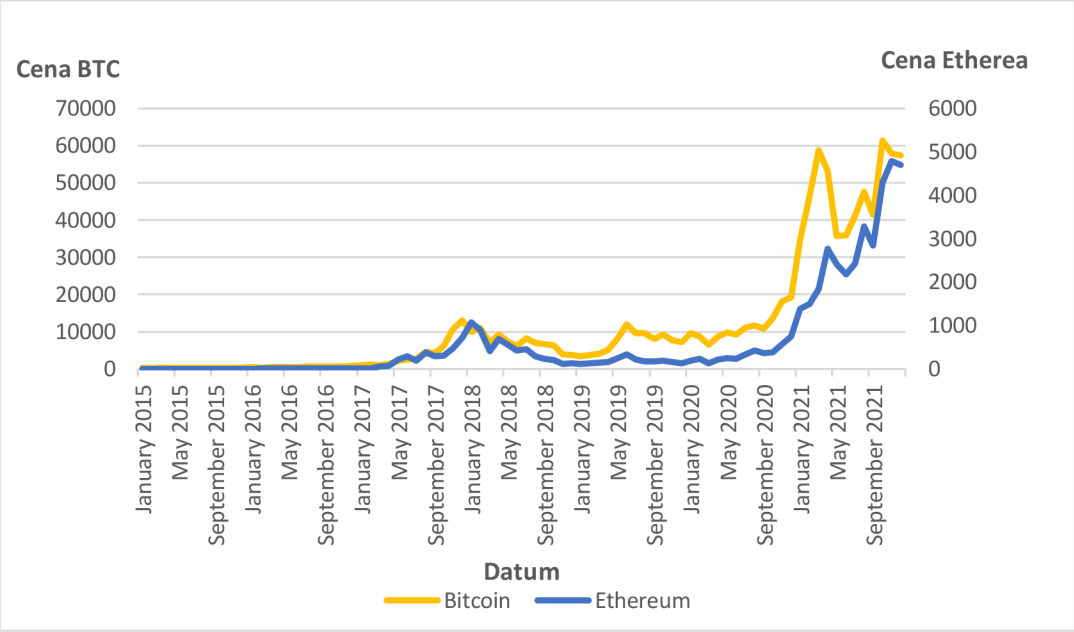
Po updatu sítě (forku) zvaném Muir Glucier 1. ledna 2020, který obsahoval vylepšení sítě etherea, jako např. zvýšení ceny operací, které jsou výpočetně náročnější nebo přidání

nového typu transakce. Cena etherea po tomto vylepšení začala opět růst. Ze 131 USD se dostala až na 277 USD/ETH.

Po tomto měsíci výrazně posílilo a v dubnu 2021 překonalo hranici 2 500 USD/ETH. V listopadu 2021 již překonalo hranici 4 500 dolarů, maxima pak dosáhlo 9. listopadu při částce 4 788 USD/BTC. To byl pro Ethereum zatím nejvyšší ATH za celý jeho vývoj a dosud nebylo překročeno.

4.3 Komparace vývoje ceny Bitcoinu a Etherea

Graf 4 Vývoj ceny bitcoinu a etherea 2015-2021



Zdroj: vlastní zpracování podle Bitinfocharts.com

Na obrázku je vidět, že ethereum od doby svého vzniku téměř kopíruje cenový vývoj bitcoinu, který má, co se kryptoměn týče, největší podíl na celkové tržní kapitalizaci. Také má největší objem mincí v oběhu, proto je vývoj hodnoty etherea přímo závislý na vývoji hodnoty bitcoinu. Graf 4 (*Graf 4 Vývoj ceny bitcoinu a etherea 2015-2021*) ukazuje rychlost růstu bitcoinu a etherea od roku 2015. Je zde vidět, že až do konce roku 2017 bylo tempo růstu obou kryptoměn prakticky zanedbatelné, ve čtvrtém kvartále tohoto roku dosáhl bitcoin svého cenového maxima, které bylo 19 497 USD, Ethereum svého cenového maxima v tomto období dosáhlo opožděně, a to až v lednu 2018, kdy jeho cena dosáhla hodnoty 1396 USD. Od této doby se pak u těchto kryptoměn projevil klesající trend přetrvávající až do ledna 2019, kdy se tento trend obrátil.

