Univerzita Hradec Králové
Fakulta informatiky a managementu
KIT – Katedra informačních technologií

Kryptoměny a jejich potenciál

Bakalářská práce

Autor: Petr, Krtička
Studijní obor: Aplikovaná informatika

Vedoucí práce: prof. RNDr. Peter Mikulecký, Ph.D.

Hradec Králové Duben 2024

Prohlášení:

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

V Hradci Králové dne 2.5.2024 Petr Krtička

Poděkování:

Děkuji vedoucímu bakalářské práce prof. RNDr. Peteru Mikuleckému, Ph.D. za metodické vedení práce, profesionální přístup, vstřícnost a trpělivost.

Anotace

Cílem práce je prozkoumat problematiku spojenou s kryptoměnami, včetně jejich původu, použití, obtížnosti jejich získání a držení. Teoretická část se zaměřuje na obecný přehled kryptoměn, popis a jejich funkci. Praktická část se dělí na dva segmenty. První se zabývá popsáním založení nové kryptoměny. Druhý se zaobírá analýzou současného trhu a popisem vybraných kryptoměn s potenciálem. Zároveň je třeba poznamenat, že kryptoměny a technologie s nimi spojené se stále rychle rozvíjejí, což představuje dynamický a proměnlivý obor, v němž nové inovace a změny v regulačním prostředí mohou ovlivnit jak celkovou strukturu trhu, tak i hodnotu a uplatnění jednotlivých kryptoměn. Tato neustálá evoluce klade důraz na důkladné sledování aktuálních trendů a nejen teoretické, ale i praktické porozumění mechanismům, které ovlivňují trh s kryptoměnami.

Klíčová slova: kryptoměna, digitální měna, blockchain, Bitcoin

Annotation

Title: Cryptocurrencies and their potential

The aim of the thesis is to explore the issues associated with cryptocurrencies, including their origin, use, difficulty of obtaining and holding them. The theoretical part focuses on a general overview of cryptocurrencies, their description and their function. The practical part is divided into two segments. The first deals with describing the creation of a new cryptocurrency from scratch. The second deals with the analysis of the current market and the description of selected cryptocurrencies with potential. At the same time, it should be noted that cryptocurrencies and the technologies associated with them continue to evolve rapidly, representing a dynamic and changing industry in which new innovations and changes in the regulatory environment can affect both the overall market structure and the value and application of individual cryptocurrencies. This constant evolution emphasizes close monitoring of current trends and not only a theoretical but also a practical understanding of the mechanisms that influence the cryptocurrency market.

Keywords: cryptocurrency, digital currency, blockchain, Bitcoin

Úvod

V dnešní době jsou kryptoměny nejen populárním trendem, ale také jedním z nejvýraznějších faktorů, které pomalu přetvářejí globální finanční trh. V posledním desetiletí představují revoluční způsob, jak přistupovat k měnovým a finančním transakcím, a nabízejí tak nevídané možnosti v oblasti decentralizace, bezpečnosti a přístupnosti.

Kryptoměny, vedle nejznámějšího zástupce Bitcoinu, otevřely nové cesty pro finanční svobodu a inovace, umožňují rychlejší a levnější transakce napříč hranicemi a nabízejí alternativy tradičním, centralizovaným bankovním systémům. Jejich vliv na dnešní dobu se neomezuje pouze na finanční sektor, ale projevuje se také v oblasti práva, politiky a sociálních změn.

Právě tímto fenoménem se zabývá tato bakalářská práce jejíž hlavním cílem je přiblížit finanční a technologickou stránku kryptoměn a jejich aktuální trh.

První kapitola vymezuje rozdíly mezi FIAT měnami a kryptoměnami a popisuje evoluci peněz. Ve druhé kapitole jsou podrobně rozepsány technické aspekty, algoritmy zajišťující bezpečnost a blockchain. Třetí kapitola vysvětluje možnosti držení a spolehlivé uchovávání digitální měny. Těžbou a konsensuálními protokoly se zaobírá kapitola čtvrtá. Jakými způsoby lze obchodovat a jaké jsou stinné stránky obchodu s kryptoměnami popisují kapitoly pět a šest.

Kapitola sedmá přináší vhled do problematiky vzniku nové kryptoměny, který je chronologicky popsán. V kapitole osmé je vypracována analýza současného trhu, kde byl vytvořen přehled top 10 kryptoměn podle kapitalizace trhu.

Stojíme na prahu nové éry, která přináší mnoho otázek a nejasností. Kryptoměny, přestože již ovlivňují ekonomiku a společnost, jsou stále relativně novou technologií, která se neustále mění a vyvíjí. Tato neustálá evoluce vyžaduje hloubkový výzkum a analýzu, aby se pochopily její dlouhodobé dopady a potenciál.

1 Ekonomické aspekty kryptoměn

V posledních letech se kryptoměny staly nejen technologickým fenoménem, ale také důležitým ekonomickým prvkem, který může mít rozsáhlé dopady na globální finanční systém. Tato kapitola se věnuje ekonomickým aspektům kryptoměn, aby poskytla ucelený vhled do jejich rostoucí role ve světové ekonomice.

1.1 Evoluce peněz

Obrázek 1: Evoluce peněz
Zdroj: https://www.eatmy.news/2022/05/evolution-of-money-6-stages-of-money.html

Evoluce peněz je pozoruhodné téma, které bylo sledováno od jednoduchých směnných obchodů až po dnešní spletité finanční systémy. Historie peněz nebyla formována jen novými technologiemi, ale byla také ovlivněna společenskými, politickými a ekonomickými změnami, které se odehrály po celém světě. Tato část se věnuje fázím vývoje peněz, od směnných obchodů až po kryptoměny. Tímto pohledem na etapy je poskytnut hlubší vhled do toho, jak se stalo, že peníze jsou nyní nezbytnou součástí našeho života, a jak je jejich role stále měněna podle potřeb a možností našeho světa.

Následující chronologicky seřazený vývoj peněz je sestaven z těchto zdrojů: (studysmarter.co.uk 2023; Beattie 2022)

1.1.1 Výměnný Obchod

Směnný obchod, nebo také barterový obchod byl používán pro směnu zboží před vznikem peněz. Systém byl velice nepraktický, a to z důvodů, že byla potřebná nabídka i poptávka obou účastníků a zároveň byl problém určit jednotnou cenu za dané zboží. Zároveň některé předměty mohou být těžké nebo objemné což komplikovalo obchod.

1.1.2 Komoditní Peníze

Příchod komoditních peněz odstranil některé z nepraktických aspektů výměnného obchodu. Komoditní peníze byly fyzické objekty, které měly vnitřní hodnotu, jako jsou zrnka kakaa, sůl nebo drahé kovy. Například v Africe byly používány kovové tyčinky a v Číně kousky kovu ve tvaru nožů. Tyto objekty sloužily jako univerzální prostředek směny a uchování hodnoty, což značně zjednodušilo obchodní procesy.

1.1.3 Kovy a Mince

Mince vyrobené ze zlata, stříbra a dalších kovů se staly populárním způsobem platby, protože byly trvanlivé, rozdělitelné a měly univerzálně uznávanou hodnotu. První známé mince byly raženy ve starověké Lýdii, v dnešním Turecku, kolem 7. století př. n. l. Mincovnictví se postupně rozšířilo do celého starověkého světa a stalo se základem mnoha měnových systémů.

1.1.4 Papírové Peníze

Papírové peníze byly revolucí ve financování. Poprvé byly použity v Číně během Tangovské dynastie, když byly vládními úředníky vydány směnky, které se daly vyměnit za kovy. Tato metoda byla původně použita k usnadnění obchodu s velkým množstvím mincí na dlouhých vzdálenostech. V 11. století se papírové peníze staly všedním platebním prostředkem. Tento koncept se později rozšířil do střední Asie, Persie, a nakonec do Evropy.

1.1.5 Bankovnictví a Úvěr

Ve středověku se rozvinulo bankovnictví, zvláště ve městech jako Florencie, Janov a Benátky. Tyto banky poskytovaly účty, úvěry a měnily mince. Úvěrové systémy se staly klíčovými pro financování obchodu a průmyslu. S rozvojem šeků a směnek se transakce staly jednoduššími a bezpečnějšími. Toto období položilo základy pro moderní finanční systém.

1.1.6 Centrální Banky a Měnová Politika

Centrální banky, jako například Bank of England (založená v roce 1694), přinesly nový rozměr finanční regulaci. Tyto instituce začaly regulovat měnovou nabídku a úrokové sazby, aby ovlivnily ekonomiku. Centrální banky začaly vydávat standardizované bankovky, které se staly zákonným platidlem.

1.1.7 Elektronické Peníze a Kreditní Karty

V 20. století přinesly technologické inovace nové formy peněz. Elektronické bankovnictví a kreditní karty umožnily rychlé a snadné transakce bez potřeby fyzických peněz. První kreditní karta byla vydána v roce 1950 společností Diners Club, a postupně se staly běžným platebním prostředkem po celém světě. Tyto technologie usnadnily globální obchod a e-commerce (elektronické obchodování).

1.1.8 Kryptoměny

Kryptoměny představují nejnovější etapu v evoluci peněz. Bitcoin, vynalezený v roce 2008, zahájil novou éru decentralizovaných digitálních měn. Oproti tradičním měnám nejsou kryptoměny regulovány centrální autoritou, ale spoléhají na kryptografii a decentralizované sítě. Ethereum a další kryptoměny poskytly nové perspektivy v podobě funkcí, jako jsou chytré smlouvy (Smart Contract). Tato nová technologie přináší možnosti i výzvy, včetně otázek regulace, bezpečnosti a volatility.

1.2 Fiat měny versus kryptoměny

1.2.1 Fiat měny

Fiat měny jsou označovány jako tradiční formy peněz, které jsou vydávány vládami a jsou uznávány jako zákonné platidlo v daných zemích. Tyto měny postrádají vlastní vnitřní hodnotu (například nejsou podloženy zlatem) a jejich kvalita je odvozena od důvěry, kterou má ve vládu, jež tuto měnu vydává. Mezi příklady nejznámějších tradičních měn spadají americký dolar (USD), euro (EUR) a britská libra (GBP). (Stroukal a Skalický 2021)

Vydávání a uznávání těchto měn spočívá v rukou centrálních bank a vlád. Tyto instituce přisuzují fiat měnám hodnotu tím, že je označují jako oficiální platidlo, jež musí být akceptováno jako prostředek směny a zákonná platba v ekonomice. Lidé jsou v tomto ohledu zavázáni přijímat fiat měny jako platbu za zboží a služby na základě předpisů a pravidel stanovených vládou. (Chen 2023)

Jejich hodnota je zcela závislá na důvěře a dohodě v rámci ekonomických účastníků. Důvěra v stabilitu ekonomiky a schopnost vlád udržet inflaci na nízké úrovni je zásadní pro stabilitu fiat měn. Pokud by nedostatek důvěry nastal, mohlo by dojít k poklesu hodnoty měn. (Chen 2023)

Měnová politika, která zahrnuje regulaci množství peněz v oběhu a nastavování úrokových sazeb, je ovlivňována centrálními bankami. Tímto způsobem mohou ekonomické podmínky ovlivňovat a reagovat na různé krizové situace.

Fiat měny mohou také podléhat změnám hodnoty v důsledku inflace (zvyšování cen) nebo deflace (snížení cen). Centrální banky se snaží udržet mírnou inflaci, která podporuje ekonomický růst, zatímco extrémně vysoká inflace může ohrozit stabilitu měny. (Stroukal a Skalický 2021)

1.2.2 Kryptoměny

Kryptoměna představuje formu měny, která existuje v digitálním prostoru a využívá k zabezpečení transakcí principy kryptografie. Nemá centrální vydávající nebo regulační autoritu, místo toho využívá decentralizovaný systém k záznamu transakcí a emisi nových jednotek. (kaspersky.com 2023a)

Kryptoměny jsou digitální platební systém uložený v digitálních peněženkách, který se neopírá o banky pro ověření transakcí. Jedná se o systém peer-to-peer (klient-klient), který umožňuje každému posílat a přijímat platby kdekoliv. Tyto platby existují pouze jako digitální záznamy v online databázi popisující konkrétní transakce . (Stroukal a Skalický 2021)

Jsou pojmenovány podle použití šifrování pro ověřování transakcí, což zajišťuje bezpečnost. První digitální měnou byl Bitcoin, který byl založen v roce 2009 a řadí se mezi nejznámější. Zájem o kryptoměny často vychází z obchodování za účelem zisku. (Stroukal a Skalický 2021)

Kryptoměny fungují na distribuované veřejné účetní knize zvané blockchain, což je záznam všech transakcí aktualizovaný a držený uživateli kryptoměn. Jednotky kryptoměn jsou vytvářeny procesem těžby, který zahrnuje použití výpočetní síly počítačů k řešení složitých matematických problémů, které generují nové mince. (kaspersky.com 2023a)

Digitální měny mohou být zakoupeny na kryptoměnových burzách nebo směnárnách a jsou uloženy v digitálních peněženkách, které uchovávají privátní klíče pro jejich zabezpečení.

Aspekt	Kryptoměny	Fiat měny
Vydavatel	Decentralizovaný. (např. Bitcoin vytváří sítě peer-to-peer uživatelů)	Centralizovaný. (např. státní vláda nebo centrální banka)
Fyzická forma	Ne. (existuje pouze digitálně)	Ano. (bankovky a mince)
Úroveň kontroly	Decentralizovaná, omezená na protokoly blockchainu.	Centralizovaná, řízená vládou nebo centrální bankou.
Bezpečnost a ochrana	Kryptografické metody a blockchain.	Závisí na regulačních úřadech a vládních opatřeních.
Přístup a použití	Otevřený pro všechny s přístupem k internetu.	Obvykle vyžaduje bankovní účet nebo jiné finanční služby.
Transakční rychlost	Může být rychlé nebo pomalé v závislosti na kryptoměně.	Může být rychlé nebo pomalé v závislosti na platebním systému.
Transakční poplatky	Obvykle nižší než u fiat měn.	Může být vysoký v závislosti na finanční službě.
Anonymita	Často vyšší než u fiat měn. (ale stále existují určitá rizika)	Obvykle nižší, jelikož transakce jsou sledovány finančními institucemi.
Uznání	Přijímáno některými obchodníky a v některých regionech.	Uznáváno na celém světě jako oficiální měna daného státu.
Cena	Může být velmi volatilní.	Obvykle stabilnější, ale může být postižena inflací.

Tabulka 1: Hlavní rozdíly mezi kryptoměnami a fiat měnami

Zdroj: Tabulka zpracována autorem

Dalo by se říct, že kryptoměny představují nový přístup k měně, který se liší od tradičních měn v mnoha zásadních aspektech, které jsou vypsány v tabulce výše. Jejich vývoj a debaty o přijetí stále probíhají a budoucí role kryptoměn v globálním finančním systému zůstává otevřenou otázkou.

1.3 Kryptoměny jako investice

V současné době jsou kryptoměny brány jako jedna z alternativních investičních možností, která přitahuje pozornost jak individuálních, tak institucionálních investorů. Jejich popularita stoupla, zejména díky potenciálním vysokým výnosům, ale také v důsledku rostoucího zájmu o decentralizované financování.

Ovšem s těmito příležitostmi přicházejí i rizika. Volatilita kryptoměn může být značná, a investice do nich je často považována za spekulativní. Nejistota ohledně regulací a možná budoucí legislativní omezení také přidávají další vrstvu nejistoty.

Někteří investoři využívají kryptoměny jako součást diverzifikovaného portfolia, kde mohou sloužit jako potenciální ochrana před inflací nebo jako nezávislý investiční nástroj, který nemusí nutně sledovat tradiční trhy.

Institucionální investoři, jako jsou investiční fondy a penzijní fondy, začínají věnovat pozornost kryptoměnám, ačkoli jejich přijetí může být stále omezeno z důvodu regulací a nedostatku transparentnosti na některých trzích.

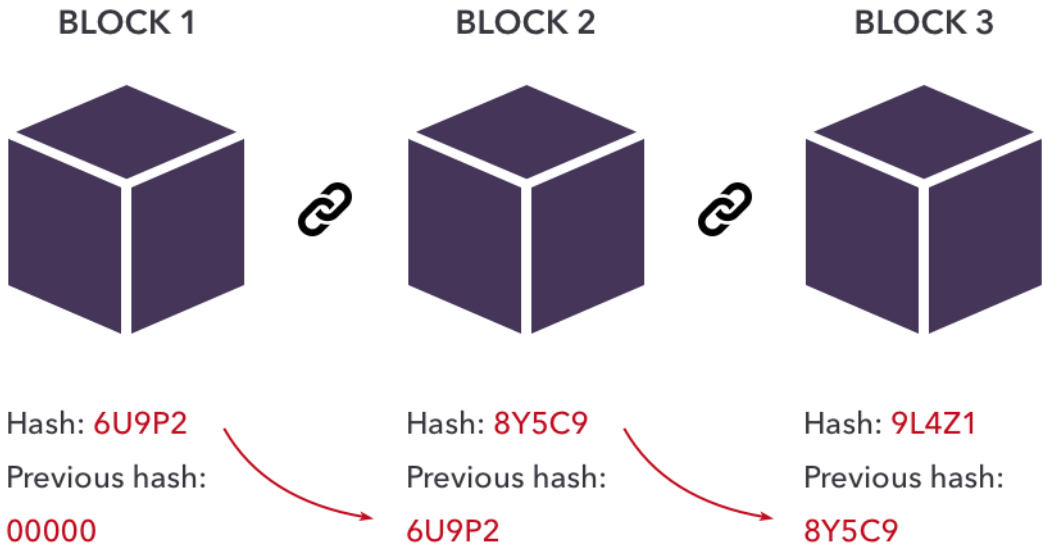
Lze tvrdit, že kryptoměny jsou stále více brány jako legitimní investiční příležitost, ale přitom je nutné mít na paměti jedinečná rizika a nejistoty spojené s tímto novým a neustále se vyvíjejícím trhem.

