Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Podpora rozhodování při investování do kryptoměn

Diplomová práce

Autor: Richard Cibere
Studijní obor: Informační management

Vedoucí práce: doc. RNDr. Kamila Štekerová, Ph.D.

Odborný konzultant:

Hradec Králové duben 2021

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 30. 4. 2021 Jméno a příjmení

Poděkování:

Děkuji vedoucí diplomové práce doc. RNDr. Kamile Štekerové, Ph.D. za metodické vedení práce a trpělivost.

Anotace

Cílem práce je využití systému pro podporu rozhodování při investování do kryptoměn. V práci používám tři nástroje analýzy pro tvorbu portfolia či k měření rizika investice. V teoretické části se zaměřuji na popsání deseti vybraných kryptoměn. Dále jsem popsal fungování blockchainu a porovnal systémy konsenzu Proof-of-Work a Proof-of-Stake. V praktické části prezentuji výsledky portfolia vyhodnoceného skrze Value-at-Risk, Markowitzovu a Monte Carlo metodu. V závěru práce vyhodnocuji dosažené výsledky a přidávám doporučení pro investory.

Annotation

Title: Decision support systems for investing in cryptocurrency

The main topic of this thesis is investment in cryptocurrencies. In the theoretical part, I describe ten selected cryptocurrencies and compared Proof-of-Work and Proof-of-Stake mining systems. I also apply Decision support systems to cryptocurrency. In the practical part of the thesis, I describe investment strategies and the tools used to calculate risk, revenue and optimal portfolio. In detail, I describe investment tools I created and analyze the results these tools yield. In the thesis conclusion, I recommend strategies for cryptocurrency investment.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Kryptoměny jsou stále velkou neznámou pro mnoho lidí. Avšak tento fakt nebrání lidem vstupovat do této neznámé řeky a začít obchodovat. Tuto práci jsem sepsal právě pro lidi, kteří chtějí začít investovat do kryptoměn. Osobně jsem se ke kryptoměnám dostal v roce 2015, kdy jsem zakoupil svůj první Bitcoin. Od té doby jsem v tomto kryptoměnovém světě zůstal. Jedná se o svět dosud divoký, rád ho osobně přirovnávám k Divokému západu, době, kdy se dobývala Amerika. Již mnoho expertů a akademiků předpovědělo úpadek bitcoinu. Lidé také rádi přirovnávají kryptoměny k tulipánové horečce a nebo k Dot-com bublině. Myslím, že nikdo nezná budoucnost kryptoměn a nemůže posoudit, jestli kryptoměny změní svět, nebo v budoucnu zůstanou jenom úsměvnou vzpomínkou. Avšak já věřím, že kryptoměny mohou změnit svět. Přál bych si svět, který využívá celý potenciál blockchainu. Na druhou stranu, vše lze využít ke zlým účelům a blockchain může být také použit ke sledování lidí, jejich názorů a uvalit svět do dystopické vize popsané v knize 1984 od George Orwella.

V práci jsem využil tří analytických metod. Konkrétně Monte Carlo, Markowitzovu metodu a VaR metodu. Tyto tři metody jsem vybral, jelikož jsou často využívány pro tvorbu portfolií a měření rizik. Součástí mé diplomové práce je mnou vytvořený kalkulátor, který využívá právě všech tří uvedených metod. Tento kalkulátor může investor použít pro výpočet rizika, potenciálního zisku a možné ztráty portfolia. Kalkulátor lze využít i pro rozhodnutí, jestli je pro investora rentabilní těžba kryptoměn. Rozhodl jsem se pro vytvoření tohoto rozsáhlého kalkulátoru, abych usnadnil investorům jejich investiční rozhodnutí. Další součástí práce je rozhodovací strom, který je součástí podpory pro rozhodování. Tento strom přehledně zobrazuje investiční možnosti, které v mé diplomové práci prezentuji.

V práci jsem investorům nabídl pohled na těžbu kryptoměn. Proto také, jednou z investičních možností je právě těžba Cardana či Etherea. Tyto dvě kryptoměny jsem vybral pro jejich vysokou tržní kapitalizaci , a také proto, abych ukázal dva odlišné styly těžby.

2 Cíl práce

Cílem mé diplomové práce je představit potencionálním investorům deset nejhodnotnějších kryptoměn. Tyto kryptoměny jsem detailně popsal na základě dostupné literatury a následně přidal svůj pohled na budoucí vývoj jednotlivých kryptoměn. Tento rozbor považuji za důležitý, jelikož investor musí být informovaný, aby mohl učinit finanční rozhodnutí. Dále jsem čtenáři představil koncepty blockchainu a způsob jeho využití , a také jak lze těžit kryptoměny. Porovnal jsem dva nejrozšířenější konsenzy Proof-of-Work a Proof-of-Stake. Dalším cílem mé práce je seznámit investora s vytvořenou investiční kalkulačkou. Představil jsem detailní návod, jak mojí kalkulačku využít a veškeré výpočty ukázal na konkrétních příkladech. Pro ukázku funkcionality našeho kalkulátoru jsem vytvořil portfolio deseti nejhodnotnějších kryptoměn a následně provedl skrze kalkulátor Monte Carlo analýzu, VaR analýzu a Markowitzovu analýzu. Výsledky mých výpočtů jsem následně zanesl do rozhodovacího stromu a přidal porovnání výnosnosti investice do těžby Cardana a Etherea. Tuto výnosnost jsem také spočítal skrze vlastní kalkulátor. Rozhodovací strom zde slouží jako systém pro podporu rozhodování. Investor přehledně vidí, k jakým výsledkům lze dojít a skrze jaká rozhodnutí.

3 Metodika zpracování

Diplomovou práci jsem rozdělil na rešeršní a praktickou část. V literární rešerši jsem provedl rozbor odborné literatury, online publikací a dalších nejnovějších poznatků o zkoumané problematice. Literární rešerše obsahuje kapitolu popisující deset vybraných kryptoměn. Dále jsem se věnoval rozboru fungování blockchainu. Čtenáře jsem seznámil s fungováním Proof-of-Work a Proof-of-Stake konsenzy a porovnal oba dva systémy. Poslední kapitola v literární rešerši je věnována popisu rozhodovacích systémů a rozhodovacímu stromu. V praktické části investora podrobně provedu kalkulátory na bázi Value-at-Risk, Monte Carlo a Markowitzovým modelem stavby portfolia. Dále mu nabídnu pohled do problematiky těžby Etherea a Cardana. Následně porovnám výnosnost těžby obou kryptoměn. Na závěr jsem mé výsledky pro přehlednost při rozhodování zanesl do rozhodovacího stromu.

4 Literární rešerše

V této části diplomové práce jsem se věnoval rozboru fungování blockchainu, těžby, kryptoměnám a systémům pro podporu rozhodování. Také jsem podrobně popsal deset vybraných kryptoměn. Dále jsem popsal metody, které následně použiji v praktické části práce. Jedná se o investiční metody a teorie, které pomáhají investorům v rozhodování.

4.1 Blockchain

Vznik blockchainu předchází vzniku bitcoinu. Často jsou tyto dvě technologie vnímány jako celek, avšak Bitcoin je digitální měna a blockchain je technologie, na které je bitcoin založený [2].

Technologie blockchainu byla poprvé popsána v bitcoinovém „Whitepaperu“ Satoshi Nakamotem v roce 2008. Identita tvůrce je dosud neznámá a jméno Satoshi Nakamoto je pravděpodobně pouze alias. Dosud není známo, jestli za vznikem blockchainu byla jenom jedna osoba, či skupina osob. Stěžejní myšlenkou blockchainu je vytvoření peer-to-peer elektronického peněžního systému, který nepotřebuje banky, jakožto prostředníky umožňující transakce mezi dvěma entitami [1].

Satoshi dále popisuje, jak lze za pomocí „řetězů“ a „bloků“ vytvořit organizovanou a matematicky ověřitelnou sdílenou databázi. V blocích jsou zapsány transakce zachycené v daném čase. Transakci zde chápeme jako přesun kryptoměny mezi dvěma uživateli sítě. Tato transakce je veřejná, neměnitelná a ověřitelná. Blockchain těchto vlastností dosahuje za pomocí „podpisů“. Podpis se skládá z privátního a soukromého klíče. Tyto klíče jsou vytvářené za pomocí kryptografie [2]. Blockchain využívá k šifrování klíčů konkrétně protokol digitálního podpisu s využitím eliptických křivek [3].

Během transakce se uživatel prokáže privátním klíčem, který mu zaručuje potřebnou unikátní autoritu, dovolující provedení požadované transakce. Jakmile je transakce provedena, je zapsána s dalšími transakcemi do bloku, který je následně zapečetěn a nakonec je blok svázán s dalšími transakčními bloky. Tyto bloky jsou uzamčeny a propojeny pomocí hashe. Výsledkem použití funkce hashe je řetězec písmen a číslic o velikosti 32 bytů [2].

Jakmile dojde k vygenerování 32bytového řetězce skládajícího se z písmen a číslic, je tento údaj zapsán do dalšího transakčního bloku. Tento nový blok se chronologicky naváže na všechny starší, již vytvořené bloky. Pokud by se někdo pokusil vyjmout jakýkoliv blok či transakci, celá síť by tento krok zaznamenala. Díky těmto vlastnostem nemůže uživatel poslat stejný bitcoin na dvě různé adresy [2].

Všeobecně lze říct, že všichni účastníci nacházející se na blockchainové sítí fungují jako nody. Existuje několik typů nodů, avšak společným prvkem je potřeba specifického hardwaru. Blockchain je decentralizovaná síť a jedním z klíčových prvků této vlastnosti jsou principy Peer-to-peer. Tato funkce zajišťuje fungování sítě bez jakékoliv centrální autority či dedikovaného serveru. Vše funguje na základu závazku mezi uživateli sítě. Závazek známe v blockchainové síti pod pojmem mechanismus konsenzu. Konsenzus aplikuje pravidla, podle kterých uživatelé sítě potvrzují a validují informace psané do bloků. Za pomocí algoritmu dokáže konsenzus zajistit spolupráci a shodu mezi uživateli. Nejznámější konsenzy používané ve spojení s blockchainem jsou Proof-of-Work a Proof-of-Stake. Detailněji se budu věnovat těmto konsensům v samostatné kapitole. Blockchain je volně dostupný a kdokoliv se může stát nodem a zabezpečit bezpečnost celé sítě [5].

Nody se dělí především na dva typy, a to na „full nodes“ a na „light nodes“. Full nody obsahují kopii celé blockchainové historie, včetně všech bloků a transakcí. Light nody obsahují pouze záhlaví bloků (seznam obsahu), aby uživatel ušetřil co nejvíce místa na svém disku. Oba nody můžou suplovat funkci kryptoměnové peněženky [5].

Důležitým full nodem je mining node, který se zabývá procesem těžby dané kryptoměny (například bitcoinu). Lidem provozující těžební node se říká těžaři nebo mineři ze slova mining. Těžaři zajišťují bezpečnost sítě a potvrzují transakce. V momentě, kdy je provedená platná transakce kryptoměny, je tato transakce zařazena do fronty ke zpracování. Každá transakce obsahuje dobrovolný poplatek pro těžaře, avšak většinou existuje povinná minimální částka za transakci. Je pravidlem, že vyšší poplatky zajišťují rychlejší zpracování transakce, jelikož více motivují těžaře tyto transakce upřednostnit. Jakmile se nahromadí v čekací frontě dostatek transakcí, ale maximálně do velikosti 1 MB (u bitcoinu), jsou transakce uloženy do bloku. Pro těžaře je nejvýhodnější vytvářet co největší bloky, jelikož jsou poté odměněny vyšší odměnou. Takto nově vytvořený blok je potvrzen splněním zadaným komplexním matematickým úkolem. Aby byl tento úkol vyřešen, musí těžaři vypočítat správný hash, kterým jsou bloky zašifrované. Systém automaticky zadá požadavky na podobu výsledného hashe. Těžaři se tento hash snaží za pomoci těžebního programu najít. Kdo jako první rozluští tento matematický úkol, dostane odměny ve formě nových Bitcoinů (či jiné kryptoměny). Ostatní těžaři ověří správnost a potvrzený blok transakci přidají do blockchainu, který zde funguje jako účetní kniha. Všechny tyto potvrzené transakce jsou transparentní, nezaměnitelné a nelze je zpětně pozměnit [4].

Další vlastností full nodů je možnost hlasování o budoucnosti sítě. Hlasuje se například o možných úpravách parametrů bloků, těžebním algoritmu atd. Jestliže 51% uživatelů provozující full node dlouhodobě nesouhlasí se směrem vývoje, může vzniknout rozdělení sítě. Rozlišujeme „hard fork“ a „soft fork“. Pokud dojde k rozdělení sítě, developer vytvoří nového klienta, do kterého vloží původní zdrojový kód a implementuje žádanou úpravu parametrů. Provozovatelé nodů následně mohou začít používat nového klienta s upraveným kódem a začít provozovat node na této nové síti. Takto vzniknou dva blockchainy se stejnou historií, ale jiným budoucím vývojem [5].

4.2 Mechanismy konsenzu

Tato kapitola pojednává o rozdílném přístupu těžby kryptoměn. Satoshi Nakamoto představil koncept Proof-of-Work, avšak krátce po zveřejnění tohoto konceptu začali přicházet další talentovaní jedinci s vlastními úpravami tohoto konceptu. Vzniklo mnoho variací Proof-of-Work a postupně vznikl konkurent. Tento konkurenční mechanismus se nazývá Proof-of-Stake.

4.2.1 Proof-of-Work

V této práci jsem již detailně popsal fungování Proof-of-Work v sekci blockchain a proto v této části se bude jednat pouze o stručné shrnutí.

Proof-of-Work je originálním algoritmem konsenzu, který byl představen v rámci Blockchainové sítě. V této síti mohli uživatelé posílat digitální tokeny jeden druhému a tyto transakce následně verifikovat a vytvářet takto bloky v blockchainovém řetězci. Za tuto činnost zodpovídají těžaři, kteří za tuto práci dostávají odměnu. Všechny transakce, které prošli validací, jsou zařazeny do bloku podle data transakce. Tento proces se nazývá těžba. Proof-of-Work protokol je resistentní vůči kybernetickým útokům, jako je například denial-of-service (DDoS) útok [8].

4.2.2 Proof-of-Stake

Tento algoritmus konsenzu má stejný cíl jako Proof-of-Stake konsenzus, avšak funguje jinak. Hlavní rozdíl je ve způsobu validace transakcí v síti. Proof-of-Stake je založený na bohatství, které má držitel (uživatel) ve svém vlastnictví v rámci sítě. Toto bohatství se v rámci Proof-of-Stake nazývá „stake“. Tento stake je souhrn všech digitálních tokenů zamčených po určitou časovou periodu. Na rozdíl of Proof-of-Work zde není vyplácena odměna za validaci a potvrzování transakcí mezi bloky. V Proof-of-Stake dostávají těžaři odměnu za splnění daných úkolů a tato odměna je získaná z transakčních poplatků zaplacených v rámci sítě. Tento algoritmus tedy funguje na základě myšlenky alokace bohatství uživatelů v rámci sítě, kdy toto bohatství je převedeno na kryptoměny. Bloky zde vznikají díky tomuto principu

a není potřeba žádného výpočetního hardware. Na rozdíl od Proof-of-Work tedy nedochází ke spotřebě elektřiny a jsou tedy ušetřeny přírodní zdroje.

V Proof-of-Stake funguje nepřímá proporcionální závislost na velikosti sítě a počtu uživatelů, kteří stakují digitální tokeny. Pokud je tedy v síti mnoho uživatelů, kteří stakují své mince, pak je následná odměna pro všechny uživatele menší. Avšak pokud uživatelé drží více digitálních tokenů po delší dobu, dosáhnou vyšší odměny z transakčních poplatků. Jedná se o podobný princip jako v bance, kde dostanete větší odměnu od banky, pokud u ní uložíte velké množství peněz po dlouhou dobu.
V Proof-of-Stake uživatel který validuje transakce a přidává nové bloky je nazýván „forger" neboli česky kovář. Kovář poskytne svůj vlastní stake, aby mohl vytvářet nové bloky a přidávat validované transakce do těchto bloků. Kováři můžou přijít o svůj stake (své tokeny), , a tedy i o právo validovat transakce. Tato ztráta může být zapříčiněna podvodnou aktivitou kováře [7].

4.2.3 Porovnání Proof-of-Work a Proof-of-Stake

Proof-of-Stake a Proof-of-Work jsou mechanismy konsenzu široce používané v blockchainové technologii. Například Ethereum je zástupcem Proof-of-Work a Cardano Proof-of-Stake. Do budoucna i Ethereum přejde na technologii Proof-of-Stake [9].

Mezi nejdůležitější aspekty blockchainové technologie patří decentralizace a nezměnitelnost informací. Mechanismy konsenzu zajišťují ověřování informací v síti a chrání před DDoS (Denial-of-service attack) útoky. Dále zabraňují podvodům, jako je například „double spending", tedy, že nikdo nemůže zaplatit stejnou kryptoměnou dvěma různým uživatelům. Mechanismy konsenzu také zabraňují přerušení chodu sítě. Využívají pro to „fork" neboli rozdělení sítě na dvě části. Hlavní rozdíl tedy mezi těmito algoritmy spočívá ve způsobu odměňování účastníku za validaci transakcí.

Proof-of-Work algoritmus byl původně vynalezen Markusem Jacobsonem v roce 1999. Satoshi Nakamoto tento algoritmus použil pro vytvoření bitcoinu. Všechny

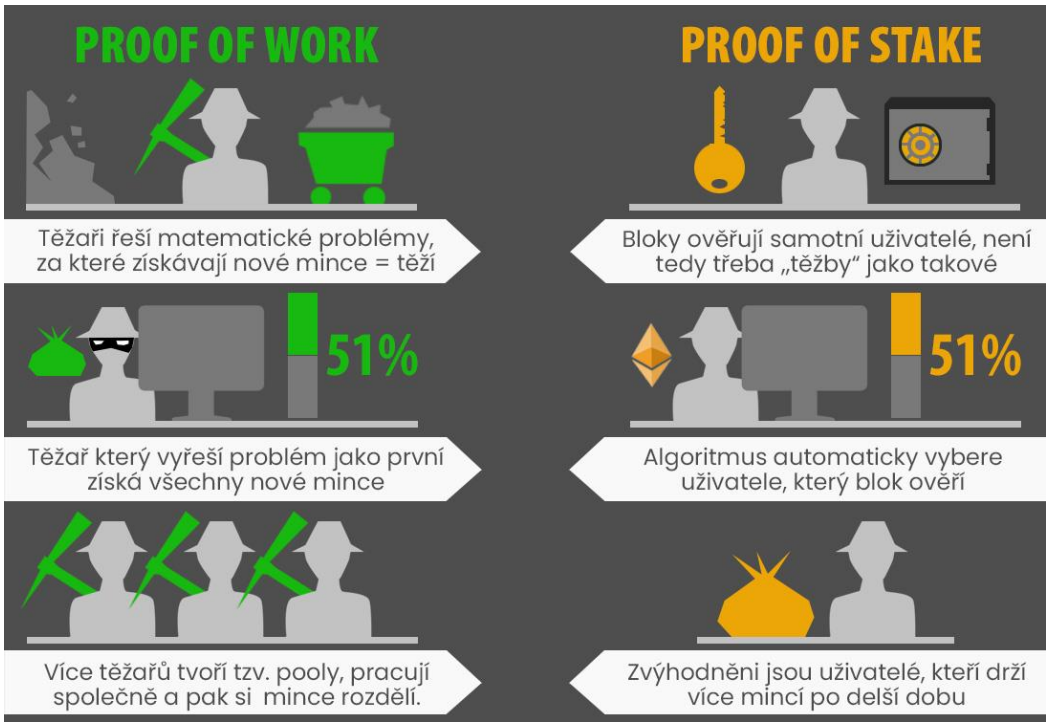
blockchainové transakce jsou umístěny do skupin. Tyto skupiny nazýváme „mempool“. V těchto skupinách těžaři verifikují každou transakci. Uživatelé bitcoinu vyžádají transakci, která je následně verifikována těžaři a přidána do dalšího bloku za pomocí zašifrovaného hashe z minulého bloku. Hash je zašifrovaná skrytá hodnota. Těžaři se poté snaží tuto hodnotu zjistit, a jakmile jí najdou, tak veřejně tuto skutečnost ohlásí ostatním uživatelům sítě. Ostatní uživatelé tuto skutečnost ověří, a pokud jí shledají za pravdivou, je tento těžař, za předpokladu že hash objevil jako první, odměněn. Těžaři pro řešení hodnoty hashe využívají velkou výpočetní sílu [8].

Těžaři musí řešit několik problémů:

- Asymetrický problém je velmi složitý na vyřešení, avšak jakmile je řešení nalezeno, ostatní těžaři jednoduše mohou ověřit správnost řešení.
- Tyto problémy nelze vyřešit jinak, než velkou výpočetní silou, neboli „brutální silou“. Avšak tento způsob vyžaduje velkou spotřebu elektřiny.

Proof-of-Stake využívá jiné principy. Skupina nodů (uživatelů), kteří poskytli stake jejich digitálních tokenů, ověřují transakce. Uživatel, který poskytl stake o vyšší hodnotě a v delším časovém pásmu, má vyšší pravděpodobnost, že dostane právo validovat transakci , a tedy i odměnu za validaci. V Proof-of-Stake není potřeba těžby jako v případě Proof-of-Work. Digitální tokeny (kryptoměny) jsou již vytvořené v síti. Validátoři mohou také přidávat bloky mnohem rychleji, jestliže jejich stake má v sítí vysokou hodnotu. Hlavní nevýhodou Proof-of-Stake je tedy možnost vytvoření monopolu jednoho uživatele. Na obrázku níže můžeme vidět grafické porovnání Proof-of-Work a Proof-of-Stake. [8].

Obrázek 1 PoW vs PoS



Zdroj:[6]

Můžeme porovnat neměnitelnost informací v síti, náklady na provoz, centralizaci a odměnu uživatelům sítě. Porovnání provedeme v tabulce 1, kterou nalezneme níže.

Tabulka 1 porovnání PoS a PoW

	PoW	PoS
Nezaměnitelnost	Z pohledu neměnitelnosti informací v síti je tento algoritmus nejlepší. Vytěžit jeden blok trvá deset minut. Jakmile je vytěženo 144 bloků (jeden celý den), tak je velmi těžké a nákladné se pokusit data změnit či zfalšovat.	Zde nedochází ke kontrole neměnitelnosti informací.
Nákladnost	Tento algoritmus vyžaduje masivní přísun elektřiny a je tedy velmi nákladným.	Tento algoritmus přímo nevyžaduje žádnou elektřinu.
Centralizace	Centralizace je zde velkou hrozbou. Vstupní bariéry pro investory jsou čím dál vyšší.	Nízké vstupní bariéry poskytují Proof-of-Stake vysokou decentralizaci sítě. Avšak hrozí zde vznik monopolu, jelikož stake se odvíjí od finanční síly investora.
Odměna	Těžaři dostávají odměnu, pokud dělají svojí práci	Validátoři nebo stakeři (lidé, kteří poskytují svůj stake) dostávají odměnu v závislosti na hodnotě a výši jejich stakovaných mincí a jak dlouho tento stake poskytují.

Zdroj: vlastní zpracování

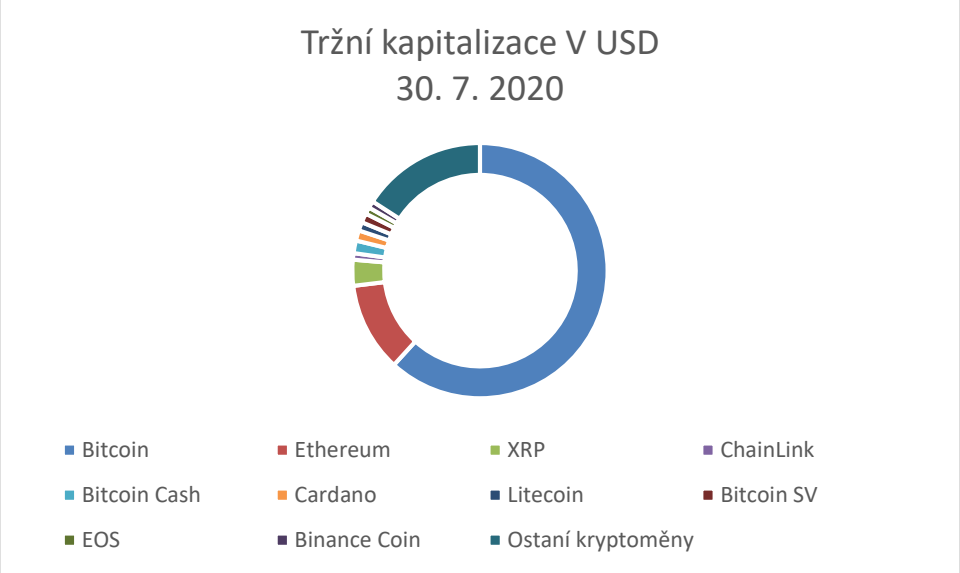
4.3 Kryptoměny

V této kapitole je stručně popsáno deset kryptoměn.

Tyto kryptoměny budou následně použity v praktické práci. Tento popis je důležitý pro případného investora, aby věděl, do čeho vkládá své finanční prostředky.