Další významný nárůst nastal v dubnu 2019, kdy se cena bitcoinu během dvou měsíců téměř ztrojnásobila. U etherea se ve stejném období cena více jak zdvojnásobila. Zhodnocení etherea v tomto období bylo více jak 136 %, u bitcoinu cena vystoupla o 206 %. Na grafu 4 (*Graf 4 Vývoj ceny bitcoinu a etherea 2015-2021*) je viditelné, že tento růst byl druhý nejvyšší za celé období obchodování s těmito kryptoměnami. Od této doby obě kryptoměny pokračují v trendovém růstu.
Po mírné korekci z března 2020, kdy se bitcoin propadl z 9 100 dolarů až na 5 000 dolarů a ethereum se propadlo z 236 na 112 USD.

4.3.1 Regulace

Většina regulací a omezení se týká pouze Bitcoinu, protože je stále více využívanou kryptoměnou než Ethereum, a tak je mu věnována větší pozornost. Již v roce 2014 byl prohlášen bitcoin britským úřadem za soukromé aktivum, tudíž nebylo nutné platit DPH. Evropská unie následně vydala dokument přes European Banking Authority, který zaujal negativní postoj vůči bitcoinu a navrhoval, aby byly kryptoměnové burzy povinnými osobami. Tím pádem byly nuceny hlásit zvýšené toky peněz skrze kryptoměny.

Na začátku července 2014 se cena BTC pohybovala okolo 649 dolarů, po vydání dokumentu se za 4 týdny snížila na 574 dolarů. Paypal 24. září začal přijímat Bitcoin jako formu placení. Cenu tato událost nijak výrazně nezměnila, spíše se od října začala mírně snižovat až na úroveň 315 dolarů.

8. srpna 2015 začal platit BitLicense právní rámec, který kladl na podnikání s bitcoinem a ostatními kryptoměnami vysoké nároky. Licenci nakonec získalo jen několik velkých firem, mezi nimi i směnárna Coinbase, která je jedna z nejúspěšnějších směnáren s kryptoměnami vůbec. Díky licenci ustala kritika kryptoměn, která považovala kryptoměny za protiprávní a rizikové. Zájem o obchodování s kryptoměnami začali mít i konzervativní institucionální investoři jako banky, pojišťovny, penzijní fondy nebo velké nadace, které by jinak nemohli do kryptoměn investovat. Po zavedení licence spadla cena v řádu týdnů o 60 dolarů z 273 na 213 dolarů.

V září 2015 začala čínská vláda s kapitálovými kontrolami, což donutilo čínské investory utéct ze země s penězi v hodnotě desítek miliard dolarů. Evropský soud uznal stížnost švédského podnikatele, který odmítal uvalení DPH na bitcoin švédskými úřady, které ho považovali za zboží, které by se muselo danit. Když Evropský soudní dvůr 22. září 2015 rozhodl, že bitcoin bude zařazen do stejné kategorie transakcí jako oběživa, bankovky

a mince, které mají podobu zákonného platidla, které je osvobozené od DPH, byl bitcoin na hodnotě 271 dolarů. Za necelé dva týdny se dostal na cenu 449 USD/BTC, což znamenalo růst 65 %.

V březnu 2016 byl bitcoin a podobné měny označen za aktivum obdobné penězům. Cena se ustálila na hranici lehce přes 400 dolarů. Ethereum v tuto dobu procházelo hard forkem.

Na konci roku znamenalo zavedení Futures kontraktů (3.3.10) přiblížení bitcoinu a etherea k statusu „normální investice“, což znamenalo příliv velkého množství kapitálu. Po hard forku bitcoinu na Bitcoin a Bitcoin Cash se cena dostala necelých 3 000 dolarů až na 19 400 USD/BTC. Ethereum začalo kopírovat vývoj bitcoinu a po hard forku z 16. října 2017 se dostalo 339 dolarů až na 1 300 dolarů v lednu 2018.

5. listopadu 2020 přišla regulace spíše pro samotné těžaře bitcoinu. Nastal totiž první halving, který snížil odměnu za vytěžení.

4.3.2 Medializace

Za růstem a popularitou Bitcoinu a Etherea stojí z velké části média a jejich medializace v televizi, novinových článcích, knihách, a hlavně na internetu, primárně na sociálních sítích jako je Facebook, Linkedin nebo Twitter. V této části bude popsány nejdůležitější mediální události spjaté s bitcoinem a etherem.

První zajímavější mediální událost se odehrála na konci roku 2014, kdy společnost Microsoft začala akceptovat bitcoin jakožto platební metodu na nákup aplikací, her a dalšího digitálního obsahu pro svá zařízení s operačním systémem Windows, mobilní telefony s Windows Phone a herní konzole Xbox.

