Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra ekonomických teorií

Bakalářská práce

HODL a staking kryptoměn – analýza výnosnosti a rizikovosti

Ivan Shevrin

© 2026 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ivan Shevrin

Informatika

Název práce

HODL a staking kryptoměn – analýza výnosnosti a rizikovosti

Název anglicky

HODL and Staking of Cryptocurrencies – Analysis of Profitability and Risk

---

Cíle práce

Hlavním cílem bakalářské práce je identifikovat výnosnost a rizikovost strategií HODL a stakingu na základě reálných investičních dat a porovnat je s tradičními investičními nástroji, jako jsou termínované vklady a nízkorizikové podílové fondy.
Dílčím cílem teoretické části je popsat fungování kryptoměn, principy blockchainu, ekonomické aspekty stakingu a dlouhodobého držení digitálních aktiv. Dále bude rozebrán vliv volatility, likvidity a regulačního prostředí na tyto investiční strategie.

Metodika

Teoretická část bude založena na popisu kryptoměn, blockchainu a investičních strategií. Budou popsány základní pojmy, principy a faktory ovlivňující výnosnost a rizikovost investic do digitálních aktiv.

V praktické části bude použita kvantitativní analýza historických cenových dat a stakingových výnosů vybraných kryptoměn. Pro výpočet výnosnosti a rizikovosti budou využity metody finanční analýzy, například výpočet standardní odchylky, Sharpeho poměru a drawdownu. Výsledky budou porovnány s tradičními investičními aktivy, jako jsou termínované vklady a nízkorizikové podílové fondy.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

bitcoin, blockchain, DEFI, HOLD, investice, kryptoměny, riziko, staking, volatilita, výnosnost

---

Doporučené zdroje informací

Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2. vydání. O'Reilly Media, 2017. ISBN 978-1491954386.

Buterin, Vitalik. Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains. Seven Stories Press, 2022. ISBN 978-1644212486.

De Filippi, Primavera a Wright, Aaron. Blockchain and the Law: The Rule of Code. Harvard University Press, 2018. ISBN 978-0674976429.

Narayanan, Arvind et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016. ISBN 978-0691171692.

Svoboda, Tomáš. Kryptoměny a daně: Jak legálně optimalizovat své příjmy z kryptoměn. Computer Press, 2021. ISBN 978-8025149906.

Tapscott, Don a Tapscott, Alex. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio, 2016. ISBN 978-1101980132.

Předběžný termín obhajoby

2025/26 LS – PEF

Vedoucí práce

Ing. Pavel Hrdlička, MBA, Ph.D.

Garantující pracoviště

Katedra ekonomických teorií

Elektronicky schváleno dne 15. 10. 2025

prof. Ing. PhDr. Lucie Severová, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 20. 10. 2025

prof. Ing. Lukáš Čechura, Ph.D.

Děkan

V Praze dne 11. 02. 2026

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci „HODL a staking kryptoměn – analýza výnosnosti a rizikovosti“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.03.2026 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu mé bakalářské práce Ing. Pavlu Hrdličkovi, MBA, Ph.D. za odborné vedení a cenné rady a za pomoc při orientaci v náročných otázkách. Jeho přístup a podpora významně přispěly ke kvalitnímu zpracování této práce.

HODL a staking kryptoměn – analýza výnosnosti a rizikovosti

Abstrakt

Bakalářská práce se zaměřuje na problematiku investování do kryptoměn prostřednictvím kombinované strategie HODL a stakingu. Práce zkoumá efektivitu těchto metod na blockchainu Solana a jejich schopnost generovat pasivní příjem v kontextu tržní volatility. Teoretická část definuje klíčové technologické principy, jako je mechanismus Proof-of-Stake, a popisuje aktuální legislativní rámec v České republice, včetně daňových změn platných od roku 2025.

Praktická část se věnuje kvantitativní analýze reálného investičního portfolia spravovaného v peněžence Phantom. Na základě tržních dat je vypočítána výnosnost a rizikovost. Výnosnost je počítána pomocí čistého zhodnocení, rizikovost investice je spočítána prostřednictvím ukazatelů Max Drawdown a Sharpeho poměru. Získané výsledky jsou následně konfrontovány s výkonností konzervativních nástrojů, konkrétně termínovaných vkladů, a s vývojem akciového indexu S&P 500.

Klíčová slova: bitcoin, blockchain, DEFI, HOLD, investice, kryptoměny, riziko, staking, volatilita, výnosnost

HODL and Staking of Cryptocurrencies – Analysis of Profitability and Risk

Abstract

The bachelor thesis focuses on the issue of investing in cryptocurrencies through the combined strategy of HODL and staking. The thesis examines the efficiency of these methods on the Solana blockchain and their ability to generate passive income in the context of market volatility. The theoretical part defines key technological principles, such as the Proof-of-Stake mechanism, and describes the current legislative framework in the Czech Republic, including tax changes effective from 2025.

The practical part is devoted to the quantitative analysis of a real investment portfolio managed in the Phantom wallet. Based on market data, profitability and risk are calculated. Profitability is calculated using ROI, while investment risk is calculated through Max Drawdown and Sharpe ratio indicators. The obtained results are subsequently compared with the performance of conservative instruments, specifically term deposits, and with the development of the S&P 500 stock index.

Keywords: bitcoin, blockchain, DeFi, HODL, investment, cryptocurrencies, risk, staking, volatility, profitability

Obsah

1 Úvod **13**

2 Cíl práce a metodika **14**

2.1 Cíl práce 14

2.2 Metodika 14

3 Teoretická východiska **15**

3.1 Výpočetní technika a Internet 15

3.1.1 Vývoj výpočetní techniky 15

3.1.2 Von Neumannova architektura 17

3.1.3 Moderní počítačové architektury 18

3.2 Internet 20

3.2.1 Vznik a historie Internetu (ARPANET) 21

3.2.2 Základní principy fungování Internetu (TCP/IP model) 22

3.3 Peníze, bankovnictví a nástup virtuálních měn 25

3.3.1 Peníze: historie a evoluce 25

3.3.2 Funkce peněz 28

3.3.3 Vlastnosti peněz 29

3.3.4 Struktura bankovního systému ČR 30

3.3.5 Virtuální peníze 33

3.4 Kryptografie 35

3.4.1 Symetrické a asymetrické šifrování 35

3.4.2 Hašovací funkce 39

3.4.3 Digitální podpisy 40

3.5 Blockchain 42

3.5.1 Základní principy a vlastnosti blockchainu 42

3.5.2 Struktura bloku, transakcí a Merkle tree 43

3.5.3 Kryptoměny 45

3.5.4 Ekologické dopady konceptu Proof-of-Work 47

3.5.5 Koncept Proof-of-Stake 49

3.5.6 Investiční strategie v prostředí blockchainu 50

4 Vlastní práce **53**

4.1 Solana (SOL) 53

4.1.1 Staking na síti Solana 54

4.1.2 Popularita a tržní hodnota 54

4.2 Phantom Wallet (Phantom) 54

4.2.1 Bezpečnost a auditní přístupy 55

4.2.2 Staking a integrace se Solana 55

4.3 Nákup a staking SOL kartou přes Phantom Wallet 55

4.3.1 Vytvoření peněženky v Phantom ... 56
4.3.2 Nákup SOL platební kartou v Phantom ... 57
4.3.3 Staking SOL v peněžence Phantom ... 58
4.4 Výnosy z relativně bezpečných investic ... 60
4.4.1 Investice do fondu sledujícího S&P 500 ... 60
4.4.2 Investice do vládních státních dluhopisů ... 62
4.4.3 Spořicí produkty v ČR ... 63
4.5 Vyhodnocení stakingu ... 65

5 Vysledky a diskuse ... 68
5.1 Vysledky ... 68
5.2 Diskuse ... 70

6 Závěr ... 72

7 Seznam použitých zdrojů ... 74

8 Přílohy ... 80

Seznam obrázků

Obrázek č. 1: Von Neumannovo schéma……..17
Obrázek č. 2: Symetrické šifrování……...36
Obrázek č. 3: Asymetrické šifrování……37
Obrázek č. 4: Princip fungování transakcí v blockchainu……44
Obrázek č. 5: Úvodní obrazovka a vytvoření nové peněženky v aplikaci Phantom……56
Obrázek č. 6: Recovery Phrase a vytvoření uživatelského jména v aplikaci Phantom……57
Obrázek č. 7: Úvodní obrazovka, nákup kryptoměny SOL a zobrazení tokenů v peněžence Phantom……58
Obrázek č. 8: Spuštění procesu stakingu a výběr validátora v aplikaci Phantom……..59
Obrázek č. 9: Zadání částky k delegování a potvrzení transakce……...60
Obrázek č. 10: Roční reálné výnosy indexu S&P 500 od roku 1950……..61
Obrázek č. 11: Roční výnosy českých státních dluhopisů od roku 2000……...62
Obrázek č. 12: Vývoj úrokových sazeb České národní banky 2017-2025……64
Obrázek č. 13: Ukončení stakingu a hlavní okno peněženky Phantom……..66
Obrázek č. 14: Vývoj ceny Solana od 12.10.2025……66
Obrázek č. 15: Vývoj hodnoty portfolia v CZK během stakingu……...68
Obrázek č. 16: Porovnání procentuálního zhodnocení nástrojů……69

Seznam tabulek

Tabulka č. 1: Přehled generací počítačů a jejich klíčových charakteristik……16
Tabulka č. 2: Srovnání Von Neumannovy a Harvardské architektury……19
Tabulka č. 3: Vrstvy modelu TCP/IP a jejich hlavní funkce/protokoly……24
Tabulka č. 4: Historické formy peněz a jejich charakteristiky……...27
Tabulka č. 5: Srovnání symetrického a asymetrického šifrování……38
Tabulka č. 6: Vlastnosti kryptografických hašovacích funkcí……...39
Tabulka č. 7: Využití hašovacích funkcí v kryptoměnách a blockchainu……..39
Tabulka č. 8: Přehled a vlastnosti vybraných kryptografických hašovacích funkcí……..40
Tabulka č. 9: Srovnání kryptoměn……46
Tabulka č. 10: Modelace ročních emisí CO_2 při různé intenzitě využití fosilních paliv…..48
Tabulka č. 11: Environmentální dopady konsenzuálního mechanismu Proof-of-Work……48
Tabulka č. 12: Srovnání PoW a PoS……..49
Tabulka č. 13: Charakteristiky jednotlivých strategií……51

Tabulka č. 14: Výpočet čistého výnosu u investice do S&P 500 62
Tabulka č. 15: Výpočet čistého výnosu u státních dluhopisů 63
Tabulka č. 16: Výpočet čistého výnosu u spořicího účtu 64
Tabulka č. 17: Srovnání čistého zhodnocení investice 500 CZK 65
Tabulka č. 18: Přehled výsledků stakingu 67
Tabulka č. 19: Srovnání výnosnosti a rizika investičních nástroje 69

Seznam použitých zkratek

ALU – Aritmeticko-logická jednotka
AML – Anti-Money Laundering
ARP – Address Resolution Protocol
ARPANET – Advanced Research Projects Agency
ASIC – Application-Specific Integrated Circuit
CBDC – Central Bank Digital Currency
DeFi – Decentralized Finance
DLT – Distributed Ledger Technology
ETF – Exchange Traded Fund
IoT – Internet of Things
IPv4 – Internet Protocol version 4
IPv6 – Internet Protocol version 6
KYC – Know Your Customer
MAC – Media Access Control
MSI – Medium Scale Integration
OS – Operační systém
P2P – Peer-to-peer
S&P 500 – Standard and Poor's 50
UCLA – University of California, Los Angeles
ULSI – Ultra Large Scale Integration
UTXO – Unspent Transaction Outputs
VHDL – VHSIC Hardware Description Language
VLSI – Very Large Scale Integration
VPN – Virtual Private Network
ČNB – Česká národní banka
ČR – Česká republika
ČVUT – České vysoké učení technické v Praze
EU – Evropská unie

1 Úvod

V posledních letech prochází finanční svět jednou z největších transformací ve své historii. Tradiční fiat měny již nemají monopolní postavení a konkurenci jim tvoří nové digitální měny. Tento posun je logickým výsledkem technologického pokroku posledních desetiletí – od prvních počítačů až po vznik globálního internetu. V takovém prostředí se objevily kryptoměny jako decentralizovaná alternativa k centralizovaným financím, které nabízejí nezávislost na státních institucích. Kryptoměny se navíc staly oblíbeným nástrojem investic a diverzifikace portfolií nejen soukromých investorů, ale také velkých institucionálních investorů.

V souvislosti s rostoucím zájmem o digitální aktiva řeší investoři důležitou a složitou otázku: jak v tomto vysoce nestabilním a volatilním prostředí nejen zachovat hodnotu aktiv, ale také efektivně vydělat? Tradiční strategie známá jako HODL (prosté dlouhodobé držení) s sebou nese vážné riziko, když kapitál leží ladem a je vystaven pouze cenovým výkyvům. Investor tak přichází o potenciální běžný výnos, který by mohl kompenzovat případné poklesy trhu.

Jedním z řešení tohoto problému je staking. Tento proces představuje způsob zvýšení hodnoty, který umožňuje držitelům kryptoměn (založených na principu Proof-of-Stake) aktivně se podílet na zajištění bezpečnosti sítě a ověřování transakcí. Při stakingu investoři uzamknou své kryptoměny, ale dostávají pravidelnou odměnu. Tento mechanismus je podobný úročení v bance, ale na rozdíl od banky funguje v decentralizovaném prostředí a často nabízí zajímavější úrokové sazby.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je identifikovat výnosnost a rizikovost strategií HODL a stakingu na základě reálných investičních dat a porovnat je s tradičními investičními nástroji, jako jsou termínované vklady a nízkorizikové podílové fondy. Tento obecný cíl je v práci konkretizován na kryptoměnu Solana (SOL) s využitím necustodiální peněženky, kde je cílem změřit efektivitu generování pasivního příjmu v krátkodobém horizontu a jeho reálnou hodnotu po započtení tržní volatility. Dílčím cílem je popsat fungování kryptoměn, principy blockchainu, ekonomické aspekty stakingu a dlouhodobého držení digitálních aktiv. V rámci tohoto dílčího cíle je záměrem analyzovat dopady nové legislativy platné v České republice od roku 2025, konkrétně zavedení časového a hodnotového testů a nařízení MiCA, na atraktivitu těchto investic pro drobné investory.

2.2 Metodika

Teoretická část bude sestavena na základě studia odborných dokumentů a literatury založených na popisu kryptoměn, blockchainu a investičních strategií. Zvláštní pozornost bude věnována mechanismu Proof-of-Stake, který představuje technický základ pro generování pasivního příjmu, a jeho odlišení od tradiční těžby.

Praktická část bude založena na empirickém výzkumu formou řízeného experimentu. V praktické části bude použita kvantitativní analýza historických cenových dat a stakingových výnosů vybraných kryptoměn. Pro tento účel bude realizována reálná investice ve výši 500 CZK do kryptoměny Solana (SOL) prostřednictvím necustodiální peněženky Phantom. Sběr dat bude probíhat v denních intervalech ve vymezeném období. Časový horizont experimentu bude stanoven na jeden kalendářní měsíc. Tento zkrácený úsek bude zvolen primárně za účelem technické verifikace procesu stakingu a ověření funkčnosti mechanismu připisování odměn, nikoliv pro simulaci dlouhodobého investičního cyklu.

Pro vyhodnocení úspěšnosti strategie budou aplikovány statistické metody. Pro výpočet výnosnosti a rizikovosti budou využity metody finanční analýzy, například výpočet standardní odchylky, Sharpeho poměru a drawdownu. Závěrem bude provedena komparativní analýza. Výsledky budou porovnány s tradičními investičními aktivy, jako jsou termínované vklady a nízkorizikové podílové fondy.

3 Teoretická východiska

3.1 Výpočetní technika a Internet

Pro pochopení komplexního fenoménu kryptoměn, jejich držení (HODL) a stakingu je nezbytné nejprve porozumět technologickým pilířům, na nichž jsou postaveny. Výpočetní technika a internet představují fundamentální infrastrukturu, která umožnila vznik a exponenciální růst digitálních měn. Tato kapitola se věnuje klíčovým historickým milníkům a principům těchto technologií.

3.1.1 Vývoj výpočetní techniky

Snaha lidstva o automatizaci výpočtů sahá hluboko do historie. Mezi nejstarší počítací pomůcky patří abakus, používaný v Číně již od 13. století. Blaise Pascal v roce 1642 vytvořil vlastní mechanický kalkulátor schopný sčítání a odčítání, který Gottfried Wilhelm von Leibniz v roce 1694 zdokonalil na tzv. krokový kalkulátor, jenž zvládal i násobení, dělení a výpočet druhé mocniny. Tyto rané stroje demonstrují kontinuální úsilí o zefektivnění a zpřesnění výpočetních procesů. Koncept programovatelnosti, neboli schopnosti stroje vykonávat různé úlohy na základě sady instrukcí, se objevil výrazně později. Charles Babbage je často považován za „otce počítače“ díky svému návrhu „analytického stroje“ z roku 1837. Ačkoliv tento stroj nebyl za jeho života dokončen, jeho koncepce zahrnující aritmetickou jednotku, paměť, vstupní jednotku a tiskárnu, řízenou programem na děrných štítcích, předjímala architekturu moderních počítačů. (1)

Vývoj výpočetní techniky nebyl vždy přímočarý a často se stávalo, že teoretické koncepty a návrhy předběhly technologické možnosti své doby. Babbageův analytický stroj je toho příkladem. Jeho komplexní návrh narážel na limity tehdejší mechanické výroby. Tento rozdíl mezi vidinou a technologickou realitou nám ukazuje, že i myšlenky o nové technologii mohou existovat dlouho předtím, než současná technologie dospěje do bodu, ve kterém bude možné je realizovat. Podobný vzorec lze pozorovat i v historii kryptoměn, kde některé základní kryptografické a síťové koncepty existovaly desítky let před vznikem Bitcoinu, který čekal na dostatečný výpočetní výkon a rozšíření internetu. Podrobný historický vývoj, od základů počítání přes klíčové matematické vynálezy jako nula a logaritmy až po elektronický počítač, je detailně popsán v publikaci „A History of Computing Technology“ od Michaela R. Williamse. (2)

Pochopení této evoluční cesty je klíčové pro ocenění komplexity současných digitálních systémů a pro uvědomění si, že i nejmodernější technologie staví na základech položených předchozími generacemi inovátorů. Následující tabulka č. 1 poskytuje přehled generací počítačů a jejich klíčových charakteristik.

Tabulka č. 1: Přehled generací počítačů a jejich klíčových charakteristik

Generace	Časové období	Klíčová technologie	Příklady počítačů	Hlavní charakteristiky/Přínosy
0.	1930–1945	Elektromagnetická relé	Zuse Z3, Harvard Mark I	Rozměrné, pomalé, první programovatelné stroje
1.	1945–1951	Elektronky	ENIAC, UNIVAC	Rychlejší než reléové, stále velké a energeticky náročné, využití pro vědecké a vojenské výpočty
2.	1951–1965	Tranzistory	IBM 7090, PDP-1	Menší, rychlejší, spolehlivější, nižší spotřeba energie, vznik OS a programovacích jazyků
3.	1965–1980	Integrované obvody (SSI, MSI, LSI)	IBM System/360, PDP-8	Další miniaturizace a zlevnění, vyšší výkon, minipočítače, multiprogramování
4.	1981–2000	Mikroprocesory (VLSI, ULSI)	IBM PC, Apple Macintosh	Osobní počítače, grafické uživatelské rozhraní, sítě, internet, masové rozšíření
Současnost	2000 – současnost	Vícejádrové procesory, mobilní procesory, SoC, cloud computing	Intel Core, AMD Ryzen, ARM	Vysoký výkon, mobilita, všudypřítomnost, paralelní zpracování, AI, IoT

Zdroj: vlastní zpracování dle (1) (2)

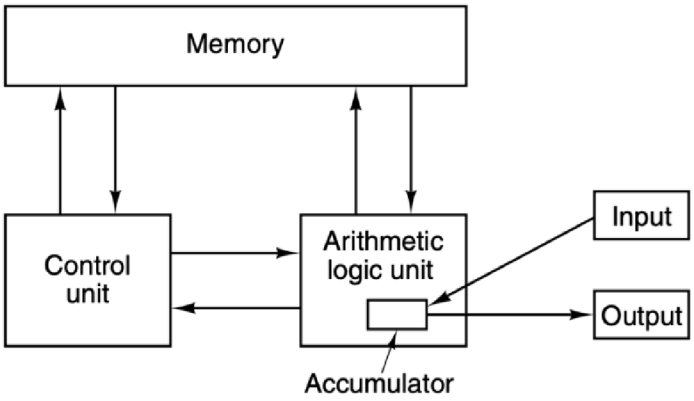
Historie výpočetní techniky, rozdělená do několika generací podle dominantních technologií, ukazuje postupný vývoj od prvních reléových a elektronkových počítačů přes tranzistorové a integrované obvody až po mikroprocesory a osobní počítače. Tento vývoj vedl k postupnému zmenšování techniky, zvyšování výkonu a větší dostupnosti výpočetních zařízení. Základní principy a architektura, na nichž je založen většina moderních počítačů, vychází z Von Neumannovy architektury, která se stala klíčovým modelem pro návrh počítačových systémů. (3)

3.1.2 Von Neumannova architektura

Zásadním milníkem ve vývoji počítačů byl návrh architektury, který v roce 1945 představil matematik John von Neumann. Tato tzv. Von Neumannova architektura (známá také jako Von Neumannův model nebo Princetonská architektura) se stala základním modelem pro drtivou většinu digitálních počítačů až do současnosti. (3)

Von Neumannova architektura je v informatice označení pro jednoduché schéma programovatelného počítače, které používá jednu sběrnici, na kterou jsou připojeny aktivní prvky (procesor, paměť, vstupy a výstupy). Její význam spočívá především v zavedení konceptu „uloženého programu“ (stored-program concept), kde jak instrukce programu, tak data, se kterými program pracuje, jsou uloženy ve stejné operační paměti a jsou zpracovávány sekvenčně. (4) Obrázek č. 1 znázorňuje Von Neumannovu architekturu.

Obrázek č. 1: Von Neumannovo schéma



Zdroj: Structured Computer Organization (1)

Podle Von Neumannova schématu se počítač skládá z pěti hlavních modulů:

1 Operační paměť: slouží k uchování zpracovávaného programu, zpracovávaných dat a výsledků výpočtů.
2 Aritmeticko-logická jednotka: provádí veškeré aritmetické výpočty (např. sčítání, násobení) a logické operace (např. porovnávání).
3 Řadič (řídicí jednotka): řídí činnost všech částí počítače pomocí řídicích signálů zasílaných jednotlivým modulům a přijímá od nich stavová hlášení.
4 Vstupní zařízení: umožňují vkládání programu a dat do počítače.
5 Výstupní zařízení: slouží k prezentaci výsledků zpracování. (5)

Centrální procesorová jednotka (CPU) je v tomto kontextu často definována jako procesor (ALU + řadič).