V následujícím grafu jsem vyobrazil tržní kapitalizaci k datu 30. 7. 2020 všech kryptoměn. Můžeme postřehnout, že Bitcoin zabírá více než 50 % celkové tržní kapitalizace. Na druhém místě nalezneme směsici ostatních kryptoměn kromě mnou vybraných devíti kryptoměn. Na dalším místě je Ethereum, následované Ripplem (XRP). Ve své práci jsem vybral deset kapitálově největších kryptoměn. Tyto kryptoměny jsem vybral, jelikož existuje tisíce kryptoměn, avšak pro investora je důležité vybrat takové kryptoměny, které odolají testu času a vydrží na předních příčkách i následující roky a cykly. Nelze opomenout, že toto pořadí se během let neustále mění, avšak nestalo se, že by jiná kryptoměna na první příčce nahradila bitcoin. Cíleně jsem vynechal Tether, který zastupuje v poměru 1:1 USD, a není tedy přímo kryptoměnou. V těchto deseti kryptoměnách nalezneme zástupce Proof-of-Work i Proof-of-Stake. Podrobně v následujících řádcích jednotlivé kryptoměny popíši, aby investor pochopil výhody, nevýhody a vlastnosti jednotlivých kryptoměn. Na konci popisu jednotlivých kryptoměn vždy také uvádím graf ceny dané kryptoměny v časově ohraničeném úseku. Tento roční úsek je vybrán za účelem následné cenové analýzy, která investorovi pomůže při finančním rozhodování.

Obrázek 2 Tržní kapitalizace



Zdroj: vlastní zpracování

4.3.1 Bitcoin

Jedná se o první kryptoměnu a je také světově nejrozšířenější. Vytvořena byla dne 3. 1. 2009 Satoshi Nakamotem. Bitcoin umožňuje provádět platby jakékoliv osobě a kdekoli na světě. Pro posílání bitcoinů není třeba žádný bankovní účet, stačí si vytvořit bitcoinovou peněženku. Peněženky jsou hardwarové či softwarové. Platby jsou provedeny za pomocí peer-to-peer technologie, která je plně decentralizovaná. Zpracování transakcí probíhá za pomocí těžařů.

Bitcoin nepřetržitě funguje již přes deset let. Během této časové periody došlo k technologickým vylepšením, snahám o regulaci , a také k hackům bitcoinových burz. Bitcoin i po deseti letech stále láká investory, kteří chtějí koupit komoditu, která nemá nad sebou centrální systém a je snadno přenositelná. Dále v této investici hledají možnost vysokého výdělku. Díky blockchainu je Bitcoin vysoce zabezpečený a neexistuje možnost Bitcoin zničit, jelikož celá sít je rozmístěna na statisících počítačů po celém světě. Každý provozovatel full nodu má ve svém počítači uloženou celou transakční historii, a tedy pro zničení Bitcoinu by útočník musel vyřadit všechny tyto počítače.

Bitcoinů je maximální množství 21 milionů. Tento limit je přímo zabudován v bitcoinovém protokolu. Avšak reálně je toto číslo menší, jelikož v průběhu let bylo mnoho Bitcoinů ztraceno. Hlavně na začátku, kdy Bitcoin stál pár centů či dolarů, mnoho lidí ztratilo své peněženky. Skoro nikdo tehdy nemohl tušit, jak moc se cena Bitcoinu změní za deset let. Bitcoin má tedy deflační mechanismus zabudovaný přímo ve svém kódu. Bitcoin je dělitelný na menší jednotky zvané satoshi. Jeden bitcoin má 100 000 000 satoshi. Do budoucna se počítá s tím, že transakce budou probíhat spíše v jednotkách satoshi než v celých Bitcoinech, vzhledem k růstu ceny. Mezi hlavní výhody bitcoinu můžeme zařadit:

- anonymitu – bitcoin lze považovat za poměrně anonymní kryptoměnu, avšak na trhu jsou již kryptoměny poskytující skoro stoprocentní anonymitu. Při zaslání bitcoinu na jinou adresu nevíte o daném účtu, komu patří. Neznáte tedy jméno vlastníka, adresu bydliště ani v jaké zemi se nachází. Stejně tak

příjemce neví žádné informace o vás. Momentálně existují jednotlivci a firmy specializující se na vyhledávání vlastníků daných peněženek a jejich adres. Firmy sledují transakce a snaží se nalézt stopy vedoucí k naleznutí majitele. Tyto služby jsou často využívány při hledání ukradených bitcoinů nebo při podezření z praní špinavých peněz.

- neovladatelnost – díky absenci centrální řídící autority nelze bitcoin řídit. Je možné ho dále vyvíjet, avšak nikdy nelze například vytvořit více než stanovených maximálních 21 milionů bitcoinů.
- masové přijetí – zaplatit bitcoinem je možné skoro po celém světě. Dále ho můžete směnit za klasické peníze díky síti bitcoinových automatů. Na tomto bankomatu se přihlásíte ke své peněžence a vyberete určitou část svého Bitcoinu ve vámi vybrané fiat měně. Avšak je potřeba počítat s poplatkem za transakci a výběr.
- Transakční rychlost – s bitcoinem lze platit 24 hodin denně, 7 dnů v týdnu. Transakce jsou provedeny během pár minut, a to i v případě, že příjemce platby je na druhé straně světa.
- Nepodléhá inflaci – díky pevně stanovenému maximálnímu množství nelze vytvořit žádné nové bitcoiny na rozdíl od klasických peněz.
- Poplatky za transakci – poplatek za transakci se může pohybovat v rámci pár korun. Avšak je potřeba zmínit, že při velké zátěži sítě tyto poplatky rostou a bitcoin přestává být vhodný pro transakční využití. Na trhu momentálně existuje mnoho lepších řešení v podobě konkurenčních kryptoměn.
- Bitcoin nelze zfalšovat – nikdo nemůže doma na svém počítači vytvořit falešný bitcoin. Díky blockchainu a síti těžařů by jakýchkoliv falešný bitcoin byl rychle odhalen a nebyl zařazen do oběhu.

Mezi nevýhody lze zařadit:

- Potřeba připojení k internetu – bitcoin nelze využít na místech, kde není pokrytí internetovou sítí. Bez internetu tedy nejste schopni odeslat transakci. Můžete transakce samozřejmě stále přijímat na adresu své peněženky.

- Volatilita – je velice složité až nemožné odhadnout budoucí cenu bitcoinu. Lze využít například technické analýzy, avšak ani ta nefunguje stoprocentně a odhadnout cenu, kterou bude mít bitcoin příští měsíc či snad rok je skoro nemožné. Lze pouze zatím předpokládat, že cena by měla být nad náklady těžby bitcoinu. Tyto náklady rostou vzhledem k vyšším cenám energie a samozřejmě díky pravidelnému „půlení“, což znamená krácení odměny, kterou těžaři dostávají za nově vytěžené bitcoiny. Také nelze opomenout rostoucí náročnost těžby.
- Nebezpečí krádeže – hackeři se neustále snaží najít způsob, jak odcizit Bitcoiny či jiné kryptoměny z vaší peněženky. Pokud používáte kvalitní hardwarovou peněženku a chováte se zodpovědně ke svým privátním klíčům a heslům, šance hackerů jsou téměř nulové. Avšak například na burzách takovéto zabezpečení není a můžete čelit krachu burzy, díky úspěšnému hackerskému útoku. Hrozeb na internetu je mnoho a technologii bitcoinu lze stále označit za poměrně mladou a mnoho nových uživatelů nezná možné nástrahy, které je mohou ohrozit.
- Zastaralost – bitcoin byl první kryptoměnou, avšak od doby jeho vzniku se na trhu objevilo tisíce nových kryptoměn. Mnoho z nich upadlo v zapomnění, jelikož se jednalo o nekvalitní projekty, mnohdy podvodné. Mnoho kryptoměn také nenalezlo uplatnění na trhu. Avšak momentálně existuje několik kryptoměn, které nabízejí lepší řešení než bitcoin či úplně nové funkce. Developerský tým vyvíjející bitcoin je silně konzervativní a jakýkoliv zásah do funkcionality bitcoinu je velice dlouho zvažován. Tato pomalá aplikace vylepšení může být i výhodou, avšak ostatní kryptoměny zlepšují své silné stránky velice rychle a mohou jednoho dne bitcoin předčít natolik, že upadne v zapomnění. Avšak tato možnost je krajně nepravděpodobná, jelikož díky prvenství a masové rozšířenosti spíše vznikne na trhu vzájemná spolupráce několika kryptoměn, jenž každá trhu nabídne jiné unikátní funkce [10].

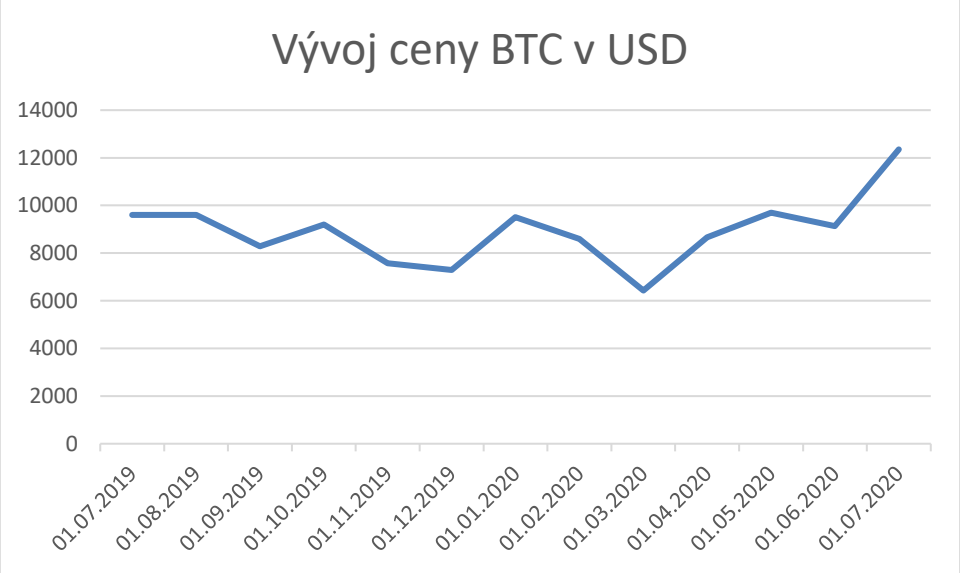
Budoucnost bitcoinu je samozřejmě nepředvídatelná, avšak díky působnosti na trhu déle než deset let, lze předpokládat že Bitcoin nezanikne. Avšak mění se struktura

uživatelů a držitelů bitcoinu. Dříve byla drtivá základna uživatelů složena z fanoušků nových technologií, kteří viděli možnost odpoutat se od bankovního sytému. Momentálně se o bitcoin zajímají technologičtí giganti a banky. Jako příklad můžeme uvést zavedení bitcoinu do sítě PayPal [11].

Trend se tedy ubírá k masové adaptaci a k institucionálnímu využití bitcoinu. Pokud tedy bereme v potaz rostoucí zájem ze strany institucí, lze díky omezenému množství Bitcoinu předpokládat růst jeho ceny. Velký zvrat pro bitcoin nastal v roce 2021, kdy šéf firmy Tesla Elon Musk (druhý nejbohatší muž na světě) oznámil, že část firemních zisků uloží právě v bitcoinu. Tento krok učinil, aby ochránil firemní zisky před inflací a také využil bitcoin jako investiční nástroj. Toto prohlášení vyvolalo masivní růst ceny bitcoinu a zájem ostatních institucí [33].

Na grafu níže vidíme vývoj ceny bitcoinu v daném časovém úseku. Tento ohraničený časový úsek byl vybrán za účelem výpočtu návratnosti investice do bitcoinu a slouží v následujících kapitolách pro analýzu vybranými metodami.

Obrázek 3 Graf BTC



Zdroj: [12]

4.3.2 Ethereum

Laická veřejnost si pod pojmem kryptoměna většinou představí nejznámější kryptoměnu bitcoin. Avšak od vzniku Bitcoinu uběhlo již mnoho let a svět kryptoměn a blockchainu se stal mnohem rozmanitější a nalezneme na tomto trhu velké množství konkurenčních projektů. Mnoho projektů upadlo do zapomnění, avšak jiné prokázaly svojí hodnotu a obstáli v časovém horizontu na trhu. Také nabídli uživatelům mnoho funkcí, které bitcoin nenabízí. Do této úspěšné skupiny můžeme zařadit právě kryptoměnu ethereum a jeho token ether.

Ethereum je momentálně kapitálově druhou nejhodnotnější kryptoměnou. Vznikl v roce 2013 a vytvořil ho tehdy devatenáctiletý Vitalik Buterin jako decentralizovanou platformu pro provoz a tvorbu aplikací. Během krátké doby toto ICO (Initial Coin Offering) nahromadilo dostatečné množství zdrojů pro ukončení vývoje a spuštění systému. V principu se ethereum od bitcoinu příliš nediferencuje. Vychází, jako i bitcoin, ze systému decentralizovaného blockchainu.

Avšak při podrobném pohledu na tuto kryptoměnu můžeme nalézt řadu rozdílů mezi oběma platformami. Bitcoin se zaměřuje na provádění decentralizovaných plateb a jeho hlavní přidaná hodnota spočívá roli směnného prostředku a slouží jako uchovatel hodnot. Na druhou stranu ethereum se zaměřuje na vytváření decentralizovaných aplikací, které slouží jako alternativa komerčních programů. Token ether, jenž je měnou v této síti, představuje pouze jeden z mnoha produktů fungujících na systému takzvaných chytrých kontraktů.

Na následujících řádcích vysvětlím princip fungování chytrých kontraktů. Principiálně se jedná o jednoduchý kód, určující směnu peněz, majetku, obsahu, podílů a dalších cenných komodit. Potřebné informace jsou zaneseny do blockchainu a k realizaci daného příkazu v kódu dojde v případě, kdy jsou splněna předem daná kritéria. Veškeré kroky využívají kryptografii a jsou prováděny skrze decentralizované sítě. Transakce se stane platnou v momentě zapsání jejího výsledku do blockchainu.

Hlavní výhodou systému chytrých kontraktů je jejich univerzálnost. V tomto daném prostředí etheru může kdokoliv vytvořit jakoukoliv situaci, v níž dvě strany uzavřou dohodu či transakci. Nemusí se nutně jednat o finanční transakci. Může se jednat například o volby, komunikaci či dojednávání služeb. Stačí pouze vytvořit potřebný kód a stanovit podmínky transakce či smlouvy.

Nutné je také pochopení tokenu etheru v ekosystému etherea. Pro realizaci chytrých kontraktů je zapotřebí výpočetního výkonu. Avšak za tento výpočetní výkon, který vyžaduje specializovaný hardware a elektrickou energii je potřeba řádně kompenzovat poskytovatele výpočetního výkonu. Zde právě na řadu přichází Ether a slouží jako „palivo" ekosystému etherea. Ether tedy slouží pro uhrazení nákladů poskytovateli výkonu, který je zprostředkovaný těžaři při provedení chytrého kontraktu. Označení palivo avšak není úplně přesné, jelikož nedochází k zániku etheru.

Můžeme tedy nalézt podobnost těžby etheru a bitcoinu, ale s tím rozdílem, že v případě etheru neexistuje horní hranice maximálního množství vytěžených tokenů. Také nedochází ke snižování intenzity těžby. Rychlost těžby je ovlivněna vznikem nových měn v rámci stejného blockchainového ekosystému a jeho rozštěpení.

Ethereum lze uložit na blockchainovou peněženku, stejně tak jako i jiné kryptoměny. Tuto kryptoměnu lze získat těžbou nebo jejím zakoupením na kryptoměnové burze či směnárně. Další možností je zakoupení této kryptoměny ve specializovaném bankomatu.

Můžeme si také položit otázku, proč je tato konkrétní kryptoměna druhou kapitálově největší kryptoměnou. Tuto pozici si ethereum vysloužilo určitými výhodami nad bitcoinem či jinými kryptoměnami. Hlavní výhody etherea jsou:

- necenzurovatelnost – žádný nápad či myšlenka není zavržena a je zde možnost realizace a implementace bez jakékoliv cenzury.
- jednoduchost – pro vytvoření chytrého kontraktu není potřeba žádného specifického vzdělání a jedná se tedy o velice jednoduchý krok.
- univerzálnost – lze vytvořit jakýkoliv transakční systém, hry či srovnávače. Všechny tyto vytvořené aplikace si zároveň udržují decentralizovaný a anonymní charakter.
- možnost úprav – platforma je plně modifikovatelná a snadno se přizpůsobí potřebám trhu.
- imunita – blockchain etherea je plně imunní vůči pokusům třetích stran o provádění nežádoucích změn a modifikací.
- bezpečnost – systém je chráněn proti únikům dat a hackerskými pokusy.

Ethereum má ovšem i slabé stránky. Díky specificky navrženému systému chytrých kontraktů má síť etherea nižší rychlost. Další nevýhodou může být nezměnitelnost již vytvořených chytrých kontaktů a nelze tedy upravit přehlednutou chybu. Také neustálý vývoj sítě může být pro někoho nepřehledný.

Jak již bylo uvedeno výše, ethereum představuje alternativní platformu pro potencionální tvorbu decentralizovaných aplikací. Hlavní ambicí etherea je nabídnout alternativu proti velkým technologickým gigantům, kteří často nabízejí citlivé osobní údaje třetím stranám. Ethereum nabízí maximální decentralizaci a anonymitu [14].

Momentálně existuje na blockchainové síti etherea 1897 DApps (digitální aplikace nebo programy, které existují na blockchainu) [13]. Níže uvádím několik zajímavých aplikací, které představují alternativu běžně používaných systémů třetích stran:

- Enzypt – umožnuje peer-to-peer kryptograficky zabezpečené posílání souborů.

- BrickGame – internetové kasino zabezpečené anonymitou a kryptografií blockchainu.
- Wibson – trh pro prodej a nákup dat.
- PledgeETH – anonymní fundraisingové kampaně.
- EtherTweet – komunikační kanál bez cenzury [13].

Jak lze z uvedených příkladu vyčíst, nejedná se o žádné revoluční nápady. Hlavním rozdílem je zde decentralizace, zachování intimních dat a anonymity uživatelů. V případě finančních produktů lze eliminovat zpronevěru finančních prostředků.

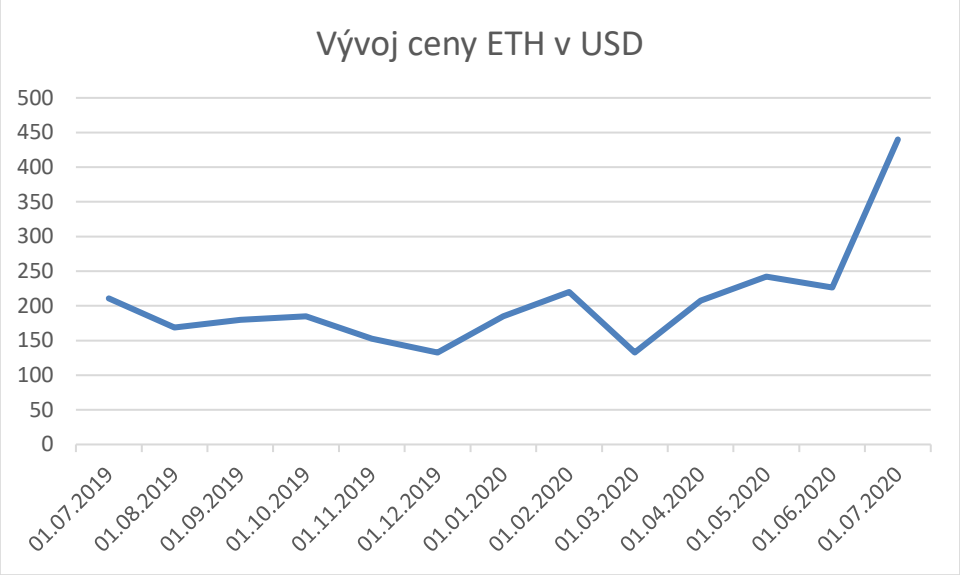
Za dobu své existence prošlo ethereum stejně jako bitcoin rozštěpením (hard forkem). V roce 2016 se komunita neshodla na řešení problému s projektem DAO. Tento projekt získal skrz komunitní financování přes 150 milionů dolarů, avšak padesát milionů dolarů následně neznámý hacker odcizil. Tisíce investorů, kteří vložili finanční prostředky, a důvěru v tento projekt bylo ohroženo. Komunita uživatelů následně rozhodla o hard forku, který odcizené peníze přesunul do nového kontraktu a okradení investoři mohli tak získat svoje finanční prostředky zpátky. Tento krok byl vnímán i negativně, jelikož se jednalo o centralizovaný zásah do ekosystému. Hlavním bodem kritiky byla změna pravidel v průběhu hry a anonymity. Tvůrci etherea museli tedy rozhodnout, zdali budou věrni své myšlence, na které je celá síť postavena, nebo jestli vrátí peníze investorům. Hlasováním došlo tedy k rozštěpení sítě a vznikly dva systémy. Nový systém dostal jméno Ethereum Classic. Oba systémy mají až do bodu rozštěpení stejnou historii, avšak od tohoto okamžiku začal jejich samostatný vývoj [15].

Budoucí vývoj ceny etherea lze pouze odhadovat na základě technických analýz či fundamentů. Avšak co se týče budoucího technického vývoje, lze dopředu říct, jakým směrem se bude ethereum vyvíjet. Podle developerů etherea se systém sítě z Proof-of-Work změní v blízké budoucnosti na Proof-of-Stake [9]. Dále se ethereum zaměří na DeFi (decentralizované finance) projekty. Hlavním aspektem DeFi je půjčování finančních prostředků v rámci blockchainové sítě a dostávat za tuto půjčku úroky. Díky technologii blockchainu je taková půjčka „bezriziková“. Dalším technologickým

vylepšením je projekt Plasma, jenž snižuje požadovaný výpočetní výkon potřebný pro realizaci chytrých kontraktů.

Níže jsem uvedl tabulku vývoje ceny etherea v období od 1. 7. 2019 do 1. 7. 2020. Z grafu lze vyčíst rostoucí tendenci ceny v posledních měsících.

Obrázek 4 Vývoj ceny ETH



Zdroj: [12]

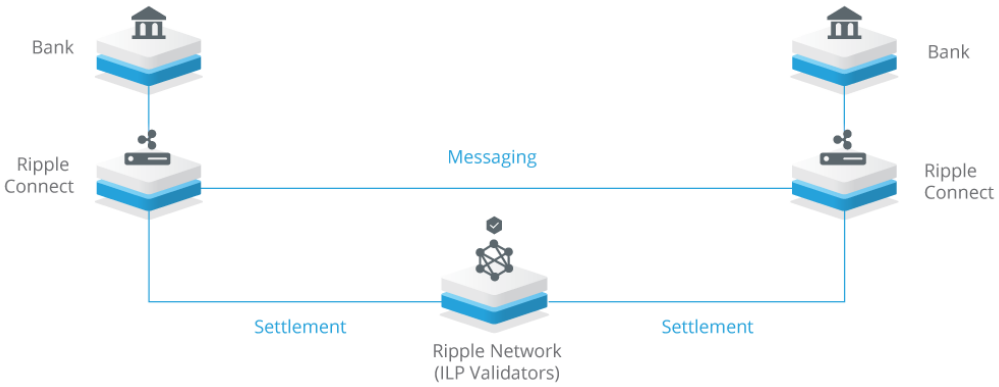
4.3.3 XRP (Ripple)

Kryptoměna XRP zaujímá třetí pozici v rámci nejhodnotnějších kryptoměn. Společnost Ripple, vznikla v roce 2012. O XRP často mylně slyšíme jako o kryptoměně ripple, avšak tento název patří společnosti, která poskytuje softwarové řešení používající právě token XRP. Tato kryptoměna se zaměřuje na převod fiat měn a dalších aktiv. Jedná se o decentralizovanou platební síť a vyznačuje se vysokou rychlostí převodu. Sít XRP je schopna převést finanční prostředky i v rámci mezinárodního převodu v průměru čtyř sekund. Další konkurenční výhodou jsou velmi nízké transakční poplatky.

Hlavním cílovým sektorem pro XRP je tedy bankovní sektor. V současnosti využívá výhod XRP desítky finančních institucí. Tyto instituce využívají především síť s názvem RippleNet. XRP tokeny jsou v síti využívány pro přenos informací a nelze je těžit jako například ethereum či bitcoin. XRP tokeny také slouží jako most mezi různými páry fiat měn a zajišťují jejich likviditu.

Pro představu fungování sítě lze uvést stručný příklad. Pokud budeme chtít poslat například tisíc korun českých do Japonska, nakoupí česká banka XRP tokeny v hodnotě tisíc korun. Tyto tokeny následně převede během 4 sekund do japonské banky, která XRP tokeny prodá a následně připíše ekvivalent jednoho tisíce korun českých na účet příjemce v japonském jenu. Informace které vznikly při převodu z české banky do japonské, jsou následně zapsány do XRP Ledgeru, který je obdobou bitcoinového blockchainu. Takto zapsána data jsou dohledatelná a volně přístupná. Bankovní instituce díky XRP technologii posilují svojí důvěryhodnost. Tokeny XRP slouží také pro úhradu transakčních poplatků. Po zaplacení převodu je token zničen, takže celkový počet tokenů klesá. Vzhledem k velmi nízkému transakčnímu poplatku a vysoké emisi tokenů, probíhá toto ničení tokenů pomalým tempem a stále existuje přibližně 99% původní emise. Na obrázku níže je zjednodušené vyobrazení transakce mezi dvěma bankami. Princip této transakce jsem již popsal výše, lze si avšak všimnout, že tato transakce je provedena validátorem.