Další událost, která značně ovlivnila kurz bitcoinu se stala koncem roku 2015, kdy se bitcoin objevil na titulní straně týdeníku The Economist, což způsobilo růst jeho o 28,5 % z 321 na 449 dolarů. Při vzrůstu v roce 2017 byl Bitcoin opět v zájmu médií, chvíli před tím, než se objevili první zmínky o financování projektů pomocí kryptoměn ICO.

19. dubna 2019 se objevila zpráva Roberta Muellera ohledně jeho vyšetřování ruských agentů, kteří měli pomocí kryptoměn ovlivnit americké volby v roce 2016. Cena v tomto období začala stoupat od 5 043 dolarů až na hranici téměř 9 000 USD/BTC na konci května 2019. V říjnu 2019 se ubrala pozornost médií na stablecoin Tether, který byl navržen, aby byl poměr mezi hodnotou amerického dolaru a tetheru 1:1. Objem obchodů tetheru

poprvé překonala objemy bitcoinu v dubnu 2019, což trvalo až do srpna 2019. Tether byl a stále je riziko pro prosperitu bitcoinu, protože se až 70 % transakcí bitcoinu provádělo skrz tether. I přes tyto zprávy hodnota bitcoinu v čase rostla. Z 4 000 dolarů se cena dostala až na 12 668 USD/BTC 26. června.

V roce 2021 bitcoinu velmi pomohl tweet od nejbohatšího muže planety, Elona Muska, který svým tweetem zvedl hodnotu o 15 %

4.3.3 Investiční potenciál

Obchodování s kryptoměnami má v současné době velký potenciál. *„Tento potenciál získaly díky své volatilitě a možnosti obchodování jak v dlouhých (long), tak v krátkých (short) pozicích, a to vše v průběhu celého týdne včetně víkendů“* (Hartman, 2018, s. 221).

Na burzách se obchoduje s kryptoměnou, kterou investor fyzicky vlastní a je možné, aby ji převedl do své peněženky nebo ji použil na jiné účely. Kryptoměny, stejně jako akcie, nemohou mít menší než nulovou hodnotu, a proto může investor držet kryptoměnu po delší dobu, bez obavy z toho, že by přišel o více peněz, než do nich investoval.

Investování do kryptoměn se prakticky neliší od investování do jiných instrumentů, jako jsou komodity nebo forex. Jediný rozdíl mezi kryptoměnami a akciemi nebo komoditami je vysoká volatilita, která je způsobena nízkou likviditou kryptoměn. Pro investora je odhadnout vhodný čas k vstupu na volatilní trh s kryptoměnami poměrně náročné a ideálním řešením je si udržet náhled na to, kam trh směřuje z dlouhodobého hlediska, a kdy se otevírají pozice směřující tímto náhledem.

Nejlepší období, kdy vstoupit do obchodu je *„těsně před tím, než se trend rozjede“* (Hartman, 2018, s. 223). Tento trend začal u Bitcoinu a Etherea v roce 2017 a přetrvává dodnes, jak je vidět v grafech 1 a 2 (*Graf 1 Vývoj ceny bitcoinu v letech 2010-2021*) a (*Graf 2 Vývoj ceny bitcoinu 2017-2021 v USD*).

Jak však tento trend rozpoznat. *„Částečným řešením může být sledování celého sektoru kryptoměn. Pokud všechny kryptoměny rostou, můžeme předpokládat, že jsou pravděpodobně v celém sektoru nakupovány "velkými hráči"“* (Hartman, 2018, s. 223). V návaznosti na tento předpoklad se dá očekávat, že trend poroste. Jak je vidět v grafu 4 (*Graf 4 Vývoj ceny bitcoinu a etherea 2015-2021*) v dubnu 2021, kdy hodnota bitcoinu začala výrazně klesat, vzhledem k regulacím ze strany Spojených států amerických a Číny, a ve spojitosti s tím začala klesat hodnota etherea. Pokud podobná situace nastane, je ideální

investiční strategií čekat na vhodnější dobu k investici, zachovat chladnou hlavu a nepropadnout FOMO.

5. Výsledky a diskuse

V praktické části byl vysvětlen a v grafech a tabulkách popsán cenový vývoj kryptoměn Bitcoin a Ethereum. Nejdříve byl popsán cenový vývoj Bitcoinu, poté Etherea. Byly zde popsány nejdůležitější události, které stály za změnou ceny těchto kryptoměn. Tyto cenové výkyvy byly v řádu několika procent, ale také byly popsány změny, kde se cena změnila např. o 10 000 %.