Ačkoliv byla Von Neumannova architektura revoluční a umožnila vznik univerzálních programovatelných počítačů, od počátku v sobě nesla inherentní omezení známé jako Von Neumannův bottleneck (Von Neumannovo úzké hrdlo). Toto omezení vyplývá ze skutečnosti, že instrukce i data sdílejí stejnou paměť a stejnou systémovou sběrnici pro přístup k této paměti. To znamená, že procesor nemůže současně načítat instrukci a pracovat s daty, což omezuje celkovou propustnost a výkon systému. Procesor je často nucen čekat na přenos dat z nebo do paměti. Tento problém se stal s rostoucí rychlostí procesorů a velikostí pamětí ještě výraznějším. (4)

Právě snaha o překonání tohoto úzkého hrdla se stala hnacím motorem pro mnoho inovací v počítačových architekturách. Navzdory tomuto omezení byl koncept uloženého programu, kdy instrukce jsou v paměti reprezentovány stejně jako data, naprosto zásadní. Umožnil totiž vznik softwaru, jaký známe v dnešní podobě. Programy mohly být snadno vytvářeny, modifikovány a nahrávány, což vedlo k vývoji operačních systémů, kompilerů, linkerů a dalších automatizovaných programovacích nástrojů. Bez této flexibility by komplexní softwarové systémy, včetně těch, na nichž běží kryptoměny, nemohly vzniknout. (2)

3.1.3 Moderní počítačové architektury

Současné počítače, ačkoliv stále z velké části vycházejí z Von Neumannových principů, se v mnoha ohledech od původního schématu liší. Tyto odlišnosti jsou výsledkem neustálé snahy o zvýšení výkonu, efektivity a přizpůsobení se novým požadavkům. Mezi základní odlišnosti patří:

- Multitasking: moderní počítače běžně zpracovávají více programů současně, což vede k lepšímu využití strojového času.
- Více procesorů: běžné jsou systémy s více procesory nebo vícejádrovými procesory, které umožňují paralelní zpracování.
- Kombinovaná I/O zařízení: existují vstupně/výstupní (I/O) zařízení, která umožňují jak vstup, tak výstup dat.
- Částečné zavádění programů: program se nemusí do paměti zavést celý, ale je možné zavádět pouze jeho části podle potřeby (virtualizace paměti, stránkování). (1)

Jednou z významných alternativ k Von Neumannově architektuře je Harvardská architektura. Jejím klíčovým rysem je oddělená paměť pro instrukce a oddělená paměť pro data, přičemž každá má vlastní sběrnici. Hlavním přínosem tohoto uspořádání je eliminace Von Neumannova bottlenecku, kdy současný přístup k instrukcím i datům výrazně akceleruje rychlost zpracování. Oddělení paměťových prostorů totiž efektivně zabraňuje tomu, aby byly přepsáné programové instrukce, ať už omylem nebo vlivem škodlivého kódu.

Harvardská architektura se často používá u jednočipových mikropočítačů a digitálních signálových procesorů, kde je prediktabilita výkonu a rychlý přístup k datům i instrukcím klíčová. (4) Následující tabulka č. 2 shrnuje klíčové rozdíly mezi Von Neumannovou a Harvardskou architekturou.

Tabulka č. 2: Srovnání Von Neumannovy a Harvardské architektury

Charakteristika	**Von Neumannova architektura**	**Harvardská architektura**
Paměť pro instrukce a data	Společná paměť	Oddělená paměť pro instrukce, oddělená paměť pro data
Sběrnice	Společná sběrnice pro instrukce i data	Oddělené sběrnice pro instrukce a data
Rychlost přenosu	Omezená (Von Neumannův bottleneck)	Potenciálně vyšší (možnost současného načítání instrukcí i dat)
Riziko přepsání programu	Vyšší (data mohou přepsat instrukce a naopak)	Nižší (oddělené paměťové prostory)
Typické použití	Univerzální počítače, osobní počítače, servery	Jednočipové mikropočítače, vestavěné systémy

Zdroj: vlastní zpracování dle (3) (5)

Další trendy v moderních architekturách zahrnují debatu mezi RISC (Reduced Instruction Set Computer) a CISC (Complex Instruction Set Computer). RISC architektury se vyznačují menším počtem jednodušších instrukcí, které lze vykonat rychleji, zatímco CISC architektury mají rozsáhlejší sadu komplexnějších instrukcí. Moderní procesory často kombinují prvky obou přístupů. Významnou roli hrají také specializované procesory, jako jsou grafické procesory (GPU), které jsou optimalizovány pro masivně paralelní výpočty, nebo numerické koprocesory. Architektura procesoru, včetně velikosti jeho slova (např. 32bitové, 64bitové), způsobu adresování paměti a konkrétní instrukční sady, významně ovlivňuje celkovou architekturu počítače. (4)

Vývoj počítačových architektur je neustálým hledáním optimálního kompromisu mezi výkonem, cenou, spotřebou energie a specializací pro konkrétní úlohy. Jak uvádí Kania: *„architektura je silně ovlivněna trendy v hardwarových i softwarových technologiích, přičemž nástup osobního mobilního computingu představuje další významný faktor formující budoucí potřeby a směřování vývoje mikroprocesorů“*. (8, s. 1)

Recenze knihy „Modern Computer Architecture and Organization“ zmiňuje klíčové koncepty moderních architektur, jako jsou digitální logika, jazyk VHDL pro popis hardwaru, techniky pro zvýšení výkonu jako caching (vyrovnávací paměti) a pipelining (zřetězené zpracování instrukcí), a nové instrukční sady jako RISC-V. (7)

Tato diverzifikace a neustálý vývoj mají přímý dopad na technologie jako je blockchain. Například energetická náročnost těžby kryptoměn založených na mechanismu Proof-of-Work (PoW), jako je Bitcoin, je úzce spjata s architekturou a výkonem specializovaného hardwaru (ASIC čipy, výkonné GPU). (6)

3.2 Internet

Internet je globální síť propojující miliardy zařízení, je naprosto nezbytnou infrastrukturou pro existenci, komunikaci a provoz kryptoměnových sítí. Pojem internet lze vymezit jako propojení počítačových sítí do jedné obří sítě, ve které spolu počítače vzájemně komunikují pomocí protokolů TCP/IP. Cílem lidí, kteří internet využívají, je vzájemně spolu komunikovat. To znamená, že počítače, které jsou k internetu připojené, si spolu vzájemně vyměňují data. (8) Blažková uvádí: *„Internet je decentralizovaná celosvětová síť spojující počítače různých vlastníků, která je odolná proti výpadku jedné nebo několika částí. Umožňuje sdílení dat, používání e-mailu a mnoho dalších služeb. Internet nekontroluje žádná autorita a celý systém je vybudován tak, aby se řídil sám.“* (9, s. 12)

Sebera ve své práci uvádí: *„Internet je v současnosti považován za fenomén lidstva. „Nebýt“ na Internetu znamená nepřizpůsobit se moderním trendům a svým způsobem být izolován. Zároveň je ovšem uživatel vystaven i rizikům a nebezpečím ať už ze strany počítačových virů nebo hackerů. Používáme-li toto celosvětově rozšířené médium, měli bychom být vybaveni i informacemi z oblasti bezpečnosti, antivirové a antispamové problematiky.“* (11, s. 156)

3.2.1 Vznik a historie Internetu (ARPANET)

Počátky internetu sahají do období studené války, konkrétně do 50. a 60. let 20. století. První snahy o dálkovou komunikaci mezi počítači byly motivovány vojenskými potřebami (např. poloautomatické radarové systémy) a potřebami velkých organizací (např. automatizované rezervační systémy aerolinií). Klíčovou roli v rané fázi sehrála agentura ARPA (Advanced Research Projects Agency) amerického ministerstva obrany. V roce 1962 iniciovala projekt počítačového výzkumu, jehož jedním z cílů bylo vytvořit robustní komunikační síť schopnou odolat i případnému jadernému útoku. (10)

Tato motivace vedla k přijetí dvou zásadních konstrukčních principů pro budoucí síť ARPANET:

1. Decentralizace: síť neměla mít žádné centrální řídicí místo, jehož zničením by došlo k ochromení celé sítě.
2. Paketový přenos dat: data měla být před odesláním rozdělena na menší části, tzv. pakety. Každý paket mohl putovat sítí k cíli jinou cestou a na místě určení se pakety opět složily do původní zprávy. Tento princip zvyšoval odolnost sítě, protože i při výpadku některých spojů mohly pakety najít alternativní trasy. (10)

První experimentální síť ARPANET byla spuštěna v roce 1969 a propojovala čtyři univerzitní uzly ve Spojených státech (UCLA, Stanford Research Institute, UC Santa Barbara a University of Utah). První komunikace proběhla 2. září 1969, resp. 29. října 1969. Síť se postupně rozrůstala a zdokonalovala. V roce 1972 Ray Tomlinson vyvinul první e-mailový program, který se rychle stal populární aplikací. V roce 1973 došlo k prvnímu transatlantickému spojení sítě ARPANET, a to s University College London ve Velké Británii. (12)

Původní síťový protokol ARPANETu, NCP (Network Control Program), se postupem času ukázal jako nedostatečný pro propojování různých typů sítí. Proto byla v 70. letech zahájena práce na nové sadě protokolů, známé jako TCP/IP (Transmission Control Protocol/Internet Protocol). Za hlavní architekty TCP/IP jsou považováni Vinton Cerf a Robert Kahn. Oficiální přechod sítě ARPANET z NCP na TCP/IP proběhl 1. ledna 1983. Tento krok je považován za klíčový moment vzniku internetu jako „sítě sítí", protože TCP/IP umožnilo propojení různorodých počítačových sítí do jednoho globálního systému. Pojem

„Internet" se začal používat přibližně v roce 1974, resp. 1987. V 80. letech došlo k dalšímu rozvoji. (12)

V roce 1983 byla z ARPANETu oddělena čistě vojenská síť MILNET. Americká Národní vědecká nadace (NSF) začala budovat vysokorychlostní síť NSFNET, která se stala páteřní sítí akademického internetu a postupně nahradila ARPANET v této roli. Byl zaveden systém doménových jmen (DNS) pro snazší adresaci počítačů. ARPANET byl oficiálně ukončen v roce 1990. Počátkem 90. let došlo k masivnímu rozšíření internetu i mimo akademickou a vojenskou sféru, zejména díky vzniku World Wide Web (WWW). Tim Berners-Lee v CERNu vyvinul v letech 1989-1991 základní technologie WWW, jako je jazyk HTML, protokol HTTP a první webový prohlížeč. Uvolnění prohlížeče Mosaic v roce 1993 a následně Netscape Navigator v roce 1994 zpřístupnilo internet široké veřejnosti a vedlo k jeho komercializaci. (12)

Československo bylo k internetu oficiálně připojeno 13. února 1992, kdy bylo realizováno připojení na Českém vysokém učení technickém (ČVUT) v Praze-Dejvicích. (13)

Principy decentralizace a odolnosti vůči selhání, které byly zakotveny již v počátcích ARPANETu, rezonují i v architektuře mnoha kryptoměn jako je například Bitcoin. Snaha o vytvoření systému, který není závislý na centrální autoritě a dokáže fungovat i při výpadku jednotlivých částí, je společným jmenovatelem. Bez existence a globálního rozšíření internetu by kryptoměny, tak jak je známe dnes, nemohly vzniknout ani fungovat. Internet poskytuje nezbytnou platformu pro peer-to-peer komunikaci uzlů kryptoměnových sítí, šíření transakcí a synchronizaci distribuované účetní knihy (blockchainu). (12)

3.2.2 Základní principy fungování Internetu (TCP/IP model)

Technickým základem dnešního internetu je rodina protokolů TCP/IP. Tato sada protokolů definuje, jakým způsobem mají být data paketizována, adresována, přenášena, směrována a přijímána v rámci propojených sítí. TCP/IP model je typicky popisován jako čtyřvrstvá architektura, která je zjednodušenou verzí sedmivrstvého referenčního modelu OSI (Open Systems Interconnection). (10)

Tyto vrstvy jsou:

1 **Vrstva síťového rozhraní**: je nejnižší vrstvou a zodpovídá za fyzický přenos dat přes konkrétní síťové médium (např. metalické kabely, optická vlákna,

bezdrátové Wi-Fi spoje). Zahrnuje technologie jako Ethernet, Wi-Fi a protokoly pro přístup k médiu. Stará se o adresaci na úrovni hardwaru (MAC adresy), rámcování dat a detekci chyb na fyzickém spoji. (10)

2 **Síťová vrstva**: hlavním úkolem této vrstvy je doručování datových paketů (datagramů) mezi zdrojovým a cílovým počítačem napříč různými sítěmi. Klíčovým protokolem této vrstvy je Internet Protocol (IP), který definuje globální adresní schéma (IP adresy) a zajišťuje směrování paketů, tedy hledání optimální cesty sítí. IP funguje na principu „maximální snahy", což znamená, že negarantuje doručení paketů, jejich správné pořadí ani ochranu proti ztrátě či duplikaci. Je to tzv. nespojovaná a nespolehlivá služba. Tato vrstva také zahrnuje protokoly jako ICMP (pro diagnostiku sítě, např. příkaz ping) a ARP (pro překlad IP adres na MAC adresy v lokálních sítích). Existují dvě hlavní verze IP protokolu: IPv4 (32bitové adresy) a novější IPv6 (128bitové adresy), která řeší problém vyčerpání adresního prostoru IPv4. (10)

3 **Transportní vrstva**: poskytuje komunikační služby mezi aplikacemi běžícími na koncových zařízeních. Rozlišuje mezi různými aplikacemi na stejném počítači pomocí čísel portů. (14) Nabízí dva hlavní protokoly:

- TCP (Transmission Control Protocol): poskytuje spolehlivou, spojovanou službu. Zajišťuje doručení dat ve správném pořadí, kontrolu chyb, potvrzování přijatých dat a řízení toku dat, aby nedošlo k zahlcení příjemce. Před samotným přenosem dat navazuje spojení mezi komunikujícími stranami. Používá se pro aplikace vyžadující vysokou spolehlivost (např. web, e-mail, přenos souborů).
- UDP (User Datagram Protocol): poskytuje jednoduchou, nespojovanou a nespolehlivou službu. Je rychlejší než TCP, protože nemá režii spojenou s navazováním spojení, potvrzováním a řízením toku. Používá se pro aplikace, kde je rychlost důležitější než stoprocentní spolehlivost, nebo které si spolehlivost řeší samy na aplikační úrovni (např. streamování videa, online hry, DNS). (14)

4 **Aplikační vrstva**: je nejvyšší vrstvou a poskytuje rozhraní a služby přímo pro uživatelské aplikace. Zahrnuje protokoly pro specifické síťové služby, jako jsou:

- HTTP (Hypertext Transfer Protocol): pro přenos webových stránek.
- FTP (File Transfer Protocol): pro přenos souborů.

- SMTP (Simple Mail Transfer Protocol): pro odesílání e-mailů.
- DNS (Domain Name System): pro překlad doménových jmen (např. www.example.com) na IP adresy (např. 192.0.2.1) a naopak. DNS je distribuovaný hierarchický systém, který je klíčový pro použitelnost internetu. (10)

Vrstvová architektura TCP/IP je jedním z klíčových důvodů úspěchu a adaptability internetu. Umožňuje flexibilitu a interoperabilitu, protože jednotlivé vrstvy mohou být vyvíjeny, modifikovány a nahrazovány relativně nezávisle na ostatních, pokud je zachováno definované rozhraní mezi nimi. Například síťová vrstva (IP) se nemusí starat o to, jaká konkrétní fyzická technologie (Ethernet, Wi-Fi) přenáší data na nejnižší úrovni, ani o to, jaká aplikace (webový prohlížeč, e-mailový klient) data na nejvyšší úrovni generuje či spotřebovává. Tento princip modularity, označovaný také jako „IP over everything" (IP může běžet nad jakoukoli přenosovou technologií) a „Everything over IP" (jakákoli aplikace může využívat IP pro komunikaci), umožnil internetu absorbovat nové technologie a služby bez nutnosti měnit jeho základní jádro. (10) Následující tabulka č. 3 přehledně shrnuje vrstvy modelu TCP/IP a jejich hlavní funkce:

Tabulka č. 3: Vrstvy modelu TCP/IP a jejich hlavní funkce/protokoly

	Hlavní funkce	**Příklady protokolů**
Aplikační vrstva	Poskytování síťových služeb aplikacím, formátování dat, správa sezení	HTTP, HTTPS, FTP, SMTP, DNS, Telnet
Transportní vrstva	Zajištění spolehlivého (TCP) nebo nespolehlivého (UDP) přenosu dat mezi procesy, segmentace a znovu sestavení dat, řízení toku	TCP, UDP
Síťová vrstva (Internetová)	Logická adresace (IP adresy), směrování paketů mezi sítěmi, fragmentace	IP (IPv4, IPv6), ICMP, ARP
Vrstva síťového rozhraní	Přenos bitů/rámců přes fyzické médium, fyzická adresace (MAC), přístup k médiu	Ethernet, Wi-Fi

Zdroj: vlastní zpracování dle (10) (12) (15)

Kryptoměnové protokoly, jako je protokol Bitcoinu, typicky operují na aplikační vrstvě modelu TCP/IP, případně přímo využívají služby transportní vrstvy (TCP nebo UDP) pro komunikaci mezi uzly v P2P síti. Spoléhají se na existující internetovou infrastrukturu pro přenos svých datových paketů (obsahujících transakce a bloky). Spolehlivost a dostupnost internetového připojení jsou tedy kritickými faktory pro fungování

kryptoměnových sítí. Případné problémy na nižších vrstvách internetu (např. nespolehlivost IP vrstvy) musí být řešeny mechanismy implementovanými na vyšších vrstvách, včetně samotných kryptoměnových protokolů, které si často zajišťují vlastní mechanismy pro ověření konzistence a doručení dat. (6)

3.3 Peníze, bankovnictví a nástup virtuálních měn

Peníze představují prostředek směny, uchovatele hodnoty a jednotku účetnictví. Jejich vývoj je úzce spjat s vývojem lidské společnosti. Od primitivního směnného obchodu (barter) se lidstvo postupně přesunulo k používání komoditních peněz (např. sůl, dobytek), dále k mincím, papírovým bankovkám, a nakonec k digitální podobě. V současnosti většina peněz existuje pouze v elektronické podobě jako zůstatky na bankovních účtech. Rejnuš O. uvádí, že: *„Ekonomická teorie považuje peníze za jeden z největších objevů lidstva. To vyplývá jednak z toho, že v moderní ekonomice je peněžní směna nutným předpokladem fungování všech existujících druhů trhů, jednak z toho důvodu, že v rámci finančního systému zabezpečují peníze ještě i další funkce, které postupně nabyly v průběhu svého vývoje. A to je také důvod, proč je zapotřebí věnovat jejich vývoji alespoň krátce pozornost.“* (16, s. 38)

Peníze jsou obecně přijímaným prostředkem směny, který usnadňuje obchodování se zbožím a službami. Vznikly jako odpověď na neefektivitu přímé výměny (barteru) a v průběhu času se vyvinuly do různých forem od hotovosti až po bezhotovostní zápisy na bankovních účtech. Moderní peníze se vyskytují především v bezhotovostní podobě a jejich většinu tvoří vklady na bankovních účtech. Celkový objem peněz v oběhu tak závisí nejen na činnosti centrální banky, ale i na komerčním bankovním sektoru. (17)

Pojem peníze je úzce spjat s pojmem měna, a proto je důležité mezi nimi rozlišovat, protože každý označuje něco jiného. Měna je specifičtějším termínem. Jedná se o peněžní systém, který je platný a právně upravený na území konkrétního státu. Aby mohla být určitá peněžní soustava považována za měnu, musí být oficiálně uznána státními institucemi, fungovat jako zákonné platidlo a zároveň plnit funkci uchování hodnoty v peněžní podobě. (19)

3.3.1 Peníze: historie a evoluce

Koncept peněz prošel dlouhým vývojem, který reflektoval měnící se potřeby společnosti, technologické možnosti a snahu o zefektivnění ekonomických interakcí. Nejstarší formou směny byl barterový obchod, tedy přímá výměna jednoho zboží nebo

služby za jiné zboží nebo službu, bez použití peněžního prostředníka. Tento systém fungoval v raných, malých a relativně jednoduchých ekonomikách. Jeho zásadní nevýhodou však byla nutnost dvojí shody potřeb. To znamená, že pro uskutečnění směny musel jedinec A, který nabízel zboží X a poptával zboží Y, najít jedince B, který nejenže poptával zboží X, ale zároveň nabízel zboží Y. S rostoucí dělbou práce a komplexitou obchodních vztahů se tento problém stával stále palčivějším a neefektivním. (21)

V reakci na neefektivitu barteru se postupně začaly objevovat všeobecné ekvivalenty, známé také jako zbožové (komoditní) peníze. Určité druhy zboží, které byly v dané společnosti všeobecně ceněné, trvanlivé, přenositelné a dělitelné, začaly plnit funkci prostředníka směny. Jako zbožové peníze v různých kulturách a obdobích sloužily například dobytek, sůl, plátno, kožešiny, mušle kauri, kakaové boby, obilniny, čaj, tabák, koření nebo různé nástroje. I když zbožové peníze představovaly pokrok oproti barteru, stále měly své nevýhody, jako:

- problematická dělitelnost (např. u dobytka),
- obtížná skladovatelnost,
- nízká trvanlivost u některých komodit (např. ryby),
- variabilita kvality.

Toto neustálé hledání univerzálního, snadno směnitelného, uchovatelného a standardizovaného statku bylo klíčovým motivem pro další vývoj peněžních forem. (21)

Následující Tabulka č. 4 poskytuje systematický přehled vývoje formy peněz a jejich klíčových atributů.