2 Základní technologie a principy

Tato kapitola poskytuje základní přehled o technologických aspektech kryptoměn. Vymezuje klíčové koncepty jako je blockchain, kryptografie a další pojmy. Dále vysvětluje metody, které zajišťují bezpečnost, transparentnost a integritu dat v kryptoměnových sítích.

2.1 Blockchain

Blockchain je speciální typ databáze, která se nazývá decentralizovaná digitální účetní kniha, a je spravována několika počítači rozmístěnými po celém světě. Data na blockchainu jsou uspořádána do chronologicky seřazených bloků, které jsou zabezpečeny kryptografií. Je to nezměnitelný systém, který zaznamenává informace o transakcích a dalších digitálních datech. (Hayes 2023a)



Obrázek 2: Blockchain
Zdroj: https://www.velotio.com/engineering-blog/introduction-to-blockchain-and-how-bitcoin-works

Decentralizace blockchainu znamená, že řízení a rozhodovací pravomoci sítě jsou rozděleny mezi její uživatele a není zde žádný ústřední orgán nebo zprostředkovatel. Díky tomu je síť bezpečnější a odolnější vůči útokům. (Hayes 2023a)

Fungování blockchainu je založeno na procesu ověřování transakcí, který je prováděn souborem pravidel nazývaných mechanismus konsenzu. Díky

kryptografickým metodám, jako je hashování a asymetrická kryptografie, jsou data na blockchainu chráněna proti manipulaci a zajišťují důvěryhodnost transakcí. (Hayes 2023a)

Existují různé typy blockchainových sítí, mezi které se řadí veřejné, soukromé a konsorciální blockchainy, které mají různé úrovně transparentnosti a přístupu. (mckinsey.com 2022)

Blockchainová technologie má široké využití, včetně kryptoměn, digitálních identit, řízení dodavatelského řetězce a chytrých kontraktů. Má potenciál revolučně změnit mnoho odvětví díky svým vlastnostem jako decentralizace, transparentnost, bezpečnost a nižší náklady na transakce. (Hayes 2023a)

Vlastnost	Blockchain	Databáze
Jak se ukládají data	Data jsou rozptýlena po síti.	Data jsou na jednom místě.
Kdo má přístup	Obvykle kdokoli, kdo je součástí sítě.	Přístup mají jen lidé s oprávněním.
Možnost změn	Data nelze měnit.	Data lze měnit nebo mazat.
Ochrana dat	Používají se šifry pro ochranu.	Ochrana se řídí pravidly a právy přístupu.
Viditelnost transakcí	Všechny transakce jsou veřejné.	Transakce jsou skryté, vidí je jen pár lidí.
Rychlost zpracování	Může být pomalejší kvůli kontrole mnoha uživatelů.	Je rychlé.
Jak se data uchovávají	Data jsou kopírována u všech uživatelů sítě.	Data jsou buď na jednom místě, nebo rozdělena.
Proč to používat	Dobré pro bezpečné a stálé záznamy.	Dobré pro běžné úpravy a různé účely.

Tabulka 2: Rozdíly mezi Blockchainem a Databází
Zdroj: Tabulka zpracována autorem

2.2 Bezpečnost

Bezpečnost blockchainu zahrnuje vrozené vlastnosti technologie, jako je kryptografie, decentralizace a konsensus, které zajišťují důvěru v transakce. Bezpečnost se liší v závislosti na typu blockchainu, je-li veřejný nebo soukromý, a zda je s povolením nebo bez povolení.

Veřejné blockchainy umožňují každému se připojit a ověřovat transakce, zatímco soukromé blockchainy jsou omezeny pouze na známé organizace. Povolené blockchainy vyžadují potvrzení identity, zatímco nepovolené blockchainy žádné omezení nemají. (IBM 2023)

Navzdory odolnému záznamu transakcí jsou blockchainové sítě stále zranitelné vůči kybernetickým útokům a podvodům. Příklady zahrnují zneužití kódu, krádež klíčů a hacknutí počítačů zaměstnanců. Podvodníci používají například phishing a útoky s 51 % k manipulaci s blockchainovou infrastrukturou.
Pro zvýšení bezpečnosti blockchainu by měly podniky implementovat tradiční a technologicky specifická opatření, včetně správy identity a přístupu, správy klíčů, ochrany dat, zabezpečené komunikace, bezpečnosti smart kontraktů a ověřování transakcí. (IBM 2023)

2.3 Kryptografie

Kryptografie používá algoritmy a klíče k transformaci vstupu (plaintextu) na zašifrovaný výstup (ciphertext). Symetrická kryptografie aplikuje stejný klíč pro šifrování i dešifrování, zatímco asymetrická kryptografie využívá odlišné klíče pro obě činnosti. Text také zdůrazňuje důležitost používání již ověřených a bezpečných kryptografických algoritmů a klíčů a varuje před návrhem vlastních kryptosystémů, které mohou být zranitelné. (kaspersky.com 2023b)

Symetrická kryptografie je rychlá a vhodná pro šifrování velkého množství dat, zatímco asymetrická kryptografie je pomalejší a používá se pro šifrování menších částí dat. Může řešit problémy týkající se důvěrnosti, integrity a dostupnosti dat. (kaspersky.com 2023b)

Důležitým aspektem je vyhýbat se vlastní tvorbě kryptosystému a upřednostnit ověřené a bezpečné algoritmy. Klíče by měly být drženy tajně a v ochraně před neoprávněným přístupem. Nejvhodnějším a doporučeným postupem je použití

hardware security modulu (HSM) pro bezpečné uchování klíčů. Dále je důležité dodržovat pravidla a standardy pro algoritmy a klíče. AES s klíči 128, 192 nebo 256 bitů je standardem pro symetrickou kryptografii, zatímco RSA a ECC s klíči minimálně 2048 bitů jsou standardem pro asymetrickou kryptografii. (kaspersky.com 2023b)

2.4 Hash

Podle Frankenfielda se hashování obvykle nepovažuje za formu šifrování (enkryptace), protože šifrování obecně zahrnuje možnost dešifrování (dekryptace) zpět na původní data pomocí klíče. Hashovací funkce transformuje vstupní data do pevně dané délky, z níž nelze původní data obnovit. (Frankenfield 2023b)

Proces hashování v bodech:

- **Konverze do binárního pole:** vstupní data jsou převedena na binární reprezentaci.
- **Inicializace konstant:** jsou nastaveny počáteční hodnoty pro hashovací algoritmus.
- **Spojení dat do bitů:** vstupní data jsou zpracována spolu s paddingem (doplněním) tak, aby jejich délka odpovídala požadavkům algoritmu.
- **Komprese dat:** proces, kdy se vstupní data zmenšují pomocí hashovací funkce.
- **Úprava finálních dat:** výsledný hash je dokončen z finálního stavu kompresní funkce.

Vlastnosti hashovacích funkcí:

- **Bez kolizí:** je velmi nepravděpodobné, že dva různé vstupy vyprodukují stejný hash výstup.
- **Odolnost proti reverznímu inženýrství:** hashovací funkce je navržena tak, aby nebylo prakticky možné získat původní data z hash výstupu.
- **Puzzle-friendly:** tato vlastnost znamená, že je náročné najít vstup, který by vyprodukoval předem určený hash výstup, což je důležité v kontextu kryptografických protokolů, jako je důkaz práce v blockchainových technologiích.

2.5 Hashovací Algoritmy

2.5.1 SHA-256 (ASIC)

Plným názvem „Secure Hash Algorithm 256-bit“ což znamená „Bezpečný hashovací algoritmus s 256 bity“. Byl vyvinut americkou vládní agenturou pro standardizaci a poprvé zveřejněn v roce 2001.

Tento algoritmus přeměňuje jakákoliv data (například text nebo obrázek) na krátký kód pevné délky 256 bitů, což je řetězec 32 bajtů. Tento kód, označovaný jako hash, je jedinečný pro každá původní data.

Hlavní přednosti SHA-256 jsou:

- **Bezpečnost proti kolizím:** je velmi obtížné najít dva různé soubory dat, které by generovaly stejný hash kód.
- **Nemožnost zpětného zjištění:** z hash kódu nelze vyvodit, jaká data byla původně zahashována.
- **Odolnost proti manipulaci:** je téměř nemožné vytvořit data, která by úmyslně generovala specifický hash kód.

Díky těmto vlastnostem je SHA-256 velmi užitečný pro zabezpečení online komunikace, ověřování pravosti digitálních souborů a v kryptoměnách, jako je Bitcoin, kde pomáhá ověřovat transakce. (Griškėnas 2023)

2.5.2 Ethash (GPU)

Ethash je kryptografický hashovací algoritmus speciálně navržený pro použití v Ethereum, což je populární platforma pro vytváření decentralizovaných aplikací a smart kontraktů (inteligentní smlouvy). Ethash je primárně zaměřen na podporu těžby kryptoměny ether pomocí procesu známého jako proof-of-work (důkaz práce), který je klíčový pro udržení bezpečnosti a správnosti Ethereum blockchainu. (ethereum.org 2023)

Ethash je navržen tak, aby byl odolný vůči použití specializovaného hardwaru, jako jsou ASIC (Application-Specific Integrated Circuits – specializované integrované obvody) procesory, které mohou dominovat těžbě a centralizovat sílu

v síti. Místo toho Ethash optimalizuje těžbu pro grafické procesory (GPU), které jsou široce dostupné a mají méně tendence k centralizaci. (ethereum.org 2023)

Jak Ethash funguje:

- **Datově náročný:** Ethash vyžaduje, aby část dat byla uložena v paměti GPU. Tento přístup ztěžuje použití ASIC, které mají obvykle omezenější paměťové zdroje.
- **Generování a ověřování:** algoritmus vytváří velký datový soubor, který roste v pravidelných intervalech a je základem pro těžební proces. Těžaři generují a ověřují nové bloky, přičemž musí pracovat s daty v rámci tohoto souboru.
- **Důkaz práce:** pro přidání bloku do blockchainu musí těžaři najít řešení složitého matematického problému, což vyžaduje výpočetní a energetický výkon. Výsledkem je hash, který musí splňovat určitá kritéria (například být menší než určitá hodnota).

Ethash tedy hraje zásadní roli v udržení decentralizace a bezpečnosti Ethereum tím, že umožňuje širší účast v těžebním procesu a brání dominantnímu vlivu jednotlivých těžařů nebo skupin.

2.5.3 Scrypt (ASIC)

Scrypt je další kryptografický hashovací algoritmus, který byl speciálně navržen tak, aby byl odolný vůči hardwarové specializaci, což znamená, že se snaží bránit dominanci specializovaných zařízení jako jsou ASIC v těžbě kryptoměn. Scrypt byl navržen Colinem Percivalem a poprvé představen v roce 2009 jako část jeho softwarového projektu Tarsnap, což je služba zálohování určená pro operační systémy Unix. (Rhodes 2020)

Klíčové vlastnosti Scrypt:

- **Náročný na paměť:** Scrypt je navržen tak, aby intenzivně využíval paměť, což ztěžuje implementaci těžby na ASIC zařízeních, která jsou optimalizována hlavně pro výkon, ale mají omezené paměťové kapacity. Tím pádem je těžba

více přístupná pro běžné uživatele s grafickými kartami (GPU) nebo dokonce s běžnými počítačovými procesory (CPU).

- **Široké použití v kryptoměnách:** kromě svého původního použití v Tarsnapu, se Scrypt stal populárním ve světě kryptoměn. Je používán jako základní hashovací algoritmus pro několik kryptoměn, včetně Litecoinu a Dogecoinu, které byly mezi prvními, kdo ho adaptovaly pro odolnost proti ASIC.
- **Generování a ověřování:** Scrypt, stejně jako jiné hashovací algoritmy, generuje hash výstup z libovolných vstupních dat. V kontextu kryptoměn se tento proces využívá pro potvrzování a ověřování transakcí a zároveň pro přidání nových bloků do blockchainu.

Scrypt se stal základem pro několik známých projektů, jako je Litecoin (LTC) a Dogecoin (DOGE). Tyto sítě používají Scrypt k zabezpečení transakcí a těžby. Nicméně, Scrypt nebyl tak úspěšný jak se původně očekávalo v odolávání ASIC těžbě a existuje několik ASIC těžebních zařízení dostupných pro těžbu Scrypt kryptoměn.(Rhodes 2020)

Za posledních pár let se Scrypt těžba stala přístupnější pro ASICy a stává se běžným prvkem v těžbě kryptoměn jako Litecoin a Dogecoin. Kromě toho byly některé blockchainové projekty, které dříve používaly Scrypt, nuceny přejít na jiné algoritmy nebo jiné mechanismy konsensu.(Rhodes 2020)

2.5.4 Cryptonight (CPU)

CryptoNight je kryptografický hashovací algoritmus, který byl navržen tak, aby byl odolný vůči těžbě pomocí specializovaných ASIC zařízení. Tento algoritmus je známý svým použitím v kryptoměně Monero, která je zaměřena na zvýšení anonymity a soukromí svých uživatelů. CryptoNight byl vyvinut jako součást protokolu CryptoNote a je optimalizován pro CPU a GPU, což umožňuje rovnoměrnější distribuci těžební síly mezi jednotlivými uživateli a tím přispívá k decentralizaci sítě. (Rhodes 2023)

Klíčové vlastnosti CryptoNight:

- **Náročný na paměť:** podobně jako Scrypt, i CryptoNight vyžaduje, aby během těžby byla využívána velká část operační paměti, což komplikuje výrobu efektivních ASIC čipů pro tento algoritmus. Těžba je tak dostupnější pro obyčejné uživatele s dostupným hardwarovým vybavením.
- **Zaměření na soukromí:** algoritmus je designován tak, aby podporoval vlastnosti kryptoměny Monero, které zahrnují skryté adresy a jednorázové klíče pro zajištění transakčního soukromí.

Použití v mnoha kryptoměnách: kromě Monera je CryptoNight používán i v dalších kryptoměnách zaměřených na soukromí, jako jsou Bytecoin, Aeon a další.

CryptoNight přispívá nejen k zabezpečení a integritě sítě, ale také podporuje principy rovného přístupu a soukromí uživatelů, což je v souladu s filosofií mnoha kryptoměn zaměřených na ochranu osobních údajů.

2.5.5 Equihash (GPU)

Equihash je kryptografický hashovací algoritmus, který je známý pro svou implementaci v několika kryptoměnách, včetně Zcash, což je měna zaměřená na soukromí. Equihash byl navržen tak, aby byl odolný proti těžbě pomocí specializovaných ASIC zařízení, podporoval decentralizaci těžebních operací a umožňoval efektivnější těžbu na běžném hardwaru, jako jsou grafické karty (GPU). (gcharang 2023)

Klíčové vlastnosti Equihash:

- **Asymetrická náročnost na paměť:** Equihash je zvláště náročný na paměť při generování proof-of-work, ale méně náročný při ověřování. Tato vlastnost znesnadňuje efektivní implementaci těžby na ASIC zařízeních, která mají typicky omezenou paměť ve srovnání s GPU.
- **Nastavitelnost:** Equihash umožňuje nastavit parametry, které určují paměťovou a výpočetní náročnost algoritmu. Tím mohou vývojáři kryptoměn přizpůsobit obtížnost algoritmu tak, aby byla zajištěna optimální rovnováha mezi dostupností pro běžné uživatele a odolností proti centralizaci těžby.

- **Široké využití:** kromě Zcash, který byl první kryptoměnou implementující tento algoritmus, je Equihash používán i v dalších kryptoměnách zaměřených na decentralizaci těžby, jako jsou Horizen a Bitcoin Gold.

Equihash tedy přináší výhody v podobě zvýšené odolnosti proti specializovaným těžebním zařízením a podporuje decentralizaci těžebních operací. Tento přístup je v souladu s původním záměrem mnoha kryptoměn, které hledají způsoby, jak zůstat přístupné širokému spektru uživatelů a zároveň zajistit bezpečnost a integritu svých sítí.