Bylo zjištěno, že na cenu měla vliv především medializace a regulace ze strany úřadů a vlád jednotlivých kontinentů a států, jako např. Evropa, Spojené státy americké nebo Čína. Vliv na cenu měli ale také forky, kterých proběhlo za vývoj kryptoměn hned několik. Po těchto forkách nastal vždy vzestup ceny, který byl způsoben tím, že se blockchain kryptoměny aktualizoval a zlepšila se rychlost transakcí nebo se změnili poplatky za platbu.

Následně byly tyto dva cenové vývoje komparovány mezi sebou. Bylo zjištěno, že se cena Etherea odvíjí od ceny Bitcoinu a kopíruje jeho vývoj, tudíž svých cenových maxim dosáhly téměř v identickou dobu.

Toto téma je velmi zajímavé a aktuální, a pro mnohé začínající nebo pokročilé investory může být tento druh investice interesantní zhodnocení vložených prostředků, avšak jak vyplynulo z praktické části této práce, tak kvůli vysoké volatilitě je trh s kryptoměnami velice rizikový, a proto doporučuji, aby byl do kryptoměn investován pouze menší objem peněz, přičemž by mělo být investiční portfolio diverzifikováno i do jiných druhů investic jako například akcie, dluhopisy nebo podílové fondy, které mají prověřenou historii, a jsou díky tomu méně rizikové. Z hlediska investičního potenciálu se jeví jako nejlepší kryptoměna Bitcoin, i přes to, že je pomalejší a technicky zastaralejší než Ethereum.

5.1 Dotazníkové šetření

V rámci dotazníkového šetření, které bylo prováděno od ledna do března 2022, byl u celkem 225 respondentů zjišťováno povědomí o kryptoměnách a názoru na kryptoměny.

Graf 5 Povědomí o kryptoměnách

Zdroj: vlastní zpracování

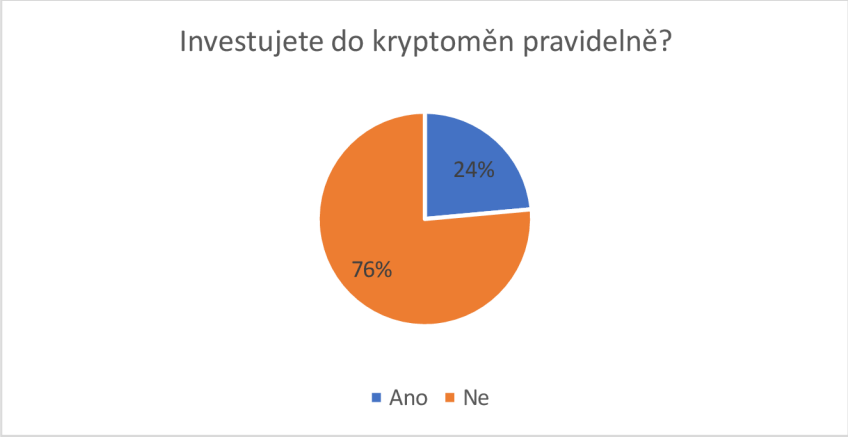
Z dotazníku z *Graf 5 Povědomí o kryptoměnách* vyplývá, že 96 % respondentů má povědomí o kryptoměnách a zná je. Toto povědomí je zapříčiněno především díky medializaci kryptoměn. Pouhá 4 % respondentů nevěděla, co to kryptoměna je.

Graf 6 Investice do kryptoměn

Zdroj: vlastní zpracování

Z grafu 6 (Graf 6 Investice do kryptoměn) vyplývá, že 35 % dotázaných někdy investovala do kryptoměn. Poměrná část, tedy 65 % nikdy do kryptoměn neinvestovala.

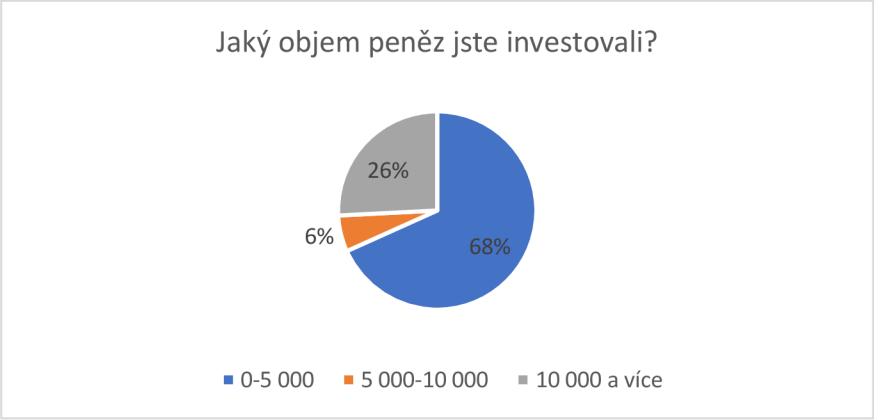
Graf 7 Pravidelná investice



Zdroj: vlastní zpracování

Na grafu 7 (*Graf 7*) lze vidět, že lidé, kteří kryptoměnu znají a investují, investují pravidelně. Těchto lidí je více jak tři čtvrtiny ze všech respondentů (76 %). 24 % respondentů neinvestuje vůbec nebo nepravidelně.