Tabulka č. 4: Historické formy peněz a jejich charakteristiky

Forma peněz	Základ hodnoty	Klíčové výhody	Klíčové nevýhody	Příklad
Barter	Přímá užitná hodnota směňovaného zboží/služby	Jednoduchost v malých komunitách	Nutnost dvojí shody potřeb, nedělitelnost některých statků, obtížné stanovení hodnoty	Výměna obilí za nástroje
Zbožové peníze	Užitná hodnota a všeobecná akceptace dané komodity	Usnadnění směny oproti barteru	Špatná dělitelnost, skladovatelnost, trvanlivost, variabilita kvality	Dobytek, sůl, mušle, plátno
Kovové mince	Vnitřní hodnota kovu (zlato, stříbro), ražba	Trvanlivost, dělitelnost, přenositelnost, vysoká hodnota v malém objemu, standardizace	Možnost znehodnocování (ořezávání, snižování obsahu drahého kovu), váha při velkých objemech	Stříbrné denáry, pražské groše, zlaté dukáty
Papírové peníze (zlatý standard)	Krytí drahým kovem (zlatem), směnitelnost	Snadná přenositelnost, dělitelnost (různé nominály)	Závislost na důvěře v emitenta a jeho schopnosti dostát závazku směnitelnosti	Bankovky směnitelné za zlato
Fiat peníze (nucený oběh)	Nařízení vlády, všeobecná důvěra a akceptace	Flexibilita pro monetární politiku, nízké výrobní náklady	Riziko inflace (při nadměrné emisi), závislost na důvěře ve stát a centrální banku	Současné národní měny (CZK, USD, EUR)
Elektronické peníze	Pohledávka vůči emitentovi, krytá fiat měnou	Rychlost a pohodlí transakcí, snadná evidence	Závislost na technologii a infrastruktuře, bezpečnostní rizika (kyberútoky)	Zůstatek na bankovním účtu, platební karta
Virtuální/ Kryptoměny	Důvěra v technologii, síť, algoritmus, poptávka/nabídka	Decentralizace (některé), transparentnost (některé), nízké transakční náklady (některé)	Vysoká volatilita, regulatorní nejistota, bezpečnostní rizika (ztráta klíčů), škálovatelnost	Bitcoin, Ethereum

Zdroj: vlastní zpracování dle (17) (19) (20)

Historie českých peněz sahá až do doby vlády Marie Terezie, kdy se v roce 1762 na území objevily první papírové peníze tzv. bankocetle. Tyto listiny však nebyly klasickými bankovkami, jak je známe dnes, ale spíše formou dluhopisů krytých zlatem. Významnou změnou prošla peněžní soustava po první světové válce, kdy bylo potřeba nahradit nefunkční a znehodnocené rakousko-uherské platidla novou měnou. Ministr financí Alois Rašín proto v roce 1919 zavedl tzv. kolkování bankovek a vytvořil základ pro vznik československé koruny, která se díky zavedení zlatého standardu brzy stala jednou z nejstabilnějších měn v Evropě. (23)

Po druhé světové válce byla v roce 1945 provedena měnová reforma, jejímž cílem bylo sjednotit různorodé měny, které se na území Československa nacházely (např. protektorátní,

slovenská nebo maďarská měna), a obnovit Národní banku Československou. Nové státovky se tiskly v londýnských tiskárnách. Po nástupu komunistického režimu následovala měnová reforma v roce 1953, která zrušila přídělový systém a zavedla nový cenový rámec, i když způsob provedení reformy způsobil ztrátu důvěry obyvatelstva v měnovou politiku státu. (24)

Další klíčový moment nastal po Sametové revoluci v roce 1989, kdy došlo ke změnám nejen politickým, ale i měnovým. Postupně byly z oběhu stahovány bankovky s komunistickými symboly a připravovala se nová měnová politika. Po rozpadu Československa v roce 1993 vznikla samostatná česká koruna. K oddělení měn došlo opět pomocí kolkování bankovek, které bylo provedeno bez znehodnocení jejich nominální hodnoty. Dnes je česká koruna národní měnou, jejíž bankovky tiskne Státní tiskárna cenin a mince razí Česká mincovna v Jablonci nad Nisou. Přestože se Česká republika dosud nepřipojila k eurozóně, česká koruna zůstává stabilní měnou. (22)

3.3.2 Funkce peněz

Aby mohl jakýkoliv statek či aktivum efektivně sloužit jako peníze, musí plnit několik základních ekonomických funkcí. Tyto funkce definují roli peněz v hospodářství a jsou kritériem, podle kterého lze hodnotit i nové formy peněz, včetně kryptoměn. (17)

Ekonomická teorie tradičně rozlišuje tři hlavní funkce peněz:

1. **Prostředek směny**: toto je nejzákladnější funkce peněz. Peníze slouží jako všeobecně přijímaný prostředník při nákupu a prodeji zboží a služeb. Tím eliminují neefektivitu barterového obchodu, kde byla nutná dvojí shoda potřeb. Místo přímé výměny zboží za zboží stupuje směna zboží za peníze a následně peněz za jiné zboží. Aby peníze mohly tuto funkci plnit, musí být široce akceptovány všemi účastníky trhu.
2. **Uchovatel hodnoty**: peníze umožňují lidem uchovat svou kupní sílu do budoucna. Pokud jedinec obdrží peníze dnes, může si je uschovat a použít k nákupu zboží či služeb později. Tato funkce umožňuje oddělit akt prodeje od aktu koupě. Je však důležité poznamenat, že peníze, zejména fiat měny, nejsou dokonalým uchovatelem hodnoty, protože jejich kupní síla může být v čase erodována inflací.
3. **Zúčtovací jednotka**: peníze poskytují společné měřítko pro vyjádření hodnoty různých statků, služeb, aktiv a dluhů. Ceny jsou kótovány v peněžních

jednotkách, což usnadňuje ekonomickou kalkulaci, porovnávání hodnot a vedení účetnictví. Bez společné zúčtovací jednotky by bylo nutné vyjadřovat ceny každého zboží relativně ke všem ostatním druhům zboží, což by bylo extrémně nepraktické. (18)

Tyto tři funkce tvoří základní pilíře, bez nichž by peníze nemohly plnit svou roli v moderní ekonomice. Jejich efektivní fungování přispívá k plynulosti obchodu, hospodářské stabilitě a důvěře ve finanční systém. (17)

3.3.3 Vlastnosti peněz

Česká národní banka (ČNB) nyní nejen kontroluje výrobu bankovek, ale také zabezpečuje jejich ochranu proti padělání pomocí řady bezpečnostních prvků. Podle ČNB jsou mezi tyto prvky zahrnuty:

- Papír: bankovky jsou tištěny na speciální papír se směsí bavlny, jejíž přesné složení zná jen ČNB a výrobce.
- Vodoznak: skrytý ochranný prvek, který je viditelný při přisvícení světlem a zobrazuje podobiznu významné české osobnosti.
- Proužek: metalický okénkový proužek z umělé hmoty zapuštěný v papíru s mikrotextem uvádějícím hodnotu bankovky a písmena ČNB.
- Skrytý obrazec: jemný detail na rameni portrétu, viditelný při držení bankovky vodorovně proti světlu.
- Barva: duo chromatická barva na motivu lipového květu, která mění odstín při pohybu bankovky vůči světlu.
- Vlákna: oranžová vlákna o délce 6 mm, zapuštěná do papíru bankovky jako další ochrana proti padělání.
- Soutisk: obrazec rozdělený na dvě části, které při prosvícení světlem vytvoří úplný vzor.
- Iridiscentní pruh: pruh na pravé straně bankovky, který při naklonění vykazuje duhové odlesky a je lemován číslicemi s hodnotou.
- Mikrotext: velmi malé písmo na specifických místech bankovky, používané ke stínování či barevným detailům. (27)

Aby peněžní forma mohla efektivně plnit tyto funkce, měla by ideálně vykazovat určité charakteristiky, mezi ně patří:

- trvanlivost (odolnost vůči fyzickému opotřebení),
- přenositelnost (snadnost přenášení),
- dělitelnost (možnost rozdělení na menší jednotky pro malé transakce),
- uniformita (stejné jednotky mají stejnou hodnotu),
- omezená nabídka (aby si udržely hodnotu),
- všeobecná přijatelnost. (26)

Peníze jsou abstraktním vyjádřením směnné síly každé země a jedná se o nespecifikovaný kolektivní obrat pro platidla. To, co ale skutečně předává informace je pojem měna. Měna je národní forma peněz, každá země má určitou měnu, a ta měna má následující základní znaky podle Revendy:

- název,
- základní hotovostní druhy,
- nominální strukturu,
- výlučnost měny jako zákonného platidla na daném území,
- zákonem upravené emise, ochranu, nabývání a platební styk na domácím území i v zahraničí,
- vztah ke zlatu (nyní se nepoužívá). (25)

3.3.4 Struktura bankovního systému ČR

Pro pochopení kontextu, ve kterém se pohybují a operují finanční inovace jako kryptoměny, je důležité porozumět struktuře a klíčovým aktérům tradičního bankovního systému. V České republice, stejně jako ve většině vyspělých ekonomik, je tento systém hierarchicky uspořádán. ČNB je zřízena Ústavou České republiky a činnost vykonává podle zákona č. 6/1993 Sb., o České národní bance. Do činnosti ČNB lze zasahovat jen na základě zákona. (28)

Bankovní systém České republiky je charakterizován jako dvoustupňový. Tento model zahrnuje:

1. Centrální banka: Česká národní banka (ČNB).
2. Komerční banky a další finanční instituce: sem patří univerzální komerční banky, spořitelny, hypoteční banky, stavební spořitelny a další specializované instituce (28).

Česká národní banka (ČNB)

Česká národní banka (ČNB) je veřejnoprávní instituce se sídlem v Praze, přičemž má také regionální pobočky v několika městech po celé České republice, a to konkrétně v Ústí nad Labem, Plzni, Českých Budějovicích, Hradci Králové, Brně a Ostravě. ČNB disponuje vlastním majetkem, který spravuje s odbornou péčí. Je součástí Evropského systému centrálních bank a také Evropského systému dohledu nad finančními trhy. Spolupracuje rovněž s Evropskou radou pro systémová rizika a dalšími evropskými institucemi odpovědnými za dohled nad finančním trhem. (29)

Většina bank působících na českém trhu jsou banky smíšeného (univerzálního) typu, což znamená, že poskytují širokou škálu jak obchodních (přijímání vkladů, poskytování úvěrů), tak investičních bankovních služeb. Kromě nich existují i specializované banky, jako je jedna čistě hypoteční banka a několik stavebních spořitelen. Dále v ČR fungují i dvě banky s přímým napojením na státní rozpočet. (28)

Hlavním cílem ČNB je péče o cenovou stabilitu. To v praxi znamená udržování nízké a stabilní inflace, od roku 2010 prostřednictvím režimu cílování inflace s cílem na úrovni 2 %. Vedle tohoto primárního cíle ČNB rovněž pečuje o finanční stabilitu, což zahrnuje dohled nad bezpečným fungováním celého finančního systému v ČR, a podporuje obecnou hospodářskou politiku vlády vedoucí k udržitelnému hospodářskému růstu, avšak pouze za předpokladu, že tím není dotčen její hlavní cíl. (19)

Klíčové funkce a pravomoci ČNB zahrnují:

- Určování a provádění měnové politiky: stanovování úrokových sazeb, operace na volném trhu, povinné minimální rezervy.
- Výhradní emise bankovek a mincí: ČNB je jediným subjektem oprávněným vydávat českou měnu.
- Řízení peněžního oběhu a platebního styku: zajišťování plynulosti a bezpečnosti platebních systémů.
- Dohled nad finančním trhem: regulace a dohled nad bankami, spořitelnami, úvěrními družstvy, pojišťovnami, penzijními společnostmi, investičními společnostmi, obchodníky s cennými papíry a dalšími subjekty finančního trhu.
- Řešení krize na finančním trhu: ČNB je orgánem příslušným k řešení krizových situací u bank a dalších finančních institucí.

- Devizové operace: správa devizových rezerv, vyhlašování kurzu české měny k cizím měnám.
- Poskytování bankovních služeb státu a veřejnému sektoru.
- Sestavování a zveřejňování statistik: měnová a finanční statistika, platební bilance atd.
- Výzkumná činnost. (19)

Pro úspěšné plnění svých úkolů, zejména v oblasti měnové politiky, je zásadní nezávislost ČNB na politických vlivech (vládě, parlamentu). Tato nezávislost je zakotvena v Ústavě a zákoně o ČNB a projevuje se ve funkční, institucionální, personální a finanční oblasti. Nejvyšším řídícím orgánem ČNB je sedmičlenná bankovní rada v čele s guvernérem, jejíž členy jmenuje prezident republiky. ČNB hraje klíčovou roli v udržování makroekonomické stability, což vytváří prostředí, ve kterém se uskutečňují veškeré ekonomické aktivity, včetně investic do kryptoměn. Její postoje, regulatorní opatření a komunikace mohou významně ovlivnit vývoj a vnímání kryptoměnového trhu v České republice. (25)

Komerční banky a jejich služby

Činnost komerčních bank v České republice je přísně regulována, primárním právním předpisem je zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů. Tento zákon upravuje podmínky pro získání bankovní licence, pravidla obezřetného podnikání bank, bankovní tajemství, pojištění vkladů a další aspekty jejich fungování. Dohled nad dodržováním těchto pravidel vykonává Česká národní banka. Komerční banky tvoří druhý stupeň bankovního systému a na rozdíl od centrální banky jsou to soukromé podnikatelské subjekty, jejichž primárním cílem je dosahování zisku. Působí jako finanční zprostředkovatelé, kteří shromažďují dočasně volné peněžní prostředky od jedněch subjektů (vkladatelů) a poskytují je jiným subjektům (dlužníkům) ve formě úvěrů. (30)

Základní služby a operace komerčních bank lze rozdělit do tří kategorií:

1. **Pasivní operace**: spočívají v přijímání vkladů od veřejnosti (fyzických osob i firem).
2. **Aktivní operace**: představují poskytování úvěrů různým subjektům. Může se jednat o spotřebitelské úvěry, hypotéky, podnikatelské úvěry atd.
3. **Zprostředkovatelské (neutrální) operace**: zahrnují širokou škálu služeb, které banky poskytují svým klientům. Patří sem zejména:

- platební styk: zajištění domácích i zahraničních bezhotovostních plateb, inkasa, trvalé příkazy,
- vydávání a správa platebních prostředků: zejména platebních karet,
- investiční operace: obchodování s cennými papíry na účet klienta nebo na vlastní účet, správa portfolií,
- devizové operace: směnárenská činnost, operace na devizovém trhu,
- další služby. (30)

3.3.5 Virtuální peníze

Pojem virtuální měna je v českém právním řádu definován především zákonem č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (AML zákon). Podle § č odst. 9 tohoto zákona je *„Virtuálním aktivem se pro účely tohoto zákona rozumí elektronicky uchovatelná nebo převoditelná jednotka, která je a) způsobilá plnit platební, směnnou nebo investiční funkci, bez ohledu na to, zda má nebo nemá emitenta, pokud se nejedná o 1. cenný papír, investiční nástroj, nebo peněžní prostředek podle zákona o platebním styku, 2. jednotku podle § 3 odst. 3 písm. c) bodů 4 až 7 zákona o platebním styku, nebo 3. jednotku, kterou je prováděna platba podle § 3 odst. 3 písm. e) zákona o platebním styku, nebo b) jednotkou podle písmene a) bodu 2 a kterou lze v konečném důsledku zaplatit pouze za úzce vymezený okruh zboží nebo služeb, který zahrnuje elektronicky uchovatelnou nebo převoditelnou jednotku podle písmene a).“* (31)

Tato definice je poměrně široká a zahrnuje různé formy digitálních jednotek používaných k platbám. Novela AML zákona účinná od 1. ledna 2021 zavedla širší pojem virtuální aktivum, který zahrnuje *„elektronicky uchovatelnou nebo převoditelnou jednotku, která je způsobilá plnit platební, směnnou nebo investiční funkci“* a není cenným papírem, investičním nástrojem nebo peněžním prostředkem podle zákona o platebním styku. (32, s. 10)

Pojem digitální měna je širší a zastřešuje všechny formy měny, které existují pouze v elektronické podobě a postrádají fyzický protějšek. Zahrnuje tedy virtuální měny, kryptoměny a také potenciální budoucí digitální měny centrálních bank (CBDC). Podle ČNB: *„CBDC tedy přestavují novou, digitální formu peněz emitovaných centrální bankou a stejně jako současné hotovostní peníze je lze využít jako prostředek směny (k placení) i jako uchovatele hodnoty (ke spoření).* (33)

Elektronické peníze jsou specifickým typem peněžních prostředků definovaným zákonem č. 370/2017 Sb., o platebním styku. Jedná se o elektronicky uchovávanou peněžní hodnotu, která představuje pohledávku vůči vydavateli a je vydávána proti přijetí peněžních prostředků za účelem provádění platebních transakcí. (34)

Elektronické peníze představují specifický typ peněžních prostředků určených k realizaci elektronických plateb, jejichž používání upravuje zákon o platebním styku. Na rozdíl od běžně používaných bezhotovostních prostředků jsou definovány jako elektronicky uložená pohledávka vůči vydavateli, kterou lze využít k placení. Podle zákona nesmí být tyto prostředky úročeny ze strany jejich vydavatele. (33)

Kryptoaktiva je termín používaný například Českou národní bankou a evropským nařízením MiCA (Markets in Crypto-Assets). Označuje digitální aktiva, která lze mezi držiteli elektronicky převádět pomocí technologie distribuované účetní knihy (DLT), často s využitím kryptografie k jejich zabezpečení. Mohou, ale nemusí představovat práva držitele vůči třetí straně a jejich emitentem může být fyzická nebo právnická osoba. Kryptoaktiva zahrnují širokou škálu tokenů, včetně kryptoměn, stablecoinů (kryptoaktiva, která se snaží udržet stabilní hodnotu prostřednictvím vazby na fiat měnu nebo jiná aktiva) a NFT (nefungibilní tokeny). (35) (36)

Kryptoměna je podskupinou virtuálních měn (a kryptoaktiv), která se vyznačuje používáním kryptografických technik k zabezpečení transakcí, kontrole vytváření nových jednotek a ověřování převodu aktiv. Většina kryptoměn je decentralizovaná a založená na technologii blockchain. Bitcoin je nejznámějším příkladem kryptoměny. (36)

Terminologie v oblasti digitálních financí se stále vyvíjí a liší se v závislosti na jurisdikci, instituci a pohledu odborníků. Regulační orgány se zaměřují na rizika, centrální banky na měnovou politiku a otázky stability plateb, zatímco akademická obec a vývojáři technologií hledají funkční a technické definice. Tato fragmentace odráží dynamiku a ranou fázi vývoje tohoto odvětví. Pro účely tohoto dokumentu je proto nezbytné jasně definovat pojmy používané na začátku mé práce, zejména „virtuální měna“ a „kryptoměna“, a důsledně se těchto definic držet, případně poukázat na možné odlišné výklady. Správné pochopení rozdílů mezi různými typy digitálních aktiv je nezbytné pro následnou analýzu jejich ziskovosti a rizikovosti v kontextu strategií HODL a staking. (36)

3.4 Kryptografie

Kryptografie je věda o metodách zajištění bezpečnosti dat prostřednictvím jejich transformace tak, aby byla chráněna před neoprávněným přístupem, modifikací či zneužitím. Využívá pokročilé algoritmy, jejichž dešifrování je pro počítače velmi náročné. Jejím hlavním cílem je umožnit bezpečnou komunikaci a uchovávání informací i v nedůvěryhodném prostředí. (38)

První zaregistrovaná kryptoměna, která měla všechny znaky decentralizované měny se nazývá Bitcoin. Byla založena skupinou anonymních vývojářů Satoshi Nakamoto a to roce 2008. Nejednalo se o první pokus o digitální měnu, ale stala se nejvýznamnější v budoucím vývoji kryptoměn. U Bitcoinu se používá kombinace hashovacích funkcí a digitálního podpisu. Kryptoměny se dále rozlišují na tzv. coiny (měny) a tokeny. (37)

V kontextu kryptoměn hraje kryptografie klíčovou roli v nahrazování potřeby důvěry v tradiční centralizované instituce (jako jsou banky) matematickými důkazy a protokoly. Kryptografie, často laicky chápaná pouze jako šifrování, je ve skutečnosti mnohem širší vědní obor zabývající se metodami zabezpečení komunikace a dat v přítomnosti potenciálních protivníků nebo nežádoucích stran. Její principy jsou pro kryptoměny absolutně fundamentální. Hlavní cíle, které se kryptografie snaží dosáhnout, zahrnují:

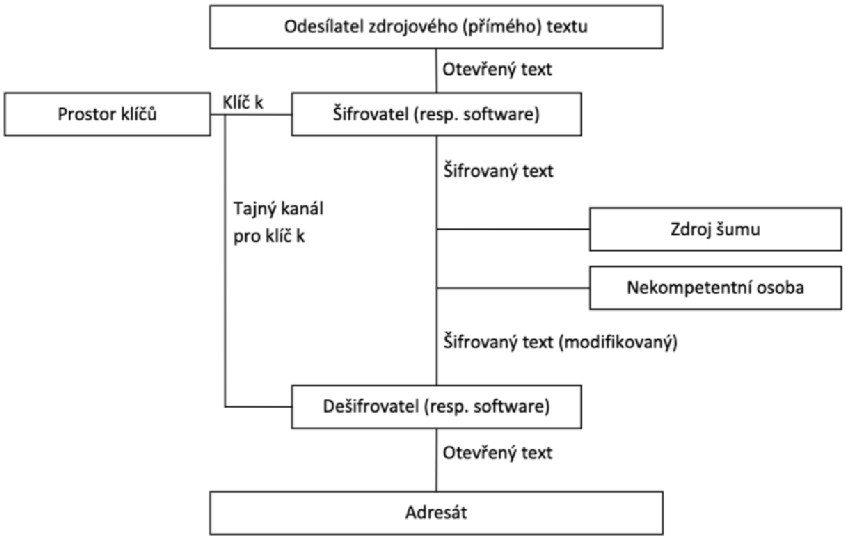
1. Důvěrnost: zajištění, že obsah zprávy nebo dat je čitelný pouze pro oprávněné osoby. Cizí strany by neměly být schopny porozumět obsahu komunikace.
2. Integrita dat: zaručení, že data nebyla během přenosu nebo uložení pozměněna, ať už náhodně nebo úmyslně. Příjemce musí mít jistotu, že obdržená data jsou identická s těmi, která byla odeslána.
3. Autentizace: ověření identity odesílatele zprávy nebo původu dat. Příjemce musí být schopen ověřit, že data skutečně pocházejí od předpokládaného zdroje.
4. Nepopiratelnost: zajištění, že odesílatel nemůže později popřít odeslání zprávy nebo autorství dat, a stejně tak příjemce nemůže popřít jejich přijetí. (38)

3.4.1 Symetrické a asymetrické šifrování

Aumasson píše*: "při symetrickém šifrování je klíč použitý k dešifrování stejný jako klíč použitý k šifrování (na rozdíl od asymetrického šifrování neboli šifrování s veřejným klíčem, kdy se klíč použitý k dešifrování liší od klíče použitého k šifrování)."* (39, s. 25) Tento

klíč musí být bezpodmínečně utajen a sdílen pouze mezi komunikujícími stranami, které si přejí vyměňovat šifrované informace. Na obrázku č. 2 je znázorněn proces symetrického šifrování. (39)

Obrázek č. 2: Symetrické šifrování



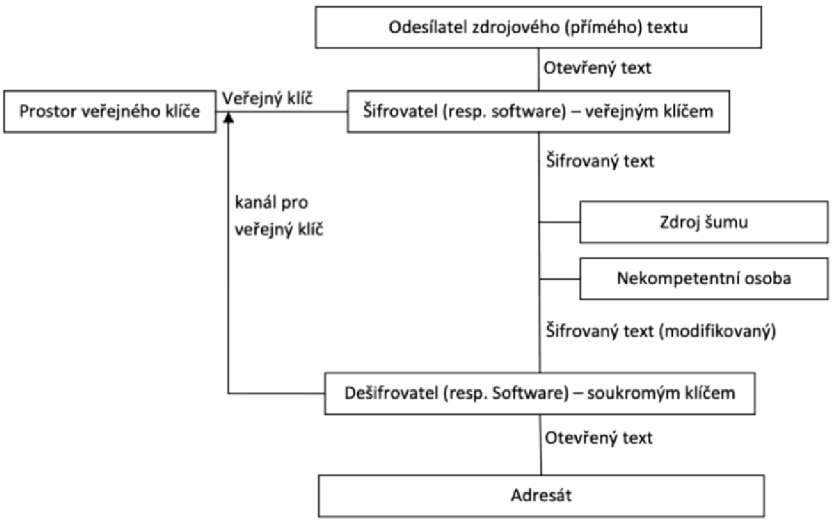
Zdroj: Ochrana dat. Kryptologie (40)

Výhody symetrického šifrování spočívají především v jeho rychlosti a výpočetní nenáročnosti ve srovnání s asymetrickým šifrováním. Díky tomu je vhodné pro šifrování velkých objemů dat. Hlavní nevýhodou a praktickým problémem symetrického šifrování je bezpečná distribuce a správa tajných klíčů. Mezi známé algoritmy symetrického šifrování patří starší standardy jako DES (Data Encryption Standard), který je dnes již považován za prolomený a nevhodný pro použití, a Triple DES (3DES), který aplikuje DES třikrát s různými klíči pro zvýšení bezpečnosti. Modernějším a v současnosti široce používaným standardem je AES (Advanced Encryption Standard), který nabízí různé délky klíčů (128, 192, 256 bitů) a je považován za velmi bezpečný. Dalšími příklady jsou RC5 nebo Blowfish. (39)

Asymetrické šifrování, známé také jako kryptografie s veřejným klíčem, představuje fundamentální koncept, na němž je postavena bezpečnost a funkčnost většiny kryptoměn. Na obrázku č. 3 je znázorněn proces asymetrického šifrování. Na rozdíl od symetrického šifrování používá pár matematicky svázaných klíčů: veřejný klíč a soukromý klíč:

- **Soukromý klíč** je, jak název napovídá, držen v tajnosti jeho vlastníkem a nesmí být nikomu prozrazen.
- **Veřejný klíč** je odvozen ze soukromého klíče, ale z veřejného klíče nelze výpočetně prakticky odvodit klíč soukromý. (39)

Obrázek č. 3: Asymetrické šifrování



Zdroj: Ochrana dat. Kryptologie. (40)

Asymetrická kryptografie má dvě hlavní využití:

1 Šifrování za účelem utajení: pokud chce odesílatel poslat příjemci tajnou zprávu, zašifruje ji pomocí veřejného klíče příjemce. Takto zašifrovanou zprávu pak může dešifrovat pouze vlastník odpovídajícího soukromého klíče, tedy zamýšlený příjemce.