2.6 P2P síť

P2P síť, nebo peer-to-peer síť, je decentralizovaná síť, ve které každý uzel (peer) funguje zároveň jako klient i server. To znamená, že každý uzel může sdílet a přijímat data s ostatními uzly. Toto je odlišné od tradičního klient-server modelu, kde jsou data centralizovaně uložena na serverech a jsou přenášena klientům na vyžádání. (Hayes 2024)

Podle (Hayes 2024) P2P sítě mají několik klíčových vlastností:

- **Decentralizace:** P2P sítě nejsou závislé na jednom centrálním bodu, což znamená, že jsou odolné vůči selhání jednoho bodu. Pokud jeden uzel selže, ostatní uzly v síti mohou pokračovat v práci bez přerušení.
- **Sdílení zdrojů:** každý uzel v síti sdílí své zdroje, jako je úložiště dat, výpočetní kapacita a šířka pásma. Toto umožňuje sítím P2P škálovat se zvyšujícím se počtem uzlů a zvyšuje celkovou efektivitu sítě.
- **Anonymita:** protože jsou data distribuována mezi mnoho uzlů, může být obtížné určit, odkud pocházejí data nebo kam jsou doručena.
- **Otevřenost:** většina P2P sítí je otevřených, což znamená, že kdokoli s přístupem k internetu se může připojit a stát se uzlem.

V kontextu kryptoměn se P2P sítě používají pro distribuci a udržování blockchainu. Například v síti Bitcoinu, každý „peer“ (také známý jako těžař) udržuje kopii celého blockchainu a potvrzuje nové transakce tím, že je do něj přidává. Toto

je základem decentralizované a důvěryhodné povahy kryptoměn, protože transakce nemohou být změněny ani cenzurovány jedním centrálním subjektem.

P2P sítě také umožňují přímé transakce mezi uživateli kryptoměny bez potřeby prostředníka, jako je banka nebo platební brána. To zvyšuje rychlost a snižuje náklady na transakce, zvláště pro mezinárodní platby.

2.7 Uzly

„Node“, neboli uzel, je základní jednotka v jakékoliv síti, která může přijímat, vytvářet, ukládat nebo odesílat data. V kontextu kryptoměn a blockchainu je uzel počítač spojený s blockchainovou sítí, který provádí různé úkoly, jako je ověřování transakcí a udržování kopie celého blockchainu.

Podle Ledgera (2023) existují tři hlavní typy uzlů v blockchainových sítích:

- **Plné uzly (Full Nodes):** tyto uzly stahují celý blockchain a ověřují všechna pravidla nastavená v dané kryptoměně. To zahrnuje ověřování platnosti každé transakce a každého bloku přidaného do blockchainu. Plné uzly tedy pomáhají udržovat bezpečnost a transparentnost sítě.
- **Těžařské uzly (Mining Nodes):** tyto uzly provádějí těžební proces v kryptoměnách, které používají proof-of-work konsensuální mechanismus, jako je Bitcoin. Těžařské uzly řeší složité matematické problémy, aby přidaly nové bloky do blockchainu a byly za to odměněny nově vytvořenými mincemi a transakčními poplatky.
- **Lehké uzly (Light Nodes):** tyto uzly stahují pouze část blockchainu, což jim umožňuje provádět transakce bez nutnosti stahování celého blockchainu. Jsou ideální pro zařízení s omezeným úložným prostorem, jako jsou mobilní telefony.

Uzly jsou zásadní pro fungování decentralizovaných sítí kryptoměn. Bez nich by nebylo možné provádět a ověřovat transakce, ani udržovat a aktualizovat blockchain.

2.8 Smart Contract

Smart kontrakty, nebo chytré kontrakty, jsou samo-vykonávací kontrakty s podmínkami dohody přímo napsanými do kódu. Jsou uloženy na blockchainu a automaticky se vykonávají, když jsou splněny dané podmínky. Toto odstraňuje potřebu důvěry a potřebu třetí strany při uskutečňování dohod. (Investopedia team 2024b)

Smart kontrakty mohou mít širokou škálu použití, včetně finančních služeb, pojišťovnictví, dodavatelských řetězců, voleb a mnoho dalšího. Například smart kontrakt může automaticky uvolnit platbu, když dodavatel splní jeho úkol, nebo může automaticky zaplatit pojistné plnění, když dojde k určité události.

Smart kontrakty jsou nedílnou součástí kryptoměn, zvláště těch, které jsou postaveny na Ethereum blockchainu. Ethereum bylo navrženo speciálně pro vytváření a provádění smart kontraktů. Každý smart kontrakt na Ethereum je transparentní a neměnný, což znamená, že jakmile je jednou na blockchainu, nemůže být změněn nebo smazán.

To umožňuje vytvoření decentralizovaných aplikací (DApps), které jsou řízeny smart kontrakty místo centrální autority. Příkladem tohoto využití jsou decentralizované finance (DeFi), kde smart kontrakty umožňují půjčování a výměnu tokenů bez potřeby banky nebo jiné finanční instituce. (Investopedia team 2024b)

Kromě Ethereum, existují i další blockchainové platformy, které podporují smart kontrakty, jako jsou Cardano, Polkadot a Solana.

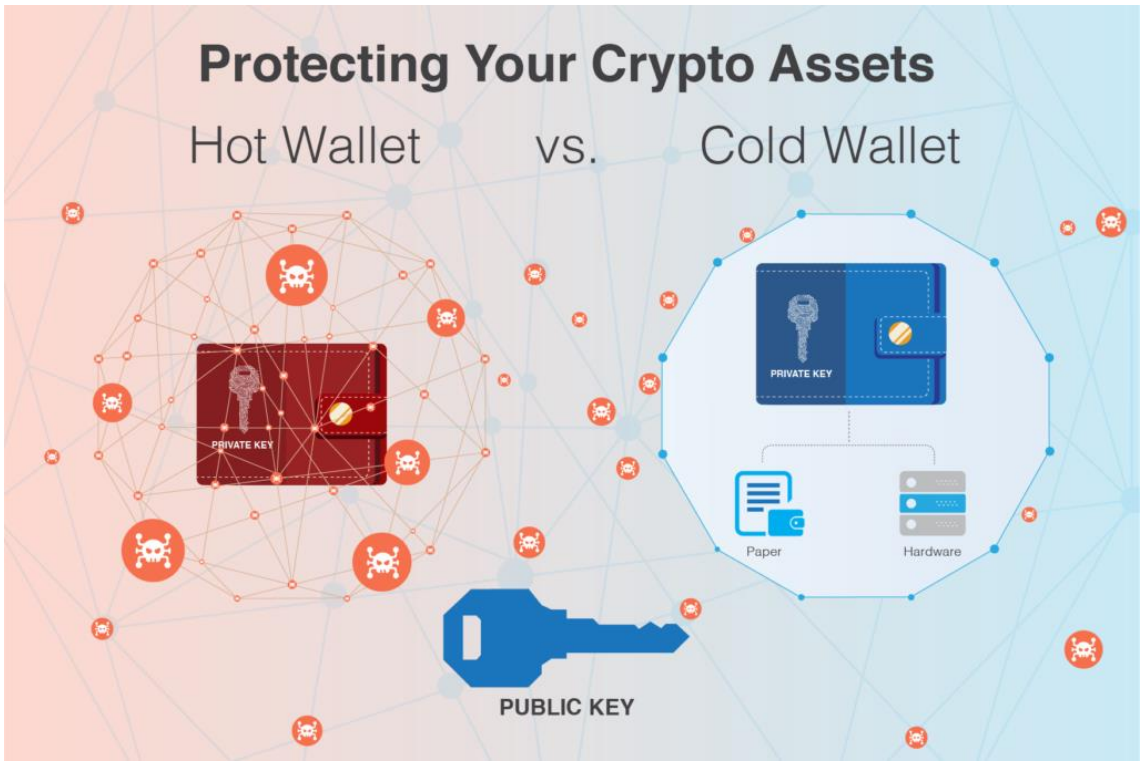
2.9 NFT

Non-fungible tokens (NFT) jsou unikátní digitální aktiva, která se vyznačují svou jedinečností a nenahraditelností, odlišují se tak od tradičních kryptoměn. Každý NFT je tokenizován pomocí blockchainu a má svůj vlastní jedinečný identifikační kód a metadata, což zajišťuje, že každý token je odlišný a má svou vlastní specifickou hodnotu. S těmito tokeny může být obchodováno na trhu, kde je možné je vyměňovat za peníze, kryptoměny nebo jiné NFT. Hodnota každého NFT je určena trhem a naceněním majitelů, což znamená, že se může výrazně lišit v závislosti na poptávce a vzácnosti. (Sharma 2023)

Historie NFT sahá až do roku 2014, kdy byly tyto tokeny poprvé vytvořeny. Avšak, jejich skutečná popularita a rozšířené využití nastalo až v posledních letech, kdy se staly centrem zájmu ve světě digitálního umění, sběratelství a investic. Tento vzestup popularity je způsoben schopností NFT tokenizovat a prodávat digitální obsah, jako jsou umělecká díla, hudba, video a další formy digitálního obsahu, což umožňuje tvůrcům získat přímé příjmy z prodeje svých děl. (Sharma 2023)

3 Peněženky

Krypto peněženky jsou jedním ze základních stavebních kamenů kryptoměn. Představují digitální rozhraní, ve kterém uživatelé mohou uchovávat, odesílat a přijímat kryptoměny. Stejně jako tradiční peněženka umožňuje nosit hotovost, kreditní karty nebo osobní doklady, krypto peněženka uchovává soukromé klíče, které jsou digitálním podpisem transakcí. Bez těchto klíčů není možné kryptoměnu ovládat, a proto je jejich bezpečné uchování klíčové. Krypto peněženky mohou mít různé formy, od online platforem po fyzická zařízení, a každá z nich přináší vlastní soubor výhod a rizik. Ve světě, kde se digitální měna stává více přijímanou, je pochopení fungování krypto peněženek nezbytné.



Obrázek 3: Hot Wallet vs. Cold Wallet
https://www.alza.cz/hardwarove-penezenky-pro-kryptomeny#co-je-hardwarova-penezenka

3.1 Online Peněženky (Hot Wallets):

Online peněženky, známé také jako „hot wallets“, jsou typem krypto peněženek, které jsou neustále připojeny k internetu. Toto připojení je důvodem, proč se jim říká „horké“ - jsou snadno přístupné, ale zároveň i více náchylné k potenciálním bezpečnostním rizikům.

3.1.1 Webové Peněženky

Typ peněženek, které jsou přístupné přes internetový prohlížeč. Uživatelé se mohou přihlásit na web peněženky a ovládat své kryptoměny přímo z prohlížeče. Výhodou je snadný přístup z jakéhokoliv zařízení s internetem. Nevýhodou může být nižší bezpečnost, jelikož klíče mohou být uloženy online. Příklad: Blockchain.com, MyEtherWallet, MetaMask. (Frankenfield 2023a)

3.1.2 Mobilní Peněženky

Tyto peněženky existují ve formě aplikací na chytrých telefonech. Umožňují rychlé a pohodlné transakce přímo z mobilního zařízení a často nabízejí funkcionalitu QR kódů pro snadné skenování adres. Bezpečnost může být silnější než u webových peněženek, ale stále existují rizika spojená s hacknutím zařízení. Příklad: Trust Wallet, Coinomi, BRD Wallet. (Frankenfield 2023a)

3.1.3 Desktop Peněženky

Softwarové aplikace instalované přímo na osobním počítači. Nabízejí vyšší úroveň kontroly a bezpečnosti než webové a mobilní peněženky, protože klíče jsou často uchovávány přímo na zařízení. Nicméně, pokud dojde k poškození nebo ztrátě počítače bez zálohy, mohou být prostředky nenávratně ztraceny. Příklad: Electrum, Exodus, Atomic Wallet. (Frankenfield 2023a)

3.2 Offline Peněženky (Cold Wallets):

Offline peněženky, nazývané také „cold wallets“, jsou typem kryptopeněženek, které nejsou pořád připojené k internetu. Díky tomuto aspektu jsou považovány za

bezpečnější, protože jsou méně náchylné k rizikům spojeným s hackery a škodlivým softwarem. Existují ve třech hlavních formách:

3.2.1 Hardware Peněženky

Hardware peněženky jsou fyzická zařízení připojena pomocí USB, která bezpečně uchovávají soukromé klíče offline. Transakce se připravují online, ale k odeslání musí být zařízení připojeno, aby mohlo poskytnout potřebný digitální podpis. To znamená, že klíče nikdy neopustí zařízení a nejsou nikdy vystaveny internetu.

Mezi nejznámější příklady patří česká společnost Trezor, která od založení v roce 2013 proslavila tento způsob držení kryptoměn. V dnešní době firma produkuje dva typy hardwarových peněženek, konkrétně Model T a Trezor One.

Obrázek 4: Krypto peněženka Trezor
Zdroj: https://trezor.io/

Ledger je další populární hardwarová peněženka pocházející z Francie.K dispozici nabízí několik modelů, které mají podle uživatelů esteticky přitažlivější design podobný běžným USB flash diskům. (Trezor.io 2023; ledger.com 2023)

Obrázek 5: Krypto peněženka Ledger
Zdroj: https://www.ledger.com/

3.2.2 Paper Wallets

Paper wallets, česky papírové peněženky, jsou dalším způsobem, jak uchovávat kryptoměny, který doslova spočívá v zápisu soukromých a veřejných klíčů na papír. Tento papír se pak fyzicky ukládá na bezpečné místo. Transakce se provádí tak, že se importuje soukromý klíč do softwarové peněženky. Tato metoda je velmi bezpečná proti digitálním útokům, ale je zranitelná vůči fyzickým rizikům, jako je oheň, voda nebo ztráta. (Frankenfield 2022)

3.2.3 Steel Wallets

Steel wallets, nebo kovové peněženky, fungují podobně jako papírové peněženky, ale místo papíru se soukromé klíče uchovávají na kovové destičce. Tento přístup je odolnější vůči fyzickým poškozením, jako je oheň nebo voda, a může být preferován pro dlouhodobé uchování kryptoměn. (Frankenfield 2022)

4 Konsensus protokoly a těžba

4.1 Proof of Work (PoW)

Podle (a.s 2020) Proof of Work (PoW) je používaný v blockchainových sítích, který zajišťuje ověření a bezpečnost transakcí a záznamů v blokovém řetězci. Hlavním účelem PoW je zabránit dvojímu utrácení (double-spending) a poskytnout jednoznačný způsob, jak se dohodnout na jednom společném stavu blockchainu v decentralizovaném prostředí.

Princip Proof of Work je založen na řešení matematických úkolů, které jsou velmi náročné na výpočetní sílu. Těžaři, kteří se snaží vytvořit nový blok v blockchainu, musí najít specifický nonce (náhodné číslo), který umožní, aby hash nového bloku byl menší než určitá hodnota, tzv. cíl (target). Toto vyžaduje průchod mnoha různými kombinacemi, neboť nonce je náhodné a neexistuje žádný známý způsob, jak předpovědět, jaké nonce bude fungovat.

Těžaři soutěží mezi sebou o právo vytvořit nový blok a získat za to odměnu v kryptoměně. Ten, kdo jako první najde vhodný nonce a úspěšně vyřeší matematický úkol, může přidat nový blok do blockchainu. Ostatní těžaři ověří a potvrdí platnost nového bloku a pokračují v těžbě dalšího bloku.

Díky Proof of Work je těžba náročná na výpočetní sílu a těžaři jsou motivováni poskytnout tuto sílu, protože mají možnost získat odměnu za vyřešení bloku. Důležité je, že pokud by někdo chtěl změnit nějakou transakci nebo vložit falešné bloky do minulosti, musel by znovu řešit všechny následující matematické úkoly v blockchainu, což by bylo prakticky nemožné, pokud by neměl nadpoloviční výpočetní sílu celé sítě. (a.s 2020)

I když PoW byl první a je stále používán u některých kryptoměn, má i své nevýhody, jako je vysoká energetická náročnost a centralizace těžby u velkých těžařských firem. Kvůli těmto problémům se některé kryptoměny začaly přiklánět k jiným mechanismům, jako je Proof of Stake (PoS), který vyžaduje účastníkům, kteří chtějí těžit nebo validovat transakce, vklad (stake) v kryptoměně místo PoW.

Příklad měny fungující na PoW: BitCoin, Litecoin, Dash.

4.1.1 CPU těžba

CPU těžba kryptoměn je proces těžby, při kterém se využívá výpočetní síly procesoru (CPU) počítače k řešení matematických problémů, které jsou nezbytné pro ověřování transakcí a vytváření nových bloků v blockchainu kryptoměny. Tato metoda těžby byla v počátcích kryptoměn, jako je Bitcoin, poměrně běžná, protože v začátcích bylo relativně snadné získat odměny pomocí CPU těžby. (Sudipto 2022)

Nicméně s rostoucí popularitou a složitostí těžby se ukázalo, že výkon běžných CPU je nedostatečný pro efektivní těžbu kryptoměn, jako je Bitcoin, Ethereum a dalších populárních digitálních měn. Důvodem je, že tyto kryptoměny používají tzv. Proof of Work (PoW), který vyžaduje enormní výpočetní sílu a rychlost pro úspěšné řešení matematických úkolů. (Sudipto 2022)

V průběhu času se proto těžba postupně přesunula na specializované zařízení ASIC a GPU těžby.