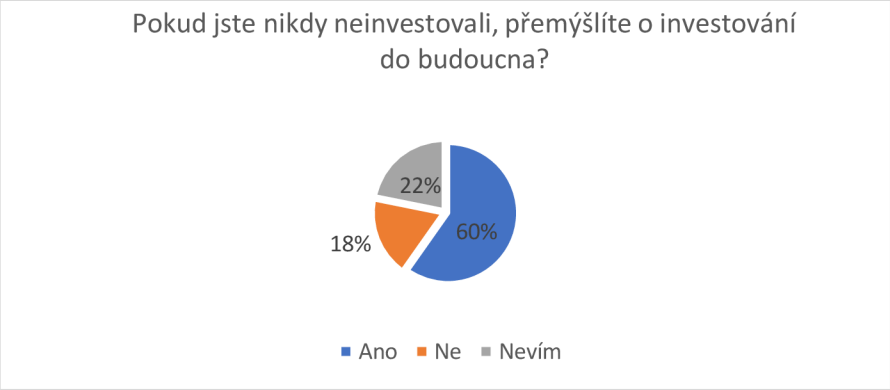
Graf 8 Objem investovaných peněz



Zdroj: vlastní zpracování

Objem peněz, který dotazovaní investovali do kryptoměn, vyplývá z grafu 8 (*Graf 8*). Nejvíce respondentů (68 %) investuje do 5 000 Kč. 26 % investuje v rozmezí 5 000 – 10 000 Kč a nejméně je těch, kteří investují více než 10 000 Kč (6 %).

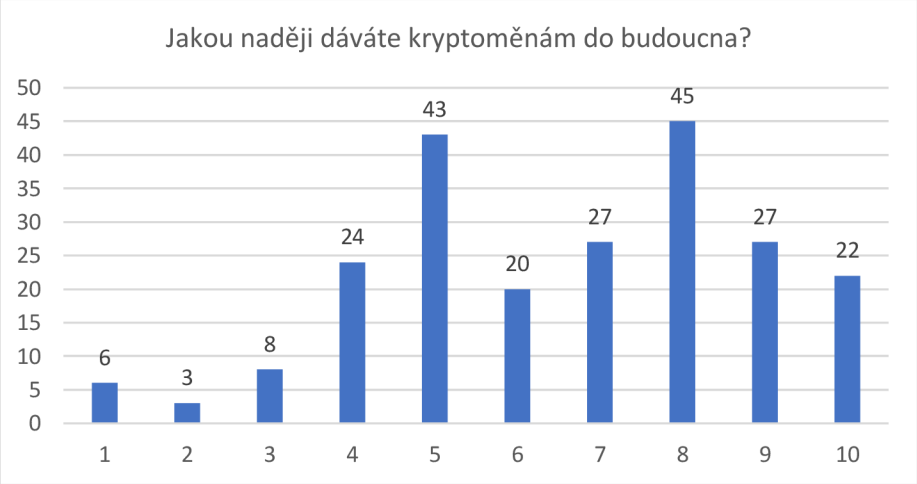
Graf 9 Investování do budoucna



Zdroj: vlastní zpracování

Z grafu 9 (*Graf 9*) lze vyčíst, že 60 % dotázaných zvažuje investici do kryptoměn. 18 % budoucí investici nezvažuje a 18 % respondentů neví.