2 Digitální podpisy: pokud chce odesílatel prokázat autenticitu a integritu zprávy, vytvoří digitální podpis pomocí svého soukromého klíče. Kdokoli, kdo má k dispozici odesílatelův veřejný klíč, pak může ověřit platnost tohoto podpisu. (40)

Mezi nejznámější algoritmy asymetrické kryptografie patří RSA (pojmenovaný po jeho tvůrcích Rivestovi, Shamirovi a Adlemanovi), Diffie-Hellmanův algoritmus pro výměnu klíčů, a DSS (Digital Signature Standard). V posledních letech získaly na popularitě algoritmy založené na eliptických křivkách (ECC – Elliptic Curve Cryptography), jako je ECDSA (Elliptic Curve Digital Signature Algorithm). ECC algoritmy nabízejí srovnatelnou úroveň bezpečnosti s výrazně kratšími klíči než například RSA, což vede k vyšší efektivitě

a nižším výpočetním nárokům. Právě ECDSA je algoritmus používaný pro digitální podpisy transakcí v Bitcoinu a mnoha dalších kryptoměnách. (39)

Asymetrická kryptografie je naprosto esenciální pro fungování kryptoměn. Vlastnictví kryptoměnových jednotek je v podstatě dáno držením soukromého klíče, který umožňuje s těmito jednotkami disponovat (tj. podepisovat transakce, které je převádějí). Veřejný klíč, nebo adresa z něj odvozená, slouží jako identifikátor, na který lze kryptoměny zasílat. Tento systém umožňuje decentralizované ověřování transakcí bez potřeby centrální autority. Bezpečnost soukromého klíče je proto pro každého uživatele kryptoměn naprosto kritická. Jeho ztráta znamená nevratnou ztrátu přístupu k asociovaným kryptoměnovým prostředkům, zatímco jeho kompromitace umožňuje útočníkovi tyto prostředky ukrást. Tento aspekt je jedním z klíčových rizik spojených s držením (HODL) i stakingem kryptoměn. (37) Po shrnutí základních principů symetrického a asymetrického šifrování je vhodné jejich hlavní charakteristiky přehledně porovnat. Následující tabulka č. 5 uvádí klíčové rozdíly mezi oběma metodami.

Tabulka č. 5: Srovnání symetrického a asymetrického šifrování

Aspekt	**Symetrické šifrování**	**Asymetrické šifrování**
Používané klíče	Jeden tajný klíč pro šifrování i dešifrování	Dva klíče – veřejný (public) a soukromý (private)
Rychlost	Vysoká – velmi rychlé a výpočetně nenáročné	Nižší – pomalejší kvůli složitějším výpočtům
Vhodnost použití	Šifrování velkých objemů dat	Bezpečná komunikace, digitální podpisy, výměna klíčů
Správa klíčů	Náročná – každá dvojice potřebuje vlastní klíč, roste kvadraticky (N*(N-1)/2)	Jednodušší – veřejný klíč může být volně dostupný
Bezpečnostní rizika	Vysoká rizika při distribuci a úschově tajných klíčů	Riziko kompromitace soukromého klíče, ale bezpečnější výměna
Škálovatelnost	Nízká – neefektivní pro větší sítě	Vysoká – vhodné pro otevřené a decentralizované prostředí
Typické použití	VPN, šifrování souborů a disků, zabezpečené přenosy velkých dat	E-maily, certifikáty, kryptoměny, internetová komunikace
Výpočetní náročnost	Nízká	Vysoká

Zdroj: vlastní zpracování dle (38) (39) (40)

Z porovnání vyplývá, že volba mezi symetrickým a asymetrickým šifrováním závisí na konkrétním způsobu využití, požadavcích na rychlost, bezpečnost a komplexnost systému. Zatímco symetrické šifrování vyniká svou efektivitou při práci s velkým množstvím dat, asymetrické nabízí vyšší bezpečnost při výměně klíčů a je nezbytné v prostředích, kde není možné předem bezpečně sdílet tajné informace. V praxi se však tyto

přístupy často kombinují, aby se využily jejich silné stránky a minimalizovaly jejich nevýhody.

3.4.2 Hašovací funkce

Hash funkce jsou dalším nezbytným kryptografickým nástrojem pro technologii blockchain a kryptoměny. Aumasson píše: „*Hašovací funkce, jako například MD5, SHA-1, SHA-256, SHA-3 a BLAKE2, představují švýcarský armádní nůž kryptografů: používají se v digitálních podpisech, šifrování s veřejným klíčem, ověřování integrity, ověřování zpráv, ochraně hesel, protokolech dohody klíčů a mnoha dalších kryptografických protokolech.*“ (39, s. 106) Jedná se o matematickou funkci, která převádí vstupní data libovolné délky na výstupní řetězec pevné, relativně krátké délky. Výstup je známý jako hash, hash hodnota, digitální otisk nebo souhrn zprávy. Kryptografické hash funkce musí splňovat řadu klíčových vlastností, aby byly považovány za bezpečné a vhodné pro kryptografické aplikace (Tabulka č. 6).

Tabulka č. 6: Vlastnosti kryptografických hašovacích funkcí

Vlastnost	Popis
Jednosměrnost	Z hashe H(x) je prakticky nemožné zpětně zjistit původní vstup x.
Odolnost vůči druhému vzoru	Nelze najít jiné $x_2 \neq x_1$ takové, že $H(x_1) = H(x_2)$, pokud známe x_1 a jeho hash.
Odolnost vůči kolizím	Je prakticky nemožné najít dvě různá data x_1 a x_2, která by měla stejný hash.
Determinističnost	Stejný vstup vždy generuje naprosto stejný hash.
Rychlost výpočtu	Hašování musí být rychlé a efektivní i při velkých objemech dat.
Lavínový efekt	I malá změna ve vstupu způsobí výrazně odlišný hash, čímž se zajišťuje vysoká citlivost funkce.

Zdroj: vlastní zpracování dle (39) (40) (41)

Hašovací funkce mají v kryptoměnách a technologii blockchain široké spektrum použití (Tabulka č. 7):

Tabulka č. 7: Využití hašovacích funkcí v kryptoměnách a blockchainu

Oblast použití	Popis
Digitální otisk transakcí a bloků	Každá transakce a blok mají unikátní hash jako identifikátor a prostředek ověření integrity.
Propojení bloků v blockchainu	Každý blok obsahuje hash předchozího, čímž vzniká kryptografický řetězec - změna v historii naruší celý řetězec.
Generování kryptoměnových adres	Adresy (např. v Bitcoinu) vznikají hašováním veřejných klíčů pomocí algoritmů jako SHA-256 a RIPEMD-160.
Digitální podpisy	Podepisuje se hash zprávy, nikoli celá zpráva - šetří místo a zvyšuje bezpečnost.
Proof-of-Work (PoW)	Těžaři hledají vstup (nonce), který vytvoří hash s požadovanými vlastnostmi (např. začínající určitým počtem nul). Slouží k zabezpečení sítě.

Zdroj: Vlastní zpracování dle (38) (39) (41)

Mezi známé hashové algoritmy patří MD5 (který je nyní považován za nefunkční z hlediska kolizí a neměl by být používán pro bezpečnostní účely), SHA-1 (rovněž oslabený a nedoporučovaný pro nové aplikace), rodina SHA-2 (která zahrnuje SHA-256, široce používaný v Bitcoinu) a novější rodina SHA-3. Kromě SHA-256 se k generování bitcoinových adres používá také RIPEMD-160, což vede k kratšímu hashování (160 bitů oproti 256 bitům u SHA-256) a tedy i kratším adresám. Následující tabulka č. 8 poskytuje přehled vybraných kryptografických hashovacích funkcí, jejich vlastností a použití:

Tabulka č. 8: Přehled a vlastnosti vybraných kryptografických hašovacích funkcí

Algoritmus	**Délka hashe (bity)**	**Odolnost vůči kolizím (stav 2024/2025)**	**Odolnost vůči preimage (stav 2024/2025)**	**Typické použití v kryptoměnách**
MD5	128	Prolomeno	Teoreticky oslabeno	Již by se nemělo používat pro bezpečnostní účely
SHA-1	160	Prolomeno (prakticky)	Dobrá	Nedoporučeno pro nové aplikace, zastaralé (např. Git)
SHA-256	256	Považováno za bezpečné	Považováno za bezpečné	Bitcoin (PoW, Merkle trees, adresy), Ethereum, mnoho dalších
SHA-512	512	Považováno za bezpečné	Považováno za bezpečné	Některé kryptoměny, vyšší bezpečnostní požadavky
SHA-3 (Keccak)	Variabilní (např. 256, 512)	Považováno za bezpečné	Považováno za bezpečné	Ethereum (původně, nyní Keccak-256), alternativa k SHA-2
RIPEMD-160	160	Považováno za bezpečné (pro svou délku)	Považováno za bezpečné	Bitcoin (generování adres z veřejných klíčů)

Zdroj: vlastní zpracování dle (38) (39) (41)

Hash funkce jsou tedy nezbytnou součástí fungování a bezpečnosti blockchainových systémů. Vytvoření neměnného řetězce záznamů, ověření integrity dat a bezpečnost transakcí jsou možné díky jejich základním vlastnostem, kterými jsou především jednosměrnost a odolnost proti kolizím. Jak dokazuje přechod od zastaralých algoritmů k spolehlivým standardům, jako je SHA-256, je pokračující vývoj a aplikace výkonných kryptografických hash funkcí přímo zodpovědný za celkovou bezpečnost této technologie.

3.4.3 Digitální podpisy

Digitální podpis je kryptografická technika, která v elektronickém světě plní podobnou funkci jako vlastnoruční podpis na papírovém dokumentu. Slouží k ověření autenticity (původu) a integrity (nezměněnosti) digitálních dat a také k zajištění nepopiratelnosti (non-repudiation) ze strany podepisujícího. Princip fungování digitálního podpisu je založen na asymetrické kryptografii, tedy na použití páru soukromého a veřejného klíče. (40)

Proces vytvoření a ověření digitálního podpisu obvykle zahrnuje následující kroky:

1 **Vytvoření hashe dat**: strana, která chce data podepsat (podepisující), nejprve z těchto dat (např. textu zprávy, souboru, transakce) vypočítá pomocí kryptografické hašovací funkce jejich unikátní otisk – hash.

2 **Zašifrování hashe soukromým klíčem**: podepisující následně tento hash zašifruje svým soukromým klíčem. Výsledkem tohoto šifrování je samotný digitální podpis.

3 **Připojení podpisu k datům**: digitální podpis je poté připojen k původním datům. Často se spolu s daty a podpisem zasílá i certifikát obsahující veřejný klíč podepisujícího, aby ověřující strana měla tento klíč k dispozici.

4 **Ověření podpisu**: strana, která chce podpis ověřit (ověřující):

- dešifruje přijatý digitální podpis pomocí veřejného klíče podepisujícího. Tím získá původní hash, který vypočítal podepisující (označme ho H1),
- nezávisle vypočítá hash z přijatých původních dat pomocí stejné hašovací funkce, jakou použil podepisující (označme tento nově vypočtený hash H2),
- porovná oba hashe (H1 a H2). Pokud se shodují, digitální podpis je považován za platný. To znamená, že data skutečně pocházejí od držitele daného soukromého klíče a nebyla po podepsání změněna. Pokud se hashe neshodují, podpis je neplatný. (40)

Digitální podpisy zajišťují:

- Autenticitu: protože k vytvoření platného podpisu je nutný soukromý klíč, který by měl znát pouze podepisující, úspěšné ověření podpisu potvrzuje, že data skutečně pocházejí od deklarovaného odesílatele (držitele soukromého klíče).
- Integritu: jelikož se podepisuje hash dat, jakákoli sebemenší změna v datech po jejich podepsání by vedla k úplně jinému hashi při ověřování, a podpis by tak nebyl platný. Tím je zaručeno, že data nebyla cestou zmanipulována.
- Nepopiratelnost: držitel soukromého klíče nemůže později popřít, že daná data podepsal (pokud svůj soukromý klíč bezpečně střežil), protože nikdo jiný by neměl být schopen platný podpis s jeho klíčem vytvořit. (40)

V kontextu kryptoměn jsou digitální podpisy klíčové. Každá transakce, při které se převádějí jednotky Bitcoinů z jedné adresy na druhou, musí být digitálně podepsána pomocí

soukromého klíče odesílatele. Tento podpis slouží jako nezpochybnitelná autorizace transakce. Uzly v síti pak mohou pomocí odpovídajícího veřejného klíče (odvozeného z adresy nebo obsaženého v transakci) ověřit platnost podpisu a v důsledku toho i oprávněnost transakce, aniž by znaly totožnost odesílatele nebo se spoléhaly na centrální ověřovací autoritu. Tento proces je základem peer-to-peer charakteru elektronických platebních systémů, jako je Bitcoin. Pro celkovou bezpečnost systému je tedy zásadní schopnost uživatelů bezpečně uchovávat své soukromé klíče. Jejich kompromitace by útočníkovi umožnila podepisovat transakce jménem oběti a ukrást její majetek, což zdůrazňuje význam bezpečných peněženek pro kryptoměny a účinných technik správy klíčů.

3.5 Blockchain

Technologie blockchain, často označovaná jako „blokový řetězec“, slouží jako základní datový rámec a systém uchovávání záznamů pro řadu kryptoměn, jako je například Bitcoin. Jedná se o novou metodu bezpečného a transparentního dokumentování transakcí v decentralizovaném prostředí bez nutnosti centrální autority. (6)

Blockchain je samostatnou formou technologie Distribuované účetní knihy (DLT). DLT obvykle označuje databázi, která je sdílena, synchronizována a replikována mezi členy distribuované sítě (uzly). Blockchain je aplikace DLT, která organizuje data (obvykle transakce) do „bloků“, které jsou následně chronologicky a neměnně propojeny pomocí kryptografie a vytvářejí „řetězec“. Je důležité zmínit, že DLT je širší pojem, přičemž blockchain je pouze jedním z typů, ačkoli se jedná o nejuznávanější formu DLT. (6)

3.5.1 Základní principy a vlastnosti blockchainu

Blockchain tedy řeší zásadní problém digitálního světa: jak vybudovat důvěru a důvěryhodný záznam událostí v prostředí, kde si hráči nemusí navzájem důvěřovat a kde neexistuje centrální arbitr. Umožňuje nové formy aplikací tím, že nabízí sdílený, neměnný a transparentní záznam ověřený distribuovanou sítí. Metoda HODL klade velký důraz na důvěru v dlouhodobou bezpečnost a neměnnost záznamů v blockchainu. Pro staking je pak klíčová funkčnost a spolehlivost mechanismu konsenzu, který daný blockchain udržuje a zabezpečuje.

Základní principy a vlastnosti blockchainu:

1 **Decentralizace**: data nespravuje jedna centrální entita, ale jsou rozložena mezi více uzlů v síti fungující na principu peer-to-peer.

2 **Transparentnost**: veřejné blockchainy umožňují viditelnost transakcí pro každého, i když identity účastníků jsou skryté pod adresami.
3 **Neměnnost**: jakmile je transakce zapsána a blok potvrzen dalšími, nelze ji zpětně změnit díky kryptografickému propojení bloků.
4 **Bezpečnost**: zajištěna kryptografií (hašování, digitální podpisy) a konsenzem mezi uzly o platnosti transakcí.
5 **Distribuovaný konsenzus**: nové bloky se přidávají na základě shody většiny uzlů pomocí algoritmů jako Proof-of-Work nebo Proof-of-Stake. (6)

3.5.2 Struktura bloku, transakcí a Merkle tree

Pro pochopení fungování blockchainu je nezbytné porozumět struktuře jeho základních stavebních prvků (bloků a transakcí) a způsobu, jakým jsou transakce v rámci bloku efektivně organizovány a zabezpečeny.

Každý blok v blockchainu se typicky skládá ze dvou hlavních částí:

1 **Hlavička bloku (Block Header)**: obsahuje metadata o bloku, která jsou klíčová pro jeho identifikaci, propojení s ostatními bloky a ověření. Mezi typické součásti hlavičky patří:

- Hash předchozího bloku: kryptografický hash hlavičky předchozího bloku v řetězci. Toto je prvek, který zajišťuje řetězení a neměnnost. Jakákoli změna v předchozím bloku by změnila jeho hash, což by zneplatnilo tento odkaz,
- Časové razítko (Timestamp): přibližný čas vytvoření bloku,
- Nonce (Number used once): náhodné číslo, které těžaři v systémech Proof-of-Work mění, dokud nenajdou hash bloku splňující podmínky obtížnosti,
- Merkle Root (Kořen Merkleova stromu): jediný hash, který reprezentuje všechny transakce obsažené v těle bloku,
- metadata, jako verze bloku, cílová obtížnost (v PoW systémech) atd. (42)

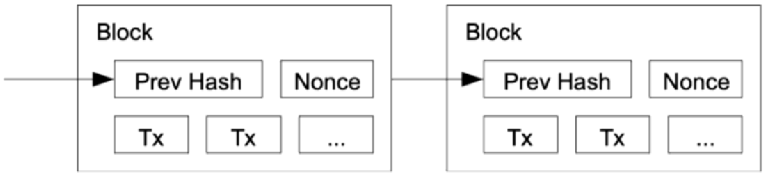
2 **Tělo bloku (Block Body)**: obsahuje seznam všech transakcí, které byly do tohoto bloku zahrnuty a potvrzeny. Počet transakcí v bloku je omezen jeho maximální velikostí.

Transakce je základní operací zaznamenávanou na blockchainu. V kontextu kryptoměn jako Bitcoin typicky reprezentuje převod hodnoty mezi adresami. Obrázek č. 4

ilustruje princip řetězení bloků a transakcí. Struktura transakce se může lišit mezi různými blockchainy, ale obecně obsahuje:

- Vstupy (Inputs): odkazy na předchozí neutracené výstupy, které slouží jako zdroj prostředků pro danou transakci. Každý vstup musí být autorizován digitálním podpisem vlastníka těchto UTXO.
- Výstupy (Outputs): definují, kam a kolik kryptoměny se převádí. Každý výstup specifikuje částku a podmínky (obvykle adresu příjemce ve formě skriptu), za kterých mohou být tyto prostředky v budoucnu utraceny,
- další metadata, jako například poplatek za transakci (transaction fee), který motivuje těžaře k zahrnutí transakce do bloku. (45)

Obrázek č. 4: Princip fungování transakcí v blockchainu



Zdroj: Bitcoin: A peer-to-peer electronic cash systém (42)

Merkle Tree (Hašovací strom) – efektivní správa a ověřování velkého počtu transakcí v rámci jednoho bloku je řešena pomocí datové struktury zvané Merkle tree.

Konstrukce Merkle Tree:

1 Nejprve se pro každou jednotlivou transakci v bloku vypočítá její kryptografický hash (TXID v Bitcoinu). Tyto hashe tvoří listy (nejnižší úroveň) Merkleova stromu.

2 Následně se sousední páry hashů zkonkatenují a z tohoto spojeného řetězce se vypočítá nový hash. Tento proces se opakuje pro všechny páry na dané úrovni stromu. Pokud je na nějaké úrovni lichý počet hashů, poslední hash se obvykle zduplikuje a zahašuje sám se sebou, nebo se použije jiná definovaná metoda.

3 Tento proces párování a hašování pokračuje směrem nahoru stromem, dokud nezůstane pouze jeden jediný hash. Tento finální hash na vrcholu stromu se nazývá Merkle root (kořen Merkleova stromu). (42) (45)

Význam a použití Merkle Tree

- Merkle root, který je uložen v hlavičce bloku, je velmi krátkým, ale unikátním otiskem všech transakcí v daném bloku. To šetří místo v hlavičce bloku.
- Efektivní ověření integrity a příslušnosti transakce (Merkle Proof). Merkle tree umožňuje velmi rychle a efektivně ověřit, zda konkrétní transakce je součástí bloku, aniž by bylo nutné stahovat a procházet všechny transakce v bloku. K tomu slouží tzv. Merkle proof (důkaz Merkle), což je sada hashů (větví stromu) vedoucích od dané transakce ke kořeni. (42) (45)

3.5.3 Kryptoměny

Kryptoměny představují virtuální typ měny, kterou nevydává centrální banka ani žádná oficiální organizace. První a nejznámější kryptoměnou je Bitcoin (BTC), jehož koncept byl poprvé představen v roce 2008 pod pseudonymem „Satoshi Nakamoto“ v dokumentu *Bitcoin: A Peer-to-Peer Electronic Cash System,* zveřejněném na webové stránce bitcoin.org. Tento dokument položil základy nového decentralizovaného platebního systému umožňujícího uživatelům provádět transakce bez závislosti na zprostředkovateli. (45)

Bitcoin funguje na základě konsensuálního mechanismu Proof of Work (PoW), který udržuje bezpečnost sítě a potvrzuje transakce prostřednictvím postupu náročného na zdroje, známého jako těžba. Těžba zahrnuje řešení složitých matematických úloh, které vyžadují značné výpočetní kapacity, a tedy i značnou spotřebu energie. (42)

Tato energetická náročnost vede ke značnému vlivu na životní prostředí. To vyvolalo odborné a společenské diskuse o životaschopnosti modelu PoW a o nutnosti přechodu na ekologičtější varianty, jako je Proof of Stake (PoS), který využívajídalší kryptoměny. Na trhu existuje i množství dalších kryptoměn, které přinášejí nové funkce, efektivnější technologická řešení nebo nižší energetickou náročnost. Mezi nejvýznamnější patří:

- **Ethereum (ETH)**: druhá největší kryptoměna podle tržní kapitalizace. Umožňuje provozování tzv. chytrých kontraktů (smart contracts) a decentralizovaných aplikací. V roce 2022 Ethereum přešlo z PoW na ekologičtější algoritmus Proof of Stake (PoS).
- **Cardano (ADA)**: zaměřuje se na vědecký přístup k vývoji, energetickou efektivitu a transparentní řízení komunity.

