

Analýza problematiky platební funkce kryptoaktiv

Michal Mrvoljak

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně

Fakulta managementu a ekonomiky

Ústav financí a účetnictví

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Michal Mrvoljak
Osobní číslo: M22430
Studijní program: B0412P050001 Finance a finanční technologie
Forma studia: Prezenční
Téma práce: Analýza problematiky platební funkce kryptoaktiv

Zásady pro vypracování

Úvod

Definujte cíle práce a použité metody zpracování práce.

I. Teoretická část

- Proveďte literární rešerši zaměřenou na problematiku kryptoaktiv a jejich platební funkce.

II. Praktická část

- Analyzujte platební funkce kryptoaktiv.
- Na základě provedené analýzy porovnejte možnosti plateb kryptoaktiv s tradičními digitálními metodami plateb.

Závěr

Rozsah bakalářské práce: **cca 40 stran**
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BURNISKE, Chris a TATAR, Jack. *Cryptoassets: the innovative investor's guide to bitcoin and beyond*. New York: McGraw-Hill, 2018. ISBN 978-1-260-02667-2.
HARVEY, Campbell R.; RAMACHANDRAN, Ashwin a SANTORO, Joey. *DeFi and the future of finance*. Hoboken, New Jersey: Wiley, 2021. ISBN 978-1-119-83601-8.
NOVÁK, Michal. *Lightning network: platby budoucnosti*. Praha: Braiins Publishing, 2023. ISBN 978-80-908709-4-9.
STROUKAL, Dominik a SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Třetí rozšířené vydání*. Praha: Grada, 2021. ISBN 978-80-271-1043-8.
TAPSCOTT, Don a TAPSCOTT, Alex. *Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world*. London: Portfolio/Penguin, 2018. ISBN 978-0-241-23786-1.

Vedoucí bakalářské práce: **Ing. Lubor Homolka, Ph.D.**
Ústav statistiky a kvantitativních metod

Datum zadání bakalářské práce: **10. února 2025**
Termín odevzdání bakalářské práce: **23. května 2025**

L.S.

doc. Ing. Michal Pilík, Ph.D.
děkan

doc. Ing. Adriana Knápková, Ph.D.
garant studijního programu

Ve Zlíně dne 10. února 2025

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato bakalářská práce se zaměřuje na analýzu problematiky platební funkce kryptoaktiv. Cílem práce je zjistit, zda kryptoaktiva naplňují základní podmínky pro využití jako prostředek směny, a následně je porovnat s tradičními digitálními platebními metodami, jako jsou Visa a Mastercard. V teoretické části jsou popsány hlavní rysy kryptoaktiv, jejich technologické základy, historie i specifické vlastnosti, které je odlišují od běžných měn. Praktická část využívá komparativní analýzu vybraných parametrů, jako je rychlost zpracování transakcí, výše poplatků a míra adopce v běžné praxi. Data byla čerpána z veřejných databází a odborných publikací. Výsledky ukazují, že některá kryptoaktiva mohou v určitých případech plnit platební funkce efektivněji než tradiční systémy, přičemž zásadní výhodou bývá decentralizace a nízké transakční náklady. Skutečné uplatnění těchto výhod však závisí na míře adopce ze strany uživatelů a obchodníků, protože bez dostatečného rozšíření zůstávají potenciální přínosy technologicky efektivních řešení nevyužity.

Klíčová slova: kryptoaktiva, platební funkce, digitální platby, blockchain

ABSTRACT

This bachelor thesis focuses on the analysis of the payment function of cryptoassets. The aim of the thesis is to assess whether cryptoassets fulfil the basic conditions for use as a medium of exchange and to compare them with traditional digital payment systems such as Visa and Mastercard. The theoretical part outlines the fundamental characteristics of cryptoassets, their historical development, technological foundations, and the specific features that distinguish them from conventional currencies. The practical part applies a comparative analysis of selected parameters, including transaction speed, fee levels, and the rate of adoption in real-world use. The data were obtained from publicly available databases and academic sources. The findings indicate that some cryptoassets may, in certain cases, perform payment functions more efficiently than traditional systems, particularly due to their decentralised nature and low transaction costs. However, the practical application of these advantages depends on the level of adoption among users and merchants, as the potential benefits of technically efficient systems remain unrealised without broader adoption.