Obrázek 5 Fungování Ripple network



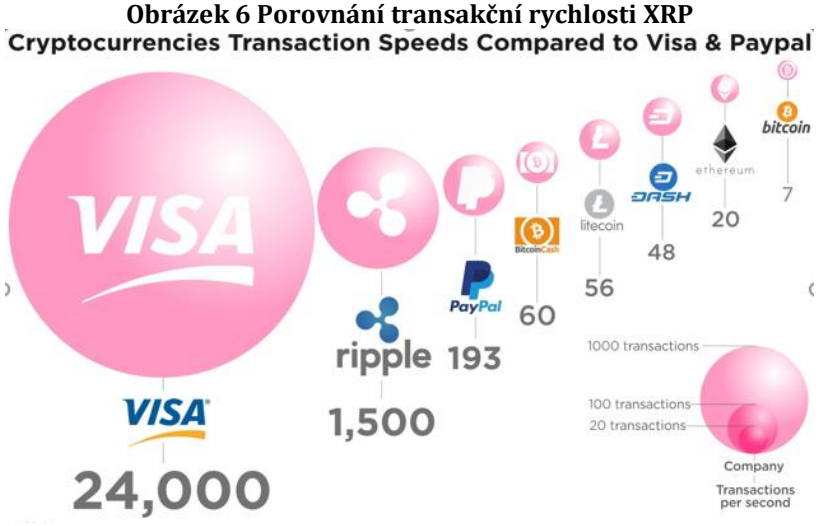
Zdroj: [16]

Transakce v síti musí být ověřena. Tuto roli plní validátoři, ale způsob ověření probíhá jinak než například u Bitcoinu. Je zde využit, takzvaný Ripple Protocol Consensus Algorithm, jenž pracuje s důvěryhodností mezi jednotlivými validátory. Jestliže se na pravosti převodu shodne 80 % validátorů, je transakce považována za ověřenou a následně je automaticky zanesena do Ledgeru. Roli validátorů zde představují banky či jiné finanční instituce. Další možnou rolí mimo ověřování transakcí je zajišťování možnosti vstupu do RippleNet skrze Ripple Gateways i běžným uživatelům.

Mimo jiné XRP umožňuje investičním fondům či bankám obchodovat také s fyzickými aktivy, jako je zlato či ropa. Do Ledgeru je proveden zápis o transakci za pomocí emisí takzvaných IOU („I Owe You“) tokenů. Nabízející strana obchodu veřejně slíbí splacení svého dluhu věřiteli za určité aktivum a zároveň vydá IOU token. Tyto tokeny lze uložit do hardwarové či softwarové peněženky. Další funkcí XRP jsou takzvané escrows. Jedná se funkci podobnou chytrým kontraktům. Uživatel uzamkne do escrows libovolný počet tokenů a při splnění předem daných podmínek dojde k odeslání tokenů na účet příjemce. Kritérium může být například datum, a pokud nedojde k naplnění kritéria, jsou tokeny po určitém čase zaslány zpátky na účet odesílatele.

Výhodou XRP je vysoký objem transakcí (až 1500 transakcí za sekundu). Pokud to porovnáme například se službou PayPal, která zvládá 193 transakcí za sekundu, je vidět velký rozdíl, avšak oproti lídru na trhu VISA, která zvládne 24 000 transakcí za sekundu, není to číslo až tak vysoké, proto je potřeba aby XRP nabídl i další konkurenční výhody. Do budoucna se díky škálovatelnosti předpokládá rychlost 50 000 transakcí za sekundu [17].

Obrázek 6 Porovnání transakční rychlosti XRP

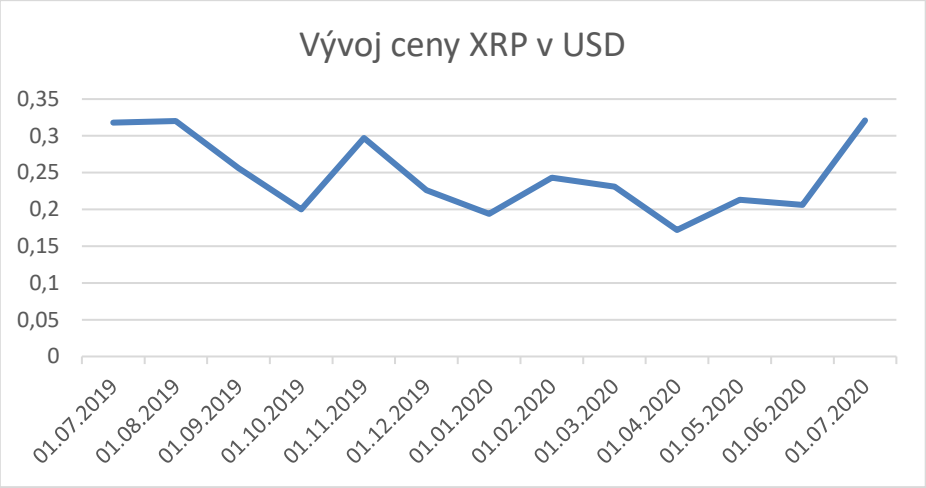


Zdroj: [18]

Zde je nutné zmínit takřka minimální poplatek za transakci, který je okolo 0.0002 dolarů. Také stoprocentní transparentnost transakcí je velikou výhodou tokenu XRP. Samozřejmě nejde opomenout i nevýhody. Síť je z pohledu kryptoměnové komunity centralizovaná, jelikož existuje pouze 871 validátorů transakcí a 60 % tokenů vlastní společnost Ripple. Také je potřeba zmínit vysokou volatilitu XRP, která nemusí být pro banky vyhovující [19].

Budoucnost tokenu XRP je nejistá. Momentálně o tuto funkci má zájem například UniCredit či Santander, avšak je otázkou, zdali je token XRP potřebný pro fungování sítě. Investor musí být opatrný při investici do tohoto tokenu, jelikož do budoucna mohou banky token XRP nevyužívat a do sítě RippleNet vnést vlastní token bez veřejné nabídky ke koupi tohoto tokenu.

Obrázek 7 Vývoj ceny XRP



Zdroj: [12]

4.3.4 ChainLink

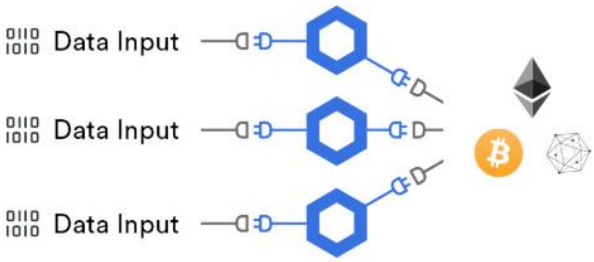
ChainLink vznikl v roce 2017, avšak teprve v roce 2019 odhalil svůj potenciál na trhu, což se projevilo masivním růstem ceny. Nativním tokenem v síti je token LINK. Cílem tohoto projektu je utvoření sítě počítačů, které budou dodávat důvěryhodná data do jednotlivých blockchainů. ChainLink řeší problém izolovaných kryptoměnových blockchainů, jelikož ty představují pouze virtuální databázi a chybí jim propojení s okolním světem. Dalším důvodem masivního růstu ceny je navázané partnerství a spolupráce s finančními a technologickými giganty, jako jsou například Microsoft, Swift či Google. ChainLink je potřebný pro adopci kryptoměn, ale i pro finanční kanály. Například již uvedenému SWIFT umožňuje důvěryhodný a bezpečný přenos dat mezi více zároveň nekompatibilními systémy.

Masová adopce kryptoměn naráží na problém, jelikož blockchainy představují uzavřené systémy, které využívají data zapsána pouze v rámci daného blockchainu. Tento problém je značný především pro chytré kontrakty, tudíž například pro ethereum a cardano. Chytré kontrakty velmi často potřebují data z okolního světa mimo daný blockchain. Tento problém lze řešit za pomocí takzvaných oraclů. Toto řešení nabízí právě ChainLink, který lze definovat i jako síť decentralizovaných oraclů, jenž poskytují chytrým kontraktům ověřená data z externích systémů. Pro

lepší uchopení problematiky lze užít příkladu. Pokud vytvoříme chytrý kontrakt, který potřebuje pro svoji funkčnost data z newyorské burzy cenných papírů, bude potřeba digitální cesta mezi tímto kontraktem a newyorskou burzou cenných papírů. Tato cesta bude vytvořena skrze operátory jednotlivých uzlů v síti ChainLinku, kteří se napojí na API newyorské burzy a následně ověří, zda všichni účastníci procesu mají validní a stejná data. Po validaci jsou poslána tato data zpátky do chytrého kontraktu, a tímto procesem je tudíž zajištěna správnost dat.

Jak již bylo zmíněno, ChainLink umožňuje interoperabilitu mezi jednotlivými blockchainy. Pokud na síti cardana existuje chytrý kontrakt, který potřebuje data ze sítě etherea, může také využít služeb operátorů uzlů fungujících v rámci sítě ChainLink. Tento princip je znázorněn na obrázku níže.

Obrázek 8 Způsob implementace dat na síti ChainLinku

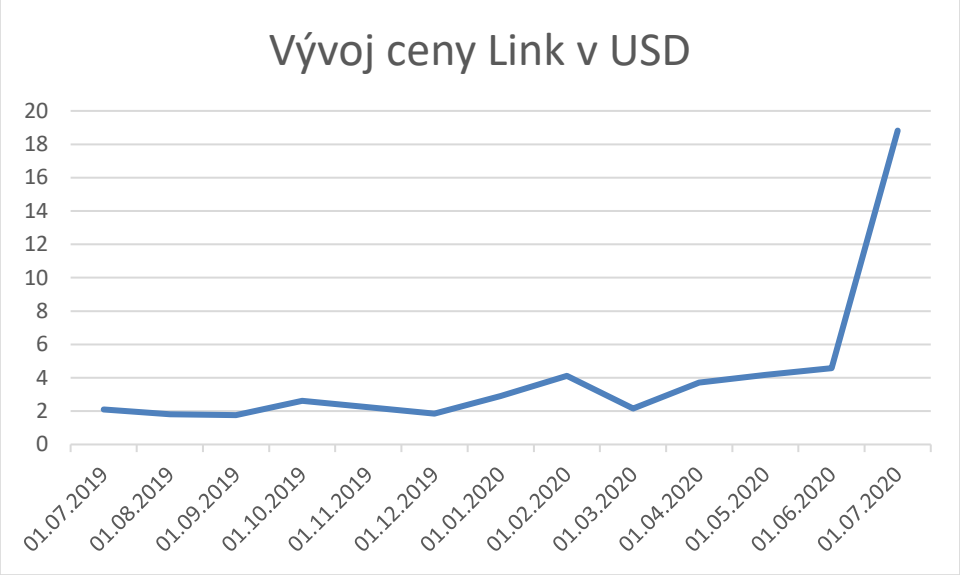


Zdroj: [20]

Token LINK v rámci ekosystému ChainLinku funguje jako platidlo. Jestliže má tvůrce chytrého kontraktu zájem na získání prokazatelně validních dat z externího systému, musí za tyto data zaplatit provozovatelům uzlů za jejich služby. Tato platba probíhá za využití tokenu LINK. Jelikož v rámci sítě lze uplatit pouze toto platidlo, lze vydedukovat, že token LINK má svojí hodnotu. Tato hodnota se bude odvíjet od množství v budoucnu vytvořených chytrých kontraktů, jelikož tvůrci jsou motivovány tento token zakoupit, aby byli schopni využít služeb ChainLinku. Momentálně ChainLink existuje především na síti etherea, avšak do budoucna bude dle vyjádření vývojářů expandovat i na ostatní platformy, které se zaměřují na tvorbu chytrých kontraktů [21].

Budoucnost ChainLinku může být zářná, jelikož jeho využitelnost je nezměrná. Již z uvedeného grafu ceny lze vyčíst, že investoři oceňují funkce této kryptoměny a věří v její budoucnost. Propojení světových dat do blockchainového světa je potřeba a ChainLink tuto funkci nabízí.

Obrázek 9 Cena Linku v USD



Zdroj: [12]

4.3.5 Bitcoin Cash

Bitcoin Cash vznikl po oddělení od blockchainu nejznámější kryptoměny – Bitcoinu. Avšak fanoušci této kryptoměny přicházejí s tvrzením, že se jedná o jediný pravý bitcoin. Na druhou stranu v kryptoměnové komunitě se najde mnoho hlasů, jenž považují Bitcoin Cash za podvod. Problematický byl již samotný vznik kryptoměny Bitcoin Cash. Díky neshodám a napjaté atmosféře v komunitě se rozhodla část těžařů bitcoinu oddělit od většiny a založily právě Bitcoin Cash.

V komunitě již od roku 2017 vznikla nespokojenost se škálovatelností bitcoinu a související pomalostí procesování transakcí. Trnem v oku byly také vysoké poplatky za transakci. Hlavními představiteli této kritizující skupiny jsou Jihan Wu a Roger Ver. Novou navrhovanou myšlenkou bylo zvýšení kapacity bloku z 1 MB

na 8 MB. Tato změna má za cíl umožnit vytěžit v jednom bloku více transakcí (dat). Druhým nápadem, se kterým přišla druhá strana komunity pro řešení škálovatelnosti Bitcoinu, bylo řešení za pomocí SegWitu. Ten odstraňuje elektronický podpis uživatelů z bloku, kteří transakci vypořádávají. Avšak skupina těžařů vedená již zmíněnými Rogerem Verem a Jihanem Wu byla proti takovéto myšlence. Po názorové neshodě proběhl v roce 2017 hard fork a bitcoin se rozdělil na bitcoin cash a bitcoin. Držitelé bitcoinu dostali stejné množství bitcoin cashe shodně s množstvím držených bitcoinů na své peněžence.
Pokud porovnáme tyto dvě kryptoměny, dostaneme se k následujícím výhodám bitcoin cashe:

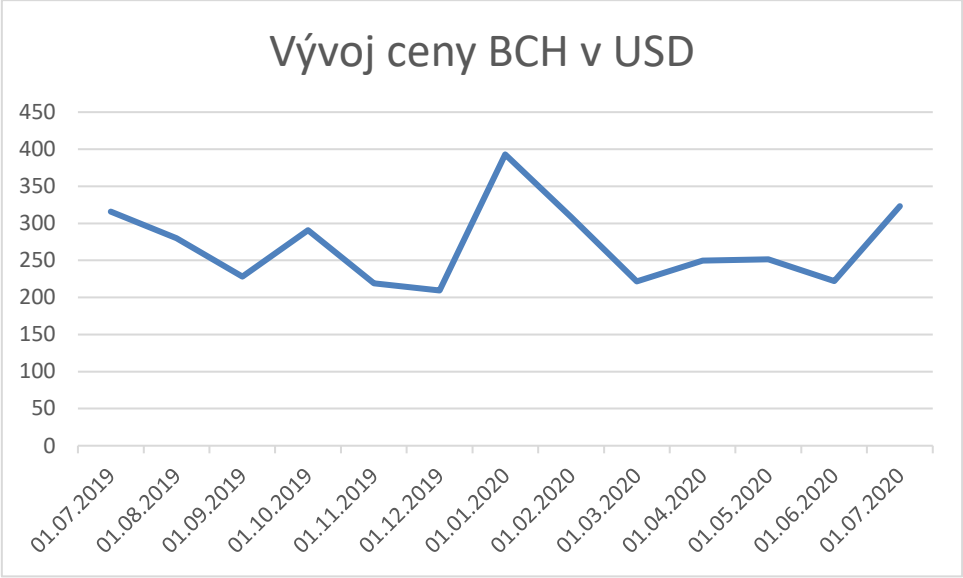
- Nižší poplatky za transakce.
- Rychlejší ověřování transakcí.
- Jednodušší těžba.
- Větší 8 MB bloky.

Mezi nevýhody bitcoin cashe patří:

- Nižší počet nodů.
- Vysoká míra centralizace.
- Menší podpora ze stran burz.
- Hrozba 51% útoku [22].

Na závěr mohu konstatovat, že bitcoin i bitcoin cash mají své místo na trhu a posouvají technologickou hranici kryptoměn. Na níže uvedeném grafu lze spatřit, že cena v daném období je spíše stabilní a osciluje kolem 250 dolarů.

Obrázek 10 Vývoj ceny BCH v USD



Zdroj: [12]

4.3.6 Cardano

Cardano je kryptoměnou třetí generace, vezmu-li v potaz koncept, který zahrnuje bitcoin, který vznikl jako konkurence bankám a ethereum jako kryptoměnu nabízející chytré kontrakty. Cardano vzniklo v roce 2015 pod vedením Charlese Hoskinsona, který se jako vývojář původně podílel na vzniku etherea. Charles se pokusil navázat na kryptoměny předešlých generací a vyhnout se chybám již učiněným a přidat nové funkce.

Hlavním bodem selhání u předešlých generací kryptoměn vidí v transakční rychlosti a v energetické náročnosti těžby. Hlavní přidanou hodnotou cardana je škálovatelnost, která je zde řešena již od vzniku dvěma vrstvami, konkrétně vyrovnávací a výpočetní. Dále pak sidechainy (přesun dat na pomocný vedlejší blockchain) a shardingem (rozdělování blockchainu na menší části). Vývoj cardana probíhá prostřednictvím programovacího jazyka Haskell, který je matematicky ověřitelný a můžeme tedy prokázat funkčnost kódu, ještě před jeho spuštěním. Hlavním vývojářem platformy je společnost Input Output.

Dalším rozdílem je řešení stylu řízení, který udává styl řešení různých situací a konfliktů v rámci sítě cardana. Jde v podstatě o řídící model přecházející situacím,

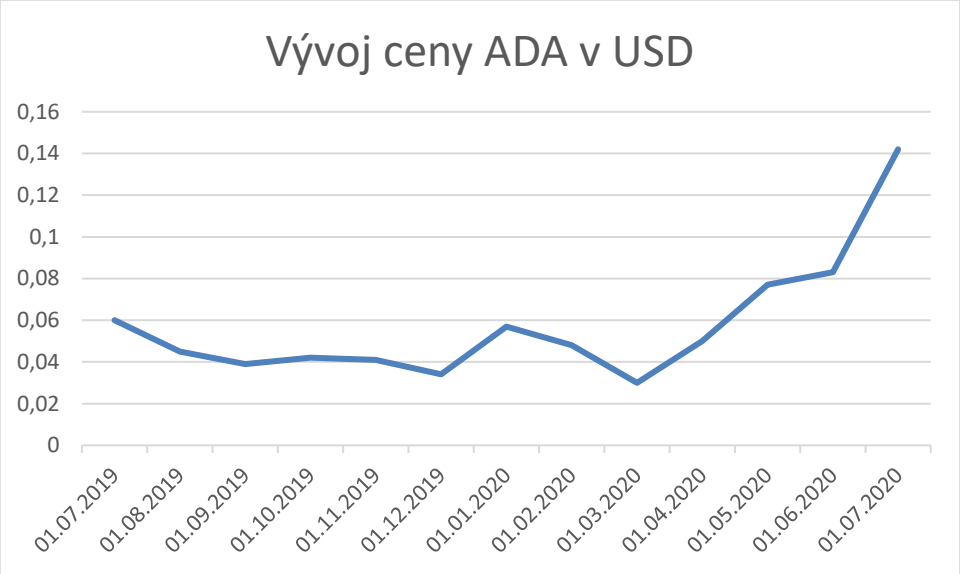
kdy se komunita neshodne a předchází se takto hard forkům. Mimo jiné cardano řeší udržitelnost vývoje, jelikož u jiných projektů, mnohdy vývojáři pracují na blockchainu dané kryptoměny zadarmo s vidinou, že s lepší funkčností a adaptivitou na trhu vzroste cena dané kryptoměny. Další možností získání finančních prostředků na vývoj kryptoměny je ICO, tedy možnost předkoupení kryptoměny před uvedením na trh. Cardano zvolilo cestu kombinující oba způsoby, ale přidává další prvek, který se nazývá treasury, neboli pokladnice. Tento mechanismus bude na vývoj cardana posílat automaticky určitou část nově emitovaných mincí. V podstatě se jedná o určitou daň putující od validátorů transakcí na podporu vývoje. Výše zmíněný řídící mechanismus bude využit pro hlasování o využití prostředků z této pokladny.
Dále cardano představuje interoperabilitu, jelikož vývojáři této kryptoměny chtějí vytvořit platformu, která bude umět rozpoznat a dále pracovat s daty z jiného blockchainu. Mimo jiné si tato kryptoměna klade za cíl pracovat s daty z tradičních finančních systémů neboli vytvořit napojení na banky a všechny tyto data propojit. Také algoritmus konsenzu není opomenut a je zde využit Proof-of-Stake, zde pod názvem Ouroboros, jehož bezpečnost je ověřena matematicky.

Cardano je od vzniku pojato jako mission critical project, neboli nelze pokračovat dále při vývoji, jestliže nejsou vyřešené jakékoliv problémy. Lze tedy vývoj přirovnat k řízení letového provozu či k letům do vesmíru, které také aplikují stejný princip. Cardano je známé spolupráci s akademickou sférou a na vývoji spolupracuje mnoho vědců ze světových univerzit a jednotlivé návrhy jsou podrobeny „peer review“. U návrhů probíhá recenze a ověření od ostatních vědců a akademiků, stejně jako u vědeckých článků. Tento přístup předchází budoucím chybám. Díky aplikaci těchto principů bývá cardano často označováno za akademický projekt, avšak hlavní vývojář Charles Hoskinson uvádí, že projekt vnímá spíše jako komerční, jelikož Cardano nabídne do budoucna chytré kontrakty, DeFi a dapps stejně jako ethereum. Cardano také aktivně navazuje kontakty s bankami, úřady, vládami a regulátory [23].

Hlavním cílem působnosti cardana je africký kontinent, jelikož právě v zemích třetího světa nalezne podle Charlese blockchain největší uplatnění, kvůli absenci stabilní a rozvinuté digitální infrastruktury[24].

Pokud bych hodnotil cardano kriticky, lze uvést, že ambice můžou být příliš vysoké a je možné, že je vývojáři nedokáží naplnit. Již nyní dochází k velkým zpožděním ve vývoji. Z pozitivního pohledu existuje více jak 600 poolů, což naznačuje aktivní komunitu a vysokou decentralizaci [25].

Obrázek 11 Vývoj ceny ADA v USD



Zdroj: [12]

4.3.7 Litecoin

Litecoin se jako kryptoměna zaměřuje na rychlé, bezhotovostní a decentralizované transakce s minimálním poplatkem. Výchozím zdrojem kódu pro litecoin je kód bitcoinu, avšak s jistými aplikovanými vylepšeními. V porovnání s bitcoinem litecoin vyřídí až osmkrát více transakcí za sekundu a transakční poplatky jsou dvacet pětkrát nižší. Další konkurenční výhodou je jeho masová rozšířenost i mimo kryptoměnovou komunitu a litecoinem lze platit například v Alze. Platforma litecoinu často slouží i jako testovací síť pro aplikaci novinek a byl první kryptoměnou, kde byl aplikován SegWit a Lighting Network. Často se o litecoinu

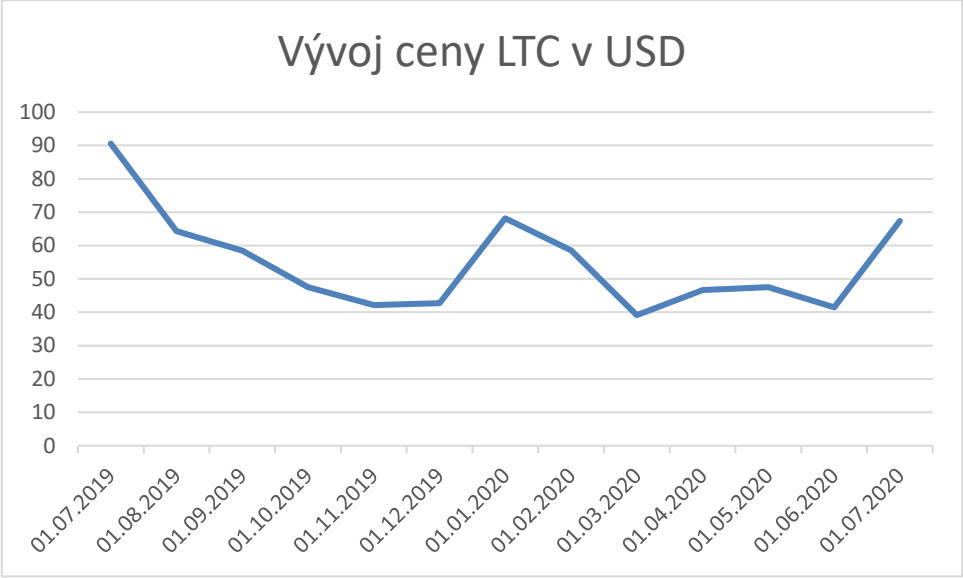
mluví jako o digitálním stříbře a bitcoin je označován jako digitální zlato. Těžba Litecoinu probíhá za pomocí algoritmu Scrypt mining a odlišuje se od bitcoinu.

Za vznikem litecoinu stojí Charles Lee, bývalý zaměstnanec firmy Google. Tato kryptoměna vznikla v roce 2011 a za implementací novinek a marketing odpovídá nezisková společnost Litecoin Foundation. Tato společnost je také spoluvlastníkem německé WEB banky. Od roku 2019 je Litecoin partnerem serveru TravelbyBit, který uživatelům umožňuje platit za ubytovací místa a do budoucna je plánováno zavedení litecoinové debetní karty. Mimo jiné lze očekávat aplikaci atomic swaps, chytrých kontraktů a anonymních transakcí [26].

Hlavní výhoda litecoinu spočívá v již zmíněných rychlých finančních transakcí, avšak na trhu jsou již konkurenční kryptoměny, které jsou znatelně rychlejší jako například již zmiňovaný XRP. Transakční poplatky se pohybují v rámci setin dolarů a litecoin je možné zakoupit v mnoha bankomatech. Litecoin můžeme také naleznout na drtivé většině kryptoměnových burz. Negativní stránka této kryptoměny spočívá již v zakladateli Charlesem Lee, jenž velmi aktivně vystupuje na sociálních sítích a negativně ovlivňuje cenu. Charles například v roce 2014 prohlásil, že litecoin již nepotřebuje žádný technologický vývoj a řada těžařů se v reakci na tento výrok od litecoinu odvrátila. Další známý výrok vynesl v roce 2017, kdy byl litecoin na maximu své ceny, kdy uvedl, že jeho kryptoměna nemá zdaleka takovou hodnotu, a cena následně dramaticky spadla.

Budoucnost litecoinu je nejistá, avšak pokud se kryptoměny dočkají masové adopce, lze předpokládat, že litecoin si udrží své místo mezi nejhodnotnějšími kryptoměnami, jelikož na trh přináší bezesporné výhody.