- **Solana (SOL)**: známá pro extrémně rychlé a levné transakce, vhodná pro decentralizované aplikace a NFT.
- **Ripple (XRP)**: využíván zejména v oblasti mezinárodních převodů a spolupráce s tradičními bankami.
- **Stablecoiny (např. USDT, USDC)**: kryptoměny navázané na hodnotu fiat měn (např. amerického dolaru), které minimalizují volatilitu a nacházejí využití např. v DeFi. (43) (44)

Následující tabulka č. 9 poskytuje srovnání vybraných kryptoměn.

Tabulka č. 9: Srovnání kryptoměn

Kryptoměna	Rok vzniku	Konsenzus	Hlavní využití	Energetická náročnost
Bitcoin (BTC)	2008	Proof of Work	Digitální zlato, uchování hodnoty	Vysoká
Ethereum (ETH)	2015	Proof of Stake	Smart kontrakty, DeFi, NFT	Nízká (po přechodu na PoS)
Solana (SOL)	2020	Proof of History + PoS	Rychlé transakce, dApps, NFT	Nízká
Ripple (XRP)	2012	Federated Consensus	Bankovní převody, rychlé platby	Nízká
USDT / USDC	2014/2018	Závisí na hostitelském blockchainu	Stabilní hodnota, obchodování	N/A (není těženo)

Zdroj: vlastní zpracování dle (43) (44)

Tento přehled ukazuje, že vývoj v oblasti kryptoměn směřuje ke snižování energetické náročnosti, vyšší škálovatelnosti a integraci s reálným světem. Na základě dat dostupných v říjnu 2025 z portálu CoinMarketCap.com, byla provedena analýza trhu a sestavena tabulka uvedená v příloze A s názvem **Přehled 50 kryptoměn s nejvyšší tržní hodnotou.** (49)

Z dat je patrné, že se Bitcoin na celkové tržní kapitalizaci trhu s kryptoměnami podílí zhruba 61 % a Ethereum přibližně 11,2 %. Na 50 nejvýznamnějších kryptoměn připadá téměř 95 % celého trhu, což svědčí o velké koncentraci kapitálu. Nejrozšířenějším konsensuálním mechanismem je Proof of Stake (PoS). Z 50 největších kryptoměn jich pouze sedm používá Proof of Work (PoW), což ukazuje na postupný odklon od energeticky náročnějšího PoW. Dalším významným vývojem je zvýšení významu stablecoinů. Největšími stablecoiny jsou USDT, USDC, USDe, World Liberty USD a DAI s celkovou tržní kapitalizací přibližně 237 miliard USD.

3.5.4 Ekologické dopady konceptu Proof-of-Work

Environmentální dopady mechanismu Proof-of-Work (PoW) představují globální problém kvůli energeticky náročným operacím. Analýza dopadů na základě modelu systémové dynamiky ukazuje na významnou spotřebu nejen elektřiny, ale i vody, a s tím spojenou uhlíkovou stopu (50) (51).

Spotřeba elektřiny

V roce 2023 spotřeba elektřiny pro těžbu kryptoměn hodnoty 119,7×106 MWh. Pro účely lepšího pochopení v mé práci, toto množství energie je srovnatelné se spotřebou země jako Argentina, která má téměř 46 milionů obyvatel. Studie zároveň kritizuje dřívější odhady jiných autorů, které často nadhodnocovaly spotřebu kvůli používání nerealisticky nízké ceny za elektřinu (např. 5 centů/kWh) ve svých modelech. Jako jedno z udržitelných řešení je navrhováno využití tzv. omezování výroby z obnovitelných zdrojů (RE curtailment). Tato strategie spočívá ve směřování přebytečné energie z obnovitelných zdrojů, kterou síť v danou chvíli nepotřebuje, do těžebních operací. Tímto způsobem mohou těžaři využívat čistou energii a snížit svou závislost na neobnovitelných zdrojích. (51)

Spotřeba vody

Těžba kryptoměn má také významnou vodní stopu, která je spojena s energetickou náročností chlazení elektráren. V roce 2023 činila spotřeba vody 1859×106m3. Tento objem je dostatečný k tomu, aby pokryl základní potřeby pitné vody a hygieny pro celou světovou populaci, která k nim v současnosti nemá přístup. Model ve studii pracoval s intenzitou spotřeby vody na úrovni 15,53m3 na každou spotřebovanou megawatthodinu elektřiny.Bez zavedení udržitelných opatření se předpokládá, že spotřeba elektřiny i vody spojená s kryptoměnami se do roku 2030 zvýší šestinásobně. (50)

Emise CO2

V roce 2022 těžba kryptoměn v Číně, USA, Rusku, Kanadě, Německu, Malajsii, Kazachstánu, Irsku a Íránu vyprodukovala 103,6 Mt CO_2 ročně. Pro srovnání, roční emise CO_2 v Řecku činí přibližně 100 Mt. Historické výpočty používaly emisní poměry kolem 0,3 kg CO_2/kWh, což vedlo k podhodnocení skutečných emisí – skutečný průměr se blíží spíše 0,8 kg CO_2/kWh. (52)

Pro snížení dopadu je třeba provést následující zásadní kroky:

- Zlepšit energetickou účinnost ASIC těžařů (zlepšení o 1 % = snížení CO_2 o 0,8 %).

- Integrovat přebytečnou obnovitelnou energii.
- Využít odpadní teplo z těžebních farem k vytápění průmyslových nebo obytných budov. (52)

V následující Tabulce č. 10 jsou vyčísleny odhadované roční emise oxidu uhličitého v závislosti na procentuálním podílu neobnovitelných zdrojů energie.

Tabulka č. 10: Modelace ročních emisí CO_2 při různé intenzitě využití fosilních paliv

Podíl fosilních zdrojů	**Výpočet**	**Emise CO_2**
70 %	119,7× 10^9 kWh × 0,7 × 0,8 kgCO_2/kWh	67 Mt
80 %	119,7× 10^9 kWh × 0,8 × 0,8 kgCO_2/kWh	76,6 Mt
90 %	119,7× 10^9 kWh × 0,9 × 0,8 kgCO_2/kWh	86,2 Mt

Zdroj: vlastní zpracování podle (51) (52)

Elektronický odpad (e-waste)

Množství elektronického odpadu produkovaného sítí Bitcoin činí k květnu 2021 30,7 kt ročně. Při maximálních hodnotách bitcoinu by se tento objem mohl v blízké budoucnosti zvýšit na 64,4 kt. Průměrná transakce v sítí Bitcoinu generuje 272 g elektronického odpadu. Přičemž železo tvoří téměř 40 % celkového objemu odpadu podle hmotnosti, což představuje 12 280 tun ročně. (53)

Ke snížení množství odpadu a spotřeby surovin jsou k dispozici následující možnosti:

- prodloužení životnosti těžařů pomocí modulárního designu,
- koordinované systémy sběru a recyklace drahých kovů,
- návrh hardwaru s vyšším podílem recyklovatelných materiálů (53).

V následující Tabulce č. 11 jsou shrnuty klíčové environmentální dopady konsenzuálního mechanismu Proof-of-Work.

Tabulka č. 11: Environmentální dopady konsenzuálního mechanismu Proof-of-Work

Aspekt	Zjištěné dopady	Projekce a řešení
Spotřeba elektřiny	119,7×106 MWh, což odpovídá spotřebě Argentiny (2023).	Očekává se šestinásobný nárůst do roku 2030. Řešením je využití přebytečné energie z obnovitelných zdrojů (RE curtailment).
Spotřeba vody	1859×106m3, což by stačilo pro globální populaci bez přístupu k vodě a hygieně (2023).	Očekává se šestinásobný nárůst do roku 2030. Dopad je přímo spojen se spotřebou elektřiny pro chlazení elektráren.
Emise CO2	103,6 Mt CO2 (2022).	Očekává se další nárůst v závislosti na podílu fosilních zdrojů. Řešením je zvyšování účinnosti a integrace obnovitelné energie.
Elektronický odpad	30,7 kt (2021)	Očekává se růst úměrný hashrate. Řešením je delší životnost zařízení a recyklace kovů z minerů.

Zdroj: vlastní zpracování dle (50) (51) (52) (53)

3.5.5 Koncept Proof-of-Stake

S rostoucími ekologickými obavami a omezenou škálovatelností mechanismu Proof of Work (PoW) se vývoj v oblasti blockchainu posunul k efektivnějším konsenzuálním modelům. Jedním z nejvýznamnějších je Proof of Stake (PoS) - inovativní přístup, který zásadně snižuje energetickou náročnost sítě. Následující tabulka č. 12 poskytuje srovnání PoW a PoS (44).

Tabulka č. 12: Srovnání PoW a PoS

Kritérium	**Proof of Work (PoW)**	**Proof of Stake (PoS)**
Spotřeba energie	Velmi vysoká	Nízká
Hardware	Vyžaduje specializované zařízení (ASIC)	Běžný serverový hardware
Ekologický dopad	Negativní	Výrazně nižší
Bezpečnost	Vysoce odolný vůči útokům	Bezpečný, ale náchylnější na centralizaci
Distribuce moci	Výhoda pro těžaře s výkonným hardwarem	Výhoda pro uživatele s větším podílem mincí
Příklad kryptoměny	Bitcoin (BTC), Litecoin (LTC)	Ethereum (ETH), Solana (SOL), Polkadot (DOT)

Zdroj: vlastní zpracování dle (6) (44) (45)

Prvním reálně fungujícím projektem byl Peercoin (2012), který PoS zavedl jako alternativu k PoW. Na rozdíl od těžby, která spoléhá na výpočetní výkon, PoS určuje validátory transakcí podle množství kryptoměny, kterou drží a „stakují“ ve svých peněženkách. Uživatelé s větším podílem mají vyšší šanci být vybráni k potvrzení bloku a získat odměnu. Tímto způsobem se eliminuje potřeba specializovaného hardwaru a spotřeba energie se výrazně snižuje, což činí PoS ekologičtější a levnější variantou. (6)

Staking představuje klíčovou součást konsenzuálního mechanismu Proof-of-Stake, neboť umožňuje uživatelům aktivně se podílet na zabezpečení a správě sítě. Držitelé kryptoměn „uzamykají“ (stakeují) své tokeny ve speciálních peněženkách nebo staking poolech, čímž přispívají k validaci transakcí a vytváření nových bloků. Jak uvádí Fahad Saleh, *„V poslední době se mezi PoS blockchainy stává populárnějším pojem staking pools. Staking pool je organizace, v níž jednotlivé zúčastněné strany spolupracují a sdílejí odměny z validace.“* (44, s. 38)

Za tuto činnost jsou odměňováni nově vytvořenými tokeny nebo transakčními poplatky. Staking tímto způsobem nahrazuje těžbu (mining) známou z Proof-of-Work systémů, ale bez nutnosti výpočetně náročného řešení matematických úloh. (44)

Výhody Proof-of-Stake:

- Nízká spotřeba energie: PoS eliminuje potřebu výkonného výpočetního zařízení.
- Větší škálovatelnost: vyšší rychlost transakcí a nižší poplatky.
- Demokratizace účasti: umožňuje i menším držitelům zapojit se do validace pomocí delegování.
- Ekologická udržitelnost: PoS je považován za „zelenou alternativu“ vůči PoW.

Nevýhody Proof-of-Stake:

- Riziko centralizace: uživatelé s velkým počtem tokenů mohou získat příliš velký vliv.
- Nižší odolnost vůči některým typům útoků: jako např. „nothing at stake“ problém.
- Komplexita implementace: návrh bezpečného PoS modelu vyžaduje sofistikovanou architekturu. (44)

Z technologického hlediska můžeme očekávat další zlepšení bezpečnosti prostřednictvím slashing mechanismů, které penalizují škodlivé chování validátorů. Současně se zvyšuje uživatelská přístupnost stakingu díky tzv. staking poolům a možnostem liquid stakingu, které umožňují zapojení i drobným držitelům tokenů, aniž by museli provozovat vlastní uzel. Závěrem lze říci, že Proof-of-Stake se v poslední době stal oblíbeným konsensuálním mechanismem pro vznikající blockchainové projekty díky své efektivitě, škálovatelnosti a ekologičnosti.

3.5.6 Investiční strategie v prostředí blockchainu

V neustále se měnícím a často nepředvídatelném prostředí trhu s kryptoměnami je důležitá pečlivě zvolená investiční strategie. Tyto přístupy se liší podle míry rizika, časového rámce, potřebných technických dovedností a míry aktivní účasti investora. Všeobecně uznávanou a trvalou strategií je HODL, která představuje udržování investic do kryptoměn po dlouhou dobu bez ohledu na dočasné změny cen. Investoři se soustředí na myšlenku, že technologie blockchain a přední kryptoměny, jako je Bitcoin nebo Ethereum, mají značný

růstový potenciál do budoucna. Přístup HODL je často považován za ideální pro začínající investory a ty, kteří chtějí investovat dlouhodobě s menší aktivní účastí na obchodování. (46)

Kromě strategie HODL existují různé další populární investiční metody. Krátkodobé obchodování zahrnuje rychlý nákup a prodej kryptoměn s cílem využít krátkodobých změn cen k dosažení zisku. Tato metoda vyžaduje průběžné pozorování trhu, technické hodnocení a větší míru odborných znalostí. Další známou metodou je staking, běžně spojované s kryptoměnami, které využívají konsenzuální mechanismus Proof of Stake (PoS). V tomto systému si uživatelé „zajišťují“ své kryptoměny v rámci sítě a dostávají odměny v podobě nově vytěžených tokenů, čímž pasivně zvyšují hodnotu své investice. (47)

V posledních letech se rovněž rozvíjí oblast decentralizovaných financí (DeFi), která nabízí pokročilé investiční nástroje jako yield farming, liquidity mining či poskytování půjček v rámci decentralizovaných protokolů. Tyto možnosti však bývají často spojeny s vyšší mírou rizika i technické složitosti. (48)

Pro lepší přehled jsou základní charakteristiky jednotlivých strategií uvedeny v následující tabulce č. 13:

Tabulka č. 13: Charakteristiky jednotlivých strategií

Strategie	Časový horizont	Riziko	Náročnost na znalosti	Aktivita investora	Možný výnos	Typ investora
HODL	Dlouhodobý (roky)	Nízké až střední	Nízká	Nízká	Střední až vysoký	Konzervativní, dlouhodobý
Trading	Krátkodobý (dny/týdny)	Vysoké	Vysoká	Vysoká	Vysoký	Aktivní, zkušený
Staking	Střední až dlouhý	Nízké až střední	Střední	Nízká	Nízký až střední	Pasivní investor
DeFi investice	Krátkodobý až střední	Vysoké	Vysoká	Střední až vysoká	Střední až vysoký	Technicky zdatný, rizikový

Zdroj: Vlastní zpracování dle (46) (47) (48)

Každý investiční plán v kryptoměnách má své výhody a nevýhody a ten nejlepší pro daného investora závisí na jeho cílech, toleranci k riziku a zkušenostech. Dlouhodobé strategie jako HODL a staking poskytují stabilitu a pasivní zisky, ale vyžadují také trpělivost a víru v dlouhodobý růst trhu. Na druhé straně pokročilé strategie DeFi nebo krátkodobé obchodování mohou přinést větší zisky, ale jsou také spojeny s větší volatilitou a technickou složitostí. Proto je zásadní zvolit strategii, která vyhovuje investičnímu profilu investora a zohledňuje jak míru rizika, tak potenciální výnos.

Vzhledem k nízkému riziku a historicky vysokým přínosům bude zvolena investiční strategie, která bude založena na kombinaci **HODL** a **stakingu**. Dlouhodobým držením kryptoměn (HODL) lze ignorovat vliv přechodných cenových výkyvů a soustředit se na dlouhodobé zvyšování hodnoty. Kromě toho, že staking nabízí pasivní výnosy, umožňuje účast na zabezpečení sítě bez nutnosti aktivního obchodování. Tato strategie je spolehlivá, efektivní a obzvláště vhodná v prostředí, kde se zvýšila volatilita trhu.

4 Vlastní práce

Praktická část se zaměřuje na implementaci strategie HODL + staking na kryptoměně Solana (SOL) s využitím Phantom Wallet. Jako výchozí kapitál byla stanovena částka 500 CZK a sledovací horizont 1 měsíc. Je nezbytné zdůraznit, že tento časový horizont byl zvolen výhradně pro demonstraci technického průběhu mechanismu stakingu, tedy procesu delegování aktiv a připisování odměn v reálném čase. Z hlediska investiční strategie HODL, která je svou podstatou dlouhodobá a cílí na několikaleté cykly, není měsíční období pro validaci ziskovosti či ekonomické efektivity relevantní. Výsledky v této práci tak slouží primárně k ověření funkčnosti technologických nástrojů (peněženky a blockchainu), nikoliv k hodnocení tržní úspěšnosti zvolené strategie.

Postup zahrnuje jednorázový nákup SOL, delegování dostupné části do stakingu, týdenní zaznamenávání hodnoty portfolia (v CZK i v SOL) a evidenci transakčních nákladů a přijatých odměn. Výstupy obsahují tabulky a grafy s časovým vývojem, výpočet absolutního a relativního zhodnocení a kritické zhodnocení omezení experimentu. Práce není investičním doporučením.

4.1 Solana (SOL)

Kryptoměna Solana (SOL) je open-source blockchainová platforma, jejíž vývoj byl zahájen týmem kolem Anatolyho Yakovenka a veřejně uvedena do provozu v roce 2020. Token SOL slouží jako nativní aktivum pro úhradu transakčních poplatků, účast v síťové správě a staking. (54)

Solana kombinuje mechanismy Proof of History (PoH) a Proof of Stake (PoS). PoH generuje sekvence hashů, které působí jako „kryptografické hodiny“, což umožňuje chronologicky řadit události bez nutnosti intenzivní synchronizace mezi uzly. Po těchto časových značkách probíhá konsenzus pomocí PoS, kde validátoři potvrzují bloky na základě delegovaných SOL tokenů. Tato architektura umožňuje síti vysokou propustnost a rychlou finalitu, přičemž průměrný čas blokace se uvádí kolem stovek milisekund. (54) (55)

Mezi klíčové výhody patří:

- vysoká rychlost zpracování transakcí,
- nízké náklady na transakce,
- schopnost podporovat paralelní vykonávání operací.

Solana rovněž těží z aktivního vývojářského ekosystému a širšího využití v DeFi, NFT a dalších oblastech. Naopak mezi rizika patří možnost centralizace validátorů (velké podíly u úzké skupiny uzlů), technické výpadky sítě při velkém zatížení a regulatorní nejistoty v oblasti kryptoměn. (54) (55)

4.1.1 Staking na síti Solana

Staking funguje prostřednictvím delegování SOL tokenů na konkrétní validátory. Uživatelé vytvářejí stake account, poté delegují prostředky, které se zapojují do konsenzu. Odměny se vyplácejí v rámci epoch, každá epocha trvá zhruba 2 dny. Výnosnost stakingu se odhaduje v rozmezí 5 % až 7 % ročně, v závislosti na výkonu validátora, inflaci a poplatcích. (54) (55)

4.1.2 Popularita a tržní hodnota

Solana patří mezi nejaktivnější blockchainové sítě podle počtu aktivních adres: podle Tokenterminalu má síť měsíčně ~39,4 milionu aktivních adres. Tržní kapitalizace SOL činí přibližně 123 miliardy USD. Solana je rovněž často zmiňována v analýzách jako významný a likvidní trh srovnatelný s bitcoiny a ethereem, s vysokou úrovní obchodování a hloubkou trhu. (56)

Vzhledem k vysoké propustnosti, nízkým transakčním nákladům, funkčnímu stakingu a silné adoptivní základně byla Solana zvolena jako optimální kryptoměna pro praktickou část práce. Tato volba umožňuje demonstrovat strategii HODL + staking v reálném prostředí s minimálními bariérami vstupu.

4.2 Phantom Wallet (Phantom)

Peněženka Phantom je ne-custodial softwarová peněženka určená pro správu kryptoměn a přístup k decentralizovaným aplikacím, dostupná jako rozšíření do prohlížeče a mobilní aplikace.

Phantom byl původně navržen pro ekosystém Solana, v průběhu vývoje byl rozšířen o podporu dalších sítí a funkcí, čímž vznikla multi-chain platforma pro tokeny a NFT. (57)

Phantom nabízí uživatelské rozhraní pro držení, odesílání, přijímání a směnu tokenů přímo v rámci peněženky, včetně integrované funkce swapu a podpory pro hardware peněženky (např. Ledger). Produktová dokumentace a vývojářská sekce popisují dostupné

formáty (prohlížečová rozšíření, iOS, Android) a integrace pro připojování dAppů pomocí standardizovaných wallet-connectorů. (57)

4.2.1 Bezpečnost a auditní přístupy

Phantom implementuje bezpečnostní prvky včetně „transaction previews“ (přehledy transakcí) a detekce podvodných transakcí, které jsou navrženy tak, aby uživatele varovaly před škodlivými podepisovanými operacemi. (57)

Nezávislé audity a bezpečnostní reporty byly publikovány s cílem ověřit implementaci bezpečnostních mechanismů a rizikové oblasti, přičemž auditní zprávy popisují konkrétní zjištění a doporučení pro zlepšení. (58)

4.2.2 Staking a integrace se Solana

Phantom umožňuje uživatelům realizovat staking SOL přímo v peněžence. Proces zahrnuje vytvoření stake účtu a delegování prostředků na zvoleného validátora. Kromě nativního stakingu Phantom podporuje i možnosti „liquid staking“, kdy je SOL za specifických podmínek zaměněn za tokenizovanou reprezentaci stakovaných prostředků (např. pSOL), čímž se udržuje likvidita stakovaných aktiv. (57)

Na základě vlastností, jako je například jednoduché uživatelské rozhraní, integrované funkce pro staking a bezpečnosti byla *Phantom Wallet* vybrána jako vhodné rozhraní pro realizaci praktické části, tedy nákup, správa a delegování SOL.