Dnes nejznámější měnou co je pomocí CPU těžena je Monero(XMR).

4.1.2 GPU těžba

GPU těžba je proces těžby kryptoměn, který využívá výpočetní sílu grafických procesorů (GPU) pro řešení matematických problémů potřebných k ověření transakcí a vytváření nových bloků v blockchainu kryptoměny. GPU jsou určena primárně pro zpracování grafiky, ale ukázalo se, že jsou také velmi efektivní při paralelním zpracování matematických úloh, které jsou nezbytné pro kryptoměnovou těžbu. (Shobhit 2023)

Kryptoměny, které používají Proof of Work (PoW), byly původně navrženy tak, aby mohly být těženy pomocí GPU. Nicméně s rostoucí popularitou těžby a zvyšující se složitostí matematických problémů, se některé kryptoměny staly neefektivními pro těžbu pomocí GPU.

Výnosnost těžby ovšem hodně klesla v posledním roce z důvodu přechodu Etherea na Proof of Stake (PoS) a těžařům zůstaly méně atraktivní altcoiny.

4.1.3 ASIC těžba

Podle (Werner 2022) je ASIC těžba proces těžby kryptoměn, při kterém se využívají specializované elektronické zařízení nazývané ASIC. Tato zařízení jsou

navržena specificky pro účely těžby konkrétních kryptoměn a jsou optimalizovány pro řešení matematických úloh používaných v dané kryptoměnové síti.

ASIC těžba se stala preferovanou metodou pro mnoho hlavních kryptoměn, jako je Bitcoin, Litecoin, Bitcoin Cash a další. Důvodem je výrazná výpočetní efektivita těchto zařízení ve srovnání s běžnými procesory (CPU) nebo grafickými kartami (GPU). ASIC jsou schopny provádět matematické výpočty mnohem rychleji a efektivněji než jiné obecné výpočetní jednotky. (Werner 2022)

Nejznámější firmou ohledně ASIC minerů je Bitmain, která tu je od roku 2013.

ASIC těžba se značně rozšířila a postoupila do tzv. farem, které jsou zaměřené na velký hashrate pro jednu kryptoměnu. Dlouhou dobu se vedla „válka" ohledně zatěžování planety kvůli těžbě kryptoměn. Jedna strana argumentovala zátěží na přírodu odpadním teplem a spotřebou energie, to ovšem těžaři odmítají, protože výkon je potřeba i pro servery v bankovním sektoru atd. (Werner 2022)

4.1.4 Mining Pool

Samotná těžba kryptoměn, jako je například Bitcoin, může být pro jednotlivce náročná a neefektivní, zejména pokud nemají dostatečně výkonný hardware. Mining pool je způsob, který umožňuje těžařům spolupracovat a sdílet svou výpočetní sílu, aby efektivněji dosáhli těžebních odměn.

Princip mining poolu spočívá v tom, že řada jednotlivých těžařů přispívá svou výpočetní kapacitou k řešení složitých matematických problémů, které jsou nezbytné pro ověřování transakcí a zabezpečení kryptoměnové sítě. Když někdo v rámci poolu získá odměnu za úspěšné vyřešení bloku, tato odměna se rozdělí mezi všechny členy poolu podle míry, jakou k těžení přispěli. Rozdělení může být založeno na podílu výpočetní síly, kterou každý těžař poskytl, nebo na jiných pravidlech, které stanovuje konkrétní mining pool. (Investopedia team 2023)

Výhody těžby v mining poolu jsou zřejmé. Těžaři mají pravidelnější a stabilnější příjmy, protože odměny jsou rozděleny mezi všechny účastníky. Navíc spolupráce v poolu umožňuje menším těžařům, kteří by sami nemohli řešit bloky často, přispět k celkové síle sítě. To zlepšuje bezpečnost kryptoměny a snižuje

pravděpodobnost 51 % útoku, kdyby někdo s kontrolou nad většinou výpočetní síly mohl zneužít síť. (Investopedia team 2023)

Mining poolů existuje mnoho a každý má svá specifika, jako je například poplatek za službu, způsob rozdělení odměn nebo zvolený kryptoměnový protokol.

4.2 Proof of Stake (PoS)

Podle (a.s 2020) je Proof of Stake (PoS) další mechanismus používaný v blockchainových sítích k ověřování transakcí. Na rozdíl od Proof of Work (PoW), který vyžaduje výpočetní sílu k řešení matematických problémů, PoS pracuje na základě účasti a vkladů (stake) kryptoměny.

Princip Proof of Stake funguje následovně:

- **Stake (Vklad):** účastníci sítě musí vložit určité množství kryptoměny do tzv. vkladového poolu (stake poolu). Tím prokazují svůj zájem na podporu a správné fungování sítě. Částka vkladu může ovlivnit šanci na vybrání jako validátor bloku.
- **Vybrání validátorů:** pro každý nový blok se náhodně vybírají validátoři, kteří mají právo vytvořit nový blok a ověřit transakce. Čím vyšší vklad má účastník, tím vyšší je jeho šance být vybrán.
- **Validace a odměny:** validátoři ověřují transakce a vytvářejí nové bloky. Za svou práci obdrží odměny v kryptoměně, kterou těží, a také poplatky za transakce v bloku.
- **Bezpečnost sítě:** stejně jako u PoW, i PoS slouží k zabránění dvojímu utrácení a zajištění shody v decentralizovaném prostředí.

Výhody PoS zahrnují:

- **Energetická účinnost:** PoS je mnohem méně energeticky náročný než PoW, protože nevyžaduje drahý a intenzivní výpočetní výkon.
- **Decentralizace:** PoS snižuje tendenci centralizace, protože nevyžaduje speciální hardwarové zařízení jako PoW.

Příklad měn fungujících na PoS jsou Ethereum a Neo.

4.3 Proof of Capacity (PoC)

Proof of Capacity (PoC), také známý jako Proof of Space (PoS), je další mechanismus používaný v některých blockchainových sítích pro ověřování transakcí a dosažení dohody o stavu blockchainu. PoC je podobný PoW a PoS, ale místo výpočetního výkonu nebo vkladu kryptoměny využívá úložný prostor na pevném disku. (Hayes 2023b)

Princip Proof of Capacity funguje následovně:

- **Příprava úložného prostoru:** těžaři vytvářejí ploty (úložné segmenty), což jsou velké soubory naplněné náhodnými daty, které jsou uloženy na jejich pevných discích. Čím více úložného prostoru má těžař k dispozici, tím více plotů může vytvořit.
- **Výběr validátorů:** když je potřeba vytvořit nový blok, náhodně se vybírají validátoři, kteří budou moci využít své ploty k řešení matematického úkolu pro ověření bloku.
- **Matematický důkaz:** validátoři musí předložit důkaz, že mají daný plot na svém disku, což se nazývá také důkaz o kapacitě (proof of capacity). Toto ověření nevyžaduje intenzivní výpočetní sílu jako u PoW, protože ploty jsou již připravené a nevyžadují další složité výpočty.
- **Ověření a odměny:** poté, co validátoři úspěšně předloží důkaz o kapacitě, mohou vytvořit nový blok a ověřit transakce. Za svou práci obdrží odměny v kryptoměně.

PoC poskytuje některé výhody oproti PoW a PoS. Je energeticky úspornější než PoW, protože nepotřebuje takovou výpočetní sílu, a zároveň je méně nákladný na začátek než PoS, protože nemusí vyžadovat velké vklady kryptoměny. Navíc podporuje využití volného úložného prostoru na pevných discích, což je často opomíjený zdroj v běžných počítačích. (Hayes 2023b)

Jednou z kryptoměn, která využívá Proof of Capacity, je například Burstcoin. I když PoC nabízí některé výhody, stále je to relativně nový a jeho přesný vliv a uplatnění v blockchainovém prostředí jsou stále předmětem zkoumání a vývoje.

4.3.1 HDD těžba

HDD těžba (Hard Disk Drive těžba) je relativně nový způsob těžby kryptoměn, který využívá kapacity a rychlosti pevných disků k řešení matematických problémů nebo pro poskytování úložného prostoru pro blockchainy některých kryptoměn.

Některé kryptoměny, jako je například Chia, používají Proof of Space and Time (PoST), který umožňuje těžbu pomocí úložného prostoru. Namísto tradičního výpočetního výkonu, těžaři dokazují, že mají určité množství volného úložného prostoru na svém pevném disku, a tím dosahují šance na získání odměn za těžbu nových bloků. (coindoo 2023)

Plotting (Příprava úložného prostoru): těžaři vytvářejí tzv. ploty, což jsou velké soubory, které obsahují náhodná data a jsou uloženy na pevném disku. Tyto ploty slouží k důkazu, že těžař má určité množství volného úložného prostoru.

Těžba: Po vytvoření plotů těžaři je přidávají do sítě kryptoměny a potvrzují, že mají dostatečný prostor pro účast v těžbě. Po ověření se účastníci soutěží o právo vytvořit nový blok a získat odměnu v kryptoměně.

4.4 Ekologické dopady těžby

Proof of Work (PoW) těžba kryptoměn, zejména u Bitcoinu a Ethereum, je velmi energeticky náročná. Odhaduje se, že Bitcoin těžba spotřebovává značné množství elektrické energie a produkuje množství odpadu. Některé odhady uvádějí, že Bitcoin spotřebovává až 85 Terawatt-hodin ročně, což je srovnatelné s energetickou spotřebou celých zemí jako Belgie nebo Finsko. (Reiff 2023b)

Energie pocházející z těžby kryptoměn má dopad na životní prostředí, zahrnuje emise skleníkových plynů a produkci elektronického odpadu. Čína, Spojené státy a Kazachstán jsou země s největším podílem na těžbě Bitcoinu a to až 72 %. (Reiff 2023b)

Alternativním mechanismem, který může být méně energeticky náročný, je Proof of Stake (PoS), ale v případě Bitcoinu je nepravděpodobné, že by změnil svůj algoritmus.

Zatímco některé kryptoměny mohou mít vysokou energetickou náročnost, je důležité si uvědomit, že i tisk a správa tradičních fiat měn a bankovního systému má své vlastní environmentální náklady.

Některé alternativní metody validace transakcí, jako PoS, se snaží snížit energetickou náročnost.

5 Obchodování s kryptoměnami

V této kapitole bude zaměřena pozornost na různé platformy, skrze které je umožněn nákup, prodej a obchodování kryptoměn, přičemž budou zdůrazněny jak hlavní rozdíly, tak i specifika jednotlivých typů burz a směnáren.

5.1 Burzy

Kryptoměnové burzy jsou platformy, které umožňují nákup, prodej a obchodování kryptoměn. Některé burzy umožňují obchodování mezi kryptoměnami a fiat měnami, jako jsou dolary, eura apod., zatímco jiné umožňují pouze obchodování mezi různými kryptoměnami. Ke dni 8.7.2023 bylo na trhu více než 650 listovaných burz. (CoinMarketCap 2023)

5.1.1 Centralizované (CEX)

Tyto burzy fungují podobně jako tradiční burzy. Jsou řízeny centrální entitou, která usnadňuje všechny obchody. Uživatelé vkládají své kryptoměny na účet burzy, který je poté používán pro obchodování. Příklady populárních CEX jsou Binance, Coinbase a Kraken. (CoinMarketCap 2023)

5.1.2 Decentralizované (DEX)

Na rozdíl od CEX, DEX nejsou řízeny žádnou centrální entitou. Místo toho používají blockchainovou technologii pro usnadnění přímých obchodů mezi uživateli. To znamená, že uživatelé nikdy nepředávají kontrolu nad svými kryptoměnami třetí straně. Příklady populárních DEX jsou OpenOcean, SushiSwap a dYdX. (CoinMarketCap 2023)

5.2 Směnárny

Směnárny kryptoměn existují již několik let. Jednou z prvních v české republice byla SimpleCoin, která byla založena v roce 2013. V prvopočátcích se zaměřovala na směnu bitcoinu a koruny, poté rozšířila o další měny. Jelikož směna peněz za kryptoměny je sledována, tak bez registrace – uvedení občanského průkazu (ověření totožnosti) je možná jen v malém množství. Po registraci je možné směnit 200 EUR / 10 dní. Cena je zde uvedena jako v klasických směnárnách – je kurz prodej / nákup, který se liší i o 30 tisíc korun, a to z důvodu nestability kryptoměn. (Simplecoin 2024)

Kurz pro směnu je vždy držen jen určitou dobu, pokud se rozhodne směnit kryptoměnu za peníze a použije se pomalá platba, bude muset být akceptován nový kurz v momentu připsání platby směnárně. Pro využití směnárny je potřeba vlastnit krypto peněženku.

5.3 Bankomaty

Krypto bankomaty se vyskytují v české republice od roku 2014, kde jedním z prvních byl WBTCB bankomat. Funguje na podobném principu jako směnárny. Výhodou je, že není potřeba vlastnit peněženku, jelikož bankomat můžepeněženkuvytvořit. Bankomaty jsou nejrozšířenější hlavně v Praze. (bitcomat.com 2023)

6 Zneužití kryptoměn

Kryptoměny, přestože nabízejí mnoho inovativních a užitečných aplikací, jsou také cílem různých podvodných praktik. V této kapitole jepopsána temnější strana kryptoměn jakož to spojení s DarkWebem, podvody a výrazná selhání krypto trhu.

6.1 DarkWeb

Darkweb, jakožto součást hlubokého webu, která není indexována běžnými vyhledávači, obsahuje webové stránky a služby, jež jsou často dostupné pouze prostřednictvím speciálních prohlížečů, jako je Tor (The Onion Router). Následující úvaha se zaměřuje na několik klíčových aspektů, které spojují kryptoměny s darkwebem.

Anonymita a Soukromí: kryptoměny, zejména ty, které jsou zaměřeny na zvýšení soukromí, jako například Monero, umožňují uživatelům provádět transakce anonymně. Na darkwebu, kde je anonymita velmi ceněna, se tato vlastnost stává atraktivní.

Nelegální Obchod: bohužel, darkweb je také známý jako místo, kde lze nalézt nelegální zboží a služby, jako jsou drogy, zbraně nebo hackované účty. V těchto případech se kryptoměny často používají jako prostředek platby, jelikož umožňují obchodníkům a kupujícím zůstat v anonymitě.

Regulační Výzvy: vzhledem k potenciálnímu využití kryptoměn na darkwebu pro nelegální aktivity se regulátoři v různých jurisdikcích snaží nalézt způsoby, jak monitorovat a regulovat tuto činnost. Tato snaha vede k diskusím o vyvážení soukromí a bezpečnosti.

Technologický Rozvoj: jako pozivitum může být bráno spojení kryptoměn s darkwebem jako důkaz technologického pokroku a inovace. Některé služby na darkwebu nabízejí legitimní a zákonné produkty a služby, a kryptoměny tam mohou sloužit jako efektivní a decentralizovaný způsob platby.

6.2 Podvodné praktiky

V této kapitole jsou některé z nejběžnějších metod, kterými se podvodníci snaží zneužít prostředí kryptoměn a pár tipů, jak se proti těmto nekalým metodám bránit.

6.2.1 Phishing

Phishing je běžný podvod v kryptoměnovém světě, kde podvodníci posílají falešné e-maily nebo zprávy, které se tváří jako legitimní organizace, jako jsou burzy nebo peněženky. Cílem je přimět uživatele, aby klikli na podvodné odkazy vedoucí na falešné webové stránky, kde zadají své přihlašovací údaje. Tyto údaje jsou pak zneužity k přístupu k účtům a krádeži kryptoměn.(Cheng 2022)

Phishingové útoky mohou vést nejen k finančním ztrátám, ale také ke kompromitaci dalších osobních a pracovních účtů. Pro ochranu před phishingem je důležité důkladně ověřovat odesílatele zpráv a URL adresy, neklikat na podezřelé odkazy, používat dvoufaktorové ověření a pravidelně se vzdělávat o nových podvodných taktikách. Phishing vyžaduje konstantní bdělost a preventivní opatření pro zajištění bezpečnosti vašich digitálních aktiv.(Cheng 2022)

6.2.2 Ponziho schéma

Ponziho schéma je typ finančního podvodu, který funguje na principu platby výnosů starším investorům z peněz získaných od nově příchozích investorů, místo z reálných zisků z investic. Tento model je neudržitelný, protože závisí na neustálém přísunu nových peněz, aby fungoval. Jakmile příliv nových investic ustane, schéma se zhroutí a většina lidí přijde o své peníze.(Chen 2024)

Ponziho schémata často lákají investory sliby vysokých výnosů s malým nebo žádným rizikem. V kryptoměnovém světě může být tento podvod zamaskován jako inovativní investiční příležitost nebo unikátní obchodní strategie.