Obrázek 12 Vývoj ceny LTC v USD



Zdroj: [12]

4.3.8 Bitcoin SV

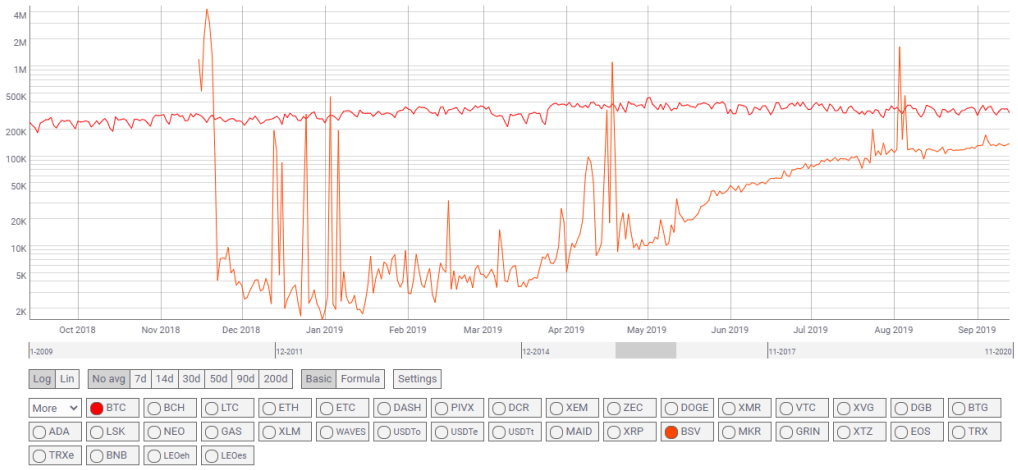
Vznik této kryptoměny provázeli kontroverze, avšak i přesto zaujímá své místo mezi deseti kapitálově nejhodnotnějšími kryptoměnami. Bitcoin SV se vyznačuje vysokou škálovatelností. Tato kryptoměna vznikla v roce 2018 po hard forku Bitcoin Cash. Tento fork byl zapříčiněný požadavkem komunity, která žádala vylepšení a úpravu nastavení zapisování transakcí v bloku. Část komunity, která s tímto krokem nesouhlasila, v čele s Craigem Wrightem a Calvinem Ayre vytvořila Bitcoin Satoshiho vize, zkráceně Bitcoin SV. Cílem této kryptoměny bylo zvýšit rychlost bloků ze stávajících 32 MB na 128 MB. Přívlastkem Satoshiho vize odkazovali na návrat k Satoshiho filozofii. Sám Craig Wright se sám označuje za původního zakladatele Bitcoinu, Satoshi Nakamota, avšak nikdy nebyl schopen toto tvrzení potvrdit a vysloužil si za toto prohlášení kritiku velké části kryptoměnové komunity.

Bitcoin SV využívá hašovací algoritmus SHA-256, stejně jako Bitcoin Cash. Lze tedy obě kryptoměny těžit na stejných těžebních zařízeních. Tento fakt vedl již od vzniku této kryptoměny k hašovací bitvě mezi Bitcoin Cash a Bitcoin SV. Za pomocí 51 % útoku se pokoušeli zastánci Bitcoin Cash vyřadit z provozu Bitcoin SV a naopak. Tato

válka si vyžádala ztráty v mnoha miliónech dolarů. Po určité době došlo k uvolnění napětí mezi znepřátelenými tábory.

Hlavní výhody Bitcoinu SV spočívají ve stabilitě, bezpečnosti, škálovatelnosti a rychlostí transakcí. Tyto výhody kryptoměna těží z již zmíněné velikosti kapacity bloku. Pro představu, Bitcoinový blok má kapacitu 1 MB. Tato vysoká kapacita může být do budoucna využita pro ukládání firemních dat, daňových záznamů či informací o nákupu zboží. Avšak momentální stav kryptoměny neodpovídá těmto cílům a její využitelnost jako platidla je minimální. Tento fakt lze vyčíst například ze srovnání počtu transakcí bitcoinu a Bitcoinu SV [28].

Obrázek 13 Porovnání bitcoinu a Bitcoinu SV



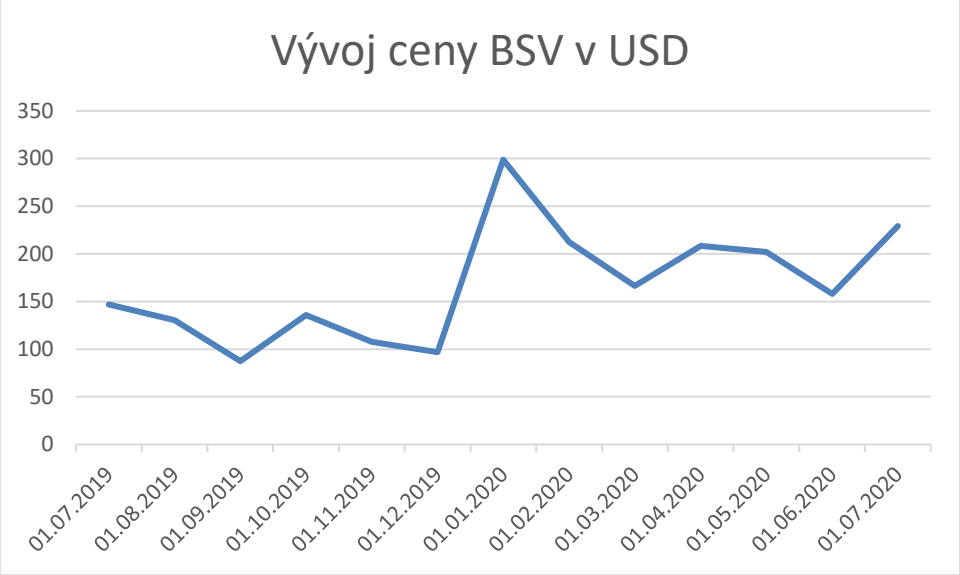
Zdroj: [27]

Ve výše uvedeném grafu lze spatřit počet transakcí v daném časovém horizontu. Lze z grafu vyčíst, že nižší čára, která patří Bitcoinu SV, dosahuje třetinové hodnoty transakcí provedených na bitcoinové síti. Momentální využitelnost kapacity bloku Bitcoinu SV je přibližně 0,5 MB. Můžeme tedy odvodit, že současná kapacita se jeví jako naddimenzovaná. Faktem zůstává, že poplatky za transakci jsou minimální a medián k dnešnímu dni (12. listopadu 2020) činní pouhých 0,0002 dolarů [29].

Pokud se zamyslíme nad budoucností Bitcoinu SV, lze konstatovat, že tato kryptoměna stojí poměrně na vratkých základech. Hlavním problémem zde vidím již v zakladatelích této kryptoměny. Dále nevidím reálné využití této kryptoměny

oproti jiným konkurenčním projektům. Také je pravděpodobné, že zde neexistuje poptávka po funkcích Bitcoinu SV. Kritika kryptoměnové komunity vůči Bitcoinu SV je vysoká a jeho technické parametry neodpovídají současným trendům. Na druhou stranu nelze opomenout umístění v top deseti kapitálově nejhodnotnějších kryptoměnách, avšak zůstává otázkou, zdali si toto umístění udrží i do budoucna.

Obrázek 14 Vývoj ceny BSV v USD



Zdroj: [12]

4.3.9 EOS

Platforma EOS.IO se zaměřuje na poskytnutí komerčního řešení chytrých kontraktů, decentralizovaného úložného prostoru a decentralizovaných aplikací (takzvaných dapps). V ekosystému EOS.IO se používá token EOS. Za vznikem EOS.IO stojí programátor Daniel Larimer a podnikatel Brandan Blumer, kteří také vytvořili společnost Black.one zodpovídající za vývoj kryptoměny. Platforma vznikla v roce 2017 a funguje na vlastním blockchainu s využitím ERC-20 technologie. Firma Black.one se snaží programátorům, kteří mají zájem vyvíjet chytré kontrakty na blockchainu EOS.IO, poskytnout co nejvíce nástrojů, aby vývoj probíhal co nejjednodušeji. Společnosti Black.one se povedlo získat finanční prostředky od investorů prostřednictvím ICO (Initial Coin Offering) v hodnotě 4 miliard dolarů

i přes minulé neúspěchy zakladatele Larimera, který v minulosti vedl kryptoměnové projekty, jež nenaplnily původní vize.

Tokeny EOS slouží pro přístup k úložnému prostoru a výpočetní kapacitě sítě. Rozdělení výpočetní i úložné kapacity je zde řešeno rovnoměrně. Jestliže bude uživatel vlastnit například dva milióny EOS tokenů, může využít až 0,2 % celkového uložiště a výpočetní sítě blockchainu. Tento blockchain simuluje fungování počítače a poskytuje technologii umožňující využití paralelního výpočetního výkonu různých zařízení napříč světem.

Platforma EOS.IO nabízí řešení pro rostoucí počet decentralizovaných aplikací a pro jejich uživatele skrze vysokou škálovatelnost a rychlé zpracování transakcí. Vývojáři plánují vytvořit prostředí, které dokáže zpracovat a provozovat tisíce dapps. Datové úložiště je přístupné z jakéhokoliv webového prohlížeče a do budoucna má konkurovat například službám jako jsou Google Drive, Oracle Autonomous Data Warehouse nebo Amazon Web Service [30].

Na platformě EOS.IO je aplikována zástupná demokracie pro řešení konfliktů či otázek budoucího vývoje. Jakákoliv fundamentální změna v blockchainu musí být odsouhlasena minimálně patnácti delegáty z celkového počtu jednadvaceti volených delegátů. V roce 2019 byl tento demokratický princip demonstrován změnou výše roční inflace, která podle developerů byla původně 5 %, avšak komunita zvolila roční míru inflace 1 % [30, 31].

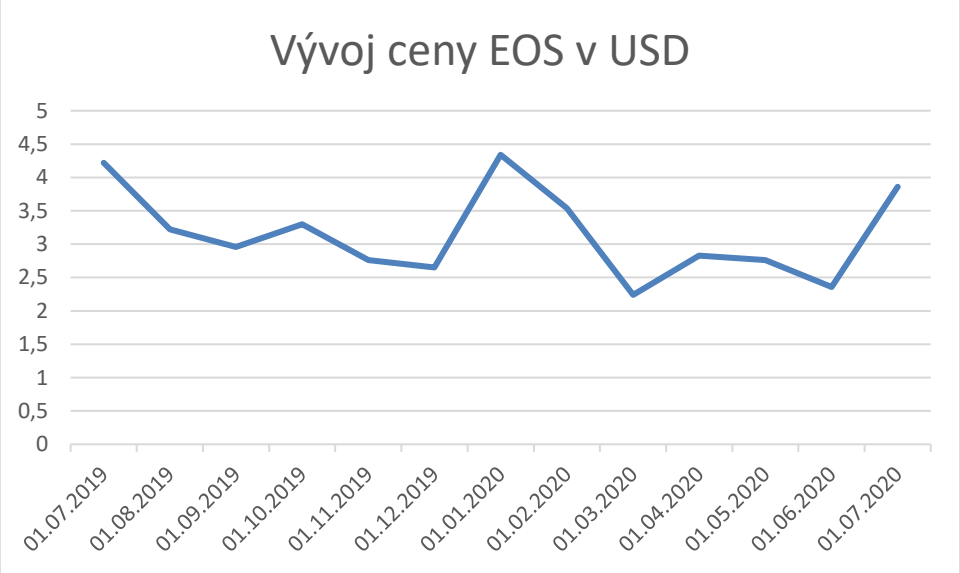
Hlavní konkurenční výhoda platformy EOS.IO spočívá v nulovém poplatku za transakci. EOS.IO je schopen vyřídit až 4 000 požadavků za sekundu, což je například dvakrát více než společnost VISA. Tato vysoká rychlost je dosažena díky využití dPOS (delegated Proof-of-Stake) protokolu. Tento systém konsenzu se vyznačuje nižšími nároky na výpočetní výkon. Další výhodou je poměrně snadná tvorba decentralizovaných aplikací a chytrých kontraktů, pro které je zde využit programovací jazyk C++. Nelze také opomenout rostoucí počet dapps a jejich uživatelů. Momentálně existuje na blockchainu 633 dapps. Pokud porovnáme toto

číslo s konkurenční kryptoměnou ethereum, který má momentálně 1897 dapps na svém blockchainu, lze vyvodit, že EOS.IO je momentálně konkurenčně pozadu, avšak EOS.IO má řádově vyšší počet vyřízených transakcí a to cca 1,4 miliónů denně. Ethereum je schopno zpracovat za den cca 90 tisíc transakcí [30, 32].

Hlavní nevýhodou EOS.IO je absence plné decentralizace, jelikož o veškeré verifikace transakcí a změny na blockchainu se stará pouze jednadvacet delegátů. Volba těchto delegátů je v kompetenci držitelů tokenů EOS, a pokud dojde k podezření na nekalé chování delegáta, může komunita rychle hlasovat o změně podvodného delegáta za nového.

Těžba tokenů probíhá za pomocí využití delegated Proof-of-Stake. Komunita volí 121 delegátů a z těchto je následně vybráno 21 delegátů, kteří dostali z celkové skupiny nejvíce hlasů. Těchto jednadvacet kandidátů zodpovídá za verifikaci transakcí a zbytek 100 delegátů slouží jako záloha. Při volbě delegátů se síla hlasu odvíjí od množství držených tokenů EOS. Delegáti netěží token EOS, ale dostávají ho jako odměnu za verifikaci transakcí. Delegáti jsou většinou vybráni podle svého výpočetního výkonu.

Obrázek 15 Vývoj ceny EOS v USD



Zdroj: [12]

4.3.10 Binance coin

Tato kryptoměna vznikla s návazností na kryptoměnovou burzu Binance, která je momentálně jednou z největších burz na světě. Binance coin slouží především k úhradě poplatků spojených s výměnou fiat měn za digitální tokeny. Při využití tohoto tokenu lze dosáhnout až padesáti procentní slevy za transakční poplatky. Mimo jiné je binance coin schopen verifikovat až 1,4 miliónů transakcí za sekundu. Díky podpoře ze strany burzy, je tento token považován za vysoce důvěry hodný a těší se oblíbenosti ze strany investorů. Na hodnotě tomuto tokenu také přidává jeho provázanost s decentralizovanou burzou Binance DEX. Společnost Binance pravidelně odstraňuje určité množství tokenů z trhu účelem stabilizace hodnoty. Jedná se tedy o druh antiinflační politiky.

Za vznikem burzy v roce 2017 Binance a binance coinu stojí Changpeng Zhao, jenž je zkušeným čínským podnikatelem. Finanční prostředky pro vznik a vývoj burzy byly získány skrze ICO. Z těchto prostředků vznikl, a také decentralizovaná kryptoměnová burza Binance DEX, která byla spuštěna v roce 2019. Jak jsem již zmínil výše, token Binance coin je využíván především pro slevy za poplatek, který vzniká při směně kryptoměn za fiat, či za směnu kryptoměn za jiné kryptoměny. Burzovní poplatek za směnu momentálně činní 0,1 % z objemu transakce, avšak při využití binance coinu se tato hodnota snižuje. V prvním roce fungování burzy se jednalo od 50 % slevu a s každým přibývajícím rokem tato sleva klesá o polovinu.

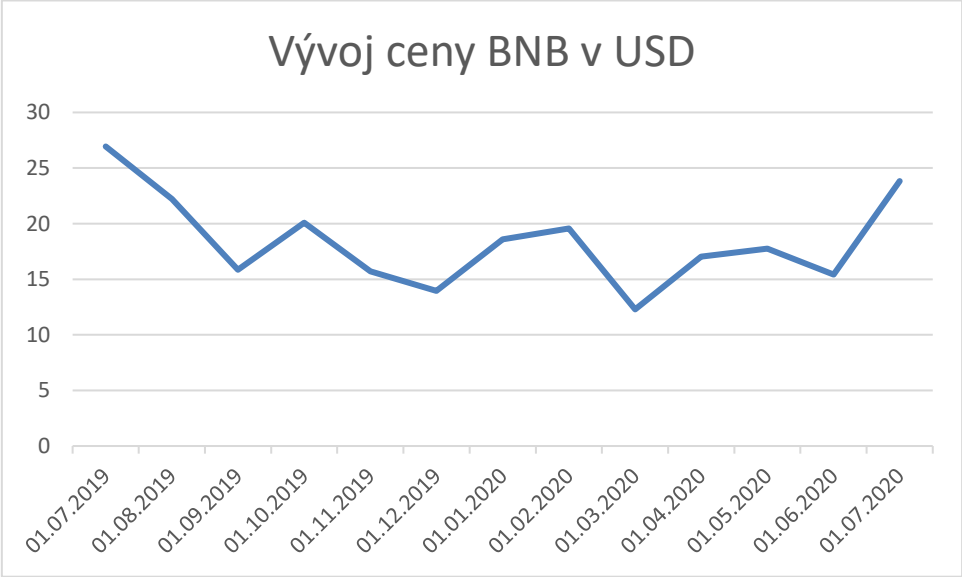
Mezi východy binance coinu lze zařadit již zmíněné odstraňování tokenu z oběhu. Tento proces označuje společnost Binance jako „pálení tokenů“. Toto pálení probíhá tak, že od vlastníků tokenu firma Binance každé tři měsíce tokeny vykoupí zpátky a následně je zlikviduje. Na nákup těchto tokenů zpátky od investorů firma vyčlenila 20 % svého zisku. Podle plánů společnosti Binance by takto mělo být postupně zlikvidováno až polovina celkového množství emise, to znamená 100 miliónů Binance tokenů. Další výhodou je možnost použít tokeny na decentralizované burze Binance DEX, kde uživatel může díky Binance chainu využít decentralizovanou

softwarovou peněženku. To znamená, že uživatel této burzy je vlastníkem privátních klíčů a opravdu vlastní své digitální aktiva. Na standartních kryptoměnových burzách tyto klíče vlastní burza a uživatel je tedy odkázán na důvěryhodnost burzy.

Na druhou stranu provázanost s burzou Binance se může ukázat i jako negativní stránka této kryptoměny, jelikož cena je silně svázána s reputací burzy. Tato burza již čelila úspěšných hackerským útokům, a bylo odcizeno několik desítek milionů dolarů. Burza tento útok ustála a funguje dále. Další nevýhodou je, že tuto kryptoměnu nelze obchodovat na jiných velkých burzách, jelikož ty většinou používají vlastní burzovní token, anebo nemají zájem podporovat konkurenční kryptoměnu binance coin.

Budoucnost binance coinu je úzce spojená s burzou Binance. Jestliže si burza udrží prvenství na burzovním kryptoměnovém trhu a bude úspěšně odolávat hackerským útokům, lze předpokládat, že cena této kryptoměny bude růst, jelikož využití tokenu roste s rostoucím počtem obchodů na burze.

Obrázek 16 Vývoj ceny BNB v USD



Zdroj: [12]

4.4 Systém pro podporu rozhodování

Systém pro podporu rozhodování lze definovat jako pomůcku pro řešení nestrukturovaných problémů za pomocí interaktivního počítače, který pomáhá tvořitelům v rozhodnutí za pomocí dat a modelů. Již na konci 70. let začaly vznikat systémy pro podporu rozhodování založených na počítačové podpoře. Očekávání od těchto systémů bylo vysoké, avšak ukázalo se, že reálná poptávka po tomto řešení není příliš vysoká. Avšak od té doby technologické možnosti postoupili a nyní se tyto systémy mezi investory a manažery těší rostoucí oblibě. Mnohé výzkumy prokázaly, že počítačem podporované systémy pro podporu rozhodování efektivně zlepšují manažerské a investiční rozhodnutí. Momentálně existuje několik druhů systémů. Některé systémy se zaměřují na podporu jednotlivce a jiné na podporu práce skupin. Tyto systémy se snaží manažerům, investorům, ale i zaměstnancům učinit expertní rozhodnutí a poskytují analytické informace.

Z historického hlediska začaly vznikat systémy pro podporu manažerů (MIS) v šedesátých letech. Tyto systémy poskytovali manažerům strukturované pravidelné zprávy. Tyto zprávy vznikali z obsahu prodejních výkazů a účetnictví. Následně z těchto systémů vznikl nový typ informačního systému, neboli systémy pro podporu rozhodování či řízení rozhodnutí [34].

Systém pro podporu rozhodování lze dělit na tyto jednotlivé kategorie:

- Systém pro podporu rozhodování založený na datech – Tento systém zahrnuje manažerské, exekutivní, informační a geografické systémy. Hlavní důraz je zde na manipulaci s velkým množstvím dat. Zdrojem těchto dat jsou především interní podnikové data, časové řady, ale i externí data.
- Systém pro podporu rozhodování založený na modelu – Zde nalezneme finanční, účetní a optimalizační modely. Jsou zde využity především analytické a statistické nástroje pro zpracování těchto modelů.

- Systém pro podporu rozhodování založený na vědomostech – V tomto případě se jedná o systém, který navrhuje a doporučuje manažerům různé akce. Tento systém je používán především pro klasifikaci, konfiguraci, diagnózu, diagnostiku a předvídání, které by bez využití tohoto systému spočívalo na lidském odborném rozhodnutí.
- Systém pro podporu rozhodování založený na dokumentech – Tento systém analyzuje datová úložiště. Příkladem může být software pro vyhledávání.
- Systém pro podporu rozhodování založený na komunikaci a skupinovém rozhodování – Zde je hlavní důraz kladen na komunikaci, spolupráci a koordinaci. Cílem tohoto systému je pomoci skupině lidí učinit rozhodnutí [43].

Ve své práci jsem zvolil rozhodovací strom, jelikož se jedná o přehledný systém pro podporu rozhodování. V praktické části práce tento rozhodovací strom použiji, abych vyobrazil výsledky mých analýz a nabídl tak investorovi možnost vybrat si vhodnou variantu investice.

4.4.1 Rozhodovací strom

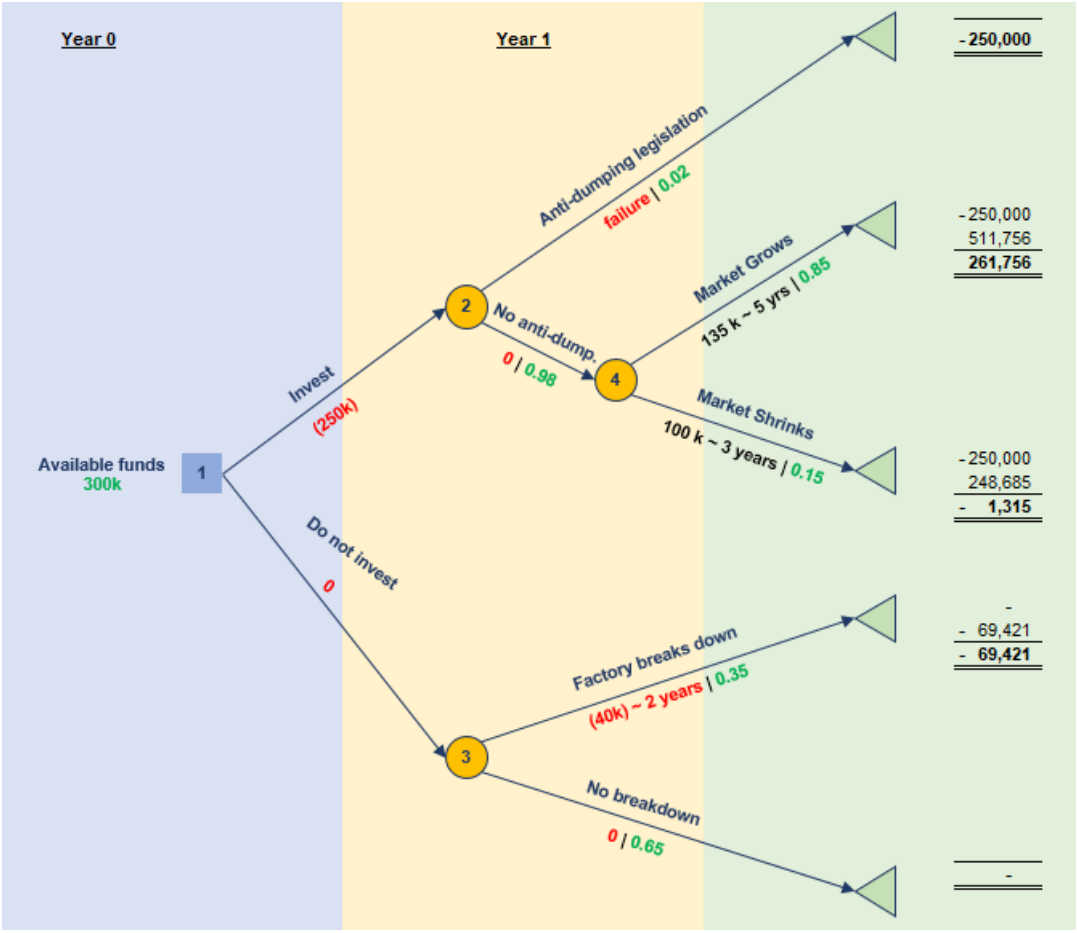
Rozhodovací strom je diagram, který lidé používají pro určení směru akce či jako ukazatel statistické pravděpodobnosti. Vizuální forma často opravdu napodobuje strom, který roste ze země, avšak častým způsobem vyobrazení je růst z levé strany do pravé. Jednotlivá větev rozhodovacího stromu reprezentuje možnou akci, reakci či výsledek. Nejvzdálenější list stromu reprezentuje výsledek celého rozhodovacího procesu. Často se s aplikací tohoto druhu systému pro rozhodování setkáme při řešení finančních a investičních problémů.

Rozhodovací strom skrze vizuální zobrazení jednotlivých kroků řešení pomáhá efektivně a přehledně investorům porozumět potenciálním možnostem a výsledkům jejich rozhodnutí. Tento rozhodovací systém také pomáhá lidem identifikovat všechny možné potenciální možnosti a jejich váhu. Mimo jiné

zobrazuje možná rizika a odměny jednotlivých rozhodnutí. Na konci každé větve je vyobrazen výsledek řetězce rozhodnutí a uživatel si může vybrat, které řešení by mu vyhovovalo a reverzní metodou dojít k potřebným informacím, jež potřebuje k dosažení vybraného výsledku.