4.3 Nákup a staking SOL kartou přes Phantom Wallet

Cílem je popsat reprodukovatelný, bezpečný a dokumentovaný postup jednorázového nákupu tokenu SOL v hodnotě 500 CZK prostřednictvím platební karty v rozhraní Phantom Wallet, včetně přednákupních kontrol, nastavení zabezpečení peněženky, detailního postupu transakce a povinných položek pro záznam a verifikaci.

Požadavky:

- Nainstalovaná a inicializovaná aplikace Phantom (mobilní aplikace nebo prohlížečové rozšíření).
- Funkční platební karta (debetní nebo kreditní) s povolenými mezinárodními platbami.
- Offline uložená seed phrase (fyzický zápis na bezpečném místě).

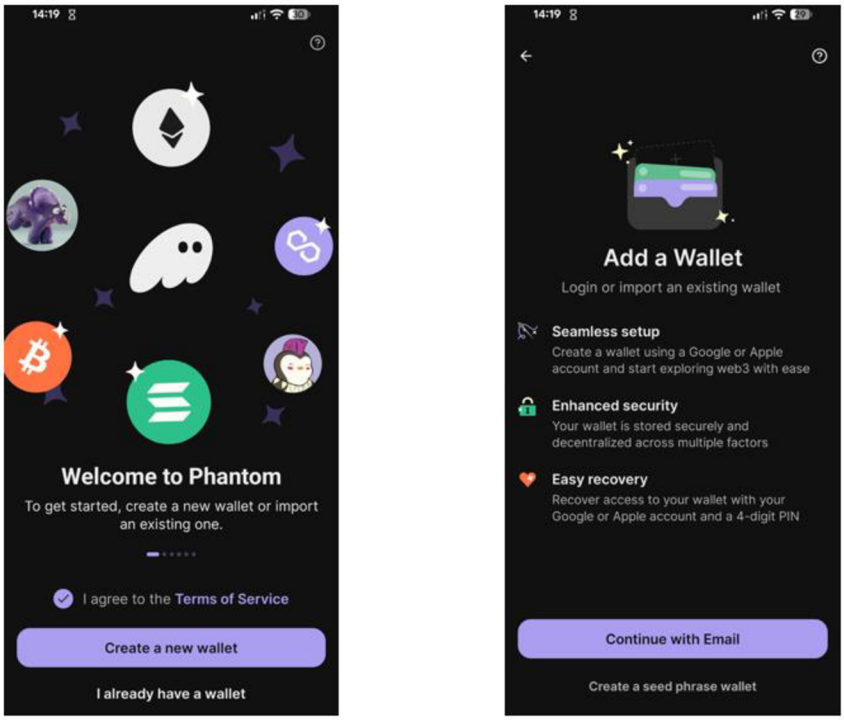
- Připravený záznamový systém (CSV/Excel šablona) pro log transakcí a screenshoty.

Před nákupem je klíčové ověřit původ aplikace, ideálně přímo na oficiálním webu či v autorizovaném obchodu. Důraz je kladen také na aktualizaci operačního systému a přítomnost antivirového softwaru, přičemž manipulace s platební kartou musí probíhat výhradně na zabezpečeném zařízení.

4.3.1 Vytvoření peněženky v Phantom

Po instalaci a přihlášení do aplikace Phantom se zobrazí hlavní uživatelské rozhraní. Následně byla po spuštění aplikace zvolena možnost „Create New Wallet“, čímž byl zahájen proces vytvoření nové peněženky. Tento proces dokumentuje obrázek č. 5

Obrázek č. 5: Úvodní obrazovka a vytvoření nové peněženky v aplikaci Phantom

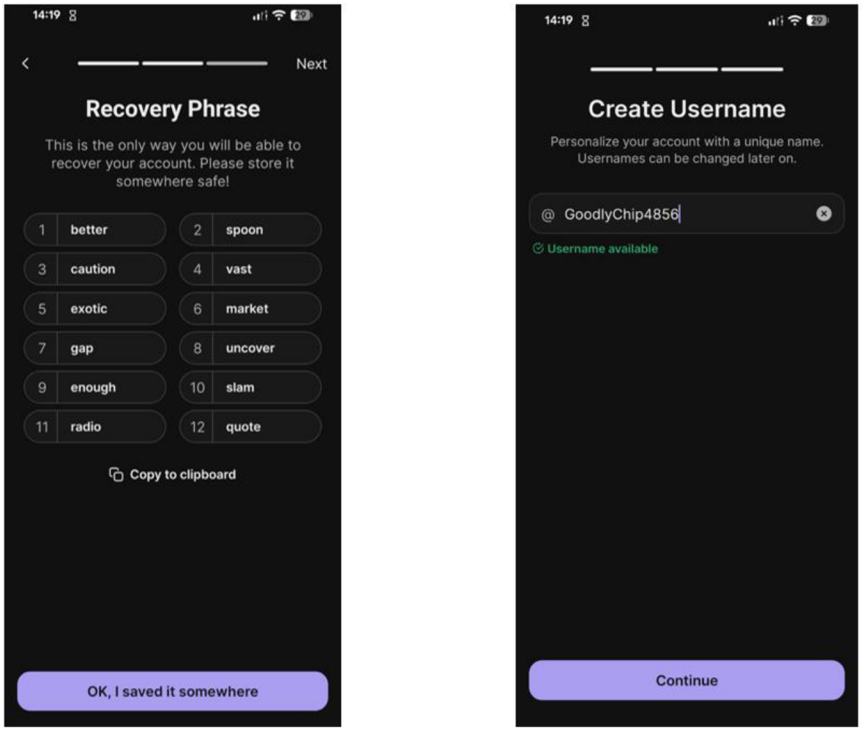


Zdroj: vlastní zpracování

Aplikace následně vygenerovala recovery phrase, tvořenou dvanácti anglickými slovy, která slouží k obnově peněženky v případě ztráty přístupu. (58) Tato fráze byla fyzicky zapsána a bezpečně uložena offline. Následně aplikace vyzvala k vytvoření uživatelského jména, které slouží pro snadnější identifikaci účtu a zobrazení v uživatelském rozhraní. Na

obrázku č. 6 jsou znázorněny dva kroky procesu vytváření peněženky – zobrazení recovery phrase a vytvoření uživatelského jména v aplikaci Phantom.

Obrázek č. 6: Recovery Phrase a vytvoření uživatelského jména v aplikaci Phantom



Zdroj: vlastní zpracování

4.3.2 Nákup SOL platební kartou v Phantom

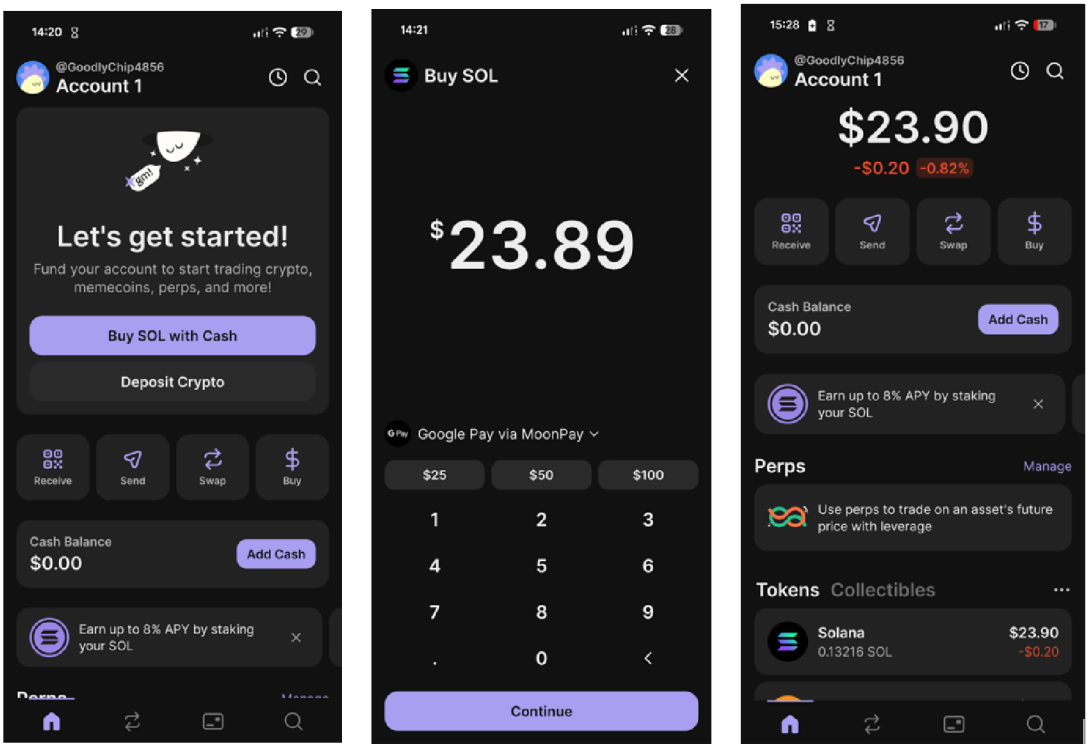
Po zadání a potvrzení uživatelského jména byla peněženka úspěšně inicializována a zobrazila se úvodní obrazovka s výchozím účtem připraveným pro přijímání a odesílání tokenů SOL. V aplikaci Phantom byla zvolena možnost Buy, která umožňuje přímý nákup kryptoměny Solana prostřednictvím platební karty. V rámci tohoto rozhraní byla nastavena částka 23,89 USD, odpovídající přibližně 500 CZK podle aktuálního směnného kurzu ČNB.

Po zadání částky byl automaticky vybrán poskytovatel služby *MoonPay*, který zajišťuje převod fiat měny na kryptoměnu. Tato služba vyžadovala ověření identity uživatele v rámci procesu KYC, tedy zadání osobních údajů, jako jsou jméno, datum narození, adresa a číslo pasu nebo občanského průkazu. (59) Tyto údaje byly použity výhradně pro účely ověření identity u poskytovatele a nebyly součástí vizuální dokumentace v této práci z důvodu ochrany osobních údajů.

Po úspěšném dokončení ověřovacího procesu proběhla platba částky 23,89 USD prostřednictvím platební karty. Transakce byla zpracována poskytovatelem *MoonPay* a zakoupené tokeny *SOL* byly po krátké době automaticky připsány do peněženky *Phantom*. Na hlavní obrazovce peněženky byl následně viditelný zůstatek odpovídající hodnotě zakoupených tokenů, vyjádřený v *SOL* a ekvivalentu USD. Tímto krokem byl proces nákupu úspěšně dokončen a peněženka byla připravena pro další činnosti, jako je staking nebo sledování hodnoty investice v čase.

Na obrázku č. 7 jsou znázorněny tři kroky: úvodní obrazovka peněženky *Phantom* po dokončení vytvoření účtu, rozhraní pro nákup kryptoměny SOL a následný přehled zůstatku po dokončení transakce.

Obrázek č. 7: Úvodní obrazovka, nákup kryptoměny SOL a zobrazení tokenů v peněžence Phantom



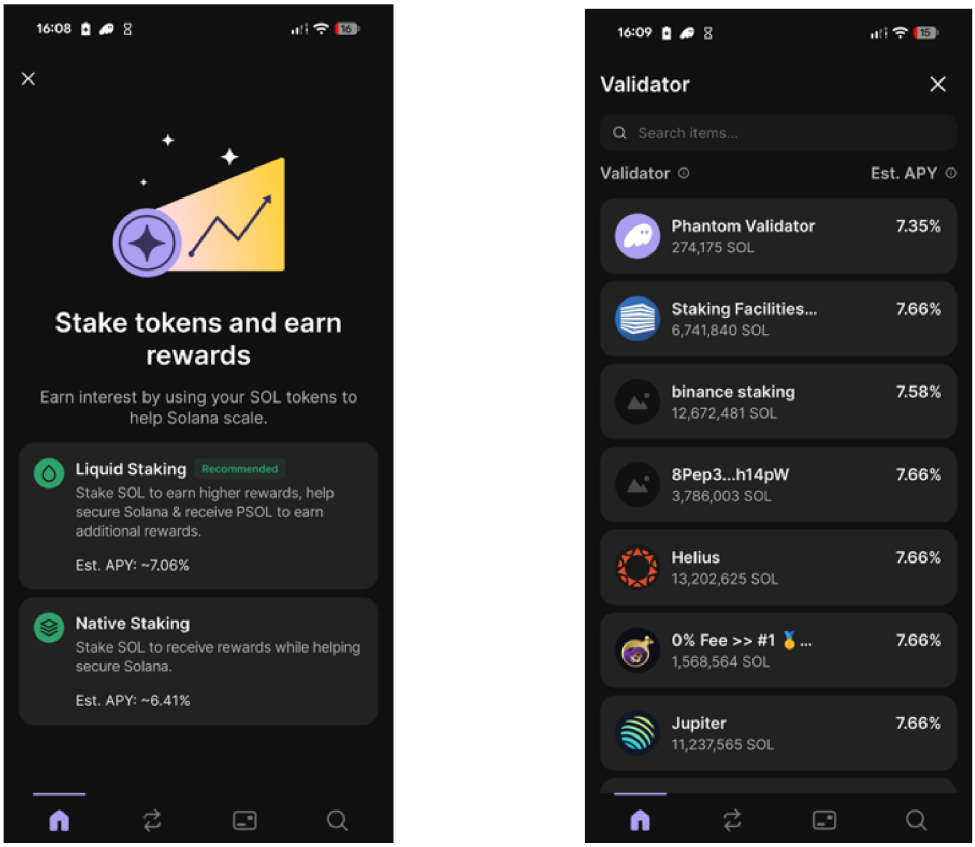
Zdroj: vlastní zpracování

4.3.3 Staking SOL v peněžence Phantom

Po úspěšném nákupu tokenů *SOL* byla zahájena fáze jejich zhodnocování prostřednictvím stakingu, tedy uzamčení určitého množství tokenů pro podporu validátorů sítě *Solana* výměnou za odměny ve formě nově emitovaných tokenů. Proces stakingu byl

proveden přímo v aplikaci *Phantom*. Obrázek č. 8 demonstruje aktivaci stakingu a výběr validátora v aplikaci *Phantom*.

Obrázek č. 8: Spuštění procesu stakingu a výběr validátora v aplikaci Phantom

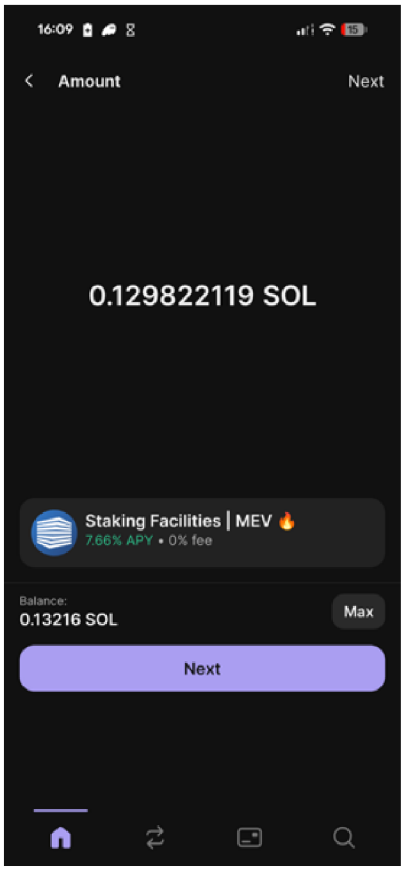


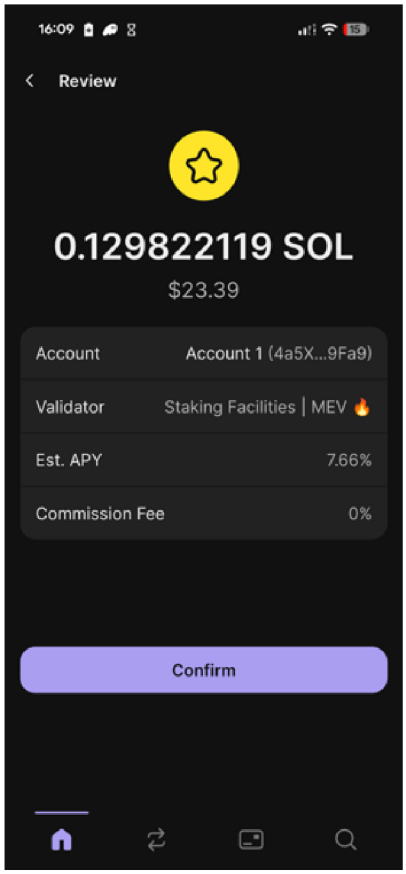
Zdroj: vlastní zpracování

Byl vybrán validátor „*Staking Facilities | MEV*" ze seznamu dostupných uzlů. Volba validátora byla provedena na základě několika kritérií, především úrovně komise (commission rate), spolehlivosti uzlu a objemu již delegovaných prostředků. Pro účely experimentu byl zvolen validátor s bez komisí, aby bylo možné realisticky sledovat běžné zhodnocení stakingu.

Po potvrzení volby validátoru byla zadána částka k delegování a potvrzena transakce. Proces byl dokončen úspěšným potvrzením transakce v blockchainu, přičemž transakční poplatek činil 0,00009 SOL. Na obrázku č. 9 je znázorněno zadání částky k delegování a potvrzení transakce.

Obrázek č. 9: Zadání částky k delegování a potvrzení transakce





Zdroj: vlastní zpracování

Od tohoto okamžiku je staking aktivní a po dobu jednoho měsíce budou sledovány změny hodnoty portfolia a získané odměny.

4.4 Výnosy z relativně bezpečných investic

V této kapitole je provedeno srovnání tří typů investic, které lze považovat za relativně bezpečnější než spekulativní aktiva, přičemž cílem je poskytnout kontext pro rozhodování o alokaci kapitálu v praktické části práce. Pro každý typ je uvedena typická roční návratnost, historické chování a klíčová rizika.

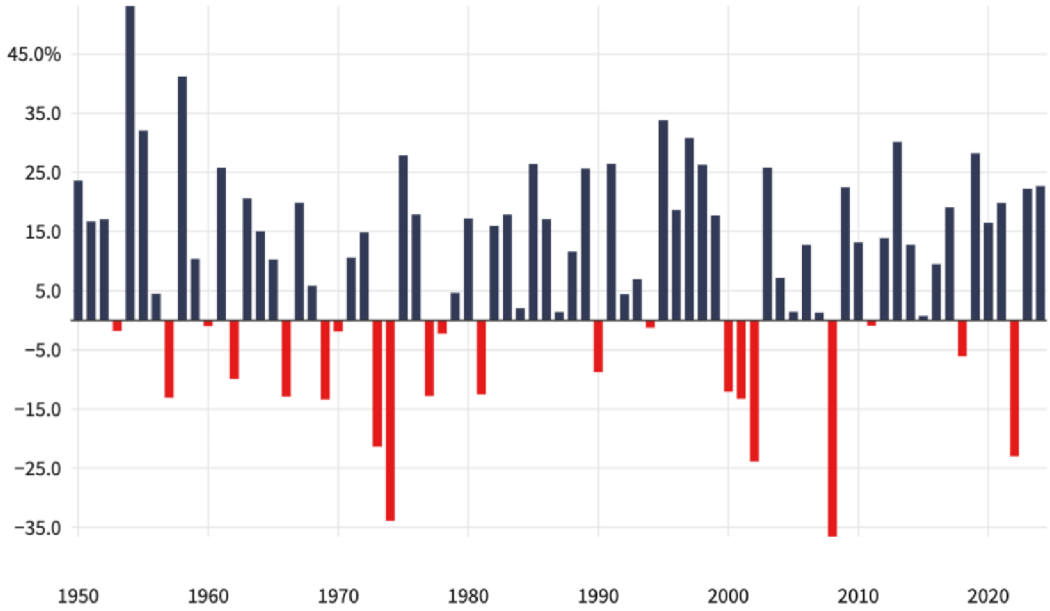
4.4.1 Investice do fondu sledujícího S&P 500

Investice do indexového fondu sledujícího S&P 500 znamená expozici vůči přibližně 500 největším americkým společnostem podle tržní kapitalizace. Index je tradičně považován za měřítko výkonnosti velkých amerických akcií a je často využíván jako základní prvek diverzifikovaných portfolií. Historicky se průměrná roční návratnost tohoto indexu pohybuje kolem 10 % ročně v rozmezí posledních desetiletí, včetně reinvestovaných

dividend. Za období od roku 1927 do současnosti index vykázal stabilní růstovou trajektorii s průměrem blížícím se oněm 8 – 10 % ročně, přičemž jednotlivé roky vykazují značnou volatilitu. (60) (61)

Obrázek č. 10 ilustruje reálné roční zhodnocení indexu S&P 500 od roku 1950, včetně jeho výrazné volatility v jednotlivých letech.

Obrázek č. 10: Roční reálné výnosy indexu S&P 500 od roku 1950



Zdroj: Investopedia (60)

Pro účely komparace s praktickou částí byla provedena simulace investice částky 500 CZK do ETF kopírujícího index S&P 500 v identickém časovém okně jako u stakingu Solana (12. 10. 2025 – 12. 11. 2025).

Pro realizaci byla zvolena platforma Trading 212, která u malých objemů portfolia (do 60 000 CZK) neúčtuje poplatky za vedení účtu ani provize za obchod. V sledovaném období zaznamenal index nárůst z hodnoty 6 628 bodů na 6 848 bodů, což představuje zhodnocení o přibližně 3,32 %. Protože doba držení investice nepřesáhla 3 roky, podléhá tento zisk v České republice zdanění sazbou 15 %.

Výpočet čistého výnosu je uveden v tabulce č. 14.

Tabulka č. 14: Výpočet čistého výnosu u investice do S&P 500

Položka	**Hodnota / Výpočet**
Počáteční investice	500,00 CZK
Hodnota indexu (nákup)	6 628 bodů
Hodnota indexu (prodej)	6 848 bodů
Hrubý výnos (%)	+3,32 %
Hrubý zisk	16,60 CZK
Poplatky (Trading 212)	0,00 CZK
Daň z příjmu (15 %)	-2,49 CZK
Čistý zisk	**+14,11 CZK**
Konečná hodnota	**514,11 CZK**

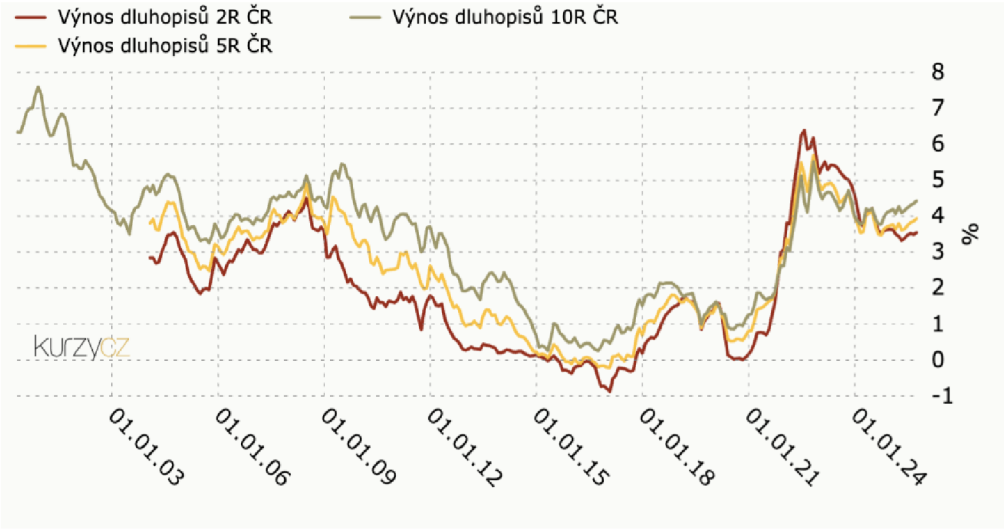
Zdroj: vlastní zpracování

4.4.2 Investice do vládních státních dluhopisů

Vládní státní dluhopisy (např. vydávané ČNB / státem ČR) jsou považovány za relativně bezpečnější aktivum, neboť nesou méně kreditního rizika než korporátní dluhopisy či akcie. Například výnos 10letých státních dluhopisů ČR v roce 2025 činil přibližně 4,0-4,4 % ročně. U dlouhodobých emisí je výnos v podobném pásmu kolem 4 % p.a. Tyto výnosy jsou nižší než u akcií, ale riziko poklesu jistiny je obecně nižší.