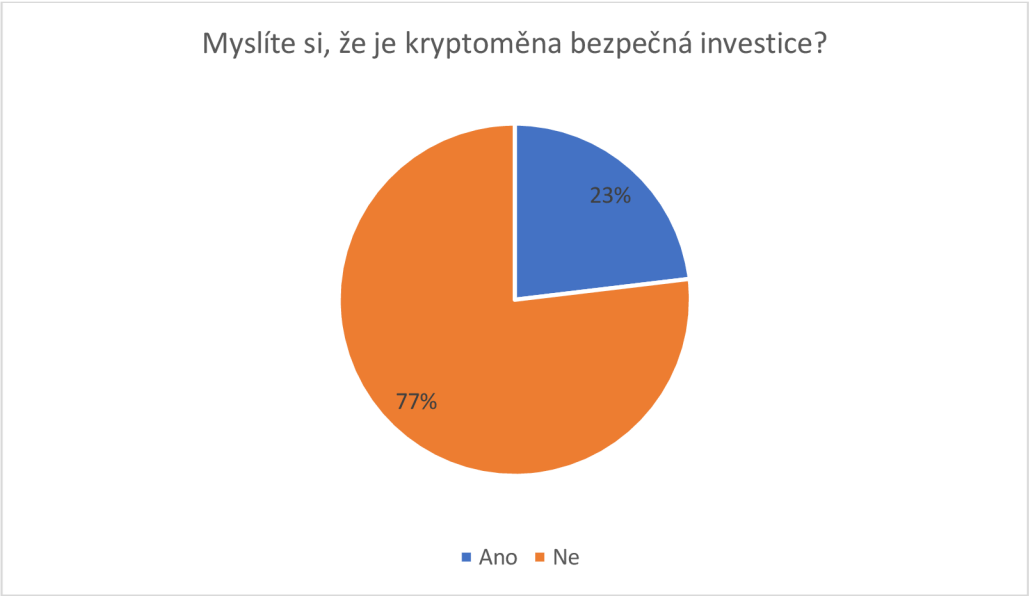
Graf 10 Perspektivnost kryptoměn



Zdroj: vlastní zpracování

V grafu 10 (*Graf 10*) je ve sloupcovém grafu zobrazeno, jak moc lidé věří, že kryptoměny uspějí v budoucnu, zda se jim zdá být kryptoměna perspektivní aktivum. Na stupnici od 1 do 10, kdy 1 znamená, že nedávají žádnou naději a 10 že jim naprosto věří, odpovědělo nejvíce respondentů (45) číslem 8 a 24 respondentů označilo číslo 4. To jsou tací, kteří v budoucnost kryptoměn věří méně. 43 respondentů má neutrální názor. Z tohoto grafu vyplývá, že se kryptoměny jeví spíše jako perspektivní.

Graf 11 Bezpečnost kryptoměn



Zdroj: vlastní zpracování

I přes to, že byly v posledních letech zavedeny opatření a zabezpečení pro zlepšení důvěryhodnosti kryptoměn, odpovědělo v grafu 11 (*Graf 11*) 77 % dotázaných, že se jim kryptoměny nejeví jako bezpečná investice. Jen 23 % z nich si myslí, že jsou kryptoměny bezpečné.

5.1.1 Výhody investice do kryptoměn

Jestliže se bude brát kryptoměna jako investice, a ne jako spekulace, tak lze na kryptoměny pohlížet jako na ostatní druhy investic, tudíž prostředek, jak zhodnotit své peníze.

Další výhodou může být samotná podstata kryptoměny, a tou je její nezávislost na centrální autoritě, která by jí mohla ovládat, popřípadě dávat rozkazy, omezovat ji nebo úplně zakázat. Decentralizovanost je zásadní pro zachování hodnoty kryptoměn, a proto je důležité, aby nebylo vlastnictví poměrné části etherea nebo bitcoinu v rukou centralizované organizace (stát, banka).

Anonymita je také nespornou výhodou, která může lákat k investování do kryptoměn. Bitcoiny zaslané z jedné adresy na druhou je těžké dohledat, nelze ani dohledat počet jednotek zaslané kryptoměny.

Výhodou se jeví i fakt, že transakce a jejich potvrzování probíhají rychle a bezpečněji než při normálním platebním styku. Některé kryptoměny mají za úkol zpracovávat transakce v co nejrychlejším čase, po celém světě a zadarmo.

Bitcoin i Ethereum jsou deflační měny, to znamená, že jich nelze vydat více, nejde snížit jejich počet ani jejich počet nelze nijak omezit.

Oproti fiat měně v hotovosti se nedá kryptoměna nijak zfalšovat. To z ní činí bezpečný a důvěryhodný nástroj k zasílání a ověřov ání plateb (Kaliský, 2018, s. 14).

5.1.2 Nevýhody investice do kryptoměn

Kryptoměna je digitální měna, což znamená, že existuje jen v elektronické podobě. To má za následek nemožnost platby bez přístupu k internetu. Člověk je tak omezen na platbu online nebo je nucen převést bitcoin na danou fiat měnu.

To, že kryptoměny jsou digitální měny ještě neznamená, že nemohou být odcizeny. Kryptoměnu lze uchovávat v peněžence, ta je však odcizitelná, stejně tak soukromý klíč, který znamená přístup k virtuálním mincím. Vykradeny můžou být i samotné burzy, nebo napadeny aplikace na nákup kryptoměn, kde mají majitelé uchovány kryptoměny pro možnost rychlého výběru nebo převodu na jinou kryptoměnu.