Pro ochranu před tímto typem podvodu je důležité důkladně prozkoumat, jak projekt generuje své výnosy a zda jsou tyto informace transparentní a ověřitelné. Je také užitečné vyhýbat se investicím, které vyžadují přivedení dalších lidí do systému pro získání zisku. Podezření by měla vzbuzovat jakákoliv investiční nabídka, která zní příliš dobře, aby byla pravdivá, neboť často také je. (Chen 2024)

6.2.3 Podvodné ICOs

Podvodné Inicializační Nabídky Mincí (ICO) jsou jednou z rizik spojených s kryptoměnovým trhem. ICO je metoda získávání kapitálu pro nové kryptoměnové projekty, kde investoři kupují nově vytvořené mince nebo tokeny v očekávání, že jejich hodnota vzroste. Některá ICO jsou však založena pouze za účelem získání peněz od investorů bez skutečného záměru rozvíjet funkční produkt nebo službu. (Reiff 2023a)

Podvodníci mohou vytvářet falešné projekty s atraktivními webovými stránkami, nadějnými obchodními plány a falešnými týmy. Často slibují zaručené vysoké výnosy a používají agresivní marketingové strategie k získání důvěry a investic od veřejnosti. Po získání financí se projekt často rozplyne a investoři přijdou o své peníze. (Reiff 2023a)

Pro ochranu před podvodnými ICO je důležité provádět důkladný průzkum jakéhokoli projektu, do kterého se uvažuje o investici. Zjišťujte informace o týmu za projektem, zkontrolujte jejich minulé zkušenosti a ověřte si, zda mají skutečné partnerství a transparentní plán vývoje. Také je dobré se vyhnout projektům, které vydávají přehnané nebo nereálné sliby výnosů. (Reiff 2023a)

6.2.4 Pump and Dump schéma

Schéma "Pump and Dump" je rozpoznáváno jako typ finančního podvodu, který se často vyskytuje na trzích s kryptoměnami. Cena kryptoměny je nejprve uměle zvyšována podvodníky, což vytváří iluzi rychlého růstu hodnoty. Tento nárůst přitahuje další investory, kteří začnou měnu nakupovat ve víře, že její hodnota bude dále růst. Jakmile je dosaženo požadovaného zvýšení ceny, podíly jsou prodávány podvodníky za vysoké ceny, což jim umožňuje dosáhnout značného zisku. Poté, co podvodníci své podíly prodají, cena kryptoměny obvykle prudce klesá, což způsobuje ztráty ostatním investorům, kteří nakoupili za vysokou cenu. (Dhir 2022)

Ochrana před tímto schématem vyžaduje opatrnost. Doporučuje se vyhnout nákupu kryptoměn, které vykazují náhlý a nevysvětlitelný růst ceny. Věření slibům o rychlém zbohatnutí bez jakéhokoliv rizika by mělo být také zpochybněno.

Důkladný průzkum a ověřování informací jsou nezbytné kroky před jakoukoliv investicí, aby bylo možné se vyvarovat potenciálních podvodů. (Dhir 2022)

6.2.5 Malware

Malware, který je specificky zaměřen na kryptoměny, je charakterizován jako software navržený tak, aby tajně infikoval zařízení a ukradl kryptoměnové fondy uživatele. Tento typ škodlivého softwaru zahrnuje různé formy, včetně keyloggerů, které jsou určeny k záznamu klávesových stisků s cílem získat přístupové klíče a hesla, a ransomware, který šifruje data na zařízení a vyžaduje výkupné v kryptoměně pro jejich obnovení. (Investopedia team 2022)

Ochrana před malwarem vyžaduje použití spolehlivého antivirového a antimalwarového softwaru, který je pravidelně aktualizován. Doporučuje se také pravidelné zálohování důležitých dat na bezpečných, oddělených médiích, aby byla minimalizována potenciální škoda způsobená ransomwarem. Využívání silných, unikátních hesel pro každý účet a zapnutí dvoufaktorové autentizace, kdekoliv je to možné, jsou další kroky, které by měly být podniknuty k zajištění lepší ochrany proti útokům zaměřeným na kryptoměnové aplikace a služby. (Investopedia team 2022)

6.2.6 Falešné burzy a peněženky

Falešné burzy a peněženky jsou identifikovány jako webové stránky nebo aplikace, které se vydávají za legitimní služby pro obchodování s kryptoměnami nebo jejich ukládání. Tato schémata jsou navržena tak, aby ukradla kryptoměny od nic netušících uživatelů. Obvykle se jedná o platformy, které lákají investory příslibem nízkých poplatků nebo výjimečných funkcí, avšak po vkladu prostředků jsou uživatelé zbaveni možnosti jakékoliv další transakce a jejich prostředky jsou ztraceny. (Stroukal 2020)

K ochraně se doporučuje provádět důkladný průzkum před registrací nebo vkladem jakýchkoliv prostředků. Kontrola recenzí ostatních uživatelů, prověření zkušeností na komunitních fórech a ověření, zda má platforma transparentní a dostupnou zákaznickou podporu, jsou klíčové kroky k ověření její věrohodnosti. Také je vhodné využívat peněženky a burzy, které jsou široce uznávané a mají dobrou pověst v kryptoměnové komunitě. (Stroukal 2020)

6.3 Významná historická selhání

Silk Road Shutdown: Silk Road bylo tržiště na dark webu, které umožňovalo uživatelům anonymně nakupovat a prodávat nelegální zboží, včetně drog a zbraní, přičemž platby probíhaly v bitcoinech. Tento portál byl uzavřen FBI v roce 2013 a jeho zakladatel Ross Ulbricht byl zatčen a odsouzen za praní peněz, počítačové hackingy a další zločiny. Silk Road byl jedním z prvních případů, kdy byla veřejnost výrazně upozorněna na možné zneužití kryptoměn v nelegálních aktivitách. (Stroukal 2020)

6.3.1 Mt. Gox Hack (2014)

Mt. Gox byla jedna z prvních a největších bitcoinových burz, která byla zasažena rozsáhlým hackerským útokem v roce 2014. Z burzy bylo odcizeno přibližně 850,000 bitcoinů, což tehdy představovalo hodnotu asi 450 milionů dolarů. Tento hack nejen že vyvolal obrovský finanční skandál, ale také vážně otřásl důvěrou veřejnosti v kryptoměny a vedl k poklesu hodnoty bitcoinu. Mt. Gox nakonec zkrachovala a tento případ je dodnes předmětem soudních sporů a vyšetřování. (Investopedia team 2024c)

6.3.2 Kolaps FTX

FTX, založená Samem Bankmanem-Friedem, se stala centrem kryptoměnového světa díky své velké uživatelské základně a široké škále nabízených služeb. V listopadu 2022 však vyšly najevo zprávy o možném zneužití uživatelských fondů a rizikovém řízení společnosti. Tato zpráva vyvolala masivní výběry aktiv, které burza nedokázala pokrýt. FTX rychle ztratila likviditu a následně vyhlásila bankrot. (Reiff 2024)

Skandál měl široké důsledky pro celý kryptoměnový průmysl, včetně masivního poklesu důvěry investorů a propadu cen mnoha kryptoměn. Vyšetřování situace pokračuje, a zahrnuje otázky týkající se regulace kryptoměnových burz, správy a transparentnosti ve finančních operacích. Tento incident zdůrazňuje potřebu pevnější regulace a lepšího řízení rizik v kryptoměnovém sektoru. (Reiff 2024)

7 Vznik nové kryptoměny

Kapitola se zaměřuje na obecný popis vzniku nové kryptoměny, proces, který zahrnuje mnoho kroků od počátečního konceptu až po jeho realizaci a nasazení.

Podkapitoly byly vytvořeny z následujících zdrojů: (Anurina 2023; Garnett 2023)

Mince vs Tokeny

V kryptosvětě je základním rozlišením mezi mincí a tokenem to, že mince operuje na svém vlastním, jedinečném blockchainu, zatímco token je vytvářen na již existujícím blockchainu. Mince, jako je Bitcoin nebo Ethereum, jsou původní digitální měny svých blockchainů a slouží primárně jako prostředek výměny nebo uchování hodnoty. (Investopedia team 2024a)

Na druhé straně, tokeny, které jsou vydávány na platformách jako Ethereum, mohou mít různé použití od reprezentace aktiv jako jsou akcie nebo nemovitosti, po fungování jako prostředky pro přístup k určitým službám v rámci dApp (decentralizovaných aplikací). Díky tomu, že tokeny využívají existující infrastruktury, jsou obvykle jednodušší a levnější na vytvoření oproti mincím, které vyžadují vývoj a udržování vlastního blockchainu.

Volba vytvoření mezi mincí a tokenem závisí na specifických potřebách a zdrojích. Vytvoření mince s vlastním blockchainem je technologicky náročnější a vyžaduje větší investice času a peněz. Na druhou stranu, vytvoření tokenu na existujícím blockchainu je mnohem dostupnější a rychlejší, což umožňuje snazší integraci a využití existujících technologií a komunit.

7.1 Definice účelu a strategie

Úspěch kryptoměny je často určován jejím jasně definovaným účelem a cílovým trhem. Například, když se má vytvořit kryptoměna pro sektor realitního trhu, je navrhována tak, aby řešila specifické problémy tohoto trhu, jako jsou zjednodušení transakcí nebo snížení nákladů na převod vlastnictví. V tomto kroku je proveden důkladný průzkum trhu, jsou identifikováni potenciální uživatelé a konkurence a je definováno, jak hodnota bude uživatelům kryptoměnou přinášena.

7.2 Výběr mezi mincí a tokenem

Rozhodnutí, zda bude vytvořena mince nebo token, je určováno technologickými potřebami a obchodním modelem projektu. Budování nebo upravování vlastního blockchainu, což je technicky náročnější a dražší, je vyžadováno při vytváření mince, ale poskytuje větší kontrolu a nezávislost. Příkladem může být Litecoin, který byl vytvořen změnou Bitcoinového kódu. Naopak, tokeny jsou obvykle vytvářeny na již existujících blockchainech, jako je Ethereum, což vývoj usnadňuje a zlevňuje. Tokeny mohou mít různé formy, jako jsou utility tokeny nebo security tokeny, které mohou reprezentovat aktiva nebo služby.

7.3 Technologický vývoj

Vývojem nebo forkováním existujícího blockchainu je zahrnut krok pro minci. Například, vytvoření nové mince může vyžadovat upravení parametrů, jako jsou velikost bloku nebo těžební algoritmus. Pro tokeny zahrnuje tento krok vývoj programování smart kontraktů, které určují pravidla tokenu, jako je jeho distribuce, transakce a jakékoliv specifické funkce, které token nabízí. Psaní kódu v Solidity pro Ethereum platformu je často zahrnuto.

7.4 Zajištění bezpečnosti a legalit

Bezpečná a v souladu s právními předpisy musí být kryptoměna, aby mohla být úspěšně uvedena na trh a přijata uživateli. Implementací silných kryptografických protokolů, testováním softwaru proti zranitelnostem a zajištěním, že projekt splňuje všechny relevantní finanční regulace, je toto zajištěno. Často je nutné konzultovat s právními odborníky, aby bylo zajištěno, že kryptoměna neporušuje žádné zákony, zejména v oblastech, kde jsou regulace kryptoměn přísné.

7.5 Těžba nebo distribuce

Metodou distribuce, která může zásadně ovlivnit přijetí a úspěch kryptoměny, jsou mince distribuovány prostřednictvím těžby, kde uživatelé používají výpočetní výkon ke generování nových jednotek. Tokeny mohou být distribuovány různými způsoby, například přes ICO (initial coin offering), kde jsou

tokeny prodávány investorům, nebo přes airdrops, kde jsou tokeny zdarma rozdávány komunitě ke zvýšení povědomí a zapojení.

Airdrop v kontextu kryptoměn je marketingová strategie, která zahrnuje distribuci tokenů nebo mincí zdarma do peněženek různých uživatelů kryptoměn. Cílem této strategie je zvýšit povědomí o nové kryptoměně, rozšířit její držitele a podpořit její používání a obchodování. Často jsou airdropy využívány jako nástroj ke zvýšení komunitního zapojení nebo k odměně stávajících uživatelů za jejich podporu projektu. Uživatelé obvykle musí splnit určitá kritéria, jako je držení určitého množství existující kryptoměny, registrace na platformě nebo účast v komunitních aktivitách, aby se kvalifikovali pro příjem airdropu.

7.6 Promo akce a získávání uživatelů

Vybudování komunity a marketingu je pro úspěch kryptoměny zásadní. To zahrnujespuštění informačních kampaní, účast na blockchainových a kryptoměnových konferencích a využití sociálních médií a influencerů k šíření povědomí o kryptoměně. Příkladem může být, jak Ethereum získalo velkou podporu prostřednictvím svého ICO a aktivní komunikace s vývojáři a investory.

7.7 Uvedení na trh a správa

Posledním krokem je uvedení kryptoměny na burzy, což umožní uživatelům ji nakupovat, prodávat a obchodovat. To vyžaduje spolupráci s burzami a splnění jejich požadavků. Současně je nutné pokračovat ve vývoji, aktualizaci softwaru a řešení jakýchkoli problémů, které mohou vzniknout. Ongoing management zahrnuje také monitoring trhu a reagování na feedback uživatelů, aby byla kryptoměna stále relevantní a bezpečná.

8 Analýza současného trhu

8.1 Regulace

8.1.1 V České republice

V České republice, kde je trh s kryptoměnami velmi liberální, nebyly v poslední době zavedeny žádné významné nové zákony nebo předpisy týkající se kryptoměn. Kryptoměny nejsou považovány za oficiální platidlo, ale jako komodity a nejsou předmětem přímé regulace státem. Na úrovni Evropské unie se však Česká republika řídí směrnicemi EU, jako je AMLD5, která se týká opatření proti praní peněz. (jamesgre 2023)

Česká republika nadále zůstává jednou z nejpřívětivějších zemí pro krypto podnikání v rámci EU, díky relativně liberálnímu přístupu k regulaci těchto technologií. Firmy provozující kryptoměnové transakce musí dodržovat obecné obchodní zákony a směrnice EU, ale nejsou vyžadovány specifické licence pro obchodování nebo správu kryptoměn, pokud neposkytují spotřebitelské úvěry nebo neprovádějí trvalé ziskové služby spojené s virtuálními aktivy. (jamesgre 2023)

8.1.2 Ve světě

Zavedení kryptoměn jako zákonného platidla je vzácné a doposud se týká pouze několika málo zemí. Zde je přehled těch, které to udělaly:

- **Salvador**: Salvador se stal první zemí na světě, která uznala Bitcoin jako zákonné platidlo. Tento krok byl učiněn v září 2021. Přijetí Bitcoinu bylo součástí širšího ekonomického plánu prezidenta Nayiba Bukeleho na podporu finanční inkluze, investic a ekonomického rozvoje.(Krishnakumar 2022)
- **Středoafrická republika**: v dubnu 2022 se Středoafrická republika stala druhou zemí na světě, která učinila Bitcoin zákonným platidlem. Tento krok byl částí snahy o modernizaci ekonomiky země a přilákání mezinárodních investorů.(Krishnakumar 2022)

Ostatní země mohou mít velmi přátelskou politiku a regulace, které podporují používání kryptoměn, ale nejedná se o oficiální zákonné platidlo. Přijetí

kryptoměn jako zákonného platidla zůstává kontroverzní a omezené na několik zemí, přičemž v mnoha jiných státech jsou regulace a postupy různé.