Investice do státních dluhopisů poskytuje stabilitu a předvídatelnost výnosů, zejména v prostředích s pevně stanovenou kupónovou sazbou. (62) (63) Obrázek č. 11 ukazuje vývoj výnosových křivek českých státních dluhopisů s různou splatností (2R, 5R, 10R) v období od roku 2000.

Obrázek č. 11: Roční výnosy českých státních dluhopisů od roku 2000



Zdroj: KURZY.CZ. Státní dluhopisy (62)

V případě investice do českých státních dluhopisů ve stejném období vycházíme z průměrného ročního výnosu, který se v daném roce pohyboval kolem 4,20 % p.a.

Zásadní výhodou pro drobné investory v ČR je osvobození výnosů ze státních dluhopisů od daně z příjmů (u emisí vydaných po 1. 1. 2021). Při měsíční alikvotní části ročního úroku a nulových vstupních poplatcích (při nákupu přes elektronický přístup ke správě majetkového účtu) vypadá zhodnocení následovně (Tabulka č. 15):

Tabulka č. 15: Výpočet čistého výnosu u státních dluhopisů

Položka	**Hodnota / Výpočet**
Počáteční investice	500,00 CZK
Roční výnos (odhad)	4,20 % p.a.
Měsíční výnos (hrubý)	0,35 %
Hrubý zisk	1,75 CZK
Poplatky	0,00 CZK
Daň z příjmu (0 %)	0,00 CZK
Čistý zisk	**+1,75 CZK**
Konečná hodnota	**501,75 CZK**

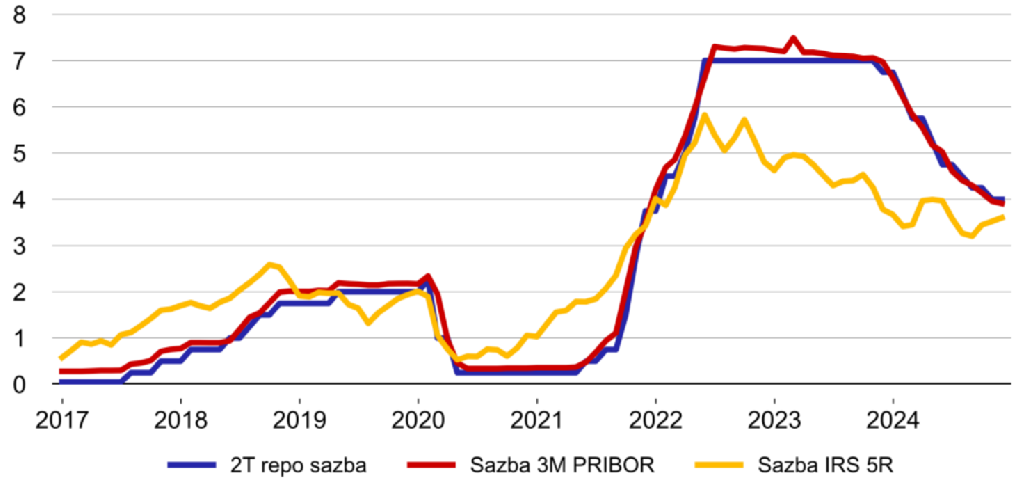
Zdroj: vlastní zpracování

4.4.3 Spořicí produkty v ČR

Stavební spoření a spořicí účty v České republice mohou být považovány za nejkonzervativnější formu investice, obzvláště pokud cílem je ochrana kapitálu a likvidita. Podle analýz se současné úrokové sazby u spořicích účtů pohybují v ČR v pásmu 0,01 % až 4 % ročně, průměrně kolem 2,5 % ročně v makroprostředí. Výše těchto sazeb se přitom do značné míry odvíjí od základních úrokových sazeb stanovených Českou národní bankou (64).

Obrázek č. 12 znázorňuje vývoj klíčových úrokových sazeb ČNB v časovém horizontu 2017–2025, který přímo souvisí s úročením vkladů u bank.

Obrázek č. 12: Vývoj úrokových sazeb České národní banky 2017-2025



Zdroj: Česká Národní Banka (65)

Výnosy této formy investice jsou velmi nízké ve srovnání s akciovými nebo dluhopisovými investicemi, ale přinášejí minimální riziko ztráty kapitálu a nejvyšší likviditu.

Jako reprezentativní příklad bankovního spořicího produktu byl zvolen spořicí účet u Raiffeisenbank, který v daném období nabízel úrokovou sazbu 4 % p.a. při plnění podmínek aktivního využívání (10 plateb kartou). Úroky na spořicích účtech v ČR podléhají srážkové dani ve výši 15 %, kterou banka odvádí automaticky. Za sledované měsíční období by zhodnocení vkladu 500 CZK vypadalo takto (Tabulka č. 16):

Tabulka č. 16: Výpočet čistého výnosu u spořicího účtu

Položka	**Hodnota / Výpočet**
Počáteční investice	500,00 CZK
Roční úroková sazba	4,00 % p.a.
Měsíční úrok (hrubý)	~0,33 %
Hrubý zisk	1,67 CZK
Poplatky	0,00 CZK
Srážková daň (15 %)	-0,25 CZK
Čistý zisk	**+1,42 CZK**
Konečná hodnota	**501,42 CZK**

Zdroj: vlastní zpracování

Z porovnání tří investičních druhů vyplývá následující:

- Fond sledující S&P 500 nabízí nejvyšší potenciální výnos, avšak s vyšším rizikem a větší variabilitou výsledků.

- Státní dluhopisy nabízejí střední úroveň výnosu a relativně nízké riziko, vhodné pro stabilnější část portfolia.
- Spořicí produkty představují nejnižší výnosovou úroveň, ale zároveň nejnižší riziko a vysokou likviditu, vhodné pro ochranu kapitálu a krátkodobější horizont.

Pro přehlednost je níže uvedena souhrnná Tabulka č. 17 porovnávající čisté výsledky všech tří konzervativnějších strategií:

Tabulka č. 17: Srovnání čistého zhodnocení investice 500 CZK

Typ investice	Riziko	Čistý zisk/ztráta (CZK)	Konečná hodnota (CZK)	Zhodnocení (%)
Index S&P 500 (ETF)	Střední/Vyšší	+14,11 CZK	514,11 CZK	+2,82 %
Státní dluhopisy ČR	Nízké	+1,75 CZK	501,75 CZK	+0,35 %
Spořicí účet	Minimální	+1,42 CZK	501,42 CZK	+0,28 %

Zdroj: vlastní zpracování

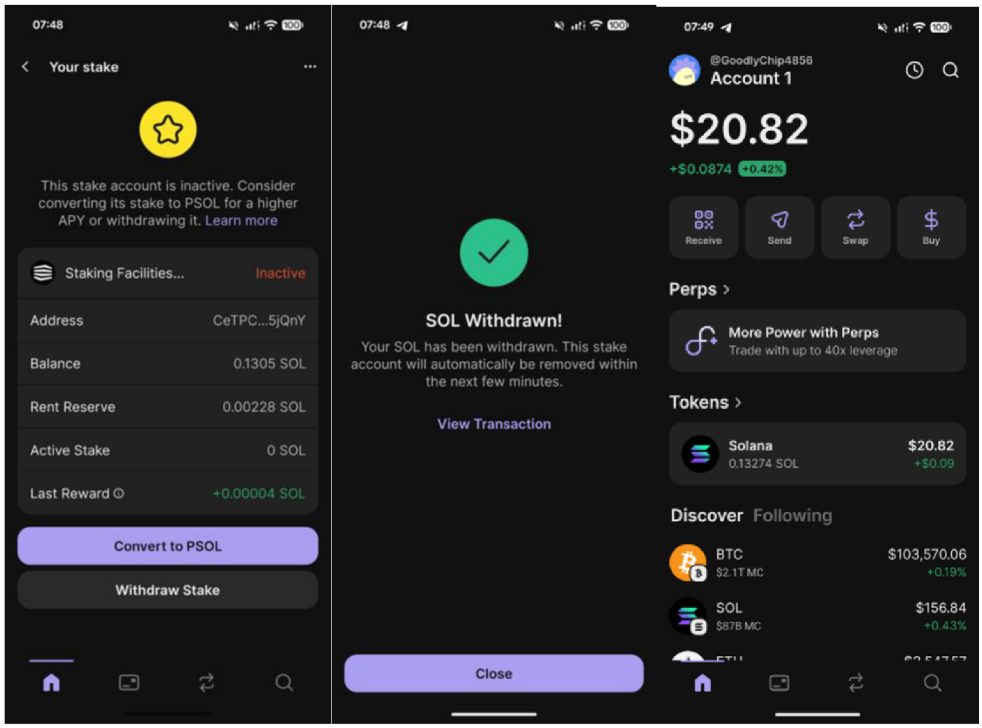
4.5 Vyhodnocení stakingu

Po uplynutí jednoho měsíce byl ukončen proces stakingu tokenů *SOL* a následně bylo provedeno jeho vyhodnocení. Na začátku bylo delegováno **0,12982 SOL**, po ukončení stakingu činil celkový zůstatek **0,13274 SOL**. Z uvedených hodnot vyplývá nárůst o **0,00058 SOL**, což představuje měsíční výnos přibližně **+0,44 %**. Tento výnos je tvořen odměnami generovanými validátorem, kterému byly tokeny delegovány, jako kompenzace za účast na zabezpečení sítě Solana a potvrzování transakcí.

Při anualizaci výsledku (přepočet na roční období při zachování konstantní výkonnosti validátora) staking odpovídá přibližně **5,28 % p.a**. Tento výnos je však mírně nižší, než bylo očekáváno. Důvodem je skutečnost, že byla delegována pouze částečná částka z celkového zůstatku z důvodu technických omezení peněženky, ovlivnilo přesnost výsledku. Navíc je třeba zohlednit, že doba stakingu byla poměrně krátká, jelikož samotná aktivace stakingu po delegování tokenů trvá několik dní, během nichž se odměny ještě negenerují.

Obrázek č. 13 zobrazuje hlavní okno peněženky Phantom po ukončení stakingu.

Obrázek č. 13: Ukončení stakingu a hlavní okno peněženky Phantom



Zdroj: vlastní zpracování

Současně však během sledovaného období došlo k poklesu tržní ceny tokenu SOL z 180,77 USD (v moment nákupu) na 156,84 USD (v moment ukončení stakingu). Tento vývoj představuje ztrátu tržní hodnoty o -12,85 %. Na obrázku č. 14 je zobrazen vývoj ceny kryptoměny Solana během sledovaného období.

Obrázek č. 14: Vývoj ceny Solana od 12.10.2025

Zdroj: Trading View (66)

I přes výnosy generované stakingem došlo k poklesu celkové hodnoty portfolia vyjádřené v CZK. Přehled výsledků shrnuje tabulka č. 18.

Tabulka č. 18: Přehled výsledků stakingu

Parametr	Hodnota při zahájení	Hodnota při ukončení	Změna
Množství SOL	0,13216 SOL	0,13274 SOL	+0,00058 SOL (+0,44%)
Cena SOL (USD)	180,77 USD	156,84 USD	-23,93 USD (-13,24 %)
Hodnota v USD	23,89 USD	20,82 USD	-3,07 USD (-12,85 %)
Hodnota v CZK	500 CZK	433,55 CZK	-66,45 CZK (-13,29 %)

Zdroj: vlastní zpracování dle (56) (62)

Výsledek investice byl negativně ovlivněn zvýšenou tržní volatilitou, která v daném období souvisela s mimořádnými politickými a makroekonomickými událostmi. V říjnu 2025 došlo ve Spojených státech amerických k federálnímu „government shutdownu“, tedy faktickému uzavření části vládních institucí v důsledku neschválení rozpočtu Kongresem. Tento stav začal 1. října 2025 a v době ukončení sledovaného období trval již více než 43 dní, čímž se stal nejdelším vládním shutdownem v historii USA. Tato událost zvýšila nejistotu investorů a vedla ke krátkodobému poklesu rizikových aktiv, včetně kryptoměn.

Výsledky tedy potvrzují, že staking lze považovat za stabilní formu pasivního výnosu, který však nezaručuje ochranu před cenovou volatilitou trhu. Zatímco technicky staking přinesl pozitivní zhodnocení drženého množství SOL, pokles tržní ceny způsobil celkový pokles nominální hodnoty investice. Z hlediska investiční strategie lze staking chápat jako nástroj dlouhodobého zhodnocování v rámci volatilního aktiva, jehož výsledky jsou vhodné porovnávat spíše s časovým horizontem delším než jeden měsíc.

5 Vysledky a diskuse

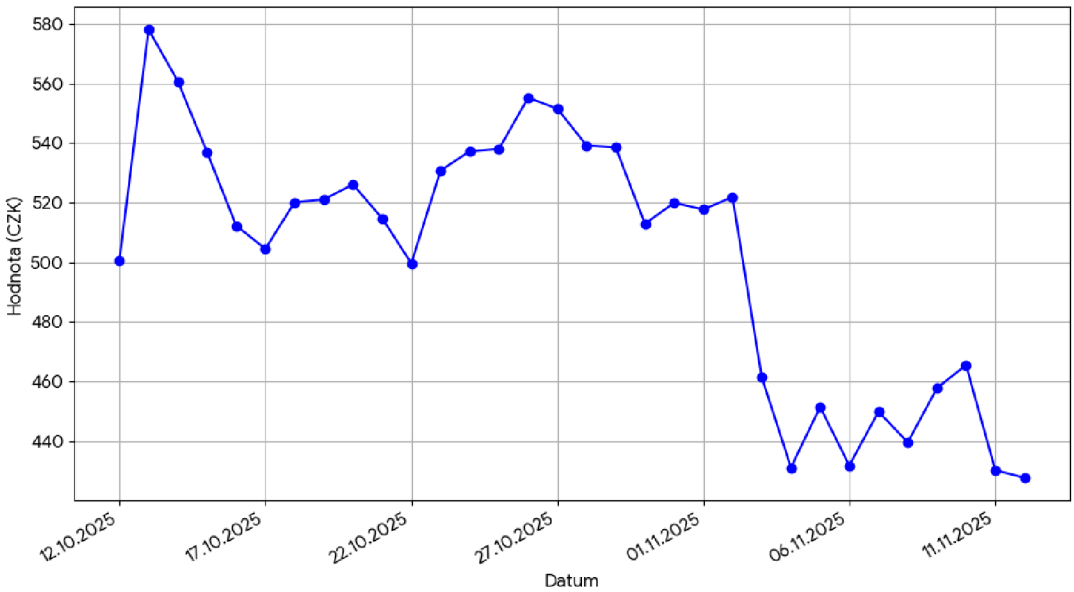
5.1 Vysledky

Hlavním cílem této práce byla identifikace výnosnosti a rizikovosti strategie HODL spojenou se stakingem. Analýza byla provedena na základě denních dat kryptoměny Solana v peněžence Phantom v období od 12. 10. 2025 do 12. 11. 2025 s počátečním vkladem 500 CZK.

Pro vyhodnocení rizikovosti byly aplikovány metody finanční analýzy stanovené v metodice práce. Výpočet Max Drawdown (poklesu od lokálního maxima k minimu) ukázal, že portfolio je extrémně volatilní. Zatímco dne 13. 10. dosáhla hodnota portfolia maxima 578,18 CZK díky krátkodobému růstu ceny, následný trend byl silně klesající. Maximální pokles z tohoto vrcholu činil 26,04 %, což indikuje vysokou míru rizika, kterou musí investor akceptovat.

Z pohledu výnosnosti generoval staking na Solaně technický výnos. Množství držených aktiv se zvýšilo o 0,00058 SOL, což odpovídá anualizovanému výnosu přibližně 5,28 %. Nicméně, při přepočtu na české koruny skončila strategie ve ztrátě. Konečná hodnota portfolia k datu 12. 11. činila 427,62 CZK.

Obrázek č. 15: Vývoj hodnoty portfolia v CZK během stakingu



Zdroj: vlastní zpracování

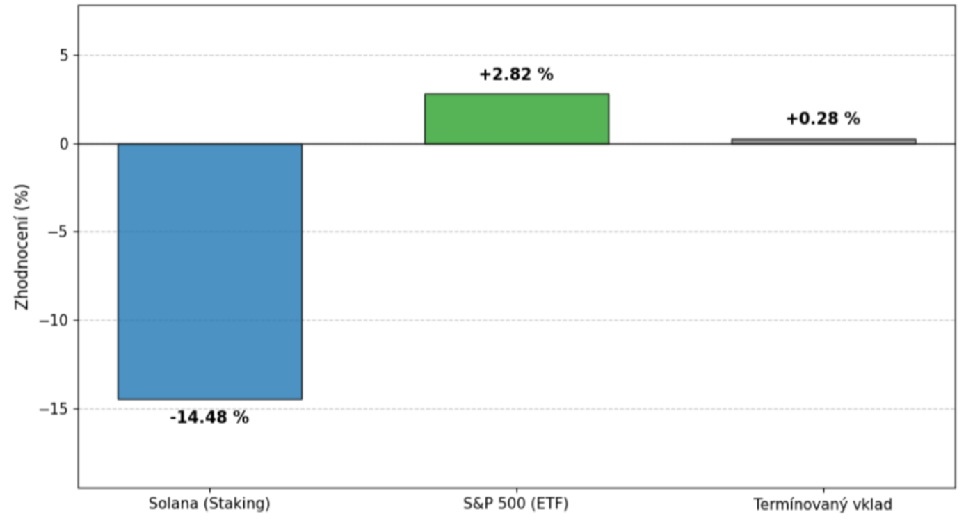
Výpočet Sharpeho poměru, který měří výnos očištěný o riziko, vyšel pro toto sledované období na hodnotě -1,63. Záporná hodnota tohoto ukazatele říká, že podstoupené riziko nebylo kompenzováno adekvátním výnosem. Ve srovnání s bezrizikovou sazbou 4 % p.a. (spořicí účet) byla investice do Solany v tomto krátkém okně neefektivní.

V souladu s cíli práce byly porovnány výsledky s tradičními aktivy (Obrázek č. 16 a Tabulka č. 19):

1 Termínované vklady a spořicí účty: tyto nízkorizikové nástroje přinesly v rámci experimenta stabilní, i když nízký výnos. Na rozdíl od Solany zde byl drawdown nulový.

2 Podílové a indexové fondy: byl zvolen ETF sledující index S&P 500. Ten dosáhl ve stejném období čistého zhodnocení +2,82 % (zisk 14,11 CZK).

Obrázek č. 16: Porovnání procentuálního zhodnocení nástrojů



Zdroj: vlastní zpracování

Tabulka č. 19: Srovnání výnosnosti a rizika investičních nástrojů

Investiční nástroj	Počáteční vklad	Konečná hodnota	Zisk/Ztráta	Max. Drawdown	Sharpeho poměr
Solana (Staking)	500,00 CZK	427,62 CZK	-14,48 %	-26,04 %	-1,63
S&P 500 (ETF)	500,00 CZK	514,11 CZK	+2,82 %	-1,20 %	1,82
Termínovaný vklad	500,00 CZK	501,42 CZK	+0,28 %	0,00 %	0,00

Zdroj: vlastní zpracování

5.2 Diskuse

V teoretické části byl stanoven cíl popsat ekonomické aspekty stakingu a vliv volatility. Praktický experiment tyto teoretické předpoklady potvrdil a výsledky je možné konfrontovat se závěry konkrétních zahraničních studií.

Výsledky práce silně korelují s výzkumem, který publikovali Lin William Cong, Zhiheng He a Ke Tang ve své studii s názvem „Staking, Token Pricing, and Crypto Carry“. Autoři v této práci rozlišují mezi „staking reward rate“ (odměnou za staking) a cenovým rizikem podkladového aktiva. V experimentu bylo potvrzeno přesně to, co Cong, He a Tang popisují: technický mechanismus generování odměn fungoval bezchybně, ale tržní cena aktiva má na celkovou krátkodobou ziskovost mnohem větší vliv. (67)

Tento závěr podporuje i Fahad Saleh ve svém článku „Blockchain without Waste: Proof-of-Stake“, kde upozorňuje, že ekonomická rovnováha v Proof-of-Stake systémech je citlivá na externí šoky, což se v mém měření projevilo negativním dopadem vládního shutdownu v USA. (44)

Zásadním faktorem, který ovlivnil analýzu, byla extrémní volatilita. Max Drawdown ve výši 26,04 % není u kryptoměny Solana výjimečný. Studie nazvaná „Comparative Performance Analysis of Bitcoin, Ethereum, and Solana in the Crypto Market“ uvádí, že Solana historicky vykazuje mnohem vyšší volatilitu než Bitcoin. Zatímco Bitcoin často funguje jako uchovatel hodnoty, Solana je v této studii klasifikována jako aktivum s „agresivním růstovým potenciálem párovaným s vysokým rizikem“, což přesně odpovídá naměřené ztrátě cca 13 % během jediného měsíce. (68)

Při srovnání s tradičními aktivy výsledky odpovídají závěrům, které přináší článek „Comparative Analysis of the Performance of Cryptocurrency, Stocks and Forex as Investment Alternatives“. Tato studie na datech z let 2021–2024 ukazuje, že ačkoliv kryptoměny mohou nabízet vyšší absolutní výnos, jejich rizikově vážený výnos (měřený Sharpeho poměrem) může být v obdobích poklesu horší než u akcií. V experimentu vyšel Sharpeho poměr pro Solanu záporný (-1,63), zatímco pro index S&P 500 byl kladný, což potvrzuje tezi zmíněnou v článku, že bez dlouhého časového horizontu je riziko ztráty u kryptoměn neúměrně vysoké. (69)

Zcela zásadní změna ale nastala v oblasti regulačního prostředí, což mění pohled na dlouhodobou udržitelnost strategie. Zatímco starší literatura upozorňovala na legislativní

vakuum, nová situace platná od 15. 2. 2025 toto mění. Jak uvádí byvalý ministr financí Zbyněk Stanjura: *„Návrh zákona umožní nastavit ochranu spotřebitelů i v této oblasti a současně zvýší stabilitu finančního prostředí.“* (70)

Tato změna má přímý dopad na provedenou komparaci s akciemi. Sněmovna schválila časový test pro osvobození od daně z příjmů. Pokud investor drží kryptoměny déle než tři roky, jejich prodej nebude zdaněn. Tím se kryptoaktiva daňově vyrovnávají akciím (S&P 500) a strategie HODL se stává mnohem atraktivnější než dříve. Pro drobné investory, jako byl realizovaný experiment s 500 CZK, je klíčový také nově zavedený hodnotový test. Transakce do 100 tisíc Kč ročně nebude třeba uvádět v daňovém přiznání. Bezpečnost investice pak zvyšuje nařízení MiCA (Markets in Crypto-Assets) a DORA (Digital Operational Resilience Act), díky kterým budou poskytovatelé služeb podléhat dohledu ČNB. (70)

6 Závěr

Hlavním cílem bakalářské práce byla identifikace výnosnosti a rizikovosti strategií HODL a stakingu na základě reálných investičních dat a jejich porovnání s tradičními nástroji, jako jsou termínované vklady a nízkorizikové podílové fondy. Na základě provedeného experimentu se stakingem kryptoměny Solana lze říct, že kombinace stakingu se strategií HODL sice umožňuje dosáhnout vyššího naturálního zhodnocení v tokenech a částečně snižovat rizika oproti prostému držení. Nicméně, ve srovnání s tradičními investičními nástroji zůstává tato strategie nadále výrazně rizikovější a volatilnější, a proto není vhodná pro konzervativní krátkodobé zhodnocení kapitálu.