Keywords: cryptoassets, payment functions, digital payments, blockchain

Rád bych poděkoval všem, kteří mě během psaní této bakalářské práce podporovali a motivovali.

Mé upřímné poděkování patří především vedoucímu práce panu Ing. Luboru Homolkovi, Ph.D., za odborné vedení, cenné rady a trpělivost, které mi pomohly tuto práci dokončit.

Velké díky patří také mé rodině a blízkým za jejich neustálou podporu během celého studia.

“If you don't believe it or don't get it, I don't have the time to try to convince you, sorry.”

- Satoshi Nakamoto

OBSAH

ÚVOD.....	11
CÍLE A METODY ZPRACOVÁNÍ PRÁCE.....	12
I TEORETICKÁ ČÁST.....	13
1 TEORETICKÉ VYSVĚTLENÍ KRYPTOAKTIV.....	14
1.1 HISTORIE A VÝVOJ KRYPTOAKTIV	14
1.2 FUNKCE A VLASTNOSTI KRYPTOAKTIV A JEJICH ROZDÍLY OPROTI TRADIČNÍM MĚNÁM.....	15
1.2.1 Funkce peněz.....	16
1.2.2 Vlastnosti peněz	16
1.2.3 Decentralizace	17
1.2.4 Soukromí	18
1.3 FUNDAMENTÁLNÍ ANALÝZA: HODNOTA A VOLATILITA KRYPTOAKTIV.....	18
2 PŘEDSTAVENÍ JEDNOTLIVÝCH KRYPTOAKTIV.....	21
2.1 BITCOIN	21
2.2 ETHEREUM	23
2.3 SOLANA.....	25
2.4 OSTATNÍ.....	27
2.4.1 Ripple	27
2.4.2 Stablecoiny	28
3 PROBLEMATIKA PLATEB KRYPROAKTIVY.....	29
3.1 RIZIKA A HROZBY (VOLATILITA, BEZPEČNOST, TECHNICKÁ RIZIKA).....	29
3.2 REGULACE A LEGISLATIVNÍ PŘEKÁŽKY	30
3.2.1 Evropská unie.....	31
3.2.2 USA.....	32
3.2.3 Asie	33
3.2.4 Legalizace plateb kryptoaktivity	35
3.3 KYBERBEZPEČNOST A OCHRANA UŽIVATELŮ	36
3.4 VLIV DECENTRALIZACE NA REGULACI A ADOPCI	37
4 POTENCIÁL A VÝZVY VYUŽITÍ KRYPTOAKTIV V PLATEBNÍM SYSTÉMU.....	38
4.1 ADOPCE KRYPTOAKTIV V PLATEBNÍM STYKU	38
4.2 VÝHODY KRYPTOAKTIV OPROTI TRADIČNÍM PLATEBNÍM METODÁM	39
4.2.1 Rychlost a nízká cena transakcí	39
4.2.2 Absence prostředníků.....	39
4.2.3 Finanční inkluze	40
4.2.4 Interoperabilita a přenositelnost.....	40
4.3 TECHNOLOGIE A ŠKÁLOVATELNOST	41