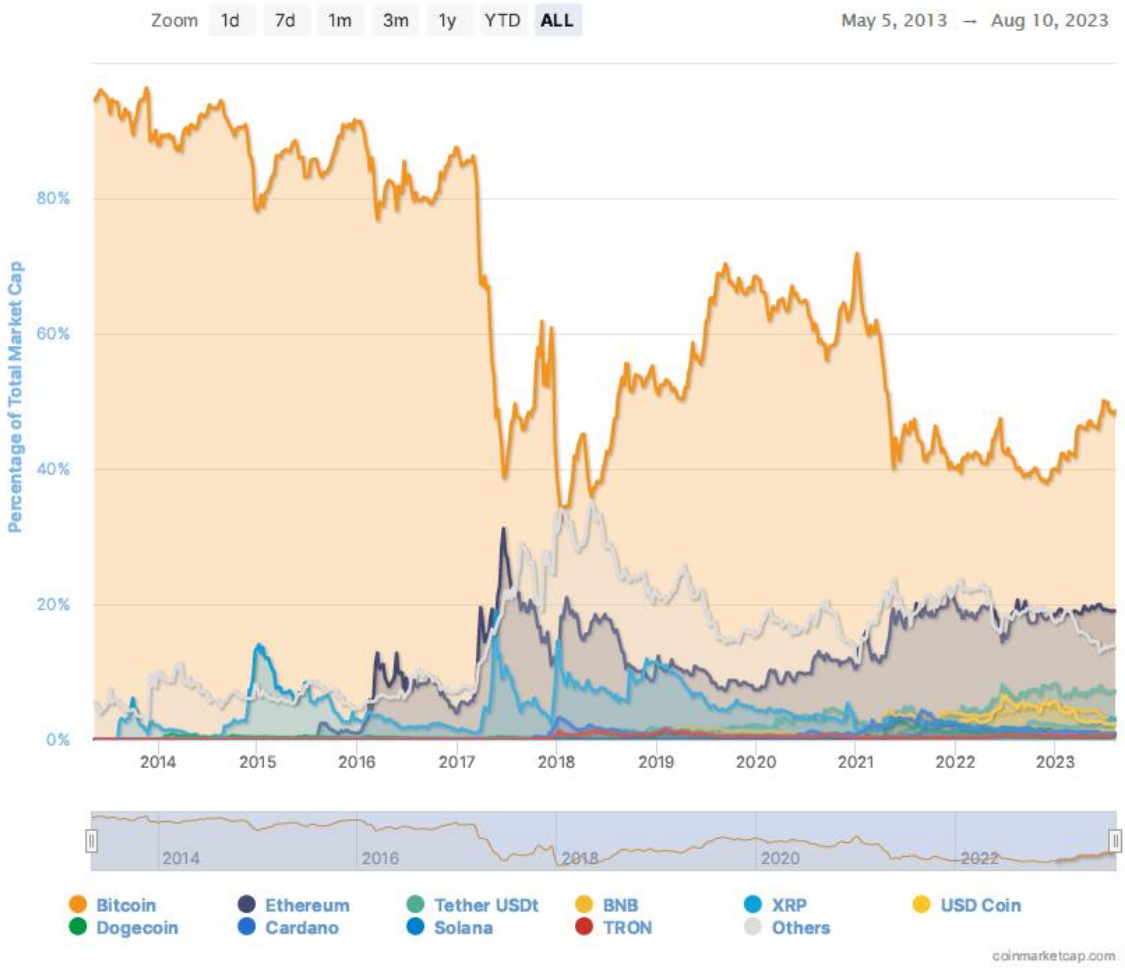
8.2 Přehled TOP 10 kryptoměn

Celková tržní kapitalizace činí přibližně 1 475 623 500 414 dolarů a více než 28 000 existujících kryptoměn a tokenů k 25. listopadu 2023, což je více než dvakrát tolik než v roce 2021. (CoinMarketCap 2023)

	Název (Zkratka)	Kapitalizace ($)	Cena mince ($)	Mince v oběhu
1.	**Bitcoin (BTC)**	738 067 358 546	37 746.53	19 552 400
2.	**Ethereum (ETH)**	250 693 290 995	2084.43	120 245 290
3.	**Tether (USDT)**	88 762 809 503	1.00	88 762 809 503
4.	**Binance Coin (BNB)**	35 576 385 709	234.53	151 699 619
5.	**XRP (XRP)**	33 485 723 138	0.62	53 816 975 568
6.	**Solana (SOL)**	24 714 452 833	58.48	423 305 488
7.	**USDC (USDC)**	24 712 853 281	1	24 712 853 281
8.	**Cardano (ADA)**	13 800 362 690	0.391	35 293 944 219
9.	**Dogecoin (DOGE)**	11 135 925 132	0.078	141 972 826 384
10.	**TRON (TRX)**	9 343 551 916	0.1055	88 577 533 164

Tabulka 3: TOP 10 kryptoměn podle tržní kapitalizace ke dni 25.11.2023
Zdroj: https://coinmarketcap.com/

Tabulka zobrazuje seznam Top 10 kryptoměn dle tržní kapitalizace ke dni 25.11.2023 podle údajů z Coinmarketcap. Nabízí přehledné porovnání tržních hodnot a ukazuje převahu Bitcoinu a Ethereum, zatímco ostatní kryptoměny mají znatelně menší kapitalizaci.



Obrázek 6: Celková tržní kapitalizaci ke dni 10.10.2023

Zdroj: https://coinmarketcap.com/charts/

Tento graf zobrazuje poměrový podíl různých kryptoměn na celkové tržní kapitalizaci kryptoměn v průběhu času, od roku 2013 až do srpna 2023. Bitcoin (oranžová) dominuje grafu s proměnlivým podílem, často přesahujícím 50% tržní kapitalizace, ale s několika poklesy. Ethereum (šedá) roste a poklesne s časem a má menší, ale stále významný podíl. Další kryptoměny jako Cardano, Solana, Binance Coin (BNB), Ripple (XRP), Dogecoin a stablecoiny jako Tether (USDT) a USD Coin mají menší a rozptýlenější přítomnost v grafu. Celkově graf ukazuje vývoj a změny v dominanci jednotlivých kryptoměn v čase.

8.3 Aktualizovaný Přehled TOP 10 kryptoměn

Celková tržní kapitalizace činí přibližně 2,32 trilionů dolarů a více než 31 000 existujícími kryptoměnami a tokeny k 14. dubnu 2024.(CoinMarketCap 2023)

K porovnání bylo vybráno pouze TOP 10 kryptoměn, které tržní hodnotou dominují současnému trhu. Vzhledem k tomu, že Bitcoin je obecně považován za otce moderních kryptoměn, lze všechny ostatní kryptoměny označit termínem altcoin, který je odvozen od slov alternative coin.

	Název (Zkratka)	Kapitalizace ($)	Cena mince ($)	Mince v oběhu
1.	**Bitcoin (BTC)**	1 261 878 075 554	64 087.51	19 681 837
2.	**Ethereum (ETH)**	360 882 213 618	3 008.67	120 070 455
3.	**Tether (USDT)**	107 469 433 300	1.00	107 359 271 607
4.	**Binance Coin (BNB)**	82 978 561 947	554.48	149 532 959
5.	**Solana (SOL)**	63 333 879 986	141.87	446 453 744
6.	**USDC (USDC)**	32 256 099 693	1	32 252 795 957
7.	**XRP (XRP)**	26 266 442 364	0.477	55 119 895 152
8.	**Dogecoin (DOGE)**	21 902 633 824	0.152	143 873 976 384
9.	**Toncoin (TON)**	21 202 105 776	6.1	3 470 779 942
10.	**Cardano (ADA)**	15 920 382 301	0.447	35 613 482 203

Tabulka 4: TOP 10 kryptoměn podle tržní kapitalizace ke dni 14.4.2024
Zdroj: https://coinmarketcap.com/

Rychlý vývoj kryptoměn vede ke vzniku stále většího počtu měn, které buď vycházejí z již zajetých kryptoměn a přizpůsobují jeho systém své vlastní podobě, nebo se snaží razit novou cestu pomocí vlastních technologií. V tabulce č.4 jsou zobrazeny kryptoměny, které jsou v práci dále zpracovány. Vzhledem k tomu, že trh s kryptoměnami je živý a neustále se měnící, hodnoty v tabulkách č.3 a č.4 jsou použity spíše jako orientační, protože se mění každou vteřinu.

8.4 Představení TOP 10 Kryptoměn

Kapitola se zaměřuje na analýzu a porovnání deseti nejvýznamnějších kryptoměn současného trhu. Cílem je poskytnout komplexní přehled o každé kryptoměně, včetně jejího historického vývoje, technologických charakteristik, tržní kapitalizace, a dalších klíčových faktorů, které ovlivňují její pozici a potenciál na trhu. Komplexní analýza umožní pochopit, jak se jednotlivé kryptoměny liší a jaké mají specifické vlastnosti, které je činí jedinečnými na trhu digitálních měn.

Je důležité zdůraznit, že veškeré informace a data použité k analýze pocházejí z veřejně dostupných zdrojů, hlavně z whitepaperů (oficiálních dokumentů) jednotlivých kryptoměn, webů s analytickými nástroji

Veškerá loga kryptoměn byla čerpána z webové stránky (CoinMarketCap 2023).

8.4.1 Bitcoin (BTC)

Bitcoin je první decentralizovaná kryptoměna, která byla vytvořena. Založení Bitcoinu se datuje k 3. lednu 2009, kdy byl vytěžen první blok, známý jako genesis blok. Jako zakladatel je označován Satoshi Nakamoto, což je pseudonym osoby nebo skupiny osob, jejichž skutečná identita dosud nebyla odhalena. (Nakamoto 2009)

Tržní kapitalizace Bitcoinu je jednou z největších mezi všemi kryptoměnami, přičemž její aktuální hodnota se pohybuje okolo 1,3 bilionu dolarů. Nejvyšší dosažená hodnota tržní kapitalizace byla zaznamenána 14. března 2024, kdy Bitcoin dosáhl cenového vrcholu blízkého 73 000 USD za jednotku. Cena za transakci se může lišit v závislosti na aktuální zátěži sítě, ale typicky se pohybuje od několika dolarů do desítek dolarů za transakci. Bitcoin funguje na principu blockchainu s mechanismem PoW. (CoinMarketCap 2023)

Celková nabídka Bitcoinu je omezena na 21 milionů mincí, z nichž většina již byla vytěžena. Bitcoin má deflační měnovou politiku, což znamená, že jeho nabídka je uměle omezena, čímž se postupem času zvyšuje jeho hodnota. (Nakamoto 2009)

Historický vývoj cen Bitcoinu vykazuje významné kolísání s několika bublinami a následnými prudkými poklesy. Tento trend odráží jeho volatilní povahu jako investičního aktiva.

Bitcoin je obchodován na mnoha hlavních kryptoměnových burzách s vysokou likviditou, což zajišťuje jeho dostupnost pro širokou veřejnost. Denní obchodní objem se často pohybuje v řádech miliard dolarů.

Právní a regulační status Bitcoinu se liší v závislosti na zemi. V některých zemích je plně legalizován a regulován, zatímco v jiných může čelit omezením nebo úplnému zákazu.

Komunita okolo Bitcoinu je rozsáhlá a aktivní, s miliony uživatelů po celém světě a silnou podporou vývojářů. Spolupracuje také s mnoha finančními a technologickými firmami.

Aplikace Bitcoinu zahrnují jeho použití jako prostředku k uchování hodnoty, způsobu platby a spekulativní investice. V České republice Bitcoin přijímá několik obchodů a online platforem jako platidlo. Jeden z prvních byla například Alza. (a.s 2022)

Udržitelnost a environmentální dopad Bitcoinu je často diskutovaným tématem, zejména kvůli vysoké energetické náročnosti jeho těžebního procesu, což vede k významným emisím skleníkových plynů. Tento aspekt vyvolává otázky ohledně jeho dlouhodobé udržitelnosti v kontextu globálních klimatických cílů.

Halvingem je nazýváno automatické snížení odměny za těžbu kryptoměny, které se děje v předem určených intervalech a slouží k omezení inflace a zvýšení vzácnosti měny. Tento proces je nejznámější u Bitcoinu, kde se odměna za blok snižuje každé 4 roky na polovinu. Například, pokud byla původní odměna 50 Bitcoinů za blok, po prvním halvingu je to 25 Bitcoinů a po druhém halvingu 12,5 Bitcoinu. Podobný princip je používán i u dalších kryptoměn, jako je Litecoin. (Nakamoto 2009)

Tento mechanismus je klíčový pro dlouhodobé udržení hodnoty kryptoměn, jelikož omezuje přísun nových jednotek do oběhu, což může podpořit růst ceny za předpokladu stálé nebo rostoucí poptávky.

8.4.2 Ethereum (ETH) 

Ethereum je decentralizovaná platforma, která umožňuje vývoj a provoz smart kontraktů a decentralizovaných aplikací bez potřeby třetí strany. Bylo založeno v roce 2015 skupinou vývojářů vedenou Vitalikem Buterinem. (Ethereum 2023)

Tržní kapitalizace Etherea je považována za druhou největší po Bitcoinu, přičemž její hodnota se často pohybuje v řádu desítek miliard dolarů. Nejvyšší dosažená hodnota tržní kapitalizace byla zaznamenána v květnu 2021, kdy cena Etherea dosáhla přibližně 4 300 USD za jednotku. Cena za transakci na Ethereum síti se liší a je ovlivněna aktuální zátěží sítě, přičemž může dosahovat od několika centů po desítky dolarů v dobách vysokého zatížení. (CoinMarketCap 2023)

Ethereum ze začátku využívalo blockchain s mechanismem Proof of Work, ale v září 2022 přešlo ne Proof of Stake v rámci upgradu na Ethereum 2.0, což bylo zaměřeno na zlepšení škálovatelnosti a snížení energetické náročnosti. Mezi speciální technologické funkce patří podpora smart kontraktů, která umožňuje automatizované, programovatelné transakce a aplikace. (Ethereum 2023)

Celková nabídka Etherea není omezena jako u Bitcoinu, ale jeho emise je regulována s cílem udržet inflaci pod kontrolou. Měnová politika Etherea zahrnuje mechanismy, jako je například spalování části transakčních poplatků, což přispívá k deflaci.

Historický vývoj cen Etherea ukazuje rychlý růst od jeho založení s několika výraznými vrcholy a poklesy, které odrážejí jeho volatilní charakter a rostoucí zájem o platformu.

Ethereum je obchodováno na všech hlavních kryptoměnových burzách a je známé svou vysokou likviditou. Denní obchodní objem Etherea se často pohybuje v miliardách dolarů. (CoinMarketCap 2023)

Právní a regulační status Etherea se také liší podle země, ale obecně je vnímáno jako legální a v některých případech regulované finanční úřady.

Komunita Etherea je velmi rozsáhlá a aktivní, což zahrnuje tisíce vývojářů a miliony uživatelů globálně. Ethereum má silnou podporu pro vývoj nových projektů a aplikací díky své otevřené a přístupné platformě.

Klíčové aplikace a praktické využití Etherea zahrnují finanční služby, hlasovací systémy, a decentralizované finance (DeFi), které jsou mezi nejpopulárnější použití platformy. V České republice je Ethereum akceptováno několika technologicky orientovanými firmami a startupy jako platidlo nebo pro technologické integrace. (Ethereum 2023)

Udržitelnost a environmentální dopad Etherea jsou v současnosti předmětem značné pozornosti, zejména s ohledem na jeho přechod na Proof of Stake, což má za cíl výrazně snížit jeho energetickou náročnost a zlepšit jeho ekologickou stopu.

8.4.3 Tether (USDT)

Tether je stabilní kryptoměna, známá jako stablecoin, která je navázána na hodnotu amerického dolaru v poměru 1:1. Tether byl založen v roce 2014 a je vydáván společností Tether Limited. (Tether 2023)

Tržní kapitalizace Tetheru se řadí mezi největší v oblasti kryptoměn, často přesahující desítky miliard dolarů. Vzhledem k jeho charakteru stablecoinu je jeho cena stabilizována blízko 1 USD, což odráží jeho účel jako prostředku pro uchování hodnoty a zprostředkování transakcí mezi různými kryptoměnami bez potřeby přechodu na tradiční měny. Cena za transakci se liší v závislosti na použité síti blockchainu, ale obecně se pohybuje v nízkých hodnotách. (CoinMarketCap 2023)

Hlavní technologickou charakteristikou Tetheru je jeho vydávání na několika blockchainech, včetně Bitcoin (přes Omni Layer), Ethereum, TRON a další, což umožňuje vysokou míru interoperability a dostupnost na širokém spektru obchodních platform. Tether nevyužívá mechanismy Proof of Work ani Proof of Stake, protože jeho hodnota je zajištěna rezervami v dolarech. (Tether 2023)

Celková nabídka Tetheru není pevně stanovena a může kolísat v závislosti na požadavcích trhu a množství dolarů držených v rezervách společností Tether

Limited. Měnová politika Tetheru je tedy zaměřena na udržení paritního kurzu s americkým dolarem.

Historický vývoj cen Tetheru je relativně stabilní s minimálními odchylkami od jeho paritního kurzu 1 USD.

Tether je široce obchodován na mnoha kryptoměnových burzách, což mu zajišťuje vysokou likviditu a denní obchodní objemy často přesahující miliardy dolarů.

Právní a regulační status Tetheru je složitý a čelí řadě vyšetřování a obav z nedostatečné transparentnosti a plného krytí vydávaných mincí americkými dolary. Tento aspekt vyvolává diskuse o jeho bezpečnosti a spolehlivosti jako finančního nástroje. (CFI Team 2023)

Komunita okolo Tetheru zahrnuje širokou škálu obchodníků a investorů, kteří využívají Tether jako prostředek pro snadné přesuny hodnot mezi různými kryptoměnami a platformami.

Hlavním praktickým využitím Tetheru je jeho role jako stabilizátoru volatilních kryptoměn, umožňující uživatelům a obchodníkům uchovávat hodnotu bez nutnosti přechodu zpět do fiat měn. V České republice je Tether přijímán několika kryptoměnovými směnárnami a platformami.