Společnosti mohou aplikovat rozhodovací strom ve firmě jako systém pro podporu rozhodování. Zaměstnancům tento strukturovaný model dovoluje nahlédnout na celkový obraz řešení a mohou takto pochopit, jak jednotlivé interní akce vedou k určitým výsledkům [36].

Obrázek 17 Investiční rozhodovací strom



Zdroj: [35]

Na uvedeném obrázku je vyobrazen příklad, jak může rozhodovací strom vypadat. Jsou zde vyobrazeny klíčové body, jednotlivé uzly a na pravé straně možné výsledky

rozhodnutí. Na konkrétním příkladu vidíme finanční investici ve výši 300 000 dolarů. Lze přehledně na pravé straně vyobrazit výsledky a následně zjistit, které kroky vedly k jakému výsledku.

4.4.2 Aplikace systému pro podporu rozhodování na investiční rozhodnutí

V této kapitole popíši využití systému pro podporu rozhodování pro investiční rozhodování. Rozeberu jiné akademické práce, které se zaměřují na využití této rozhodovací techniky. Některé tyto akademické práce pojednávají o investicích do akcií, které jsou svým charakterem velmi podobné investicím do kryptoměn a proto jsem se je rozhodl zařadit do své práce. Některé kryptoměny také dávají vlastníkovy hlasovací právo a držitelé těchto kryptoměn obdrží odměnu, která je velice podobná dividendám. Také nelze opomenout, že není mnoho akademických prací pojednávající o využití systému podpory rozhodování v rámci kryptoměn. Tento nedostatek lze pravděpodobně přitknout k faktu, že kryptoměny jsou poměrně novou záležitostí a investování do tohoto sektoru je pro mnohé profesionální investory novou zkušeností.

Akademická práce Hulya Baydase Hazara se věnuje faktorům, které ovlivňují investory při investování do kryptoměn. Dalším cílem je odhalení preferencí investora za pomocí conjointové analýzy. V této metodě jsou posuzovací kritéria přiřazená k několika atributům, které mají více levelů. Tyto levely a atributy jsou dále v práci transformovány za použití ortogonální metody. Výsledkem je svazek levelů a atributů, které investor dále využije pro své rozhodování. Následně za použití dotazníku autor vyhodnotil preference investorů. V závěru této studie autor dochází k zjištění, že na kryptoměnovém trhu existuje mnoho konkurentů bitcoinu a investor může na základě tabulky níže rozhodnout pro tuto konkurenci. Vyhodnotil, že tyto atributy jsou pro investora klíčové [44].

Tabulka 2 Svazky atributů

Atributy	Svazek 1	Svazek 2	Svazek 3	Svazek 8	Svazek 9
Ziskovost	Velmi vysoká	Velmi vysoká	Velmi vysoká	Vysoká	Vysoká
Dostupnosti informací	Velmi vysoká	Vysoká	Střední	Střední	Nízká
Anonymita	Anonymní	Pseudonymní	Pseudonymní	Obtížná dohledatelnost investora	Dohledatelnost investora
Bezpečnost	Vysoká	Střední	Nízká	Velmi nízká	Střední
Účetnictví	Přehledné	Neadekvátní požadavky	Pochopitelné	Jistá nepřehlednost	Přehledné

Zdroj: [44]

V akademické práci napsané Jörgem Gottschlichem a Oliverem Hinzem je využit systém pro podporu rozhodování za pomocí kolektivní moudrosti. Tato práce se zaměřuje na podporu investora pomocí skupinového hlasování, při kterém investoři vyjadřují názor na určitou akcii. Tento systém může investor využít pro tvorbu svého portfolia. Sledované parametry jsou například, jestli ostatní investoři doporučují akcii koupit či prodat. Dále trh rozdělili na segmenty a podle času. Data pro svůj prototyp získali z veřejně dostupné hlasovací databáze. Jejich prototyp dokázal překonat obchodní měřítko a srovnatelné veřejné fondy [45].

V další akademické práci od autorů Chenghang Zhu, Jianping Yin a Qian Li je použit model pro podporu rozhodování, který využívá tzv. „ oscillation box theory" a „deep belief networks“. Jedná se o teorii, že cena akcie osciluje v určitém pásmu v daném čase. Autoři implementovali automatický akciový systém pro podporu rozhodování, který má za cíl investorovi pomoci při investicích. Tento nástroj radí, jestli akcii koupit či prodat. Pro analýzu zde bylo využito 400 akcií. Výsledkem této práce je fungující nástroj, který dokáže nabídnout investorovi poměrně přesné predikce a pomoci mu tak k zisku. Hlavní nevýhodou je pomalost, jelikož je potřeba pro tento nástroj mnoho historických dat, které musí zpracovat [46].

4.5 Nástroje analýzy

V této kapitole jsem popsal analytické modely použité v praktické části práce. Jedná se o Value-at-Risk, Markowitzův model a Monte Carlo analýzu. V teoretické části jsem se věnoval především teoretickému pochopení těchto tří modelů a v praktické části práce jsem podrobně popsal fungování těchto nástrojů na příkladech. V praktické části jsem také rozepsal všechny potřebné vzorce nutné pro výpočet. Všechny tři modely jsou použity v mnou vytvořené kalkulačce, kterou může investor použít a zároveň bez hlubokých znalostní problematiky těchto analytických modelů získat potřebné informace nutné pro investiční rozhodnutí.

4.5.1 Value-at-Risk

Jedná se o kvantitativní metodu používanou v pojišťovnictví a bankovnictví k řízení rizika. Díky tomuto ekonomickému ukazateli dokážeme odhadnout nejvyšší potencionální ztrátu z daného portfolia finančních aktiv. Fungování modelu je založeno na statistickém odhadu, který udává nejhorší možnou ztrátu, ke které může za určité pravděpodobnosti a v určitém období dojít. V bankovnictví často tento model využívají pro výpočet vnitřních modelů a pro kalkulaci tržního rizika (především portfolií). Na rozdíl od zátěžového testování se VaR používá k měření rizika v běžných, každodenních podmínkách.

Metody VaR vycházejí ze standardních metod měření rizika podle pravidel Basel I, jež obsahují detailní návod pro výpočet kapitálového požadavku v závislosti na rizicích. Negativní stránkou tohoto přístupu bylo vynechání rozložení rizik v portfoliu a volatility jednotlivých rizikových faktorů. Tento fakt vedl k nadměrnému kapitálovému požadavku. Na tyto nedostatky odpověděl Basel II, a vznikl model VaR.

Využití VaR lze datovat od osmdesátých let dvacátého století. Tato metoda si získala oblíbenost mimo jiné díky své jednoduchosti a přehlednosti. Metodu lze také snadno aplikovat na rizika při investování prakticky jakýchkoliv finančních instrumentů. Tuto metodu bezplatně zveřejnila v roce 1994 banka JP Morgan na internetu.

Definici této metody lze popsat podle JP Morgan takto: „*Maximální odhadnutá ztráta v tržní hodnotě dané pozice, která může být utrpěna, než je pozice neutralizována nebo nahrazena*“[38]. Statisticky jde o jednostranný kvantil z rozdělení zisků a ztrát drženého portfolia v průběhu určité doby stanovený na základě relevantního minulého období. Nelze opomenout fakt, že použití pouze metody VaR není z investičního hlediska možné doporučit, jelikož investor by takto mohl mylně zvolit velmi rizikovou metodu. Musíme tedy VaR doplnit o další analytické metody. Například zátěžovými testy.

Pro výpočet VaR existují tři metody:

- Analytická – metoda varianci a kovariancí.
- Metoda historických nebo stochastických simulací – metoda historické simulace.
- Metoda Monte Carlo [37].

4.5.2 Markowitzův model

Markowitz ve svém novinovém článku z roku 1952 uvedl myšlenku o výběru a kombinaci určitých tříd aktiv, které napomohou snížit celkovou volatilitu portfolia a zároveň takové portfolio je schopno si zachovat stejnou výnosnost. Před uveřejněním této práce spočíval investiční management především v určení volatility a výnosů cenných papírů. Markowitz prokázal provázanost mezi jednotlivými třídami cenných papírů a dokázal využít tyto jednotlivé třídy pro tvorbu efektivního portfolia [39].

Ve své teorii Markowitz kalkuloval s těmito předpoklady:

- Existují dokonale efektivní kapitálové trhy.
- Všichni investoři investují na stejně dlouhé období.
- Investoři volí svá aktiva na základě očekávaných výnosů a rizik.
- Investoři jsou rizikově averzní.
- Investoři rozhodují při investování na základě očekávaných užitků.

Teorii portfolia lze definovat jako model, jenž se zabývá optimální alokací aktiv na škále výnos - riziko.

Jestliže chceme vypočítat výnos portfolia, řídíme se následujícím vzorcem:

$$E(R_p) = \sum_{i=1}^{n} w_i R_i$$

Pro riziko portfolia musíme vypočítat rozptyl výnosů přes tento vzorec:

$$\sigma_p^2 = \sum_i \sum_j w_i w_j \sigma_i \sigma_j p_{ij}$$

Následně spočítáme směrodatnou odchylku jako odmocninu z této hodnoty. Jestliže do portfolia zahrneme aktiva, jež nejsou perfektně korelovaná, můžeme získat kombinaci aktiv, jenž nám přinese výhodnější rizikově-výnosný profil, který předčí koupi jakéhokoliv jednotlivého aktiva [40].

4.5.3 Monte Carlo

Metoda Monte Carlo využívá třídu algoritmů pro simulaci systémů. Jedná se tedy o stochastickou metodu využívající pseudonáhodných čísel. Tato metoda má široké využití, lze ji použít pro simulaci experimentů či pro výpočet integrálů a diferenciálních rovnic. Jádro metody Monte Carlo spočívá v určení střední hodnoty veličiny, která je výsledkem náhodného děje. Je nutné vytvořit počítačový model a následně vytvořit dostatečná počet simulací. Následně jsou data zpracována klasickými statistickými metodami. Na závěr je potřeba určit průměr a směrodatnou odchylku [41].

Monte Carlo metoda začala vznikat ve čtyřicátých letech dvacátého století a svého využití došla již během druhé světové války. Zakladatelem metody byl John von Neuman a Stanislaw Marcin Ulam. Oba zakladatelé tehdy pracovali pro Národní laboratoř Los Alamos, kde zkoumali chování neutronů. Hlavním předmětem vědeckého výzkumu těchto vědců byla problematika chování neutronů a jejich

prostupnost různým materiálem. Ani přes velké množství informací nebylo možné tento problém vyřešit teoreticky ani matematicky. K výsledku je dovedla až Monte Carlo metoda. Tato metoda byla inspirována principem rulety [42].

Současná metoda Monte Carlo využívá výpočetní techniku pro získání:

- kvalitních náhodně generovaných čísel.
- výběru racionálního algoritmu výpočtu.
- kontroly přesnosti získaného výsledku.

Využití Monte Carlo metody je široké, lze jí uplatnit kdekoliv, kde je řešení možné nalézt za použití mnohokrát opakovaných náhodných pokusů. Například se jedná o matematické problémy, fyziku, finance, pojišťovnictví, hazardní hry a další [47].

5 Praktická část

V této části práce jsem zpracoval deset kryptoměn, které jsou popsány v praktické části práce. Vytvořil jsem kalkulátor pro výpočet Value-at-Risk (VaR) , a také kalkulátor využívající principů Markowitzova teorie portfolia. Pro tyto dva kalkulátory vytvořené v Excelu jsem vytvořil tabulku cen zachycených vždy na konci měsíce. Celkově jsou v tabulce zanesena data z období od 30. 7. 2019 do 30. 7. 2020, tedy celý jeden rok. Tato tabulka bude využita pro výpočet Value-at-Risk a Markowitzova portfolia.

Tabulka 3 Portfolio 1/2

Datum	BTC	Změna	ETH	Změna	XRP	Změna	Link	Změna	BCH	Změna
30.07.2019	9607		210,52		0,318		2,09		315,93	
30.08.2019	9598	0%	168,83	-20%	0,32	1%	1,81	-13%	279,87	-11%
30.09.2019	8293	-14%	179,87	7%	0,256	-20%	1,76	-3%	228,12	-18%
30.10.2019	9205	11%	184,69	3%	0,2	-22%	2,62	49%	290,63	27%
30.11.2019	7569	-18%	152,54	-17%	0,297	49%	2,24	-15%	218,91	-25%
30.12.2019	7293	-4%	132,63	-13%	0,226	-24%	1,84	-18%	209,4	-4%
30.01.2020	9508	30%	184,69	39%	0,194	-14%	2,91	58%	392,97	88%
29.02.2020	8599	-10%	219,85	19%	0,243	25%	4,11	41%	308,33	-22%
30.03.2020	6429	-25%	132,9	-40%	0,231	-5%	2,15	-48%	221,54	-28%
30.04.2020	8658	35%	207,6	56%	0,172	-26%	3,72	73%	249,84	13%
30.05.2020	9700	12%	242,35	17%	0,213	24%	4,17	12%	251,3	1%
30.06.2020	9137	-6%	226,31	-7%	0,206	-3%	4,57	10%	221,99	-12%
30.07.2020	12353	35%	440	94%	0,321	56%	18,82	312%	323	46%

Zdroj: vlastní zpracování

Tabulka 4 Portfolio 2/2

Datum	ADA	Změna	LTC	Změna	BSV	Změna	EOS	Změna	BNB	Změna
30.07.2019	0,06		90,57		146,88		4,22		26,94	
30.08.2019	0,045	-25%	64,33	-29%	130,41	-11%	3,22	-24%	22,22	-18%
30.09.2019	0,039	-13%	58,42	-9%	87,42	-33%	2,96	-8%	15,86	-29%
30.10.2019	0,042	8%	47,48	-19%	135,88	55%	3,3	11%	20,09	27%
30.11.2019	0,041	-2%	42,2	-11%	107,68	-21%	2,76	-16%	15,72	-22%
30.12.2019	0,034	-17%	42,75	1%	96,98	-10%	2,65	-4%	13,95	-11%
30.01.2020	0,057	68%	68,16	59%	298,82	208%	4,34	64%	18,59	33%
29.02.2020	0,048	-16%	58,54	-14%	212,29	-29%	3,54	-18%	19,58	5%
30.03.2020	0,03	-38%	39,14	-33%	166,44	-22%	2,24	-37%	12,29	-37%
30.04.2020	0,05	67%	46,71	19%	208,3	25%	2,83	26%	17,03	39%
30.05.2020	0,077	54%	47,54	2%	201,84	-3%	2,76	-2%	17,74	4%
30.06.2020	0,083	8%	41,47	-13%	158,15	-22%	2,36	-14%	15,41	-13%
30.07.2020	0,142	71%	67,36	62%	229,1	45%	3,86	64%	23,84	55%

Zdroj: vlastní zpracování

Pro přehlednost jsem rozdělil tabulky na dvě části. Data v tabulce jsou převzata ze stránky www.coinmarketcap.com [12]. V tabulce je také vypočtena měsíční procentuální změna dané kryptoměny vždy za jeden měsíc. Ceny za jednotlivé kryptoměny pro dané období jsou vždy uvedeny v USD.

5.1 Výpočet Value-at-Risk metody

Vytvořil jsem kalkulátor pro výpočet Value-at-Risk v Excelu, jelikož pro investora může být tato možnost snadnější. Díky této možnosti nemusí investor rozumět matematickým vzorcům a výpočet je téměř automatický. V této kapitole popíši krok po kroku fungování kalkulátoru. Následně provedu několik testů, abych předvedl fungování principů Value-at-Risk a dále vyhodnotím vypočtené hodnoty. Tento model pomůže investorovi zjistit maximální možnou ztrátu portfolia za určité pravděpodobnosti a v daném časovém horizontu. V ukázkovém příkladu jsem počítal s měsíčními hodnotami a následně vypočetl i roční variantu.

Krok 1 – vytvoření portfolia

V tomto kroku investor vytvoří své portfolio. Ve svém ukázkovém výpočtu jsem vybral deset kryptoměny s nejvyšší tržní kapitalizací.

Tabulka 5 Kryptoměny

Kryptoměna	Zkratka	Množství	Cena	Objem	Podíl
			$	$	%
Bitcoin	BTC	1	12353	12353	10%
Ethereum	ETH	28,076	440	12353	10%
XRP	XRP	38480	0,321	12352	10%
ChainLink	Link	656,4	18,82	12353	10%
Bitcoin Cash	BCH	38,245	323	12353	10%
Cardano	ADA	86990	0,142	12353	10%
Litecoin	LTC	183,39	67,36	12353	10%
Bitcoin SV	BSV	53,92	229,1	12353	10%
EOS	EOS	3200,3	3,86	12353	10%
Binance Coin	BNB	518,16	23,84	12353	10%
	Suma:			123530	100%

Zdroj: vlastní zpracování

Do této tabulky investor zanese potřebná data. V tomto případě je potřeba doplnit názvy kryptoměny, jejich zkratky, množství, cenu, objem a procentuální podíl.

Já jsem se pro ukázkový příklad kalkulátoru rozhodl pro 10% podíl všech kryptoměny v portfoliu. Celková suma investice je 123 530 USD. Následně investor vypočte procentuální změnu ceny za každý měsíc. Výsledná tabulka je znázorněna v této diplomové práci jako tabulka číslo 5.

Krok 2 – výběr intervalu spolehlivosti

V tomto kroku investor vybere úroveň spolehlivosti modelu z intervalu 0,90 až 0,99. Ve svém ukázkovém modelu jsem vybral úroveň intervalu v hodnotě 0,95. Toto číslo vyjadřuje pravděpodobnost, že potencionální ztráta portfolia nebude vyšší než vypočtená hodnota Value-at-Risk.

Krok 3 – kalkulace K-koeficientu

K-koeficient je inverzní hodnota ke standartnímu normálnímu rozdělení. K výpočtu této hodnoty využijeme funkci NORMSINV. Výpočet proběhne takto: NORMSINV(0,95) a výsledná hodnota je 1,64474327. Číslo 0,95 jsem určil již v kroku 2.

Krok 4 – výpočet průměrné měsíční změny a standartní směrodatné odchylky

Vypočteme průměrnou měsíční změnu pro každou kryptoměnu a následně vypočteme směrodatnou odchylku za pomocí funkce STDEV.

V našem příkladu jsou hodnoty následující:

Tabulka 6 směrodatná odchylka

	BTC	ETH	XRP	Link	BCH	ADA	LTC	BSV	EOS	BNB
Průměrná měsíční změna	4%	12%	3%	38%	4%	14%	1%	15%	3%	3%
Směrodatná odchylka	21%	37%	28%	93%	34%	40%	31%	67%	32%	29%

Zdroj: vlastní zpracování

Krok 5 – kalkulace volatility

Nyní investor provede tyto kroky:

1. Vytvoří propojení s počtem množství tokenů kryptoměn v řádku 1.
2. Vytvoří propojení s cenou jednotlivých kryptoměnových tokenů v řádku 2.
3. Vypočítá hodnotu pozice: cena x množství.
4. Vytvoří propojení k měsíční volatilitě.
5. Vypočte násobek volatility: měsíční volatilita x hodnota pozice.
6. Vytvoří propojení k průměrné měsíční volatilitě.
7. Spočítá průměrnou měsíční změnu v dolarech: průměrná měsíční změna x hodnota pozice.

Tabulka 7 Kalkulace volatility

Roční násobek volatility	8861	15900	12156	39923	14667	17130	13313	28780	13901	12600
Průměrná roční změna v $	5875	17103	4983	56650	6628	20234	2009	22656	5054	4099

Zdroj: vlastní zpracování

Krok 6 – Výpočet násobku roční volatility

V tomto kroku investor vypočítá násobek volatility pro jeden rok. Výpočet je jednoduchý, jelikož stačí vynásobit měsíční násobek volatility odmocninou dvanácti, protože počítáme s dvanácti měsíci. Podobně proběhne i výpočet průměrné změny ceny pro jeden rok, kdy průměrnou měsíční změnu vynásobíme dvanácti.

Tabulka 8 násobek roční volatility

Kryptoměna	BTC	ETH	XRP	Link	BCH	ADA	LTC	BSV	EOS	BNB
Množství tokenů	1	28,076	38480	656,4	38,245	86990	183,39	53,92	3200,3	518,16
Podíl v dolarech	12353	440	0,321	18,82	323	0,142	67,36	229,1	3,86	23,84
Hodnota pozice	12353	12353	12352	12353	12353	12353	12353	12353	12353	12353
Měsíční volatilita	21%	37%	28%	93%	34%	40%	31%	67%	32%	29%
Násobek volatility	2558	4590	3509	11525	4234	4945	3843	8308	4013	3637
Průměrná měsíční změna v %	4%	12%	3%	38%	4%	14%	1%	15%	3%	3%
Průměrná měsíční změna v $	490	1425	415	4721	552	1686	167	1888	421	342

Zdroj: vlastní zpracování

Krok 7 – Nalezení korelace mezi kryptoměnami

Zde investor za pomocí korelační matice vypočte korelaci mezi vybranými kryptoměnami. Pro tento výpočet použijeme funkci CORREL.

Tabulka 9 korelační matice

Korelační matice	BTC	ETH	XRP	Link	BCH	ADA	LTC	BSV	EOS	BNB
BTC	1,00	0,87	0,33	0,75	0,62	0,86	0,57	0,47	0,62	0,76
ETH	0,87	1,00	0,30	0,95	0,39	0,96	0,34	0,46	0,39	0,53
XRP	0,33	0,30	1,00	0,31	0,10	0,27	0,55	-0,30	0,32	0,57
Link	0,75	0,95	0,31	1,00	0,30	0,92	0,19	0,42	0,28	0,37
BCH	0,62	0,39	0,10	0,30	1,00	0,34	0,72	0,73	0,93	0,68
ADA	0,86	0,96	0,27	0,92	0,34	1,00	0,29	0,46	0,32	0,46
LTC	0,57	0,34	0,55	0,19	0,72	0,29	1,00	0,25	0,88	0,87
BSV	0,47	0,46	-0,30	0,42	0,73	0,46	0,25	1,00	0,50	0,23
EOS	0,62	0,39	0,32	0,28	0,93	0,32	0,88	0,50	1,00	0,80
BNB	0,76	0,53	0,57	0,37	0,68	0,46	0,87	0,23	0,80	1,00

Zdroj: vlastní zpracování

Krok 8 – vytvoření dvou sloupců pro měsíční a roční násobek volatility

Investor v tomto kroku propojí měsíční násobek volatility násobitele, které jsem vypočítal v kroku 5 a 6 podle předem daného pořadí.

Tabulka 10 souhrn měsíční a roční volatility

Volatilita v $	1 měsíc	rok
BTC	2557,95	8860,982
ETH	4589,8	15899,53
XRP	3509,08	12155,8
Link	11524,7	39922,8
BCH	4234,01	14667,05
ADA	4945,09	17130,29
LTC	3843,04	13312,68
BSV	8308,12	28780,17
EOS	4012,91	13901,13
BNB	3637,24	12599,77

Zdroj: vlastní zpracování

Krok 9 – výpočet Value-at-Risk pro jeden měsíc a pro celý rok

Všechny výpočty jsou provedeny jedním vzorcem, ale jestliže nahlédneme na jednotlivé akce postupně, bude výpočet pro jeden měsíc probíhat takto:

- Vynásobíme dvě matice: matice násobků volatility a korelační matici.
- Vynásobíme výsledek měsíční matice volatility vypočítané v kroku 8.
- Spočítáme odmocninu z výsledku.
- Pro násobení matic použijeme funkci MMULT.

Pro roční výsledek je výpočet obdobný. Dále vypočteme průměrnou změnu portfolia. Sečteme průměrné změny všech kryptoměn za jeden měsíc, které jsem spočítal v pátém kroku a následně sečteme roční změnu kryptoměn, vypočtené v kroku šestém.

A jako poslední krok vypočítáme Value-at-Risk. Kalkulace proběhne za pomocí vzorce: Průměrná změna portfolia – (K-koeficient x absolutní hodnota volatility portfolia)

Tabulka 11 VaR

	1 měsíc	rok
Volatilita portfolia	38000,2	131636,7
Průměrná změna portfolia	12107,5	145290,4
VaR portfolia	-50397	-71232,65

Zdroj: vlastní zpracování

Krok 10 – interpretace výsledku

Na závěr výpočtu Value-at-Risk je potřeba interpretovat výsledek. Ve vzorovém příkladu jsem investoval 123 530 USD a všechny kryptoměny byly v portfoliu zastoupeny rovnoměrným podílem. Podle Value-at-Risk metody nebude ztráta portfolia v dolarovém vyjádření větší než 50397,29 dolarů za měsíc, a v procentuálním vyjádření vyšší jak 41 %. Maximální roční ztráta portfolia nebude vyšší než 70232,6 USD a v procentuálním vyjádření větší jak 58 %. Obě hodnoty jsou platné s 95 % pravděpodobností.

5.2 Testování Value-at-Risk

V této kapitole jsem provedl testování metody Value-at-Risk. Konkrétně tuto metodu použiji pro testování různých skladeb portfolia. V ukázkovém příkladu jsem již vypočítal variantu s rovnoměrným zastoupením všech kryptoměn v portfoliu. V této části práce jsem přidal další dvě různé varianty, a to variantu s dominantním zastoupení bitcoinu, jelikož se jedná o kapitálově největší kryptoměnu a poslední variantou bude portfolio založené na co největším zastoupením rizikových kryptoměn. Při testování vždy nejprve zadám vstupní hodnoty a následně výsledek. Vše bylo vypočteno v mém Value-at-Risk kalkulátoru.

Dominantní zastoupeni bitcoinu v portfoliu

V této analýze bude největší podíl v portfoliu představovat bitcoin. Vybral jsem právě tuto kryptoměnu, jelikož se jedná o nejznámější kryptoměnový token a jeho tržní kapitalizace je nejvyšší. Je také považován za cenově stabilní kryptoměnu. V tomto případě jsem zvolil 73 % podíl v portfoliu. Zbývající kryptoměny jsou rozloženy v 3 % poměru v portfoliu.