4.3.1	Škálovatelnost	41
4.3.2	Trilema a kvadrilema škálovatelnosti blockchainu	42
4.3.3	Lightning network	43
5	SHRnutí TEORETICKÉ ČÁSTI.....	46
II	PRAKTICKÁ ČÁST	47
6	PLATEBNÍ FUNKCE KRYPTOAKTIV VE SROVNÁNÍ S TRADIČNÍMI SYSTÉMY	48
6.1	RYCHLOST PLATEBNÍCH SYSTÉMŮ	48
6.1.1	Bitcoin	48
6.1.2	Ethereum	49
6.1.3	Solana	49
6.1.4	Visa.....	50
6.1.5	Mastercard.....	50
6.1.6	Komparativní analýza rychlosti platebních systémů	51
6.2	TRANSAKČNÍ POPLATKY	52
6.2.1	Transakční poplatky kryptoaktiv	52
6.2.2	Transakční poplatky u platebních karet.....	53
6.2.3	Komparativní analýza poplatků platebních systémů	55
7	PRAKTICKÉ VYUŽITÍ KRYPTOAKTIV V PLATEBNÍM STYKU.....	57
7.1	MOŽNOSTI ZÍSKÁNÍ A NÁKUPU KRYPTOAKTIV	57
7.2	MOŽNOSTI PLATBY KRYPTOAKTIVY	58
7.2.1	Přímá platba obchodníkovi.....	58
7.2.2	Nepřímá platba	59
7.2.3	Platba přes zprostředkovatele	59
7.3	VYUŽITÍ KRYPTOPLATEB PŘI BĚŽNÉM PLATEBNÍM STYKU	60
7.3.1	Lightning peněženky	61
7.3.2	Praktická ukázka platby přes Lightning Network	61
7.3.3	Porovnání Lightning Network a platební karty Visa.....	69
	ZÁVĚR.....	71
	SEZNAM POUŽITÉ LITERATURY	73
	SEZNAM OBRÁZKŮ	79
	SEZNAM TABULEK.....	80
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	81

ÚVOD

V posledním desetiletí došlo k rychlému rozvoji digitálních technologií, který významně ovlivnil oblast platebních systémů. Jedním z nejdiskutovanějších témat se stala kryptoaktiva, která přináší nové možnosti v oblasti převodu hodnoty. Jejich využití již dávno nepředstavuje pouze spekulativní nástroj, ale stále častěji bývají zvažována i jako alternativa ke klasickým platebním metodám.

Kryptoaktiva, jako je například Bitcoin nebo Ethereum, byla původně vyvíjena s cílem vytvořit nezávislý platební prostředek mimo kontrolu centrálních institucí. Postupně se však začala rozšiřovat i jejich praktická využitelnost, především v oblasti mezinárodních plateb, mikrotransakcí nebo e-commerce. Přesto však zůstává otázkou, zda jsou tato digitální aktiva schopna efektivně naplnit základní platební funkce, a jak obstojí ve srovnání s tradičními digitálními platebními metodami, jako jsou Visa či Mastercard.

Bakalářská práce se proto zaměřuje na analýzu platební funkce kryptoaktiv. Cílem je zhodnotit jejich vlastnosti z pohledu praktického využití při platbách a porovnat je s běžně používanými platebními systémy. Práce je rozdělena na část teoretickou a praktickou. V teoretické části je pozornost věnována vymezení základních pojmů, historickému vývoji, charakteristice vybraných kryptoaktiv a technickým i legislativním aspektům. Praktická část následně analyzuje konkrétní parametry, jako jsou rychlost transakcí, transakční náklady či míra adopce, a porovnává tyto ukazatele mezi kryptoaktivy a tradičními platebními nástroji.

Téma bylo zvoleno s ohledem na aktuálnost problematiky, její rostoucí význam v ekonomické praxi i na základě osobního zájmu o oblast digitálních financí.

CÍLE A METODY ZPRACOVÁNÍ PRÁCE

Cílem bakalářské práce je prozkoumat platební funkce kryptoaktiv v platebním systému a posoudit jejich význam při praktickém využití. Pozornost je zaměřena na to, zda jsou kryptoaktiva schopna naplňovat základní podmínky pro použití jako prostředek směny, a zda v některých ohledech představují efektivnější alternativu k tradičním digitálním platebním metodám, jako jsou Visa a Mastercard.

Teoretická část práce vychází z literární rešerše odborných publikací, studií a datových zdrojů zaměřených na vlastnosti, funkce a vývoj kryptoaktiv. Popsány jsou také rozdíly oproti klasickým měnám, přínos decentralizace, problematika bezpečnosti a regulace, stejně jako faktory ovlivňující širší adopci kryptoplateb v reálném světě.