Pokud jde o udržitelnost a environmentální dopad, Tether představuje menší zátěž oproti tradičním kryptoměnám, které vyžadují energeticky náročnou těžbu, vzhledem k tomu, že jeho vydávání a transakce jsou prováděny na existujících blockchainech bez dalšího významného energetického vstupu. (CFI Team 2023)

8.4.4 Binance Coin (BNB)

Binance Coin je kryptoměna, která byla vytvořena burzou Binance. Burza Binance byla založena v roce 2017, a Binance Coin (BNB) byl uveden na trh v rámci počáteční nabídky mincí (ICO) krátce po založení burzy. (BNB 2023)

Zakladatelem Binance a klíčovým členem projektového týmu je Changpeng Zhao, známý také jako CZ, který je významnou postavou v kryptoměnovém průmyslu. Pod jeho vedením se Binance rychle stala jednou z největších kryptoměnových burz na světě.(BNB 2023)

Tržní kapitalizace Binance Coinu se často řadí mezi prvních deset kryptoměn podle velikosti tržní kapitalizace, která může dosahovat několika miliard dolarů. Nejvyšší dosažená hodnota Binance Coinu byla zaznamenána v květnu 2021, kdy cena dosáhla přibližně 690 USD za jednotku. Cena za transakci s Binance Coinem závisí na aktuálních podmínkách sítě, ale obvykle je nižší ve srovnání s mnoha jinými hlavními kryptoměnami. (CoinMarketCap 2023)

Hlavní technologické charakteristiky Binance Coinu zahrnují jeho integraci s ekosystémem burzy Binance, včetně využití pro snížení poplatků za transakce, účast v tokenových prodejích a další výhody pro uživatele. Binance Coin původně využíval blockchain Ethereum s tokenovým standardem ERC-20, ale později byl převeden na Binance Chain, což je vlastní blockchain vyvinutý burzou Binance. (BNB 2023)

Distribuce nabídky Binance Coinu byla omezena na 200 milionů mincí, ale v rámci měnové politiky Binance probíhají pravidelné pálení mincí, což má za cíl snížit celkovou nabídku a zvýšit její hodnotu. (BNB 2023)

Historický vývoj cen Binance Coinu ukazuje rychlý růst po jeho uvedení na trh, s několika výraznými vzestupy, zejména během býčích trhů v letech 2019 a 2021.

Binance Coin je obchodován na burze Binance a řadě dalších platform, což zajišťuje vysokou míru likvidity s významnými denními obchodními objemy.

Právní a regulační status Binance Coinu, stejně jako celé burzy Binance, se setkává s pozorností regulačních orgánů v různých zemích, což ovlivňuje jeho právní pozici a dostupnost.

Komunita okolo Binance Coinu je úzce spojena s uživateli burzy Binance, kde je aktivně podporován vývoj a spolupráce na nových projektech a službách, které rozšiřují jeho použití a funkčnost.

Pokud jde o udržitelnost a environmentální dopad, Binance Chain a Binance Smart Chain jsou navrženy tak, aby byly energeticky efektivnější než mnohé jiné blockchainové platformy, které využívají PoW model. Oba tyto řetězce využívají konsenzusní mechanismus zvaný Byzantine Fault Tolerance (BFT), který je méně náročný na energetické zdroje a zajišťuje rychlejší a levnější transakce. Tímto způsobem Binance Chain a Binance Smart Chain snižují svůj uhlíkový otisk a přispívají k větší ekologické udržitelnosti v digitálním světě. (BNB 2023)

8.4.5 Solana (SOL) 

Solana je vysoce výkonná blockchainová platforma, která byla navržena pro podporu decentralizovaných aplikací a kryptoměn. Byla založena v roce 2017 Anatoly Yakovenkem, který společně s dalšími členy týmu vyvinul technologii, jež umožňuje dosáhnout vysoké rychlosti transakcí a škálovatelnosti. (Yakovenko 2023)

Tržní kapitalizace Solany často dosahuje několika miliard dolarů, což ji řadí mezi největší kryptoměny na trhu. Nejvyšší dosažená hodnota tržní kapitalizace byla zaznamenána v listopadu 2021, kdy cena jedné Solany dosáhla přibližně 260 USD. Cena za transakci na Solana blockchainu je známá svou nízkostí, což je jedna z klíčových vlastností platformy, přičemž se často pohybuje okolo několika centů. (CoinMarketCap 2023)

Solana využívá inovativní konsenzusní mechanismus známý jako Proof of History (PoH) společně s Proof of Stake (PoS), což umožňuje rychlé a efektivní zpracování transakcí. Mezi další technologické vlastnosti patří podpora pro smart

kontrakty a možnosti vysoké škálovatelnosti díky kombinaci těchto konsenzusních mechanismů, které umožňují zpracování až tisíců transakcí za sekundu. (Yakovenko 2023)

Celková nabídka Solany je limitována na 489 milionů mincí, z nichž velká část je již v oběhu. Měnová politika zahrnuje stále pokračující procesy jako je staking a validace, které podporují její hodnotu a zabezpečení sítě. (Yakovenko 2023)

Historický vývoj cen Solany odhaluje rychlý vzestup od jejího založení, přičemž cena dramaticky vzrostla zejména během roku 2021, což odráží rostoucí popularitu a přijetí této platformy.

Solana je obchodována na většině hlavních kryptoměnových burz, což jí poskytuje vysokou likviditu a značné denní obchodní objemy, které často přesahují stamiliony dolarů.

Právní a regulační status Solany se vyvíjí, stejně jako u mnoha kryptoměn, a je předmětem zkoumání a interpretace v různých jurisdikcích.

Komunita Solany je dynamická a rychle rostoucí, s velkým množstvím vývojářů a uživatelů, kteří přispívají k jejímu rozvoji a využívají její technologii pro různé aplikace.

Klíčové aplikace a praktické využití Solany zahrnují rychlé a nízkonákladové transakce, které jsou vhodné pro různé aplikace od mikroplateb po decentralizované finance (DeFi). Solana je rovněž populární pro vývoj a provoz herních platforem a digitálních kolekcí typu NFT. (Yakovenko 2023)

Udržitelnost a environmentální dopad Solany jsou relativně nízké ve srovnání s tradičními PoW blockchainy, díky jejímu efektivnímu konsensnímu mechanismu, který vyžaduje méně energetického vstupu.

8.4.6 USD Coin (USDC) 

USD Coin je stabilní kryptoměna, známá jako stablecoin, která je navázána na hodnotu amerického dolaru v poměru 1:1. Byla založena v roce 2018 společnostmi Circle a Coinbase. (Circle 2023)

Tržní kapitalizace USD Coinu se pohybuje v řádu desítek miliard dolarů, což reflektuje jeho pozici jako jednoho z nejvíce obchodovaných stablecoinů na trhu. Cena za transakci se může lišit v závislosti na zvolené blockchainové síti, ale obecně jsou náklady na transakce s USD Coinem nízké díky efektivitě a širokému přijetí stablecoinů pro převody mezi tradičními a digitálními měnami. (CoinMarketCap 2023)

Hlavní technologické charakteristiky USD Coinu zahrnují jeho dostupnost na několika blockchainech, včetně Ethereum, což zajišťuje interoperabilitu a flexibilitu při transakcích. USD Coin nepoužívá vlastní konsenzní mechanismy jako PoW nebo PoS, protože jeho hodnota je přímo kryta dolarovými rezervami. (Circle 2023)

Celková nabídka USD Coinu je dynamická a mění se v závislosti na poptávce a množství dolarů držených v rezervě. Tyto rezervy jsou pravidelně auditovány externími firmami, což zajišťuje transparentnost a důvěryhodnost emise coinů.
Historický vývoj cen USD Coinu ukazuje jeho stabilitu, s cenou konzistentně blízkou 1 USD, což je klíčovým atributem pro stablecoin. (Circle 2023)

USD Coin je široce obchodován na mnoha kryptoměnových burzách, což zajišťuje jeho vysokou likviditu. Denní obchodní objemy často dosahují vysokých hodnot, což reflektuje jeho klíčovou roli jako most mezi tradičními finančními systémy a kryptoměnovým ekosystémem.

Právní a regulační status USD Coinu je poměrně stabilní, jelikož spolupráce s regulovanými finančními institucemi a pravidelné audity zajišťují soulad s americkými a mezinárodními finančními předpisy.

Komunita okolo USD Coinu zahrnuje široké spektrum uživatelů od individuálních investorů po velké finanční instituce, které využívají USD Coin pro své operace z důvodu jeho stability a efektivity.

Klíčové aplikace a praktické využití USD Coinu zahrnují mezinárodní převody peněz, platby, ukládání hodnoty a použití ve světě decentralizovaných financí (DeFi), kde poskytuje stabilní a spolehlivý prostředek pro transakce.

Udržitelnost a environmentální dopad USD Coinu jsou minimální, neboť se neopírá o energeticky náročné procesy těžby jako některé jiné kryptoměny, a jeho operace jsou založeny na efektivnějších blockchainových technologiích. (Circle 2023)

8.4.7 XRP

XRP je kryptoměna, která je známá pro své rychlé a efektivní přeshraniční platby. Byla založena v roce 2012 společností Ripple Labs, která se zaměřuje na vytváření lepších platebních řešení pro globální finanční systém. (Chase a MacBrough 2018)

Tržní kapitalizace XRP často dosahuje několika miliard dolarů, což ji řadí mezi největší kryptoměny na trhu. Nejvyšší dosažená hodnota XRP byla zaznamenána v lednu 2018, kdy cena dosáhla téměř 3,84 USD. Cena za transakci s XRP je extrémně nízká, což je jedním z důvodů, proč je populární pro rychlé a levné mezinárodní převody. (CoinMarketCap 2023)

Hlavní technologické charakteristiky XRP zahrnují použití konsenzusního algoritmu Ripple Protocol Consensus Algorithm (RPCA), místo běžnějších systémů jako je PoW nebo PoS. Tento algoritmus umožňuje rychlé a energeticky úsporné transakce.

Celková nabídka XRP je pevně stanovena na 100 miliard jednotek, z nichž většina byla vydána při založení sítě. Aktuálně je v oběhu méně než polovina této nabídky.

Historický vývoj cen XRP ukazuje značnou volatilitu, s obdobími výrazných cenových vzestupů a poklesů, což často odráží obecné trendy na trhu kryptoměn.
XRP je obchodováno na mnoha kryptoměnových burzách po celém světě, což mu zajišťuje vysokou likviditu a značné denní obchodní objemy.

Komunita okolo XRP je velmi aktivní, s velkým počtem podporovatelů a vývojářů, kteří pracují na rozšíření jeho použití a integrace do finančních systémů.

Klíčové aplikace a praktické využití XRP zahrnují jeho roli jako prostředku pro rychlé a nákladově efektivní mezinárodní platby, což je podpořeno širokou adopcí mezi finančními institucemi prostřednictvím RippleNetu. (Chase a MacBrough 2018)

Udržitelnost a environmentální dopad XRP jsou relativně nízké ve srovnání s mnoha jinými kryptoměnami, díky použití energeticky úsporného konsenzusního algoritmu, což činí XRP atraktivnějším z hlediska ekologické udržitelnosti.

8.4.8 Dogecoin (DOGE)

Dogecoin je kryptoměna, která byla původně vytvořena jako parodie na množství vážně míněných kryptoměn. Byla založena v prosinci 2013 Jacksonem Palmerem a Billym Markusem s cílem zjednodušit používání kryptoměn a zpřístupnit je širšímu publiku.(Dogecoin 2023)

Tržní kapitalizace Dogecoinu často kolísá, avšak v obdobích vysokého zájmu veřejnosti může dosáhnout několika miliard dolarů. Nejvyšší dosažená hodnota byla zaznamenána v květnu 2021, kdy cena jednoho Dogecoinu dosáhla přibližně 0,73 USD. Cena za transakci s Dogecoinem je obvykle nízká, což odpovídá jeho původnímu záměru být dostupnou a uživatelsky přívětivou kryptoměnou.(CoinMarketCap 2023)

Hlavní technologické charakteristiky Dogecoinu zahrnují využití konsenzusního algoritmu PoW, podobně jako Bitcoin. Avšak Dogecoin používá algoritmus Scrypt, který je méně náročný na hardware, což umožňuje širší zapojení veřejnosti do procesu těžby.(Dogecoin 2023)

Celková nabídka Dogecoinů je teoreticky neomezená, což je významný rozdíl oproti mnoha jiným kryptoměnám s pevně stanovenou maximální nabídkou. Aktuálně je v oběhu přes 130 miliard Dogecoinů a každý rok je vytěženo několik miliard nových mincí.(Dogecoin 2023)

Historický vývoj cen Dogecoinu ukazuje několik období rychlého růstu, které často reflektují širší zájem veřejnosti a mediální pokrytí, zejména v kontextu sociálních médií a veřejných osobností, jako je Elon Musk, který často vyjadřuje svou podporu této měně.

Dogecoin je obchodován na mnoha kryptoměnových burzách a díky své popularitě si udržuje vysokou likviditu a značné denní obchodní objemy.

Právní a regulační status Dogecoinu je podobný jako u ostatních kryptoměn, avšak specifické regulační výzvy nejsou často zdůrazňovány vzhledem k jeho původně humornému charakteru.

Komunita Dogecoinu je známá svou přátelskou atmosférou a činnostmi, které často zahrnují charitativní sbírky a jiné komunitní projekty. Tato aktivní a zapojená komunita je klíčovým prvkem jeho dlouhodobé popularity.

Klíčové aplikace a praktické využití Dogecoinu zahrnují jeho roli jako prostředku pro tipování a drobné transakce na internetu, kde je ceněn pro svou rychlost a nízké transakční náklady.(Dogecoin 2023)

8.4.9 Toncoin (TON)

Toncoin je kryptoměna, která byla vyvinuta původně pod hlavičkou projektu Telegram Open Network, avšak po právních sporech s americkými regulátory byl projekt přejmenován a nyní je veden nezávislou komunitou pod názvem The Open Network. Tento projekt byl zahájen v roce 2018. (TON 2023)

Tržní kapitalizace Toncoinu se pohybuje v řádech několika miliard dolarů, čímž se řadí mezi významné hráče na trhu kryptoměn. Cena za transakci s Toncoinem je nízká, což podporuje jeho použití pro různé druhy platebních transakcí a smart kontraktů. (CoinMarketCap 2023)

Hlavní technologické charakteristiky Toncoinu zahrnují využití unikátního konsenzusního mechanismu a podporu pro různé typy operací, včetně smart kontraktů a decentralizovaných aplikací. Díky tomu je Toncoin vhodný pro širokou škálu aplikací od plateb až po komplexní decentralizované služby. (TON 2023)

Celková nabídka Toncoinů je stanovena na 5 miliard jednotek, z nichž většina je postupně uvolňována do oběhu podle plánu, který má zajistit dlouhodobou udržitelnost a hodnotu měny. (TON 2023)

Historický vývoj cen Toncoinu ukazuje jeho růstový potenciál, zejména v kontextu rostoucího zájmu o decentralizované finance a služby propojené s populární komunikační platformou Telegram.

Toncoin je obchodován na několika hlavních kryptoměnových burzách a díky své propojenosti s Telegramem si udržuje vysokou míru pozornosti a likviditu.

Právní a regulační status Toncoinu je složitější vzhledem k jeho historii a změnám ve vedení projektu. Nicméně komunitní přístup a nezávislost projektu z něj činí atraktivní volbu pro investory hledající inovativní a autonomní kryptoměnu.

Komunita kolem Toncoinu je silná a činná, s mnoha vývojáři a uživateli, kteří spolupracují na rozšíření možností využití Toncoinu a na integraci s dalšími blockchainovými projekty a technologiemi.

Klíčové aplikace a praktické využití Toncoinu zahrnují jeho využití pro decentralizované finance, smart kontrakty a integraci do Telegramu, což umožňuje rychlé a bezpečné komunikační a transakční operace mezi uživateli platformy. (TON 2023)

Udržitelnost a environmentální dopad Toncoinu jsou minimalizovány díky efektivním technologickým řešením, které zohledňují energetickou náročnost a snaží se o co nejnižší dopad na životní prostředí. (TON 2023)

8.4.10 Cardano (ADA)

Je kryptoměna, která byla navržena s důrazem na vědecký přístup a pečlivě zvažované architektury. Projekt Cardano byl založen v roce 2017 Charlesem Hoskinsonem, který je také jedním ze zakladatelů Etherea. (Cardano 2015)

Tržní kapitalizace Cardano dosahuje desítek miliard dolarů, což reflektuje jeho významnou pozici na trhu kryptoměn. Nejvyšší dosažená hodnota Cardana byla

zaznamenána v roce 2021, kdy cena jednoho ADA, což je jednotka Cardana, přesáhla 3 USD. Cena za transakci v síti Cardano je relativně nízká, což je umožněno využitím efektivního konsenzusního mechanismu. (CoinMarketCap 2023)

Hlavní technologické charakteristiky Cardana zahrnují použití konsenzusního algoritmu PoS s názvem Ouroboros. Tento mechanismus je navržen tak, aby byl energeticky účinnější a bezpečnější ve srovnání s tradičními systémy PoW. Cardano také nabízí podporu pro smart kontrakty a decentralizované aplikace, což umožňuje široké využití v různých oblastech. (Cardano 2015)

Celková nabídka Cardana je stanovena na 45 miliard jednotek ADA, z nichž většina je již v oběhu. Měnová politika Cardana je zaměřena na dlouhodobou udržitelnost a stabilitu hodnoty.