Tabulka 12 VaR vstupní data

Kryptoměna	Zkratka	Množství	Cena	Objem	Podíl
			$	$	%
Bitcoin	BTC	7,3	12353	90177	73%
Ethereum	ETH	8	440	3520	3%
XRP	XRP	11545	0,321	3706	3%
ChainLink	Link	197	18,82	3708	3%
Bitcoin Cash	BCH	11	323	3553	3%
Cardano	ADA	26098	0,142	3706	3%
Litecoin	LTC	55	67,36	3705	3%
Bitcoin SV	BSV	16	229,1	3666	3%
EOS	EOS	960	3,86	3706	3%
Binance Coin	BNB	155	23,84	3695	3%
			Suma:	123141	100%

Zdroj: vlastní zpracování

Tabulka 13 VaR výstupní data

	1 měsíc	Rok
Volatilita portfolia	28550,2	98900,9
Průměrná změna portfolia	7025,42	84305,03
VaR portfolia	-39936	-78372,48

Zdroj: vlastní zpracování

Výsledek interpretujeme tak, že maximální možná ztráta portfolia za měsíc je 39936 USD a 78372 USD za rok. Jedná se tedy o nižší měsíční ztrátu než v případě rovnoměrného rozložení kryptoměnu v portfoliu, avšak roční ztráta portfolia je vyšší. Toto může být zapříčiněno vyšší volatilitou ostatních kryptoměn v posledních měsících roku, kdy bitcoin vykazoval stabilnější cenové změny.

Dominantní zastoupení rizikových kryptoměn v portfoliu

Zde jsem aplikoval strategii vytvoření portfolia při vysokém podílu cenově rizikových kryptoměny. Zvolil jsem posledních pět kryptoměn z portfolia, jelikož jsou kapitálově nejmenší. Přiřadil jsem těmto kryptoměnám 15% zastoupení a zbývající kryptoměny byly zastoupeny 5% podílem.

Tabulka 14 VaR vstupní data

Kryptoměna	Zkratka	Množství	Cena	Objem	Podíl
			$	$	%
Bitcoin	BTC	0,5	12353	6177	5%
Ethereum	ETH	14,0375	440	6177	5%
XRP	XRP	19241,43	0,321	6176	5%
ChainLink	Link	328,1881	18,82	6177	5%
Bitcoin Cash	BCH	19,12229	323	6176	15%
Cardano	ADA	130489,4	0,142	18529	15%
Litecoin	LTC	275,0817	67,36	18530	15%
Bitcoin SV	BSV	80,87953	229,1	18530	15%
EOS	EOS	4800,389	3,86	18530	15%
Binance Coin	BNB	777,2441	23,84	18529	15%
			Suma:	123530	100%

Zdroj: vlastní zpracování

Tabulka 15 VaR výstupní data

	1 měsíc	Rok
Volatilita portfolia	37209,6	128897,7
Průměrná změna portfolia	10558	126696,4
VaR portfolia	-50646	-85321,39

Zdroj: vlastní zpracování

Podle výsledků posledního Value-at-Risk testu můžeme vyčíst, že maximální měsíční možná ztráta je 50646 USD a roční ztráta portfolia je maximálně 853211 USD za jeden rok. V procentuálním vyjádření je maximální měsíční ztráta 41 % a roční ztráta nepřesáhne 69 %.

Value-at-Risk shrnutí výsledků

V tabulce jsem shrnul výsledky tří strategií sestavení portfolia. Jak můžeme z tabulky vyčíst, podle Value-at-Risk strategie je nejlepší volba z dlouhodobého hlediska rovnoměrné portfolio, jelikož možná maximální roční ztráta je nejnižší.

Tabulka 16 Souhrn výsledků VaR

	Měsíční VaR portfolia v USD	Roční VaR portfolia v USD	Pravděpodobnost
Rovnoměrné portfolio	-50397	-71232	0,95
Portfolio s dominancí BTC	-39936	-78372	0,95
Portfolio s dominancí rizik. kryptoměn	-50646	-85321	0,95

Zdroj: vlastní zpracování

5.3 Výpočet Markowitzovy metody

V této části jsem detailně popsal svůj kalkulátor vytvořený v programu Excel, který vypočítává maximální možný zisk portfolia za určitého rizika. Vybral jsem stejných deset kryptoměn jako v případě Value-at-Risk metody. Pro vstupní data jsem využil tabulky 3 a 4. Tento kalkulátor je zjednodušením Markowitzovy metody, aby pro investora bylo snadné dostat potřebné údaje, avšak je potřeba dodat, že se vždy jedná pouze o odhad založený na historických datech. V modelu jsem počítal s měsíčními a ročními daty.

Krok 1 – kalkulace individuálního rizika a zisku

V tomto kroku nejprve vypočítáme očekávaný zisk za každou jednotlivou kryptoměnu. Toho dosáhneme zprůměrováním měsíčních cenových změn jednotlivých kryptoměn. Ve třetím sloupci bude vypočtena váha kryptoměn v portfoliu, avšak v prvním kroku je toto pole prázdné, jelikož bude doplněno později.

Tabulka 17 očekávaný zisk a váha

	Očekávaný zisk	Váha
	e	w
BTC	4%	
ETH	12%	
XRP	3%	
Link	38%	
BCH	4%	
ADA	14%	
LTC	1%	
BSV	15%	
EOS	3%	
BNB	3%	

Zdroj: vlastní zpracování

Krok 2 – kalkulace matice kovariance

Matici kovariance vytvoříme za pomocí funkce COVAR

Tabulka 18 matice kovariance

	BTC	ETH	XRP	Link	BCH	ADA	LTC	BSV	EOS	BNB
BTC	0,04	0,06	0,00	0,13	0,05	0,07	0,05	0,09	0,06	0,05
ETH	0,06	0,13	0,03	0,29	0,08	0,12	0,09	0,11	0,10	0,09
XRP	0,00	0,03	0,07	0,11	-0,01	0,02	0,02	-0,03	0,01	0,01
Link	0,13	0,29	0,11	0,80	0,17	0,23	0,20	0,20	0,22	0,20
BCH	0,05	0,08	-0,01	0,17	0,11	0,10	0,08	0,20	0,09	0,07
ADA	0,07	0,12	0,02	0,23	0,10	0,15	0,10	0,16	0,10	0,09
LTC	0,05	0,09	0,02	0,20	0,08	0,10	0,09	0,14	0,09	0,07
BSV	0,09	0,11	-0,03	0,20	0,20	0,16	0,14	0,41	0,16	0,12
EOS	0,04	0,10	0,01	0,22	0,09	0,10	0,09	0,16	0,10	0,08
BNB	0,05	0,09	0,01	0,20	0,07	0,09	0,07	0,12	0,08	0,08

Zdroj: vlastní zpracování

Krok 3 – kalkulace návratnosti portfolia a standartní odchylky

Vzorec pro návratnost portfolia:

$$\mathrm{E}(R_p) = \sum_i w_i \, \mathrm{E}(R_i)$$

Pro zjednodušení výpočtu využijeme funkci SUMPRODUCT. Tato hodnota bude vypočítána v pozdější fázi kalkulace a momentálně ukazuje nulovou hodnotu, jelikož váhy kryptoměn v portfoliu jsou v této fázi také nulové. Vzorec pro výpočet rizika v portfoliu má následující podobu:

$$\sigma_p^2 = \sum_i w_i^2 \sigma_i^2 + \sum_i \sum_{j \neq i} w_i w_j \sigma_i \sigma_j \rho_{ij},$$

Avšak pro zjednodušení výpočtu využijeme násobení matic. V tomto kroku je portfoliové riziko rovno výstraze „#HODNOTA!“, avšak po použití modulu SOLVER bude toto číslo automaticky vyhodnoceno.

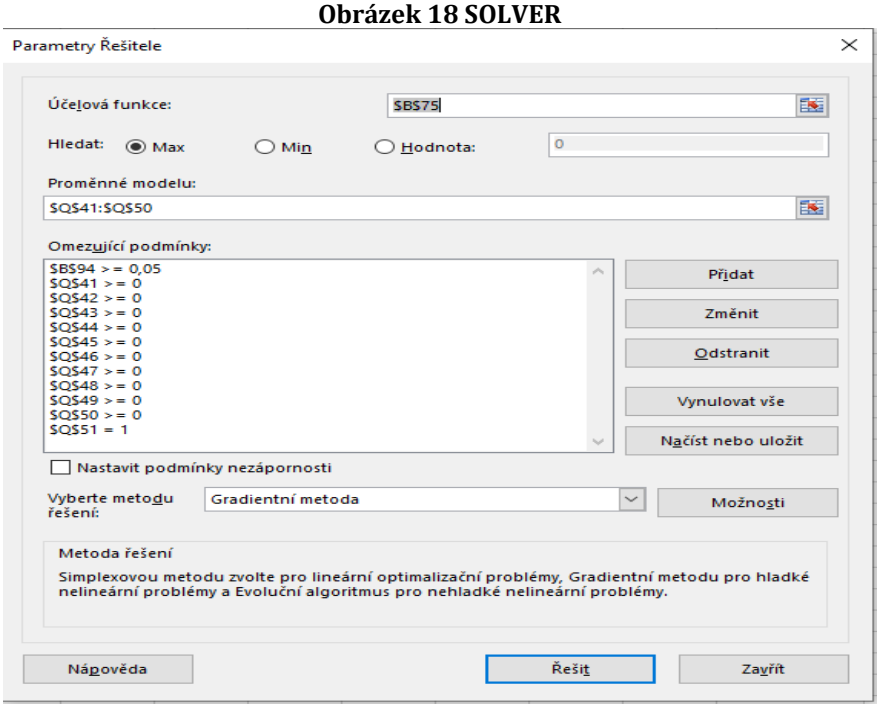
Krok 4 – použití modulu SOLVER

V posledním kroku využijeme modulu SOLVER. Najdeme ho v Excelu pod záložkou data. Pokud tam není, je třeba ho nainstalovat. Do SOLVERu musíme doplnit data.

- Účelová funkce – zde vybereme buňku, která obsahuje vzorec pro výpočet návratnosti portfolia.
- Hledat – zvolíme Max, jelikož hledáme maximální zisk za daného rizika.
- Proměnné modelu – zde vložíme sloupec obsahující váhy všech vybraných kryptoměn.
- Omezující podmínky – zde doplníme dvanáct omezujících podmínek.
    - Váha každé kryptoměny by neměla být menší než nula.
    - Suma všech vah je rovna jedné.
    - A risk portfolia je menší jak 5 %.

Dále zaškrtneme nastavení pro podmínky nezápornosti a vybereme Gradientní metodu řešení. Jako poslední krok spustíme SOLVER za pomocí tlačítka „řešit“.

Obrázek 18 SOLVER



Zdroj: vlastní zpracování

5.4 Testování Markowitzovy metody

V této kapitole provedu testování mnou vytvořeného kalkulátoru využívající Markowitzovu metodu stavby portfolia.

V tabulkách níže můžeme vidět, že pokud bude růst riziko, bude celkový zisk klesat. Toto je zapříčiněno tím, že s vyšším rizikem budeme dosahovat vyšších ztrát. Dále

v tabulkách 20 a 21 můžeme na názorném příkladu vyobrazit různou váhu BTC a ETH při rozdílném riziku.

Tabulka 19 Výnos portfolia při určitém riziku

Riziko	Výnos portfolia	Celkový zisk
5%	46941,4	170471,4
10%	45706,1	169236,1
15%	44470,8	168000,8
20%	43235,5	166765,5
25%	43235,5	166765,5
30%	42000,2	165530,2

Zdroj: vlastní zpracování

Tabulka 20 Váha kryptoměn při 30 % riziku

	Očekávaný zisk	Váha
	E	w
BTC	4%	13%
ETH	12%	87%
Riziko	30%	

Zdroj: vlastní zpracování

V tabulce 20 vidíme váhu a očekávaný zisk kryptoměn. Váha zde reprezentuje hodnotu, která ukazuje kryptoměnu s nejvyšším podílem na zisku.

Tabulka 21 Váha kryptoměn při 5 % riziku

	Očekávaný zisk	Váha
	E	w
BTC	4%	2%
ETH	12%	98%
Riziko	5%	

Zdroj: vlastní zpracování

Díky Markowitzově metodě můžeme zjistit, kolik procent zisku může dané portfolio za určitého rizika vygenerovat. Také nám tento model ukáže, které kryptoměny jsou pro portfolio rozhodující. V tabulce 20 vidíme váhu BTC a ETH při 30% riziku a v tabulce 21 můžeme pozorovat váhy těch samých kryptoměn při 5% riziku.

5.5 Výpočet Monte Carlo metody

Pro cardano a ethereum jsem se rozhodl využít Monte Carlo metodu. Tato metoda pomůže investorovi určit možný profit na bázi několika tisíců testů, ze kterých vypočítáme průměrnou hodnotu zisku.

Cardano

Investor vyplní potřebná data do tabulky. Já jsem zvolil období od 30. 7. 2019 do 30. 7.2020 stejně jako v případě výpočtu VaR metody a Markowitzova portfolia. Dále jsem doplnil ceny vždy na konci měsíce a vypočítal procentuální změnu. Počítal jsem s hodnotou investice 123530 USD. Tuto investici jsem rozdělil do pravidelné měsíční investice, tedy 10294,167 USD měsíčně. Za tuto částku každý měsíc investor dokoupil ADA tokeny. Tato cena byla vždy na konci měsíce rozdílná oproti předešlému nákupnímu období, proto investor každý měsíc nakoupil jiný počet tokenů ADA. Dále jsem vypočítal průměrný obrat, odchylku obratu, průměrnou cenu, maximální cenu a minimální cenu. Jako poslední krok vypočítáme profit, kdy vezmeme průměrný profit za celý rok a odečteme částku složenou z násobku průměrné ceny s průměrem zakoupených tokenů za celý rok. Všechny tyto výpočty jsou zobrazeny v následujících tabulkách.

Tabulka 22 Počet zakoupených ADA tokenů během 1 roku

Datum	ADA	Změna	Počet zakoupených tokenů	Obrat
30.07.2019	0.06		171569.4444	10294.17
30.08.2019	0.045	-25%	228759.2593	18014.79
30.09.2019	0.039	-13%	263952.9915	25906.99
30.10.2019	0.042	8%	245099.2063	38194
30.11.2019	0.041	-2%	251077.2358	47578.78
30.12.2019	0.034	-17%	302769.6078	49749.74
30.01.2020	0.057	68%	180599.4152	93698.15
29.02.2020	0.048	-16%	214461.8056	89197.87
30.03.2020	0.03	-38%	343138.8889	66042.84
30.04.2020	0.05	67%	205883.3333	120365.6
30.05.2020	0.077	54%	133690.4762	195657.1
30.06.2020	0.083	8%	124026.1044	221197.3
30.07.2020	0.142	71%	72494.13146	388728.1
	Průměrně zakoupeno		210578.6077	

Zdroj: [12]

Tabulka 23 Průměrný obrat a odchylka obratu cardana

Průměrný obrat	104971.1866
Odchylka průměrného obratu	103015.1271

Zdroj: vlastní zpracování

Tabulka 24 Průměrná, maximální a minimální cena cardana

Průměrná cena	0.057538
Maximální cena	0.142
Minimální cena	0.03
Profit	**92854.91**

Zdroj: vlastní zpracování

Aplikace Monte Carlo metody na cardano

Pro Monte Carlo metodu jsem zvolil placený doplněk pro Excel od firmy Oracle. Investor může zvolit jakýkoliv jiný program pro výpočet těchto dat. Po spuštění doplňku Crystall Ball od firmy Oracle, dostaneme tyto hodnoty pro cardano:

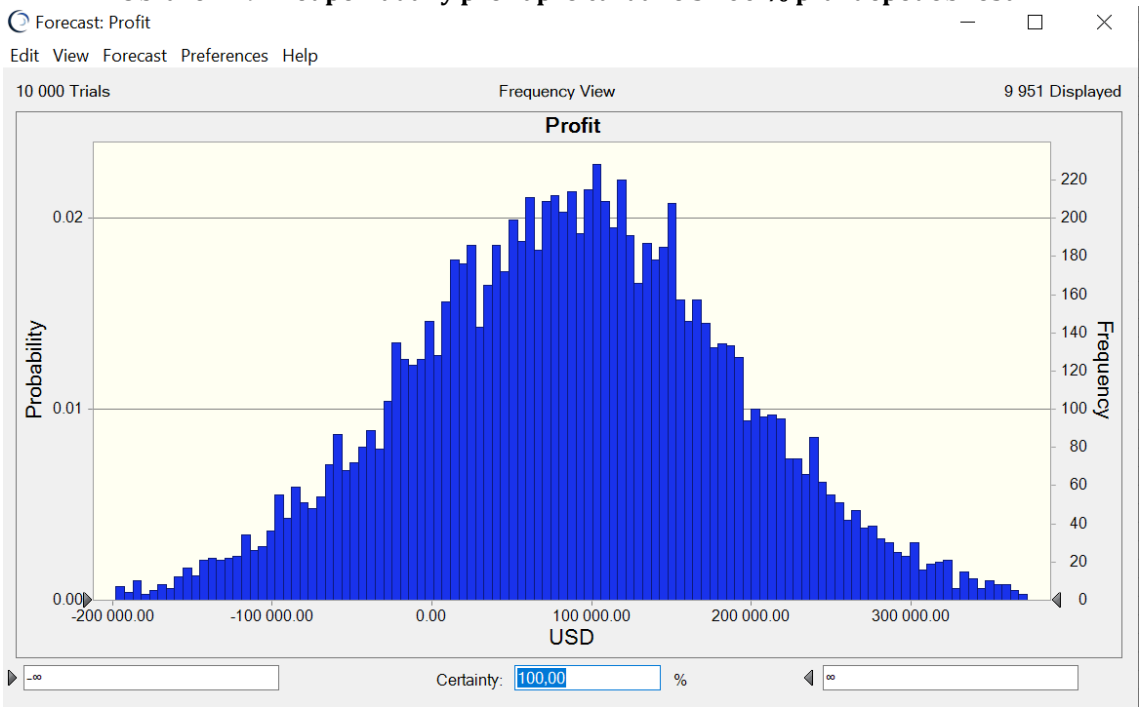
Tabulka 25 Hodnoty pro Monte Carlo analýzu cardana

Statistic	Forecast values
Trials	10 000
Base Case	92 854,91
Mean	87 348,87
Median	88 234,74
Mode	---
Standard Deviation	101 867,25
Variance	10 376 937 553,16
Skewness	-0,0255
Kurtosis	3,03
Coeff. of Variation	1,17
Minimum	-285 723,05
Maximum	463 377,88
Mean Std. Error	1 018,67

Zdroj: vlastní zpracování

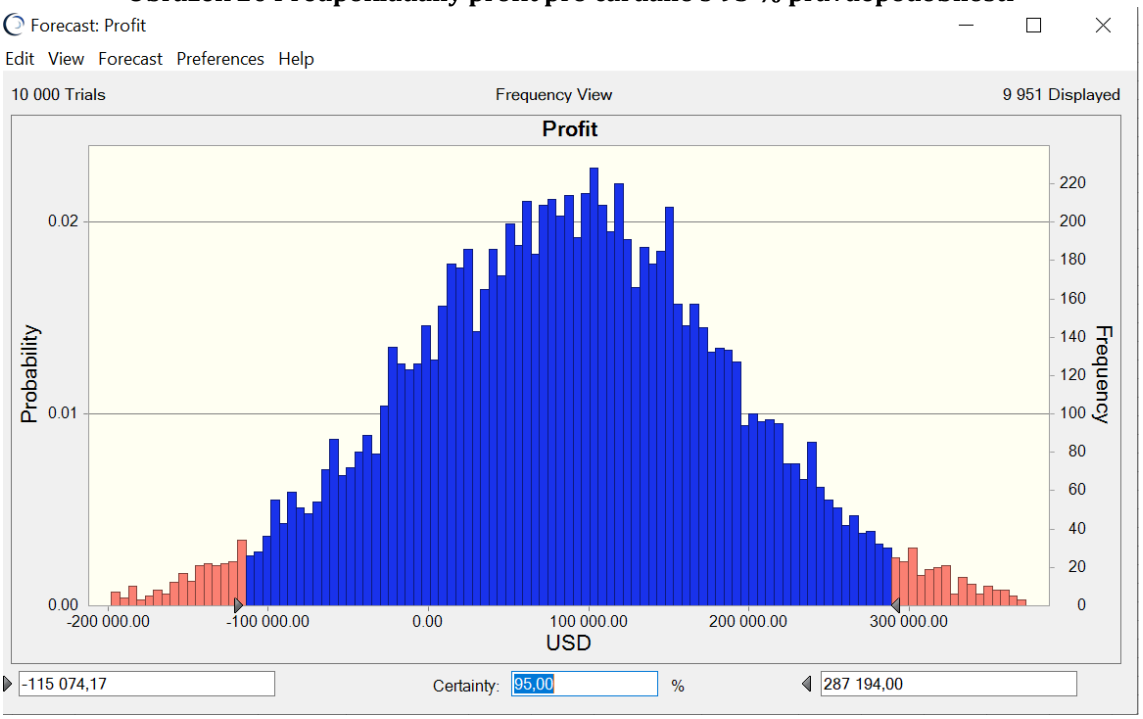
V tabulce vidíme vyplněné hodnoty pro výpočet Monte Carlo metody. Proběhne 10 000 testů, průměrný zisk je 87 348 dolarů, Maximální zisk činí 463 377,8 dolarů a maximální ztráta je 285 723,05 dolarů. Důležitá hodnota pro investora je nejlepší možná hodnota, neboli „base case“. V tomto případě tato hodnota činí 92 854 dolarů a s tímto číslem dále počítám ve své práci jako s předpokládaným ziskem. V grafech níže uvádím výpočty s určitou pravděpodobností. Jedná se o pravděpodobnost 100 %, 95 %, 90 % a 85 %. Tyto hodnoty jsem zvolil pro ilustraci rozmezí, v jakém se může zisk a ztráta pohybovat. Je nutné podotknout, že 100 % jistota se v manažerském prostředí tolik nepoužívá a spíše se volí o něco nižší.

Obrázek 19 Předpokládaný profit pro cardano s 100 % pravděpodobností



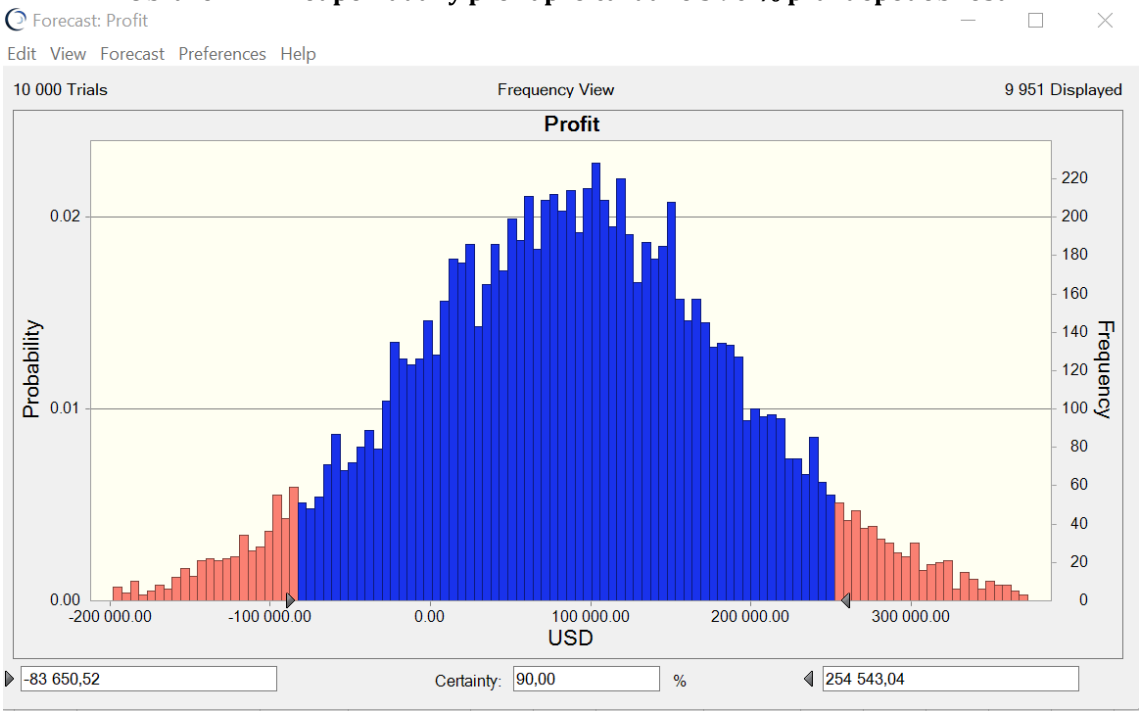
Zdroj: vlastní zpracování

Obrázek 20 Předpokládaný profit pro cardano s 95 % pravděpodobností



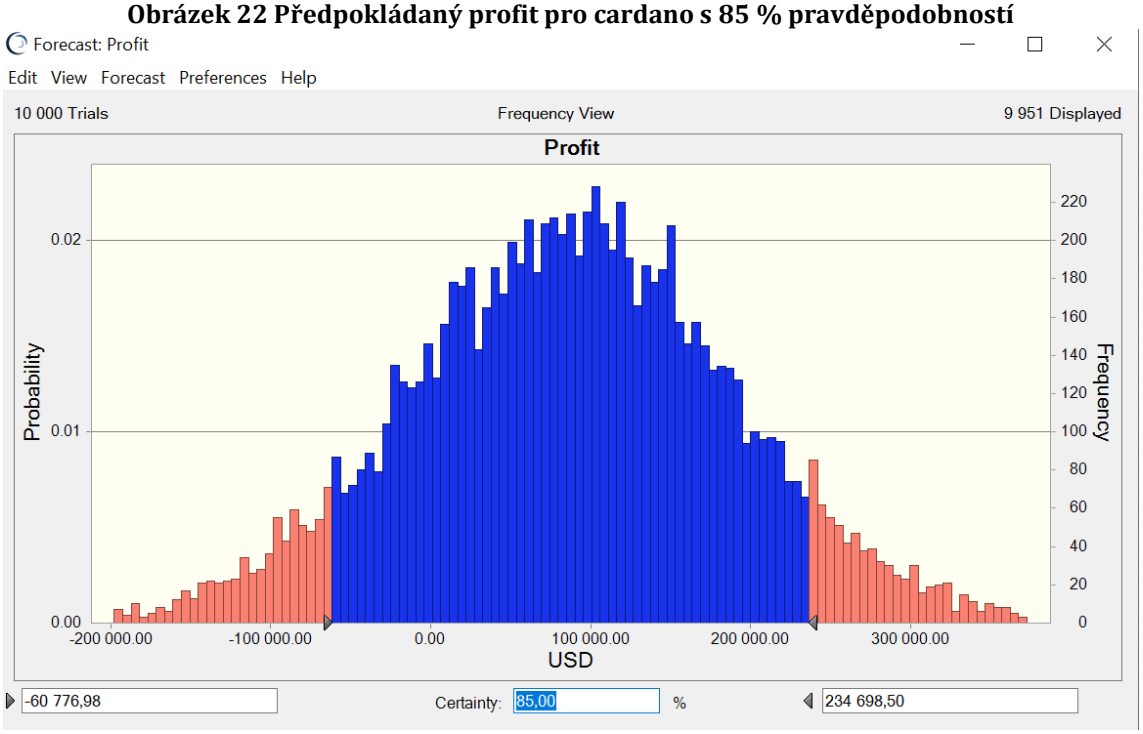
Zdroj: vlastní zpracování

Obrázek 21 Předpokládaný profit pro cardano s 90 % pravděpodobností



Zdroj: vlastní zpracování

Obrázek 22 Předpokládaný profit pro cardano s 85 % pravděpodobností



Zdroj: vlastní zpracování

Ethereum

Provedl jsem stejné výpočty i pro kryptoměnu ethereum. Metoda výpočtu je stejná jako pro cardano. Investujeme zde do etherea každý měsíc rovnoměrnou částkou. Celková hodnota investice je 123530 USD. Měsíčně investor zakoupí ethereum v hodnotě 10294 USD. V tabulce níže je zobrazen počet zakoupených tokenů etherea, datum, procentuální změna oproti minulému měsíci a obrat.