Praktická část je postavena na komparativní analýze vybraných platebních parametrů. Konkrétně jsou porovnávány transakční poplatky, rychlost zpracování, dostupnost, likvidita a technologické možnosti různých platebních řešení. Zvláštní důraz je kladen na využití Lightning Network v rámci kryptoplateb. Data byla čerpána z veřejných odborných zdrojů, technologických dokumentací, statistik a aktuálních sazeb poskytovatelů. Získané informace jsou vyhodnoceny a interpretovány ve vztahu k výzkumné otázce, do jaké míry jsou kryptoaktiva v současnosti schopna naplnit požadované platební funkce a zda mohou být reálnou alternativou k zavedeným digitálním platebním systémům.

I TEORETICKÁ ČÁST

1 TEORETICKÉ VYSVĚTLENÍ KRYPTOAKTIV

Pro pochopení praktického fungování kryptoaktiv v oblasti platebního styku je nejprve nezbytné vymezit základní teoretické pojmy a souvislosti, které s touto problematikou souvisejí. Tato kapitola se proto zaměřuje na historický vývoj kryptoaktiv, jejich klíčové vlastnosti a technologické principy, které odlišují tento typ digitálních aktiv od tradičních forem peněz. Současně je vysvětleno, jaké funkce musí aktivum splňovat, aby mohlo být považováno za platidlo, a do jaké míry jsou tyto požadavky naplňovány u kryptoaktiv. Zvláštní pozornost je věnována otázkám decentralizace, ochrany soukromí a hodnotové stability, které představují zásadní faktory při posuzování jejich využitelnosti jako prostředku směny.

1.1 Historie a vývoj kryptoaktiv

Historie kryptoaktiv počíná koncem 20. století. Americký vědec a kryptograf David Chaum založil společnost DigiCash, která následně v roce 1990 spustila první elektronické peníze s názvem eCash. Tento projekt, který je považován za prvního předchůdce kryptoaktiv, ale brzy skončil, jelikož firma po 8 letech vyhlásila bankrot. I přesto tento koncept, který Dr. Chaum vytvořil, byl pro další vývoj velmi zásadní. Dalšími projekty, které položily základ pro kryptoaktiva, v podobě, v jaké je známe dnes, byli projekty E-Gold, Bit Gold, B-Money a Hashcash (Reiff 2024)

Průlom nastal v roce 2009, kdy záhadný tvůrce Satoshi Nakamoto spustil decentralizovanou peer-to-peer měnu s názvem Bitcoin. Představil tak zásadní inovaci kryptoaktiv s velmi důležitou inovací v podobě vytvoření tzv. blockchainu. Ten si můžeme představit jako veřejnou účetní knihu, která se skládá z bloků, do kterých se zaznamenávají transakce. Každý blok navazuje na předešlý a musí se v komunitě uživatelů sítě schválit. Jednoduše je to tedy jeden lineární řetěz bloků s údaji o transakcích sdílený mezi všemi uživateli. Celý tento systém, který Satoshi vymyslel, řeší problém tzv. dvojité útraty (anglicky double-spend), tedy aby se virtuální aktiva nemohla v síti duplikovat (Stroukal a Skalický 2021).

Krátce po uvedení Bitcoinu se začalo diskutovat o jeho nedostacích, což vedlo k vytvoření nových kryptoaktiv. Jelikož je Bitcoin open-source, plno vývojářů se inspirovalo jeho zdrojovým kódem s cílem vymyslet lepší alternativu. Tyto alternativy jsou často označovány jako altcoiny. Toto nové spektrum kryptoaktiv následně otevřelo další možnosti pro využití technologie blockchainu (Burniske a Tatar 2018)

Dalším významným pokrokem se stalo kryptoaktivum s názvem Ethereum. V roce 2014 přišlo s novým využitím blockchainu, jakožto platformou pro chytré kontrakty (anglicky smart contracts). Ty umožňují definovat interakce mezi uživateli sítě a řídit jejich aktiva. Vznikl tak základ pro decentralizované aplikace, tzv. dApps. Ty umožňují uživatelům přímo interagovat mezi sebou, a to bez centrální autority. Brzy se tak ukázalo, že dApps budou významné hlavně v oblasti financí. Tato oblast se začala označovat jako decentralizované finance, tedy zkráceně DeFi (Harvey et al. 2021).