Historický vývoj cen Cardana ukazuje výrazný růst, zejména během období zájmu o kryptoměny v roce 2021. Vývoj cen také odráží postupné uznání technologických inovací a širší adopce Cardana v kryptoměnovém ekosystému.

Cardano je široce obchodováno na mnoha kryptoměnových burzách, kde si udržuje vysokou likviditu a značné denní obchodní objemy. Toto zajišťuje snadný přístup a obchodování pro investory a uživatele.

Právní a regulační status Cardana je v souladu s mezinárodními standardy, a projekt se snaží aktivně spolupracovat s regulátory, aby zajistil plnou kompatibilitu s právními normami.

Komunita okolo Cardana je rozsáhlá a aktivní, s velkým množstvím vývojářů, výzkumníků a uživatelů, kteří se podílejí na rozvoji a implementaci nových technologií a aplikací.

Klíčové aplikace a praktické využití Cardana zahrnují jeho použití ve finančních službách, zdravotnictví a vládních systémech, kde jeho technologické řešení umožňuje zvýšení bezpečnosti, transparentnosti a efektivity. (Cardano 2015)

Udržitelnost a environmentální dopad Cardana jsou minimalizovány díky použití konsensního algoritmu PoS, který je výrazně méně energeticky náročný než tradiční metody těžby kryptoměn.

9 Závěr

V této bakalářské práci byl prozkoumán potenciál kryptoměn a technologie, které je obklopují, s důrazem na jejich vývoj, technické aspekty a ekonomický dopad. Práce systematicky představuje kryptoměny nejen z hlediska jejich finančního a investičního významu, ale i jejich technologické podstaty, která je základem pro jejich fungování a inovace v digitálním světě.

Zvláštní pozornost byla věnována deseti nejvýznamnějším kryptoměnám, jejichž podrobná analýza ukazuje rozmanitost a specifika každé z nich. Toto porovnání není jen teoretické, ale je podloženo aktuálními daty a trendy v kryptoměnovém sektoru, což práci dodává praktickou relevanci. Důraz byl kladen na technologii blockchainu, která je fundamentálním prvkem pro většinu kryptoměn, a na rozličné způsoby jejího využití, od zajištění bezpečnosti a transparentnosti transakcí až po možnosti využití ve smart kontraktech a decentralizovaných aplikacích.

Kapitola o ekonomických aspektech kryptoměn zdůrazňuje jejich rostoucí význam jako alternativní investiční příležitost, která může významně ovlivnit finanční trhy a nabízí nové možnosti pro investory. Práce také osvětluje regulační a bezpečnostní výzvy, které kryptoměny představují, a nabízí pohled na potenciální budoucí vývoj v této oblasti.

Celkově práce poskytuje důkladný přehled o kryptoměnách a technologických principech, na nichž jsou založeny, a zdůrazňuje význam neustálého vzdělávání a adaptace ve světě, který je stále více digitální a kde kryptoměny hrají stále důležitější roli.

10 Zkratky

ASIC	Application Specific Integrated Circuit
BTC	Bitcoin
ETH	Ethereum
DOGE	Dogecoin
XRP	Ripple
USDT	Theter
USDC	USDCoin
SOL	Solana
TRX	Tron
BNB	Binance coin
ADA	Cardano
CPU	Central Processing Unit
FPGA	Field Programmable Gate Array
GPU	Graphics Processing Unit
HDD	Hard disk drive
PoC	Proof of Capacity
PoS	Proof of Stake
PoW	Proof of Stake
P2P	Peer to peer
PoST	Proof of Space and Time
AES	Advanced Encryption Standard
HSM	Hardware Security Module
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
DAG	Directed Acyclic Graph
TBX	Tenebrix
KDF	key derivation function
LTC	Litecoin
DOGE	Dogecoin
EMC	Einsteinium

dPoW	delayed Proof of Work
APoW	Adaptive Proof of Work
DApps	decentralized application
DeFi	Decentralized finance
NFT	non-fungible token
CEX	Centralized Exchanges
DEX	decentralized exchange
WBTCB	world bitcoin business

11 Seznam použitých zdrojů

ANURINA, Olha, 2023. *How to Create a Cryptocurrency Step by Step | Updated Guide 2023* [online] [vid. 2024-05-03]. Dostupné z: https://mlsdev.com/blog/how-to-create-your-own-cryptocurrency

A.S, Alza, 2020. Proof of Work a Proof of Stake (VŠE, CO VÍME) | Alza.cz. *Alza* [online] [vid. 2024-05-01]. Dostupné z: https://www.alza.cz/proof-of-work-a-proof-of-stake

A.S, Alza, 2022. Hardwarové peněženky pro kryptoměny (INFORMACE) | Alza.cz. *Alza* [online] [vid. 2023-08-10]. Dostupné z: https://www.alza.cz/hardwarove-penezenky-pro-kryptomeny

BEATTIE, Andrew, 2022. The History of Money: From Bartering to Banknotes to Bitcoin. *Investopedia* [online] [vid. 2023-08-16]. Dostupné z: https://www.investopedia.com/articles/07/roots_of_money.asp

BITCOMAT.COM, 2023. Kúpiť Bitcoin (BTC) a iné kryptomeny z našich ATM. *bitcomat.com* [online] [vid. 2023-11-26]. Dostupné z: https://bitcomat.com/sk

BNB, 2023. BNB Chain - Build Web3 dApps on the Most Popular Blockchain. *BNB Chain* [online] [vid. 2023-08-09]. Dostupné z: https://www.bnbchain.org/en

CARDANO, 2015. *Introduction* [online] [vid. 2023-08-09]. Dostupné z: https://docs.cardano.org/introduction/

CFI TEAM, 2023. Tether. *Corporate Finance Institute* [online] [vid. 2024-05-03]. Dostupné z: https://corporatefinanceinstitute.com/resources/cryptocurrency/tether/

CIRCLE, 2023. *Ushering in the next chapter for USDC* [online] [vid. 2024-05-03]. Dostupné z: https://www.circle.com/blog/ushering-in-the-next-chapter-for-usdc

COINDOO, 2023. Hard Drive Mining | Your Comprehensive Guide. *Coindoo* [online]. [vid. 2024-05-02]. Dostupné z: https://coindoo.com/hard-drive-mining/

COINMARKETCAP, 2023. Cryptocurrency Prices, Charts And Market Capitalizations. *CoinMarketCap* [online] [vid. 2023-08-09]. Dostupné z: https://coinmarketcap.com/

DHIR, Rajeev, 2022. Pump-and-Dump: Definition, How the Scheme is Illegal, and Types. *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/terms/p/pumpanddump.asp

DOGECOIN, 2023. *Do Only Good Everyday* [online] [vid. 2024-05-03]. Dostupné z: https://dogecoin.com/

ETHEREUM, 2023. Ethereum Whitepaper. *ethereum.org* [online] [vid. 2023-08-09]. Dostupné z: https://ethereum.org

ETHEREUM.ORG, 2023. Ethash. *ethereum.org* [online] [vid. 2023-11-27]. Dostupné z: https://ethereum.org

FRANKENFIELD, Jake, 2022. Cold Storage: What It Is, How It Works, Theft Protection. *Investopedia* [online] [vid. 2023-08-17]. Dostupné z: https://www.investopedia.com/terms/c/cold-storage.asp

FRANKENFIELD, Jake, 2023a. Hot Wallet: Definition, Types, Examples, and Safety Tips. *Investopedia* [online] [vid. 2023-08-17]. Dostupné z: https://www.investopedia.com/terms/h/hot-wallet.asp

FRANKENFIELD, Jake, 2023b. What Is a Hash? Hash Functions and Cryptocurrency Mining. *Investopedia* [online] [vid. 2023-08-16]. Dostupné z: https://www.investopedia.com/terms/h/hash.asp

GARNETT, Allie, 2023. How to Make a Cryptocurrency. *Investopedia* [online] [vid. 2024-05-03]. Dostupné z: https://www.investopedia.com/how-to-make-a-cryptocurrency-5215343

GCHARANG, 2023. Equihash: An Overview & Guide of the Equihash Algorithm. *Komodo Academy | En* [online] [vid. 2024-05-01]. Dostupné z: https://komodoplatform.com/en/academy/equihash-algorithm/

GRIŠKĖNAS, Saulius, 2023. *What is the SHA-256 algorithm, and how does it work? | NordVPN* [online] [vid. 2023-08-16]. Dostupné z: https://nordvpn.com/blog/sha-256/

HAYES, Adam, 2023a. Blockchain Facts: What Is It, How It Works, and How It Can Be Used. *Investopedia* [online] [vid. 2023-08-16]. Dostupné z: https://www.investopedia.com/terms/b/blockchain.asp

HAYES, Adam, 2023b. Proof of Capacity (Cryptocurrency) Overview. *Investopedia* [online] [vid. 2024-05-01]. Dostupné z: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp

HAYES, Adam, 2024. Peer-to-Peer (P2P) Service: Definition, Facts, and Examples. *Investopedia* [online] [vid. 2024-05-01]. Dostupné z: https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp

CHASE, Brad a Ethan MACBROUGH, 2018. *Analysis of the XRP Ledger Consensus Protocol* [online]. 20. únor 2018. B.m.: arXiv. [vid. 2023-08-09]. Dostupné z: http://arxiv.org/abs/1802.07242

CHEN, James, 2023. Fiat Money: What It Is, How It Works, Example, Pros & Cons. *Investopedia* [online] [vid. 2023-08-16]. Dostupné z: https://www.investopedia.com/terms/f/fiatmoney.asp

CHEN, James, 2024. Ponzi Schemes: Definition, Examples, and Origins. *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/terms/p/ponzischeme.asp

CHENG, 2022. Phishing: What it is And How to Protect Yourself. *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/terms/p/phishing.asp

IBM, 2023. *What is Blockchain Security?* | *IBM* [online] [vid. 2023-08-16]. Dostupné z: https://www.ibm.com/topics/blockchain-security

INVESTOPEDIA TEAM, 2022. Cybersecurity: Meaning, Types of Cyber Attacks, Common Targets. *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/terms/c/cybersecurity.asp

INVESTOPEDIA TEAM, 2023. Mining Pool: Definition, How It Works, Methods, and Benefits. *Investopedia* [online] [vid. 2024-05-01]. Dostupné z: https://www.investopedia.com/terms/m/mining-pool.asp

INVESTOPEDIA TEAM, 2024a. What Are Crypto Tokens, and How Do They Work? *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/terms/c/crypto-token.asp

INVESTOPEDIA TEAM, 2024b. What Are Smart Contracts on the Blockchain and How Do They Work? *Investopedia* [online] [vid. 2024-05-01]. Dostupné z: https://www.investopedia.com/terms/s/smart-contracts.asp

INVESTOPEDIA TEAM, 2024c. What Was Mt. Gox? Definition, History, Collapse, and Future. *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/terms/m/mt-gox.asp

JAMESGRE, 2023. Guide to Cryptocurrency Regulation in the Czech Republic. *City - Dog* [online]. [vid. 2024-05-03]. Dostupné z: https://city-dog.cz/tech/jamesgre/guide-to-cryptocurrency-regulation-in-the-czech-republic/

KASPERSKY.COM, 2023a. What is cryptocurrency and how does it work? *www.kaspersky.com* [online] [vid. 2023-08-16]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency

KASPERSKY.COM, 2023b. What is Cryptography? *www.kaspersky.com* [online] [vid. 2023-08-16]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography

KRISHNAKUMAR, Arunkumar, 2022. Countries where Bitcoin (BTC) is legal. *Cointelegraph* [online] [vid. 2024-05-03]. Dostupné z: https://cointelegraph.com/explained/countries-where-bitcoin-btc-is-legal

LEDGER, 2023. Crypto Nodes: What Are They And How Do They Work? *Ledger* [online] [vid. 2024-05-01]. Dostupné z: https://www.ledger.com/academy/what-is-a-node-and-why-should-i-operate-one

LEDGER.COM, 2023. Hardware Wallet & Cold Wallet - Security for Crypto. *Ledger* [online] [vid. 2023-08-10]. Dostupné z: https://www.ledger.com

MCKINSEY.COM, 2022. *What is blockchain? | McKinsey* [online] [vid. 2023-08-16]. Dostupné z: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain

NAKAMOTO, Satoshi, 2009. Bitcoin: A Peer-to-Peer Electronic Cash System.

REIFF, Nathan, 2023a. How to Identify Cryptocurrency and ICO Scams. *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/tech/how-identify-cryptocurrency-and-ico-scams/

REIFF, Nathan, 2023b. What's the Environmental Impact of Cryptocurrency? *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/tech/whats-environmental-impact-cryptocurrency/

REIFF, Nathan, 2024. The Collapse of FTX: What Went Wrong With the Crypto Exchange? *Investopedia* [online] [vid. 2024-05-02]. Dostupné z: https://www.investopedia.com/what-went-wrong-with-ftx-6828447

RHODES, Delton, 2020. Scrypt Mining Algorithm Overview. *Komodo Academy | En* [online] [vid. 2023-11-27]. Dostupné z: https://komodoplatform.com/en/academy/scrypt-algorithm/

RHODES, Delton, 2023. CryptoNight: An Overview Of The CryptoNight Mining Algorithm. *Komodo Academy | En* [online] [vid. 2024-05-01]. Dostupné z: https://komodoplatform.com/en/academy/cryptonight/

SHARMA, Rakesh, 2023. Non-Fungible Token (NFT): What It Means and How It Works. *Investopedia* [online] [vid. 2023-11-26]. Dostupné z: https://www.investopedia.com/non-fungible-tokens-nft-5115211

SHOBHIT, Seth, 2023. GPU Usage in Cryptocurrency Mining. *Investopedia* [online] [vid. 2024-05-01]. Dostupné z: https://www.investopedia.com/tech/gpu-cryptocurrency-mining/

SIMPLECOIN, 2024. Simplecoin - Největší směnárna kryptoměn v ČR. *Simplecoin* [online] [vid. 2024-05-01]. Dostupné z: https://www.simplecoin.eu

STROUKAL, Dominik, 2020. *Dark Web: sex, drogy a bitcoiny*. První vydání. Praha: Grada. ISBN 978-80-271-2934-8.

STROUKAL, Dominik a Jan SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Třetí rozšířené vydání. Praha: Grada Publishing. ISBN 978-80-271-1043-8.

STUDYSMARTER.CO.UK, 2023. Evolution of Money: Introduction & Timeline | StudySmarter. *StudySmarter UK* [online] [vid. 2023-08-16]. Dostupné z: https://www.studysmarter.co.uk/explanations/macroeconomics/financial-sector/evolution-of-money/

SUDIPTO, Paul, 2022. What Is CPU Mining? How to Use Your Idle Computing Power. *G2* [online] [vid. 2024-05-01]. Dostupné z: https://www.g2.com/articles/cpu-mining

TETHER, 2023. *Transparency* [online] [vid. 2023-08-09]. Dostupné z: https://tether.to/en/transparency/#usdt

TON, 2023. TON: The Open Network for everyone. *TON* [online] [vid. 2024-05-03]. Dostupné z: https://ton.org

TREZOR.IO, 2023. *Trezor Hardware Wallet (Official) | Bitcoin & Crypto Security* [online] [vid. 2023-08-10]. Dostupné z: https://trezor.io/

WERNER, Vermaak, 2022. What Is ASIC Mining? | CoinMarketCap. *CoinMarketCap Academy* [online] [vid. 2024-05-01]. Dostupné z: https://coinmarketcap.com/alexandria/article/what-is-asic-mining

YAKOVENKO, Anatoly, 2023. Solana: A new architecture for a high performance blockchain.

12 Seznam obrázků

13 Seznam tabulek

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Petr Krtička**
Studium:	I1800718
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Kryptoměny a jejich potenciál**
Název bakalářské práce AJ:	CryptoCurrency and Their Potential

Cíl, metody, literatura, předpoklady:

Cílem práce je popsat a vysvětlit problematiku kryptoměn a souvisejících pojmů, jako jsou blockchain, hash, a pod. Podrobně vysvětlit, co jsou kryptoměny, k čemu slouží, jak fungují, a popsat v současnosti existující kryptoměny.

Praktická část bude zaměřena na vytvoření a popsání vlastní kryptoměny spolu s analýzou současného trhu.

Doporučená literatura:

Strukal, D., Skalický, J. Bitcoin - peníze budoucnosti. IDDE Praha 2015, ISBN 978-80-87733-26-4

Lánský, J. Kryptoměny. C.H.Beck, Praha 2018, ISBN 978-80-7400-722-4

Další literaturu doporučí zadavatel

Garantující pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	prof. RNDr. Peter Mikulecký, Ph.D.
Datum zadání závěrečné práce:	21.1.2020