Anonymita může být i zneužita pro nákup drog, zbraní nebo financování terorismu. Vysoká volatilita je nepříjemností, kterou kryptoměny doprovází. Kurz kryptoměn je nevyzpytatelný a těžko odhadnutelný, a protože Bitcoin nemá dostatečnou historii (Ethereum už vůbec ne) jako jiné investice (např. akcie a komodity), tak se stále pro mnohé investory jeví jako riziková až nesmyslná a nebezpečná investice.

Na kryptoměny se nevztahuje žádné pojištění vkladů, takže je stále vnímána jako investice a nelze ji brát jako náhradu fiat měny.

6. Závěr

Cílem práce bylo analyzovat vývoj kryptoměn Bitcoin a Ethereum od jejich vzniku, tedy u Bitcoinu od roku 2009 a u Ethera od roku 2015 až po současnost. V teoretické části byly definovány kryptoměny a jejich vlastnosti. Byla popsána struktura blockchainu a jeho fungování a v návaznosti na to byly vysvětleny jednotlivé prvky, díky kterým může kryptoměna fungovat. Tyto prvky má Bitcoin odlišné od Etherea. Byly charakterizovány i způsoby uložení kryptoměn a rizika spojené s kryptoměnami.

V praktické části byla zaměřena pozornost především na vývoj ceny obou kryptoměn a činitele, kteří cenu v průběhu vývoje ceny ovlivňovali. Nejdříve byl analyzován cenový vývoj Bitcoinu, poté byl rozebrán cenový vývoj Etherea. U obou těchto kryptoměn byla popsána trendová složka, která je rostoucího charakteru. Od jejich vzniku zaznamenáváme u těchto zvolených kryptoměn cenové výkyvy, které přetrvávají až dodnes. Analýzou ceny v jednotlivých dnech, měsících a letech pomocí grafů, bylo zjištěno, že ani jedna z kryptoměn neobsahuje ani periodickou, ani náhodnou složku, tudíž je velmi obtížné predikovat budoucí cenový vývoj. Následně byl cenový vývoj těchto dvou kryptoměn komparován. Porovnáním bylo zjištěno, že jsou cenové výkyvy a celkový vývoj téměř identické jak u Bitcoinu, tak u Etherea.

Praktická část obsahovala i popis specifikovaných činitelů, kteří v průběhu let ovlivňovali cenu méně významně, nebo na ni působili výrazně, a změnili ji v řádu tisíců procent. Při pozorování byl zjištěn cenový růst po forku u obou kryptoměn, který však neměl periodické opakování, tudíž byl čistě náhodný a závisel spíše na přetíženosti a použitelnosti celé sítě kryptoměny.

Vytvořeným dotazníkovým šetřením byl zkoumán celkový pohled populace na kryptoměny a jejich vývoj. Analýzou výsledků bylo zjištěno, že je povědomí o kryptoměnách velmi rozšířené, je zde i zájem o investice do kryptoměn, avšak se kryptoměny nejeví jako příliš bezpečná investice.

V závěru byly popsány výhody a nevýhody investice do kryptoměn, což by měl zhodnotit každý investor, který přemýšlí o investici do kryptoměn. V porovnání s fiat měnou se může Bitcoin, Ethereum nebo jiná kryptoměna z hlediska technického pohledu jevit jako revoluční záležitost, ovšem má i svá úskalí, která nelze jen tak přehlédnout. Jen čas ukáže, jestli Bitcoin, přezdívaný „digitální zlato“, nebo Ethereum přijme většina společnosti jako zavedený prostředek ke směně.

7. Bibliografie

CAPITAL.COM, Tým, 2021. Předpověď ceny etherea: jaký je výhled druhé největší kryptoměny v roce 2021 a dál?. In: *Fxstreet.cz* [online]. [cit. 2022-02-15]. Dostupné z: https://www.fxstreet.cz/tym-capitalcom-predpoved-ceny-etherea-jaky-je-vyhled-druhe-nejvetsi-kryptomeny-v-roce-2021-a-dal.html

ČTK, 2021. Bitcoin od začátku pandemie zdražil o 450 procent. Poptávka po něm roste i v Česku. In: *Zpravy.aktualne.cz* [online]. [cit. 2022-02-15]. Dostupné z: https://zpravy.aktualne.cz/ekonomika/bitcoin-od-pocatku-pandemie-zdrazil-o-450-procent-na-1-2-mil/r~2baee028751511eba22aac1f6b220ee8/