Tabulka 26 Počet zakoupených ethereum tokenů během 1 roku

Datum	ETH	Změna	Počet zakoupených tokenů	obrat
30.07.2019	210.52		48.89875863	10294.17
30.08.2019	168.83	-20%	60.97356315	18549.74
30.09.2019	179.87	7%	57.23114842	30056.9
30.10.2019	184.69	3%	55.73754219	41156.51
30.11.2019	152.54	-17%	67.48503125	44286.33
30.12.2019	132.63	-13%	77.61567267	48800.11
30.01.2020	184.69	39%	55.73754219	78249.32
29.02.2020	219.85	19%	46.82359184	103440.1
30.03.2020	132.9	-40%	77.45798846	72824
30.04.2020	207.6	56%	49.58654464	124050.8
30.05.2020	242.35	17%	42.47644591	155109.8
30.06.2020	226.31	-7%	45.48701633	155138
30.07.2020	440	94%	23.39583333	311918.9
	Průměrně zakoupeno		54.531283	

Zdroj: vlastní zpracování

Tabulka 27 Průměrný obrat a odchylka obratu etherea

Průměrný obrat	91836.51
Odchylka průměrného obratu	78780.99

Zdroj: vlastní zpracování

Tabulka 28 Průměrná, maximální a minimální cena etherea

Průměrná cena	206.3677
Maximální cena	440
Minimální cena	132.63
Profit	80583.02

Zdroj: vlastní zpracování

Aplikace Monte Carlo metody na ethereum

Pro ethereum jsem také využil Crystal Ball software a dostat tyto hodnoty:

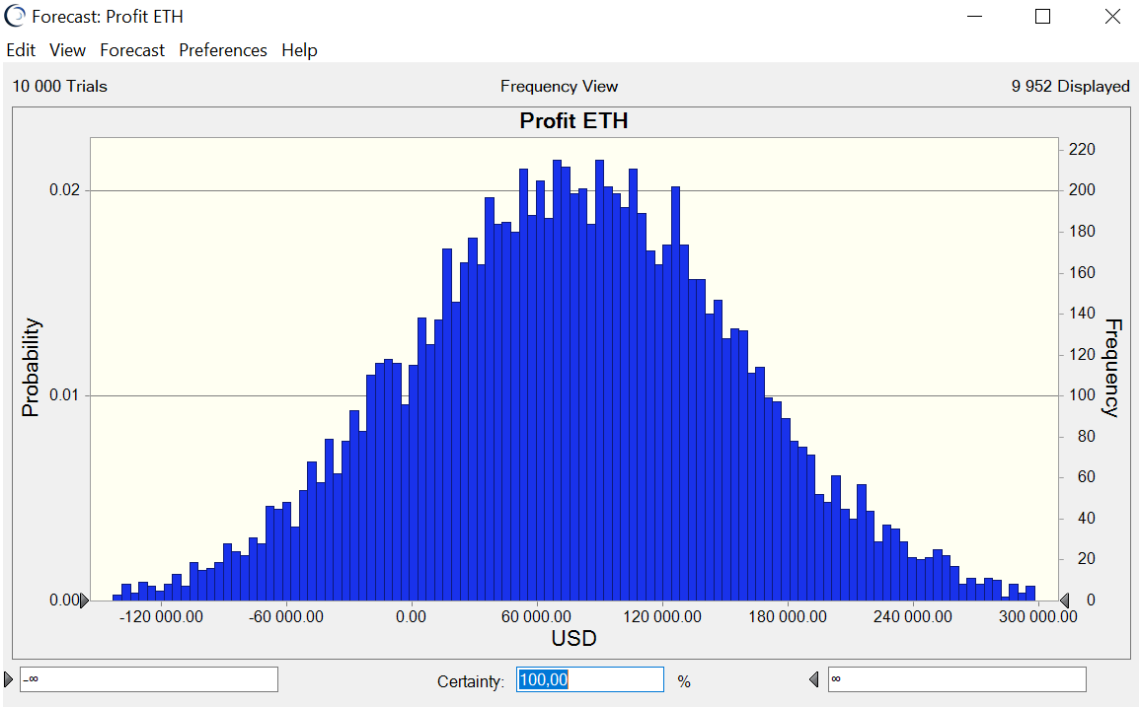
Tabulka 29 Hodnoty pro Monte Carlo analýzu ethera

Statistic	Forecast values
Trials	10 000
Base Case	80 583,02
Mean	77 380,72
Median	77 466,54
Mode	---
Standard Deviation	78 712,61
Variance	6 195 675 079,25
Skewness	0,0101
Kurtosis	3,04
Coeff. of Variation	1,02
Minimum	-237 175,24
Maximum	403 380,58
Mean Std. Error	787,13

Zdroj: vlastní zpracování

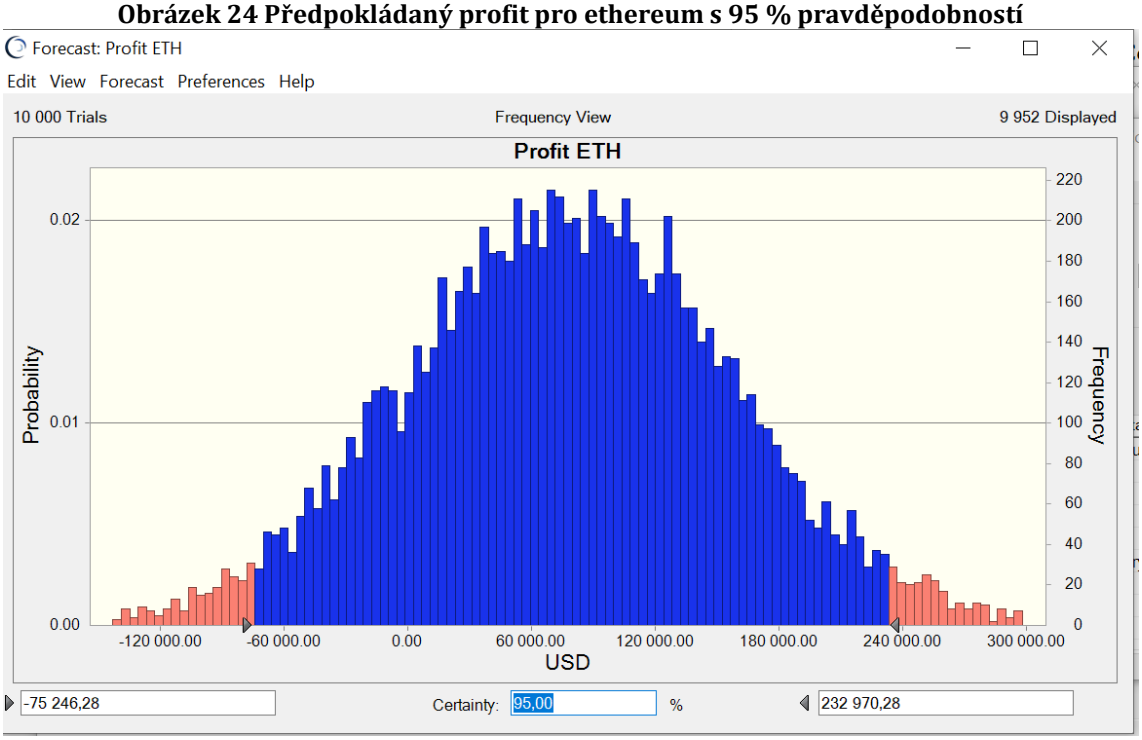
V tabulce nahoře vidíme hodnoty pro analýzu Monte Carlo metodou. Proběhne 10 000 testů, průměrný zisk je 77 380 dolarů, maximální zisk činí 403 380 dolarů a maximální ztráta je 237 175 dolarů. Pro další výpočty jsem kalkuloval s nejlepším možným ziskem, tedy s hodnotou 80 583 dolarů. V dalších grafech níže jsem vyobrazil rozložení možného zisku, ztráty a průměrného zisku etherea po 10 000 testech, vždy za určité pravděpodobnosti.

Obrázek 23 Předpokládaný profit pro ethereum s 95 % pravděpodobností



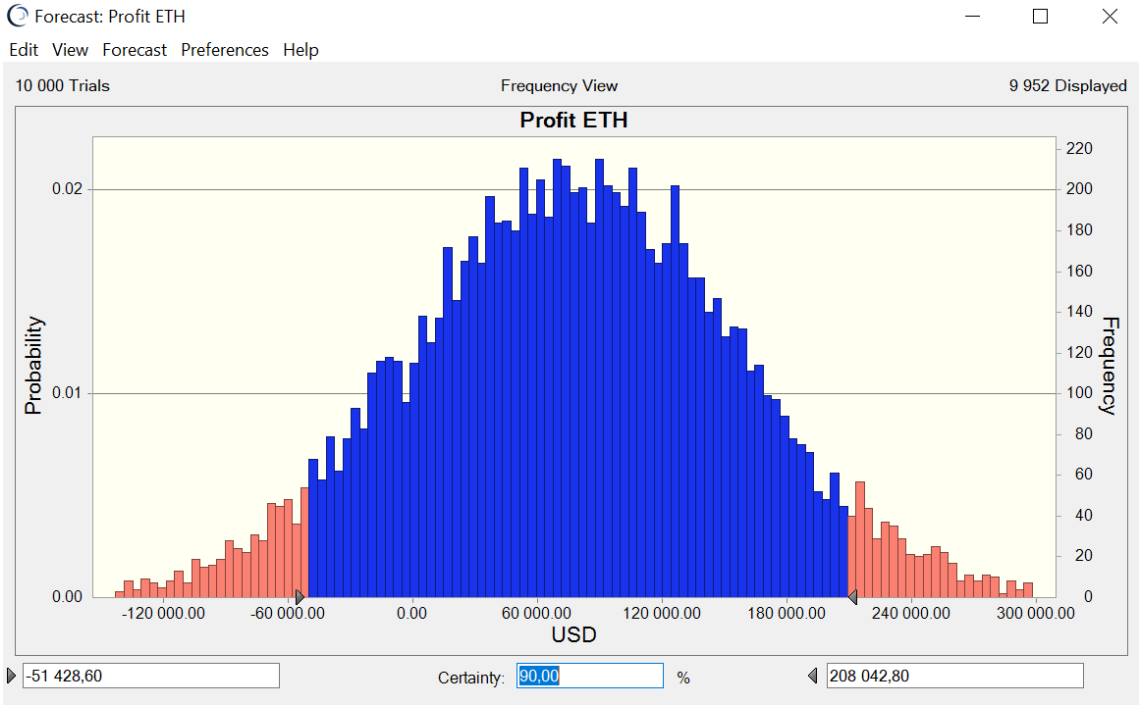
Zdroj: vlastní zpracování

Obrázek 24 Předpokládaný profit pro ethereum s 95 % pravděpodobností



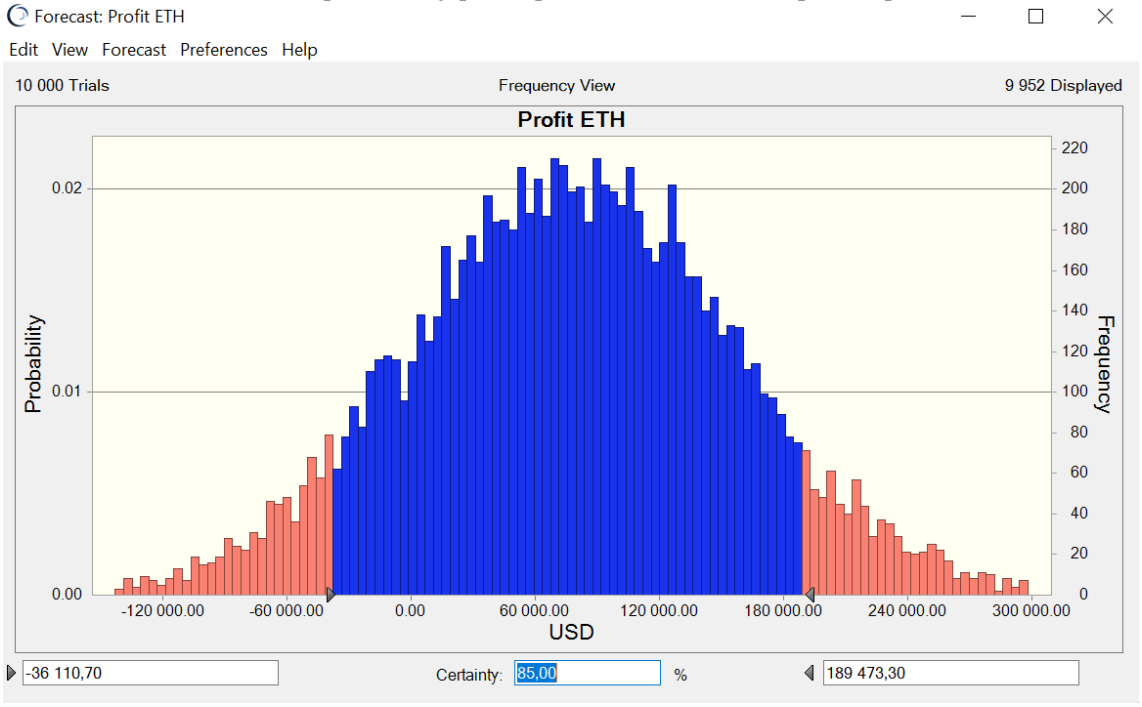
Zdroj: vlastní zpracování

Obrázek 25 Předpokládaný profit pro ethereum s 90 % pravděpodobností



Zdroj: vlastní zpracování

Obrázek 26 Předpokládaný profit pro ethereum s 85 % pravděpodobností



Zdroj: vlastní zpracování

5.6 Výpočet těžby etherea a cardana

Zde jsem vypracoval teoretický výpočet těžby dvou kryptoměn. Jedná se o alternativu pro investora, kterou považuji za méně rizikovou.

Cardano

Těžba cardana je jednoduchá a bezpečná. Podrobně jsem popsal způsob těžby v praktické části, takže zde provedu pouze výpočet za pomocí oficiální kalkulačky výnosnosti těžby [48]. Investici jsem ponechal ve stejné výši jako v předchozích příkladech, kde jsem počítal výnosnost portfolia. Jedná se o částku 123530 USD. Investice teoreticky proběhla 30. 7. 2020, tedy v poslední měsíc časového úseku, s kterým jsem počítal v předešlých příkladech. Pro zjednodušení příkladu nebudu kalkulovat s měsíčním dokupováním. Jedná se víceméně o podobný princip, jako při spoření, které je běžným investičním nástrojem.

Obrázek 27 Kalkulačka pro těžbu cardana

Zdroj: [48]

V tabulce níže je vyobrazena cena cardana, velikost investice v dolarech a v cardano tokenech. Dále je zde vypočítaná konečná suma tokenů, které investor získá na konci roku. Tato suma je součtem zakoupených a vytěžených tokenů. Investor na konci roku bude disponovat 914 645 tokeny cardana.

Tabulka 30 Počet vytěžených tokenů cardana za jeden rok

	USD	Cardano tokenů	Cena 30. 7. 2020 v USD
Investice	123530	869929,5775	0,142
Počet vytěžených tokenů na konci roku		44716	
Suma		914645,5775	

Zdroj: vlastní zpracování

V další tabulce jsem vypočítal, jakého zisku či ztráty může investor dosáhnout. Velice záleží na ceně cardana v době prodeje. Díky těžbě cardana bude investor vždy mít více tokenů cardana, avšak pokud je vymění za dolary, může se ocitnout i ve ztrátě. V tabulce jsem vypočítal zisk a ztrátu, pokud by investor prodával při průměrné roční ceně. Také jsem uvedl, jakého zisku by investor dosáhl, pokud by prodával za maximální roční cenu. Posledním vyobrazením je ztráta, pokud investor prodá svoje cardano tokeny za minimální cenu. Těžba cardana investorovi vynesla 5 % zisk cardano tokenů za rok.

Tabulka 31 Výsledná hodnota investice do těžby cardana

		Potencionální zisk těžby v USD	Celková hodnota investice v USD	Zisk/Ztráta
Průměrná cena	0,0575	2572,889846	52627,29938	-57%
Maximální cena	0,142	6349,672	129879,672	5%
Minimální cena	0,03	1341,48	27439,36732	-78%

Zdroj: vlastní zpracování

Ethereum

Těžba etherea probíhá za pomocí hardwaru. Většinou se jedná GPU procesory neboli grafické karty. V tomto příkladu budu také počítat s investicí 123530 USD. Za tyto peníze teoreticky investor musí zakoupit potřebné grafické karty. Dále zde budu

počítat s cenou elektřiny, protože ta je klíčovým prvkem pro kalkulaci profitu. Nebudu zde zahrnovat náklady na pronájem haly, jelikož toto číslo by bylo příliš nahodilé, jelikož těžba může probíhat například i doma. Pro výpočet využiji kalkulátory ze stránky www.cryptocompare.com [49]. Dle mého názoru a zkušeností se jedná o důvěryhodnou stránku pro výpočet zisku či ztráty těžby kryptoměny. Investor má několik možností, jakou grafickou kartu zakoupí, avšak já osobně jsem se vybral Nvidia GeForce GTX 1070, jelikož vykazuje nejlepší výkon k/ke poměru ceny. Tuto kartu lze zakoupit například na www.amazon.com za cenu 599 USD [50].

Lze tedy spočítat, že investor může nakoupit 206 grafických karet Nvidia GeForce GTX 1070.Pro výpočet musíme také znát MH/s. Tento údaj můžeme naleznout například na stránce www.miningchamp.com [51]. Zde je uvedeno, že Nvidia Geforce GTX 1070 dosahuje 31.246 MH/s a má spotřebu 95 W. Cenu elektřiny v České republice jsem převzal ze stránky www.cenyenergie.cz. Podle této stránky je průměrná cena 0,196 dolarů za kWh [52].

Tabulka 32 Investice do těžby etherea

	USD
Investice	123530
Cena G. Karty	599
Počet zakoupených G. karet	206
MH/s jedné karty	31,246
Spotřeba jedné karty (w)	95

Zdroj: [50,51]

V následující tabulce jsem vypočetl celkový výpočetní výkon všech zakoupených grafických karet. Dále jsem spočítal celkovou spotřebu energie těchto karet, abych mohl vypočítat celkové náklady za energie.

Tabulka 33 Výkon a spotřeba Nvidia GeForce GTX 1070

	MH/s	W
Celkový výpočetní výkon	6443,77	
Celková potřeba energie		19591,57

Zdroj: [51]

Ve výsledku investor vytěží 127 etherea a za energie zaplatí 33640 dolarů.

Tabulka 34 Počet vytěžených ETH a cena elektřiny za jeden rok

Ročně vytěžených ETH	127,36
Roční cena za energie v USD	33640

Zdroj: vlastní zpracování

Tabulka 35 Výsledná hodnota investice do těžby etherea

	USD	Potencionální obrat těžby v USD	Potencionální zisk těžby v USD
Průměrná cena	206,3677	26282,98929	-7357,010708
Maximální cena	440	56038,4	22398,4
Minimální cena	132,63	16891,7568	-16748,2432

Zdroj: vlastní zpracování

Pokud investor nebude prodávat svoje grafické karty, které může i nadále využívat pro další těžbu, můžeme se zaměřit na počet vytěženého etherea. Pokud by investor prodal všechny své etherea za průměrnou roční cenu, ocitl by se ve ztrátě 7357 dolarů. Jestliže by prodával za maximální roční cenu, zisk by činil 22394 dolarů. Ztráta při prodeji za minimální roční cenu etherea činí 16748 dolarů. Velmi tedy záleží, za jakou cenu se investor rozhodne vytěžené ethereum prodat. Oproti těžbě cardana je zde investor v nevýhodě, jelikož se musí rozhodnout, co udělat se svými grafickými kartami. Také musí zaplatit za cenu elektřiny, za již vytěžené ethereum a pokud se rozhodne těžit i do budoucna, musí počítat s tímto poměrně vysokým poplatkem.

5.7 Rozhodovací strom

Zde jsem sestavil pro investora rozhodovací strom, který využije při výběru strategie své investice. V tabulce níže jsem roztřídil míru rizika investice.

Tabulka 36 Tabulka míry rizika

Vysoké riziko	Střední riziko	Nízké riziko
Cardano	Rovnoměrné portfolio	Těžba Cardana

Zdroj: vlastní zpracování

Rozhodovací strom se skládá z několika částí, které odráží mé výpočty provedené v této práci. Hlavní tři větve jsou: Těžba, Portfolia a Monte Carlo. Těžba se skládá ze dvou dalších větví, a to to těžba etherea a cardana. Jak můžeme z rozhodovacího stromu vyčíst, tak v případě větve těžba vychází cardano při jakékoliv ceně jako zisková volba. Je to zapříčiněné tím, že nespekuluji na hodnotu celé investice jako takové, ale pouze na počet vytěžených cardano tokenů a následně jejich prodej za průměrnou, minimální či maximální cenu. V případě etherea musíme počítat s náklady, které nám vznikají, při těžbě na Proof of Work síti. Hlavním nákladem zde je cena elektřiny. Také nekalkuluji s variantou, kde po jednom roce investor prodá všechny zakoupené grafické karty, jelikož hardwarová těžba není vhodná pro krátké období.

Další větev nese název Monte Carlo, kde investor může uvažovat o investici do cardana či etherea. Investice probíhá fixní částkou, za kterou každý měsíc nakoupí investor tokeny etherea či cardana. Investice je zde také 123530 USD, které investuje do každé kryptoměny zvlášť. V rozhodovacím stromu investor může vidět, že podle analýzy Monte Carlo dosáhne vyššího zisku investicí do cardana.

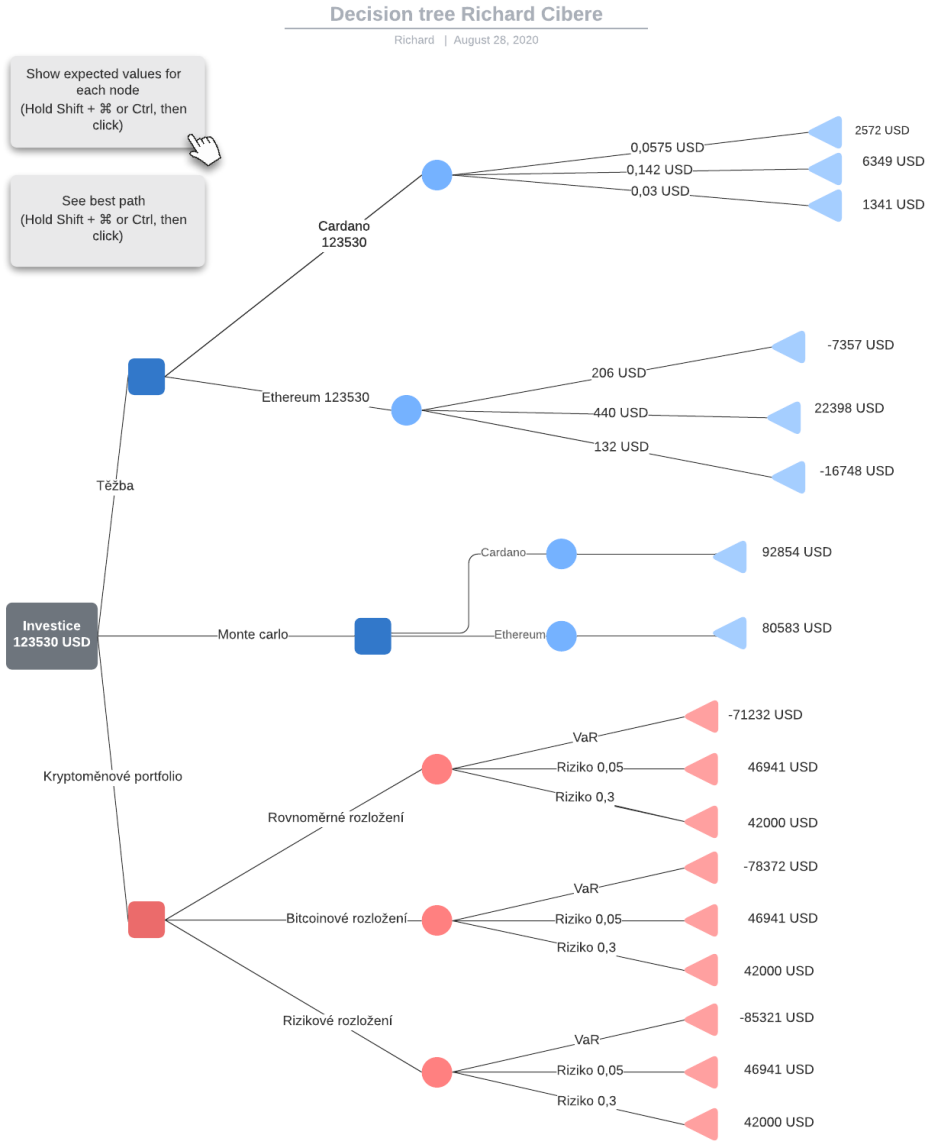
Poslední větev kalkuluje se třemi portfolii , vytvořené za využití poznatků z Value at Risk a Markowitzovy metody. Value at Risk je zde vyjádřeno maximální možnou ztrátou jednotlivého portfolia a Markowitzova metoda je zde vyjádřená jako

potencionální zisk za daného rizika. V rozhodovacím stromu je Markowitzova metoda vyjádřena rizikem a to v hodnotě pět procent nebo třicet procent.