Z výsledků práce vyplývá, že strategie Solana (Staking) dosáhla nejhoršího ekonomického výsledku a skončila ve ztrátě. Naopak tradiční nástroje, tedy akciový index S&P 500 a termínovaný vklad, dokázaly hodnotu kapitálu navýšit. Strategie Solana byla identifikována jako investice s nejvyšší mírou podstoupeného rizika.

Je však nezbytné zohlednit fakt, že prezentovaná data pokrývají pouze velmi krátký časový úsek, který může být v kontextu dlouhodobých tržních cyklů zavádějící. Trh kryptoměn je extrémně volatilní a krátkodobé měření nemusí reflektovat celkový trend. Historický vývoj ukazuje masivní výkyvy, kdy například Solana v roce 2023 klesla o 96 % vůči svému maximu, aby následně k lednu 2025 zaznamenala růst o 3500 %. Lze tedy konstatovat, že ačkoli staking s jistotou generuje technický zisk v podobě nových jednotek kryptoměny, výsledná hodnota ve fiat měně je v takto omezeném časovém horizontu téměř zcela závislá na aktuální tržní ceně daného aktiva. Přestože nově implementované legislativní rámce přinášejí do tohoto prostředí vyšší míru právní jistoty, trh virtuálních měn si z globálního hlediska nadále zachovává vysoce spekulativní charakter a jeho reálný budoucí vývoj nelze spolehlivě predikovat.

V teoretické rovině práce byly vymezeny základní pojmy, bez kterých nelze problematiku pochopit. Základem je měna, chápaná jako univerzální prostředek směny a uchovatel hodnoty. Klasická fiat měna představuje peníze s nuceným oběhem, jejichž hodnota stojí a padá na důvěře v centrální autoritu. Virtuální měny tento koncept mění, jelikož fungují decentralizovaně. Neemituje je žádná banka, ale vznikají na základě kryptografických protokolů.

Technologickým pilířem je zde blockchain. Jde o distribuovanou účetní knihu, která zajišťuje, že záznamy jsou transparentní a zpětně neměnné. Prvním a nejvýznamnějším zástupcem této technologie je Bitcoin. Jeho zabezpečení zajišťuje mechanismus Proof-of-Work, který je založen na procesu těžby. K validaci transakcí je zde nutné vynaložit reálný výpočetní výkon a značné množství elektrické energie. To s sebou nese zásadní nevýhody: extrémní ekologickou zátěž a vysoké náklady, spojené především s vysokou spotřebou elektřiny.

Zcela odlišný přístup nabízí mechanismus Proof-of-Stake. Ten energeticky náročnou těžbu nahrazuje nutností vlastnit určitý podíl dané měny. Typickým představitelem této moderní architektury je síť Solana, která byla využita v praktické části práce. Vyznačuje se vysokou propustností transakcí a minimálními síťovými poplatky. A právě v kontextu zkoumané strategie byl klíčový proces stakingu, který je s protokolem Proof-of-Stake neoddělitelně spjat. Je to aktivní uzamčení aktiv v síti, kdy investor přispívá k bezpečnosti systému a výměnou dostává odměnu. Tím se tato metoda zásadně liší od pasivní strategie HODL, která je ve své podstatě pouhým držením kryptoměn.

Významnou roli hraje i legislativní rámec. Implementace nařízení MiCA spolu se zavedením časového a hodnotového testů přináší celému sektoru jasná pravidla v EU. Pro drobné investory to znamená vyšší právní jistotu a přiblížení k tradičním investičním nástrojům.

7 Seznam použitých zdrojů

1. TANENBAUM, Andrew S. *Structured Computer Organization. 6th Edition*, Pearson, 2013. ISBN: 978-0132916523
2. WILLIAMS, Michael R. *A History of Computing Technology (Perspectives #6) (Paperback).* Wiley-IEEE Computer Society PR, 1997. ISBN: 978-0818677397
3. STALLINGS, William. *Computer Organization and Architecture: Designing for Performance*. 10th Edition, Pearson, 2015. ISBN: 978-0134101613
4. OGBAN, Felix & Arikpo, Iwara & Eteng, Idongesit. *Von Neumann Architecture and Modern Computers.* Global Journal of Mathematical Sciences Vol. 6, No. 2, 2007. ISSN 1596-6208
5. HENNESSY, John L., PATTERSON, David A. *Computer Architecture: A Quantitative Approach*. 6th Edition, Morgan Kaufmann, 2017. ISBN: 978-0128119051
6. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016. ISBN 978-0691171692
7. Mark Lamourine *Modern computer architecture and organization.* USENIX, 2021. [online]. [cit. 27. 05. 2025]. Dostupné z: <https://www.usenix.org/publications/loginonline/modern-computer-architecture-and-organization>.
8. Jay Pankajkumar Kania. *Modern Computer Architecture using different Technique.* International Journal of Computer Applications, 2021. [online]. [cit. 27. 05. 2025]. Dostupné z: <https://www.ijcaonline.org/archives/volume183/number36/32166-2021921751/>.
9. Martina Blažková. *Jak využít internet v marketingu: krok za krokem k vyšší konkurenceschopnosti.* Grada Publishing, 2005. ISBN: 8024710951
10. KUROSE, James F., Keith W. ROSS. *Computer Networking: A Top-Down Approach. 8th Edition*. Pearson, 2021. ISBN: 978-0136681557.
11. Martin Sebera. *Úvod do internetu.* [online]. [cit. 20. 06. 2025]. Dostupné z: <https://is.muni.cz/el/fsps/jaro2005/t628/um/internet.pdf>.
12. TANENBAUM, Andrew S., David J. WETHERALL. *Computer Networks. 6th Edition. Pearson, 2021. ISBN:* 978-0136764052
13. CESNET. *30 let sítě CESNET rok po roku* [online]. Praha: CESNET, 15. 06. 2023

[cit. 2025-06-24]. Dostupné z: <https://www.cesnet.cz/pro-media/30-let-site-cesnet-rok-po-roku-64>.

14. Jiří Peterka. *Transportní vrstva.* Archiv článků a přednášek Jiřího Peterky, 2015. [online]. [cit. 20. 06. 2025]. Dostupné z: <https://www.earchiv.cz/a92/a224c110.php3>.
15. Jiří Peterka. *Báječný svět počítačových sítí, část IV.* Rodina protokolů TCP/IP. [online]. [cit. 20. 06. 2025]. Dostupné z: <https://www.earchiv.cz/b05/b0600001.php3>.
16. REJNUŠ, O. *Finanční trhy.* 4. vyd. Praha: Grada 2014, dotisk 2017. 768 s. ISBN 978-8024736716.
17. ČNB Česká Národní Banka. *Podstata peněz a role centrálních bank.* [online]. [cit. 27. 06. 2025]. Dostupné z: <https://www.cnb.cz/cs/menova-politika/vzdelavani/1.-podstata-penez-a-role-centralnich-bank/>.
18. ČERNOHORSKÝ, Jan a Petr TEPLÝ. *Základy financí.* Praha: Grada, 2011. 304 s. ISBN 978-80 24736693.
19. JÁNOŠÍKOVÁ, Petra a Petr MRKÝVKA. *Finanční a daňové právo.* 2. aktualizované a doplněné vydání. Plzeň: Aleš Čeněk, 2016. 492 s. ISBN 978-8073807962.
20. KARFÍKOVÁ, Marie. *Teorie finančního práva a finanční vědy.* Praha: Wolters Kluwer, 2018. 356 s. ISBN 978-8075529350.
21. ŠVARCOVÁ, Jena. *Ekonomie - stručný přehled.* CEED 2002. ISBN 978-8087301296.
22. VONDRA, Roman. *Peníze v moderních českých dějinách*. Praha: Academia, 2012. ISBN 978-8020021304.
23. SURGA, Leopold. *České bankovky a mince 1993-2012.* Praha: Jerome, 2012. ISBN 978-8090326682.
24. VENCOVSKÝ, František a Půlpán, Karel. *Dějiny měnových teorií na českém území*. Praha: Oeconomica, 2005. ISBN 80-245-0992-X
25. REVENDA Z. *Peněžní ekonomie a bankovnictví*. Praha, 2014: Management Press, 423 s. ISBN 978-8072612406
26. Zdeněk Ďuriš. *Šest vlastností kvalitních peněz*. Okénko investora, 2018. [online]. [cit. 27. 06. 2025]. Dostupné z: <https://zpravy.kurzy.cz/458712-sest-vlastnosti-kvalitnich-penez/>.

27. ČNB Česká Národní Banka. *Ochranné prvky 1000 Kč.* [online]. [cit. 27. 06. 2025]. Dostupné z: <https://www.cnb.cz/cs/bankovky-a-mince/bankovky/ochranne-prvky-1000-kc/>.
28. ČESKO. *Zákon č. 6/1993 Sb., České národní rady o České národní bance.*
29. ČNB Česká Národní Banka. *O ČNB.* [online]. [cit. 27. 06. 2025]. Dostupné z: <https://www.cnb.cz/cs/o_cnb/>.
30. ČESKO. *Zákon č. 21/1992 Sb., o bankách.*
31. ČESKO. *Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.*
32. Tvrdý, Jiří, Vavrušková, Adriana. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu*. 2. vyd. Praha: C. H. Beck, 2018. ISBN 978-80-7400-688-3
33. Česká Národní Banka. *Digitální peníze centrálních bank (CBDC)*. [online]. [cit. 27. 06. 2025]. Dostupné z: <https://www.cnb.cz/cs/platebni-styk/digitalni-penize-centralnich-bank-cbdc/>.
34. Zákon č. 370/2017 Sb., o platebním styku. In: Zákony pro lidi.cz. © AION CS 2010-2025 [online]. [cit. 29. 6. 2025]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2017-370>.
35. Česká národní banka. *Kryptoaktiva*. [online]. [cit. 31. 06. 2025]. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/kryptoaktiva>.
36. Evropský parlament a Rada. *Nařízení (EU) 2023/1114 o trzích s kryptoaktivy (MiCA)*. EUR-Lex. [online]. [cit. 31. 05. 2025]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32023R1114>.
37. STROUKAL, Dominik, SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: Třetí rozšířené vydání.* Praha: Grada Publishing, 2021. ISBN 978-8027110438
38. STINSON, Douglas R., PATERSON, Maura. *Cryptography: Theory and Practice. 4th edition*. Boca Raton: CRC Press, 2018. ISBN 978-1138197015
39. AUMASSON, Jean-Philippe. *Serious Cryptography: A Practical Introduction to Modern Encryption*. San Francisco: No Starch Press, 2017. ISBN 978-1593278267
40. ZELENKA, J., ČAPEK, J., FRANCEK, J., JANÁKOVÁ, H. *Ochrana dat. Kryptologie.* Hradec Králové: GAUDEAMUS Univerzity Hradec Králové, 2003. ISBN 80-7041-737-4.

41. HOFFSTEIN, Jeffrey; PIPHER, Jill; SILVERMAN, Joseph H. *An Introduction to Mathematical Cryptography. 2nd edition.* New York: Springer, 2014. ISBN 978-1441926746
42. NAKAMOTO, Satoshi. *Bitcoin: A peer-to-peer electronic cash system*. [online]. [cit. 11. 07. 2025]. Dostupné z: <https://bitcoin.org/bitcoin.pdf>.
43. Buterin, Vitalik. Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform. 2013. [online]. [cit. 11. 07. 2025]. Dostupné z: https://ethereum.org/en/whitepaper
44. Saleh, Fahad. (2020). Blockchain without Waste: Proof-of-Stake. The Review of Financial Studies. 34. 10.1093/rfs/hhaa075.
45. ANTONOPOULOS, Andreas M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2nd Edition*, O'Reilly Media, 2017. ISBN: 978-1491954386
46. INVESTOPEDIA. HODL: *The Cryptocurrency Strategy of „Hold on for Dear Life" Explained.* [online]. [cit. 11. 07. 2025]. Dostupné z: <https://www.investopedia.com/terms/h/hodl.asp>.
47. INVESTOPEDIA. *How to Stake Ethereum.* [online]. [cit. 11. 07. 2025]. Dostupné z: <https://www.investopedia.com/how-to-stake-ethereum-7482623>/.
48. INVESTOPEDIA. *What Is Decentralized Finance (DeFi) and How Does It Work?* [online]. [cit. 11. 07. 2025]. Dostupné z: <https://www.investopedia.com/decentralized-finance-defi-5113835>.
49. COINMARKETCAP. *CoinMarketCap: Cryptocurrency Prices, Charts and Market Capitalizations.* [online]. [cit. 18. 07. 2025]. Dostupné z: https://coinmarketcap.com
50. Siddik, Md A. B.; Amaya, Maria; Marston, Landon. *The water and carbon footprint of cryptocurrencies and conventional currencies.* Journal of Cleaner Production, vol. 411, no. 9, s. 137268. DOI: 10.1016/j.jclepro.2023.137268
51. Wendl, Moritz; Doan, My Hanh; Sassen, Remmer et al. *The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review*. Journal of Environmental Management, vol. 326, (Epub 10 listopadu 2022), s. 116530. DOI: 10.1016/j.jenvman.2022.116530
52. MAHSA Bashari, SALEH Ghavidel Doostkouei, MEHDI Fathabadi, Masoud Soufimajidpour. *The environmental cost of cryptocurrency: Analyzing CO2 emissions in the 9 leading mining countries*. Sustainable Futures, Volume 10, 2025, ISSN 2666-1888,

53. Alex de Vries, Christian Stoll. *Bitcoin's growing e-waste problem*. Resources, Recycling, Volume 175,2021, ISSN 0921-3449
54. SOLANA. *A new architecture for a high performance blockchain (Whitepaper)* [online]. [cit. 05.10.2025]. Dostupné z: <https://solana.com/solana-whitepaper.pdf>.
55. SOLANA. *Learn about Solana* [online]. [cit. 05.10. 2025]. Dostupné z: <https://solana.com/learn>.
56. COINMARKETCAP. *Solana (SOL) Price, Chart, Market Cap, and Info* [online]. [cit. 05. 10. 2025]. Dostupné z: <https://coinmarketcap.com/currencies/solana>.
57. PHANTOM TECHNOLOGIES. *Phantom: The crypto wallet for everyone* [online]. [cit. 06. 10. 2025]. Dostupné z: <https://phantom.com>.
58. LEAST AUTHORITY. *Phantom Wallet - Final Audit Report* [online]. [cit. 06. 10. 2025]. Dostupné z: <https://leastauthority.com/wp-content/uploads/2024/07/Least-Authority-Phantom-Wallet-Final-Audit-Report.pdf>.
59. MOONPAY. *What is KYC and why does MoonPay need to verify my identity?* [online]. [cit. 08. 10. 2025]. Dostupné z: <https://support.moonpay.com/hc/en-gb/articles/4408348240529-What-is-KYC-and-why-does-MoonPay-need-to-verify-my-identity>.
60. INVESTOPEDIA. *What is the average annual return for the S&P 500?* [online]. [cit. 28. 10. 2025]. Dostupné z: https://www.investopedia.com/ask/answers/042415/what-average-annual-return-sp-500.asp
61. SOFI. *Average stock market return: S&P 500 historical performance* [online]. [cit. 28. 10. 2025]. Dostupné z: https://sofi.com/learn/content/average-stock-market-return/
62. KURZY.CZ. *Státní dluhopisy* [online]. [cit. 28. 10. 2025]. Dostupné z: <https://www.kurzy.cz/dluhopisy/statni-dluhopisy/>.
63. TRADING ECONOMICS. *Czech Republic - Long Term Government Bond Yields* [online]. [cit. 28. 10. 2025]. Dostupné z: <https://tradingeconomics.com/czech-republic/long-term-gov-bond-yields-eurostat-data.html>.
64. UŠETŘENO.CZ. *Na co si dát pozor u spořících účtů?* [online]. [cit. 28. 10. 2025]. Dostupné z: <https://www.usetreno.cz/clanky/vyhody-a-nevyhody-sporicich-uctu/>.
65. ČESKÁ NÁRODNÍ BANKA. *Jak úrokové sazby ČNB ovlivňují českou ekonomiku* [online]. [cit. 28. 10. 2025]. Dostupné z: <https://www.cnb.cz/cs/menova-politika/vzdelavani/4.-jak-urokove-sazby-cnb-ovlivnuji-ceskou-ekonomiku/>.

66. TRADING VIEW. [cit. 28. 10. 2025]. Dostupné z: <https://www.tradingview.com/>.
67. Cong, Lin & He, Zhiheng & Tang, Ke. (2022). *Staking, Token Pricing, and Crypto Carry*. SSRN Electronic Journal. 10.2139/ssrn.4059460.
68. Prashayuniar, Adiiba & Syafrida, Ida. (2025). Comparative Performance Analysis Of Bitcoin, Ethereum, And Solana In The Crypto Market. Syntax Idea. 7. 942-954. 10.46799/syntaxidea.v7i7.13345.
69. Fendriansyah, Heru & Abubakar, Alamsyah. (2026). Comparative Analysis of the Performance of Cryptocurrency, Stocks, and Forex as Investment Alternatives, 2021-2024. Eduvest-Journal of Universal Studies. 6. 387-400. 10.59188/eduvest.v6i1.52141.
70. Ministerstvo financí ČR. *Vláda schválila zákon o digitálních financích*. [online]. [cit. 16. 02. 2026]. Dostupné z: <https://mf.gov.cz/cs/ministerstvo/media/tiskove-zpravy/2024/vlada-schvalila-zakon-o-digitalnich-financich-55549>.

8 Přílohy

Příloha č. 1: Seznam 50 kryptomen s nejvyšší trzni hodnotou (06.2025)

Název	**Tržní kapitalizace (USD)**	**Konsenzus mechanismus (česky)**
Bitcoin	2,360,911,766,955	Důkaz práce (PoW)
Ethereum	434,686,115,713	Důkaz podílu (PoS)
XRP	201,563,433,142	Konsenzusový protokol XRP Ledger
Tether USDt	160,319,178,217	Omni vrstva na Bitcoin blockchainu
BNB	102,309,842,771	Důkaz sázek autority (PoSA)
Solana	96,376,783,719	Důkaz podílu (PoS) + Důkaz historie (PoH)
USDC	64,475,132,630	Centralizovaný stablecoin
Dogecoin	35,522,064,384	Důkaz práce (PoW)
TRON	30,992,479,718	Delegovaný důkaz podílu (DPoS)
Cardano	30,004,857,753	Důkaz podílu (PoS)
Hyperliquid	15,361,503,593	Neznámý / Smíšený konsenzus
Stellar	14,771,442,419	Stellar konsenzusový protokol (SCP)
Sui	13,906,946,450	Neznámý / Smíšený konsenzus
Chainlink	12,532,127,311	Důkaz podílu (PoS)
Hedera	11,349,148,545	Hashgraph konsenzus
Bitcoin Cash	10,521,416,951	Důkaz práce (PoW)
Avalanche	10,226,394,548	Avalanche konsenzusový protokol
Shiba Inu	8,848,004,785	Na základě Ethereum (zděděný PoS konsenzus)
UNUS SED LEO	8,247,348,749	Neznámý / Smíšený konsenzus
Litecoin	8,232,511,686	Důkaz práce (PoW)
Toncoin	8,060,990,173	Neznámý / Smíšený konsenzus
Polkadot	7,043,051,156	Nominovaný důkaz podílu (NPoS)
Uniswap	6,733,134,039	Na základě Ethereum (zděděný PoS konsenzus)
Monero	6,200,037,536	Důkaz práce (PoW)
Bitget Token	5,855,986,791	Neznámý / Smíšený konsenzus
Pepe	5,747,293,420	Na základě Ethereum (zděděný PoS konsenzus)
Ethena USDe	5,614,366,497	Neznámý / Smíšený konsenzus
Dai	5,365,247,117	Na základě Ethereum (zděděný PoS konsenzus)
Aave	4,983,393,013	Na základě Ethereum (zděděný PoS konsenzus)
Bittensor	3,947,665,570	Neznámý / Smíšený konsenzus
Cronos	3,847,818,839	Důkaz podílu (PoS)
Ethereum Classic	3,682,019,004	Důkaz práce (PoW)
NEAR Protocol	3,650,834,198	Důkaz podílu (PoS)
Aptos	3,555,364,539	Důkaz podílu (PoS)
Pi	3,448,837,444	Neznámý / Smíšený konsenzus

Ondo	3,282,039,826	Na základě Ethereum (zděděný PoS konsenzus)
Internet Computer	3,208,896,880	Threshold Relay + BLS consensus
OKB	2,921,100,183	Proof-of-Authority (PoA)
Bonk	2,828,426,663	Na základě Solana (PoS + PoH)
Algorand	2,641,762,093	Důkaz účasti (Pure PoS)
Ethena	2,619,079,929	Na základě Ethereum (zděděný PoS konsenzus)
Mantle	2,610,663,694	Na základě Ethereum (zděděný PoS konsenzus)
POL (prev. MATIC)	2,563,586,581	Důkaz podílu (PoS)
Kaspa	2,540,112,691	BlockDAG (PoW)
Arbitrum	2,432,999,261	Na základě Ethereum (zděděný PoS konsenzus)
VeChain	2,379,441,716	Proof-of-Authority (PoA)
World Liberty USD	2,204,584,452	Na základě Ethereum (zděděný PoS konsenzus)
Render	2,195,367,902	Na základě Ethereum (zděděný PoS konsenzus)
OFFICIAL TRUMP	2,086,209,881	Na základě Ethereum (zděděný PoS konsenzus)
Sei	2,085,985,458	Tendermint (Cosmos SDK) - BFT konsenzus

Zdroj: vlastní zpracování dle (49)