Po úvodním období, které bylo charakterizováno vznikem Bitcoinu a později Etherea, byl zahájen dynamický rozvoj celého trhu s kryptoaktivy. Původní pojetí alternativy k tradičním měnám se postupně rozšířilo o nové formy a aplikace. Tím došlo k rozšíření spektra využití technologie blockchainu. Významný posun byl zaznamenán především v období po roce 2015, kdy byly představeny platformy umožňující vznik decentralizovaných aplikací a vydávání vlastních tokenů prostřednictvím chytrých kontraktů. Vývoj obchodování na trzích s kryptoaktivy vykazoval postupné přibližování k charakteristikám tradičních finančních trhů. K určitému přelomu došlo během pandemie Covid-19, kdy byl zaznamenán posun ve vnímání této oblasti. Z těchto čistě spekulativních nástrojů se kryptaaktiva staly součástí širšího finančního ekosystému. Jejich chování začalo více korelovat s tradičními třídami aktiv. Tím byl zahájen proces jejich postupné integrace do globálního finančního systému (Wątarek et al. 2021).

1.2 Funkce a vlastnosti kryptoaktiv a jejich rozdíly oproti tradičním měnám

Kryptoaktiva, jako je například Bitcoin nebo Ethereum, se často zmiňují jako alternativní forma peněz. Abychom mohli porovnat jejich schopnost plnit platební funkci s tradičními měnami, je nejprve nutné porozumět tomu, co jsou peníze, jaké mají funkce a vlastnosti, a jak se v těchto aspektech kryptaaktiva liší. Tato kapitola proto přehledně shrnuje základní funkce a vlastnosti peněz, přičemž zvláštní pozornost je věnována funkci všeobecného prostředku směny, která je stěžejní pro praktické využití kryptoaktiv při platbách.

1.2.1 Funkce peněz

Podle Mishkina (2022) plní peníze v ekonomice tři základní funkce:

- Všeobecný prostředek směny
- Zúčtovací jednotka
- Uchovatel hodnoty

Zejména první zmíněná, tedy funkce prostředku směny, je podle autora tou, která peníze zásadně odlišuje od ostatních forem majetku, jako jsou akcie, dluhopisy nebo nemovitosti. Právě schopnost sloužit jako všeobecně přijímaný nástroj směny je v praktickém ekonomickém životě nejdůležitější a činí peníze nenahraditelnými v moderní ekonomické výměně.

1.2.2 Vlastnosti peněz

Aby mohl určitý prostředek efektivně plnit základní funkce peněz, měl by splňovat několik klíčových vlastností. Ve své knize Mishkin (2022) uvádí, že každé aktivum, které má fungovat jako peníze, by mělo být:

- Standardizovatelné – hodnota by měla být snadno rozpoznatelná a vyjádřitelná. To umožňuje jednoznačně stanovit, kolik daný předmět či jednotka měny stojí.
- Široce akceptované – musí být všeobecně přijímané obyvatelstvem i institucemi jako platidlo. Bez této důvěry nelze efektivně zprostředkovávat transakce.
- Dělitelné – je nutné, aby šlo měnovou jednotku rozdělit, aby bylo možné hradit i malé částky.
- Snadno přenositelné – peníze by měly být praktické pro běžné používání, tedy jednoduše a rychle přenositelné mezi lidmi nebo subjekty.
- Trvalé – hodnota a fyzická či digitální forma peněz by neměla být snadno zničitelná nebo znehodnocená používáním či časem.

Digitální povaha kryptoaktiv některé z uvedených vlastností zajišťuje s vysokou mírou efektivity, zejména přenositelnost a dělitelnost jsou v digitálním prostředí realizovány téměř bez omezení. Transakce mohou probíhat bez ohledu na geografické hranice, a to i v hodnotách výrazně nižších než u běžných měn. Zároveň kryptoaktiva přinášejí i nové

vlastnosti, které tradiční peníze zpravidla nenabízejí, např. decentralizaci a v některých případech také vyšší úroveň soukromí a pseudonymity (Bouška 2023).