DVOŘÁK, Miroslav, 2021. Salvador píše kryptoměnovou historii. Jako první země světa zavedl bitcoin coby oficiální platidlo, už jich drží stovky. In: *Cc.cz* [online]. [cit. 2022-01-14]. Dostupné z: https://cc.cz/salvador-pise-kryptomenovou-historii-jako-prvni-zeme-sveta-zavedl-bitcoin-coby-oficialni-platidlo-uz-jich-drzi-stovky/

HARTMAN, Ondřej, 2018. *Začínáme na burze: jak uspět při obchodování na finančních trzích: akcie, komodity, forex a kryptoměny*. Nové rozšířené vydání. Brno: BizBooks. ISBN 978-80-265-0780-2.

HOSP, Julian, 2018. *Kryptomeny*. Bratislava: TATRAN. ISBN 9788022209458.
KALISKÝ, Boris, 2018. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. [Praha]: IFP Publishing. ISBN 978-808-7383-711.

KOHOUT, Pavel, 2018. *Investice: nová strategie* [online]. Praha: Grada [cit. 2022-03-09]. ISBN 978-80-271-2101-4. Dostupné z: https://www.bookport.cz/kniha/investice-4996/
Kurz.cz: Co je to kryptoměna. In: *Kurz.cz: Co je to kryptoměna* [online]. [cit. 2022-03-09]. Dostupné z: https://www.kurzy.cz/kryptomeny/co-je-kryptomena

LÁNSKÝ, Jan, 2018. *Kryptoměny*. V Praze: C.H. Beck. ISBN 978-80-7400-722-4.

MÁLEK, Petr, Gabriela OŠKRDALOVÁ a Petr VALOUCH, 2010. *Osobní finance*. 2010. Brno. ISBN 9788021051577.

Moneta.cz: Investice. In: *Moneta.cz* [online]. [cit. 2022-03-09]. Dostupné z: https://www.moneta.cz/slovnik-pojmu/detail/co-je-investice

MUNOZ, J. a Michael FRENKEL, 2020. *The Economics of Cryptocurrencies* [online]. Taylor & Francis Group [cit. 2022-01-10]. ISBN 978-0-367-1910-0. Dostupné z: https://ebookcentral-proquest-com.infozdroje.czu.cz/lib/czup/reader.action?docID=6371520&query=The+Economics+of+Cryptocurrencies

PARKE, Soňa, 2021. *Ethereum: První česká kniha o Ethereu nejen pro individuální investory* [online]. Brno [cit. 2022-03-14]. Dostupné z: https://www.darujbitcoin.cz/ethereum-prvni-ceska-kniha-o-ethereu-nejen-pro-individualni-investory/?variantId=638

STROUKAL, Dominik a Jan SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Třetí rozšířené vydání. Praha: Grada Publishing. Finance pro každého. ISBN 978-802-7110-438.

ZIMA, Jakub, 2021. Poptávka po Bitcoinu klesá, protože instituce přecházejí do DeFi a altcoinů. In: *Cryptosvet.cz* [online]. [cit. 2022-02-15]. Dostupné z: https://cryptosvet.cz/poptavka-po-bitcoinu-klesa-instituce-prechazeji-do-defi-a-altcoinu/

8. Přílohy

Příloha 1 – Dotazníkové šetření na kryptoměny

Vážené dámy, vážení pánové,

jmenuji se Marek Mach a jsem studentem třetího ročníku bakalářského studia na České zemědělské univerzitě v Praze, obor Podnikání a administrativa. Vaše účast na výzkumu mi pomůže k úspěšnému dokončení studia.

Tento dotazník je anonymní a bude využit na zpracování praktické části bakalářské práce na téma Kryptoměny: porovnání výkonu a faktory úspěchu Bitcoinu a Etherea. Dotazník bude uzavřen k datu 10. březnu 2022

Tímto Vám děkuji za jeho vyplnění.

1.Vaše pohlaví
2. Nejvyšší dosažené vzdělání
3. Věk
4. Víte, co je to kryptoměna?
5. Investovali jste někdy do kryptoměn?
6. Investujete pravidelně?
7. Jaký objem peněz jste investovali?
8. Pokud jste nikdy neinvestovali, přemýšlíte o investovaní do budoucna?
9. Víte, co je to decentralizace? Popište.
10. Jaké znáte kryptoměny?
11. Jakou naději dáváte kryptoměnám do budoucna?
12. Myslíte si, že je kryptoměna dobrá investice?
13. Myslíte si, že je kryptoměna bezpečná investice?
(Parke, 2021, s. 12)