Prvním portfoliem je rovnoměrná investice do deseti kryptoměn. Investice 123530 USD je rozdělena do deseti částí. Druhé portfolio je založené na bitcoinové dominanci v portfoliu, kde zaujímá většinový podíl a zbytek kryptoměn je zastoupeno rovným podílem. V posledním portfoliu je do pěti kapitálově nejmenších kryptoměn investováno patnáct procent do každé z nich. Jedná se o rizikové portfolio.

Z tabulky míry rizika můžeme vyčíst, že nejrizikovější investicí je investice do samotného cardana. K tomuto poznatku jsem dospěl za pomocí metody Monte Carlo. Na druhou stranu díky investici do cardana můžeme dosáhnout nejvyššího zisku. Také můžeme k této strategii připojit těžbu cardana, jelikož tyto dvě metody se doplňují. Investor může zakoupit každý měsíc cardano za fixně danou částku , a takto zakoupené tokeny delegovat do poolu.
Druhá nejrizikovější investice je rovnoměrné portfolio, které má nejnižší ztrátu podle Value at Risk a zároveň podle Markowitzovy strategie tvorby portfolia dosahuje vysokého zisku.

Obrázek 28 Rozhodovací strom s výsledky



Zdroj: vlastní zpracování

6 Výsledky

Ve své diplomové práci jsem detailně popsal fungování blockchainu a těžbu kryptoměn. Zaměřil jsem se především na popsání fungování těžby na Proof of Work a Proof of Stake protokolech. Dále jsem tyto mechanismy konsenzu porovnal a poukázal na rozdíly. Detailně jsem investora seznámil s deseti kryptoměnama, jelikož považuji za nutné, aby investor věděl, do čeho investuje. Mezi těmito kryptoměnama můžeme nalézt zástupce Proof of Work i Proof of Stake. Dále jsem popsal druhy systémů pro podporu rozhodování, jelikož jsem dále v práci využil rozhodovacího stromu, jenž pod tyto systémy spadá. V této sekci jsem také představil tři vybrané akademické práce, které se zaměřují na využití systémů na podporu rozhodování a následnou aplikaci na kryptoměny či akcie.

Následně jsem podrobně představil tři analytické nástroje. Jedná se o Value at Risk, Markowitzův model a Monte Carlo analýzu. Tyto modely se běžně používají při investičním rozhodování. V práci jsem vysvětlil principy těchto metod. Tyto nástroje jsem využil v praktické části práce pro výpočty a sestrojení vlastní kalkulačky v Excelu, která může investorovi pomoci při rozhodování a stavbě portfolia. Ve své práci jsem také podrobně popsal, jak tato kalkulačka funguje, aby investor mohl krok za krokem vyplnit potřebné údaje a mohl za pomocí této kalkulačky učinit investiční rozhodnutí. Investor může tuto kalkulačku využít na jakoukoliv jinou kryptoměnu či akcii. Za pomocí Value at Risk metody jsem vypočítal maximální možnou ztrátu portfolia. Pro svoje výpočty jsem vytvořil tři ukázková portfolia (rizikové, rovnoměrné a s dominantním podílem bitcoinu). Dále jsem v práci použil Markowitzovu metodu pro výpočet maximálního možného zisku portfolia za určitého rizika. Provedl jsem simulaci pro 5 % a 30 % riziko.

Následně jsem aplikoval Monte Carlo metodu na investici do cardana a etherea. Po provedení 10 000 testů v aplikaci Crystal Ball, která dokáže simulovat velké množství testů, jsem investorovi ukázal dosažitelný profit, kterého může dosáhnout, pokud investuje do těchto dvou kryptoměn.

Také jsem ve své práci představil investici do těžby etherea a cardana. Rozhod jsem se právě pro tyto dvě kryptoměny, jelikož jsem mohl ilustrovat rozdíl mezi Proof of Work a Proof of Stake. Popsal jsem výhody a nevýhody a názorně ukázal, jakých zisků či ztrát může investor dosáhnout, pokud se rozhodne investovat do těžby kryptoměn.

Na konci práce jsem všechny dosažené výsledky zanesl do rozhodovacího stromu. V tomto systému pro podporu rozhodování může investor přehledně vybrat investici, která mu přijde vhodná. Rozhodovací strom je jednoduchým a přehledným pomocníkem. Pomohl mi zanést všechny výsledky do grafického vyjádření.

Také bych rád porovnal svojí práci s akademickými pracemi představenými v kapitole 4.4.2. Autoři těchto prací využili kolektivní moudrost investorů, ortogonální a dotazníkovou metodu a také strojového učení pro podporu rozhodování investora. Všechny tři práce dospěly k závěru, že vytvořili systémy dostatečné dobré, aby je investor mohl využít pro investiční rozhodnutí. Já jsem naopak zvolil jednoduchý rozhodovací strom, který je přehledný a jednoduchý na pochopení. Hlavní rozdíl však vidím v tom, že jsem tento rozhodovací strom doplnil o svojí kalkulačku, kterou může investor využít pro své investiční rozhodnutí. Výsledky z této kalkulačky může zanést do rozhodovacího stromu. Díky tomu může uvažovat o investici do jakékoliv kryptoměny a sestavení svého preferovaného portfolia. Nebo může dojít k závěru, že je pro něj vhodné kryptoměny těžit. Za využití Monte Carlo modelu, Markowitzovu modelu a Value at risk, bude investor vědět maximální možnou ztrátu, maximální zisk a pravděpodobný zisk. Může také doplnit údaje v mé kalkulačce pro výpočet rentability těžby.

7 Závěry a doporučení

Kryptoměny jsou stále velmi rizikovou investicí a je možné, že tomu tak bude ještě dlouhou dobu. Pravděpodobně státy budou volat po regulaci tohoto finančního trhu, jelikož chtějí „ochránit“ své občany před finanční ztrátou. Avšak v poslední době je znát určitý obratu myšlení velkých společností. Tyto společnosti se velmi obávají inflace, jelikož jim znehodnocuje zisky. A tak tyto společnosti hledají další investiční příležitosti a kryptoměny jsou jednou z nich. Druhý nejbohatší muž světa, Elon Musk, sám investoval do bitcoinu. Mnoho dalších menších manažerů a vlastníků firem následovali jeho příkladu. Dokonce i velké banky, jako Goldman Sachs a J. P Morgan budou nabízet svým klientům investici do kryptoměn. Samozřejmě za poplatek a klient nebude opravdovým vlastníkem kryptoměny, jelikož banky budou vlastníky seedu a privátního klíče. Satoshi Nakamoto vytvořil bitcoin jako nástroj proti inflaci a proti bankám. Je trošku ironií, že banky budou na jeho vynálezu profitovat. Na druhou stranu mnohé státy vnímají bitcoin jako hrozbu své národní měny. V zemích, kde je velká míra inflace je bitcoin vyhledávaným artiklem. Mnoho totalitních zemí chápe, že bitcoin může sloužit jak platidlo, které tyto státy nemohou snadno kontrolovat. Můžeme se tedy setkat se zákazy používat bitcoin například při nákupu, anebo zablokování bankovního účtu, pokud banka má podezření, že peníze pocházejí z kryptoměnových zisků.

Tato práce vznikala především v roce 2020 a je zde jedinečná příležitost porovnat moje výsledky se skutečností. Pokud by se investor rozhodl následovat mých příkladů, došel by k zajímavým výsledkům. Pro ilustraci použiji stejnou výše investice, jako v mých výpočtech, tedy 123 530 dolarů.

Tabulka 37 Reálné výsledky investice

Druh investice	Zisk v USD
Těžba cardana	1 234 770
Těžba ethera	318 273
Investice do cardana	3 723 028
Investice do etherea	1 963 191
Rovnoměrné portfolio	785 280

Zdroj: vlastní zpracování

Jak můžeme z tabulky vyčíst, investor by byl v zisku, ať by vybral jakoukoliv variantu. Nejvyššího zisku by investor dosáhl, pokud by pouze každý měsíc po dobu jednoho roku nakupoval cardano. Naopak nejnižšího zisku by investor dosáhl u těžby etherea, jelikož je třeba odečíst i cenu za energie. Samozřejmě lze namítnout, že k dnešnímu datu jsou kryptoměny v tzv. „bull marketu“. Avšak pokud investor vybere kvalitní kryptoměnu, tak lze očekávat v dlouhodobém horizontu růst ceny. Moje vlastní doporučení pro investory, které je podpořené reálným výsledkem, je vybrat si kvalitní kryptoměnu a kupovat ji každý měsíc za předem vyhrazenou částku. Tento styl se mně osobně osvědčil, jelikož jsem imunní na cenu a tedy nejsem ovlivněn negativně ani pozitivně změnou ceny. Kryptoměny se zatím chovají cyklicky, to znamená, že jejich cena se pohybuje v několikaletých cyklech a růstové období nahrazuje klesající a naopak. Avšak mnou doporučený styl investování pokryje oboje období. Osobně si myslím, že pokud si chce člověk šetřit na důchod, je toto daleko vhodnější varianta, než státní dluhopisy, stavební spoření nebo penzijní fondy. Další velkou výhodou je, že vy jste pánem své investice a ne stát nebo jiná třetí strana.

V této práci jsem spojil informační technologie, statistiku a investiční rozhodování. Všechny tyto kategorie patří do mého oboru. Dosáhl jsem svého cíle a využil jsem systém pro podporu rozhodování pro investiční rozhodování. Vytvořil jsem kalkulačku, která může investorovi velmi dobře posloužit pro finanční rozhodnutí. Pro tvorbu této kalkulačky jsem využil znalostí Monte Carlo a Markowitzovy analýzy a také Value at Risk modelu. Přesvědčivě jsem popsal výhody a nevýhody Proof of work a Proof of stake a porovnal oba tyto konsenzy. Vše jsem poté úspěšně dosadil do rozhodovacího stromu.

8 Seznam použité literatury

1. *Blockchain: A Guide To Blockchain, The Technology Behind Bitcoin, Ethereum And Other Cryptocurrency (Volume 1)* [online]. 1. CreateSpace Independent Publishing Platform, 2018 [cit. 2020-11-16]. ISBN 198614240X. Dostupné z: https://books.google.cz/books?id=0oxODwAAQBAJ&printsec=frontcover&dq=blockchain&hl=cs&sa=X&ved=2ahUKEwic0-j91-vqAhWHiqQKHRKVAAYQ6AEwAXoECAAQAg#v=onepage&q=blockchain&f=false
2. LAURENCE, Tiana. *Introduction to Blockchain Technology* [online]. 1. van Haren Publishing, 2019 [cit. 2020-11-16]. ISBN 9789401804998. Dostupné z: https://books.google.cz/books?id=uD-4DwAAQBAJ&printsec=frontcover&dq=blockchain&hl=cs&sa=X&ved=2ahUKEwjpyPCu3evqAhWJSEEAHWQtBQI4ChDoATAAegQIAxAC#v=onepage&q=blockchain&f=false
3. *The Cryptography of Bitcoin* [online]. 2019 [cit. 2020-11-16]. Dostupné z: https://www.pluralsight.com/guides/the-cryptography-of-Bitcoin
4. Těžba Bitcoinů teoreticky: Jaký je princip těžení? *Master.cz* [online]. 2018 [cit. 2020-11-16]. Dostupné z: https://www.master.cz/blog/tezba-Bitcoinu-jake-jsou-principy-tezeni-teoreticky/
5. EVANS, Johan. What is a Node in a Blockchain Network? *Nodes.com* [online]. [cit. 2020-11-16]. Dostupné z: https://nodes.com/
6. Proof of Work nebo Proof of Stake – Jaké jsou typy těžby kryptoměn? Finex [online]. 2019 [cit. 2021-04-18]. Dostupné z: https://finex.cz/kryptomeny-proof-of-work-proof-of-stake/
7. FRANKENLFIELD, Jake. Proof of Stake (PoS). *Investopedia* [online]. 2019 [cit. 2020-11-16]. Dostupné z: https://www.investopedia.com/terms/p/proof-stake-pos.asp
8. *Proof-of-Work Vs Proof-of-Stake: A Comparative Analysis and an Approach to Blockchain Consensus Mechanism* [online]. Saúdská Arábie, 2018 [cit. 2020-11-16]. Dostupné z: https://repository.psau.edu.sa/jspui/retrieve/1bc090a5-2be2-4cdc-9ba2-a4c3db26e19e/Proof-of-Work%20Vs%20Proof-of-Stake%20A%20Comparative.pdf. International Journal for Research in Applied Science & Engineering Technology (IJRASET). Department of Computer Science, Prince Sattam Bin Abdalaziz University. Vedoucí práce Husneara Sheikh1 , Rahima Meer Azmathullah2 , Faiza Rizwan.
9. HU, Kun. Is Ethereum's Move to PoS Really an Upgrade? *News blockchain* [online]. 2020 [cit. 2020-11-16]. Dostupné z: https://blockchain.news/insight/is-ethereums-move-to-pos-really-an-upgrade

10. NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-peer Electronic Cash System* [online]. 2008 [cit. 2020-11-16]. Dostupné z: https://Bitcoin.org/Bitcoin.pdf. Akademické práce.
11. PayPal allows Bitcoin and crypto spending. *BBC news* [online]. 2020, 21.10.2020 [cit. 2020-11-16]. Dostupné z: https://www.bbc.com/news/technology-54630283
12. *CoinMarketCap: Today's Cryptocurrency Prices by Market Cap* [online]. 2020 [cit. 2020-11-16]. Dostupné z: https://coinmarketcap.com/
13. Explore Decentralized Applications. *State of the dapps* [online]. 2020, 2020 [cit. 2020-11-16]. Dostupné z: https://www.stateofthedapps.com/
14. BUTERIN, Vitalik. Ethereum Whitepaper. *Ethereum.org* [online]. 2013 [cit. 2020-11-16]. Dostupné z: https://ethereum.org/en/whitepaper/
15. SIEGEL, David. Understanding The DAO Attack. *Coindesk* [online]. 2016, 25.6.2016 [cit. 2020-11-16]. Dostupné z: https://www.coindesk.com/understanding-dao-hack-journalists
16. *E-money Chat: Ripple(XRP) cryptocurrency Analysis | How is it different from Bitcoin?* [online]. 2020 [cit. 2020-11-16]. Dostupné z: https://www.emchat.net/emchat/2017/12/29/what-is-ripple-how-is-it-different-from-Bitcoin
17. SCHWARTZ, David, Noah YOUNGS a Arthur BRITTO. *The Ripple Protocol Consensus Algorithm* [online]. 2018 [cit. 2020-11-16]. Dostupné z: https://ripple.com/files/ripple_consensus_whitepaper.pdf. Protocol.
18. Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal? *Howmuch.net* [online]. 2018 [cit. 2020-11-16]. Dostupné z: https://howmuch.net/articles/crypto-transaction-speeds-compared
19. *Xrpcharts: Validator Registry* [online]. 2020 [cit. 2020-11-16]. Dostupné z: https://xrpcharts.ripple.com/#/validators
20. HUXTABLE, Jhonny. Analysis of Chainlink — The Decentralised Oracle Network. *Medium.com* [online]. 2018 [cit. 2020-11-16]. Dostupné z: https://medium.com/@jonnyhuxtable/analysis-of-chainlink-the-decentralised-oracle-network-7c69bee2345f
21. ELLIS, Steve, Ari JUELS a Sergey NAZAROV. *ChainLink A Decentralized Oracle Network* [online]. 2017 [cit. 2020-11-16]. Dostupné z: https://link.smartcontract.com/whitepaper. Vědecký článek.
22. *BitcoinCash* [online]. 2020 [cit. 2020-11-16]. Dostupné z: https://www.Bitcoincash.org/
23. KIAYIAS, Aggelos, Alexander RUSSELL, Bernardo DAVID a Roman OLIYNYKOV. *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol* [online]. 2018 [cit. 2020-11-16]. Dostupné z: https://whitepaperdatabase.com/cardano-ada-whitepaper/. Vědecká práce.
24. Cardano's Strategy in Africa, Blockchain's Benefits for the Supply Chain Industry & EMURGO's Role in Driving Success. *Emurgo.io* [online]. 2019

[cit. 2020-11-16]. Dostupné z: https://emurgo.io/en/blog/cardano-strategy-africa
25. *ADApools.org: Cardano Szake pools* [online]. 2020 [cit. 2020-11-16]. Dostupné z: https://adapools.org/
26. MCFARLANE, Greg. CRYPTOCURRENCY STRATEGY & EDUCATION: What Is Litecoin, and How Does It Work? *Investopedia* [online]. 2019 [cit. 2020-11-16]. Dostupné z: https://www.investopedia.com/articles/investing/040515/what-litecoin-and-how-does-it-work.asp
27. *Coinmetrics: CM Network Data Charts* [online]. [cit. 2020-11-16]. Dostupné z: https://coinmetrics.io/charts/#assets=btc,bsv_left=TxCnt_zoom=1536792747738.6934,1568328747738.6934
28. *Finex.cz: Bitcoin Satoshi Vision (BSV) – Kurz, graf ceny, kde koupit* [online]. 2020 [cit. 2020-11-16]. Dostupné z: https://finex.cz/kryptomena/Bitcoin-sv/
29. *Bitinfocharts.com: Bitcoin Cash Avg. Transaction Fee historical chart* [online]. [cit. 2020-11-16]. Dostupné z: https://bitinfocharts.com/comparison/Bitcoin%20cash-transactionfees.html
30. EOSIO / Documentation: EOS.IO Technical White Paper v2. *Github.com* [online]. 2018 [cit. 2020-11-16]. Dostupné z: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
31. Reduce the annual rate of inflation to 1%. *EOS poll* [online]. 2019 [cit. 2020-11-16]. Dostupné z: https://eosauthority.com/polls_details?proposal=inflation_20190307
32. *DappRadar: Top EOS Dapps* [online]. 2020 [cit. 2020-11-16]. Dostupné z: https://dappradar.com/rankings/protocol/eos
33. Elon-musk-explains-teslas-Bitcoin-buy. *Foxbusiness.com* [online]. 2021 [cit. 2021-04-18]. Dostupné z: https://www.foxbusiness.com/markets/elon-musk-explains-teslas-Bitcoin-buy
34. TURBAN, Efraim, et al. Decision Support and Business Inteligence Systems. 8th edition. New Jersey : PEARSON, c2007. xxviii, 772 s. ISBN 0-13-158017-5.
35. Decision-trees-financial-analysis. Magnimetrics.com [online]. 2019 [cit. 2021-4-25]. Dostupné z: https://magnimetrics.com/decision-trees-financial-analysis/
36. Decision-making-tree. *Decision-making-solutions* [online]. [cit. 2021-4-25]. Dostupné z: https://www.decision-making-solutions.com/decision-making-tree.html

37. Jorion, Philippe (2006). Value at Risk: The New Benchmark for Managing Financial Risk (3rd ed.). McGraw-Hill. ISBN 978-0-07-146495-6.
38. POLOUČEK, Stanislav. Bankovnictví. V Praze: C.H. Beck, 2006. Beckovy ekonomické učebnice. ISBN 80-717-9462-7.
39. SVOBODA, M. Jak investovat: aneb anatomie burzovních lží. 3. aktualizované vydání. Brno: CP Books, 2005. 198 s. ISBN 978-80-2510-527-6.
40. MUSÍLEK, P. Trhy cenných papírů. Vyd. 1. Praha: Ekopress, 2002. 459 s. ISBN 80-86119-55-6
41. Kroese, D. P.; Brereton, T.; Taimre, T.; Botev, Z. I. (2014). "Why the Monte Carlo method is so important today". WIREs Comput Stat. 6 (6): 386–392. doi:10.1002/wics.1314. S2CID 18521840
42. N. Metropolis, “The Beginning of the Monte Carlo Method,” Los Alamos Science Special Issue, Vol. 15, 1987, pp. 125-130.
43. Decision-support-systems-sifting-data-for-better-business-decisions. *Www.cio.com* [online]. 2020 [cit. 2021-4-29]. Dostupné z: https://www.cio.com/article/3545813/decision-support-systems-sifting-data-for-better-business-decisions.html
44. Yilmaz, N.K.,Hazar, H.(2018). Determining the factors affecting investors’ decision-making process in cryptocurrency investments. PressAcademia Procedia (PAP), V.8, p.5-8.
45. Gottschlich, J., & Hinz, O. (2014). A decision support system for stock investment recommendations using collective wisdom. Decision Support Systems, 59, 52–62. doi:10.1016/j.dss.2013.10.005
46. ZHU, Chengzhang, Jianping YIN a Qian LI. A Stock Decision Support System based on DBNs. Changsha 410073, China, 2014. Akademická práce. College of Computer, National University of Defense Technology
47. FABIAN, František; KLUIBER, Zdeněk. Metoda Monte Carlo a možnosti jejího uplatnění. Praha: PROSPEKTRUM s.r.o., 1998. ISBN 80-7175-058-1. Kapitola 1.3, s. 152.
48. How Much Can You Earn From Staking Ada? Cardano.org [online]. [cit. 2021-4-30]. Dostupné z: https://cardano.org/calculator/?calculator=operator
49. ETH mining calculator. Cryptocompare [online]. [cit. 2021-4-30]. Dostupné z: https://www.cryptocompare.com/coins/eth/overview/
50. GeForce-GTX-1070. www.amazon.com [online]. [cit. 2021-4-30]. Dostupné z: https://www.amazon.com/GeForce-GTX-1070/s?k=GeForce+GTX+1070
51. Nvidia-GTX-1070-hashrate. *Miningchamp* [online]. [cit. 2021-4-30]. Dostupné z: https://miningchamp.com/gpus/123/Nvidia-GTX-1070-hashrate

52. Jaka-je-aktualni-cena-kwh-a-mwh-elektriny. Www.cenyenergie.cz [online]. [cit. 2021-4-30]. Dostupné z: https://www.cenyenergie.cz/jaka-je-aktualni-cena-kwh-a-mwh-elektriny/#/promo-ele-mini

9 Kopie zadání práce

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor:	**Bc. Richard Cibere**
Studium:	I1700358
Studijní program:	N6209 Systémové inženýrství a informatika
Studijní obor:	Informační management
Název diplomové práce:	**Podpora rozhodování při investování do kryptoměn**
Název diplomové práce AJ:	Decision support systems for investing in cryptocurrency

Cíl, metody, literatura, předpoklady:

Cílem práce je využití systému pro podporu rozhodování při investování do kryptoměn. V práci využiji tři nástroje analýzy pro tvorbu portfolia, či k měření rizika investice. V teoretické části se zaměřím na popsání deseti vybraných kryptoměn, popíší fungování blockchainu a porovnám systémy konsenzu Proof-of-Work a Proof-of-Stake. V praktické části budu prezentovat výsledky svého portfolia vyhodnocené skrze Value-at-Risk, Markowitzovy a Monte Carlo metody. V závěru práce vyhodnotím své výsledky a přidám doporučení pro investory.

1. Úvod
2. Cíl práce
3. Metodika zpracování
4. Literární rešerše
    1. Blockchain
    2. Mechanismy konsenzu
    3. Kryptoměny
    4. Systém pro podporu rozhodování
5. Praktická část
6. Závěry a doporučení
7. Seznam použité literatury
8. Přílohy

Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailin list at https://metzdowd.com.

Petro, Hrytsiuk {\& Babych, Tetyana {\& Bachyshyna, Larysa. (2019). Cryptocurrency portfolio optimization using Value-at-Risk measure. 10.2991/smtesm-19.2019.75.

Stavroyiannis, Stavros. (2018). Value-at-Risk and related measures for the Bitcoin. The Journal of Risk Finance. 19. 00-00. 10.1108/JRF-07-2017-0115.

ZORNIĆ, Nikola a Aleksandar MARKOVIĆ. Forecasting cryptocurrency investment return using time series and monte carlo simulation [online]. Belgrade, Serbia, 2018 [cit. 2020-11-12]. Dostupné z: http://archive.ceciis.foi.hr/app/public/conferences/2018/Proceedings/ICTEI/ICTEI-1.pdf. Akademická práce. University of Belgrade, Faculty of Organizational Sciences.

Garantující pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	doc. RNDr. Kamila Štekerová, Ph.D.
Oponent:	Ing. Ivan Soukal, Ph.D.
Datum zadání závěrečné práce:	15.10.2018

10 Přílohy

Excelový soubor – investiční kalkulačka