Nutno však podotknout, že tyto vlastnosti nejsou klasickými funkcemi peněz ve smyslu ekonomické teorie, ale spíše dodatečnými technologickými rysy, které mohou mít praktický význam pro uživatele. Lze se domnívat, že kryptoaktiva lze v určitém rozsahu používat jako prostředek směny, avšak vzhledem k omezenému objemu přijatých transakcí a nízké míře adopce ve srovnání s tradičními měnami zatím nelze hovořit o jejich všeobecném použití.

1.2.3 Decentralizace

Digitální transakce u tradičních měn jsou ověřovány centrální autoritou, nejčastěji bankou, u které máme sjednaný účet. Většina kryptoaktiv ale centrální autoritu nemá. Hovoříme tedy o tom, že jsou transakce ověřovány decentralizovaně. Důvodem je, že blockchain je distribuován mezi uživatele sítě, kteří se navzájem kontrolují při ověřování transakcí, například v případě Bitcoinu dochází k ověřování transakcí v rámci procesu těžby (Stroukal a Skalický 2021).

V závislosti na způsobu přístupu může být blockchain rozdělen na dva typy. V systému bez povolení není přístup do sítě nijak omezen a účastníkem se může stát kdokoli. Naopak v systému s povolením je přístup umožněn pouze na základě schválení správcem sítě. Mohou tedy být rozlišovány varianty s omezeným nebo veřejným přístupem. Kryptoaktiva používají kryptografii, konkrétně veřejné a soukromé klíče, k dosažení vysoké úrovně bezpečnosti a udržení důvěrnosti a soukromí. Veřejný klíč slouží jako adresa a k ověření identity uživatele. Soukromý klíč je využíván k vytváření digitálních podpisů. Decentralizace kryptoaktiv spočívá v tom, že žádná centrální autorita neřídí síť ani databázi transakcí. Díky tomu může být každému uživateli, kdykoli a odkudkoli, umožněno provádět neomezené množství transakcí bez zásahu třetí strany. Tím se eliminuje možnost zamítnutí transakce nebo její kontroly. Transakční poplatky u kryptoaktiv jsou velmi nízké. Malé částky jsou účtovány pouze za ověření a zpracování transakcí. Na rozdíl od tradičních bank, které mohou účtovat poplatky za převody, vedení účtů a správu, je u kryptoaktiv tento model výrazně efektivnější. Vzhledem k tomu, že není vyžadováno schválení od centrálních institucí, je umožněno rychlejší provádění transakcí (Qaroush et al. 2022).

1.2.4 Soukromí

Soukromí a anonymita byly považovány za některé z klíčových vlastností od počátků vývoje digitálních aktiv. V tradičních finančních systémech je každá transakce spojena s konkrétní identitou, zatímco u kryptoaktiv byla snaha umožnit převody bez vazby na určitou osobu. Kryptoaktiva jsou však více připodobňována hotovostním transakcím, u nichž je obtížné zjistit, mezi jakými subjekty byly provedeny. V minulosti byly vyvíjeny projekty, jejichž cílem bylo zajistit co nejvyšší míru anonymity při převezech prostředků. Právě tyto projekty však často narazily na regulační omezení kvůli svému využívání v rámci trestné činnosti. Přesto zájem o anonymní digitální platby přetrval a byl částečně naplněn vznikem Bitcoinu. Přestože bylo soukromí jedním z hlavních důvodů, proč lidé začali kryptoaktiva využívat, v praxi se ukázalo, že úroveň ochrany soukromí je v případě většiny kryptoaktiv nižší, než se očekávalo. Přiřazení příchozích a odchozích transakcí ke stejné adrese může vést k odhalení identity majitele. Ukázalo se tedy, že ani tyto systémy nejsou plně anonymní a lze u nich nalézt metody, jak získat informace o proběhlých transakcích. Zvýšená pozornost je věnována otázce důvěryhodnosti v případě tzv. stablecoinů, jejichž hodnota je navázána na klasickou měnu. Pokud nejsou tyto prostředky vydávány centrální bankou, je nutné řešit, kdo konkrétně zajišťuje jejich stabilitu a správu (Goodell a Aste 2019).

1.3 Fundamentální analýza: Hodnota a volatilita kryptoaktiv

Fundamentální analýza se zaměřuje na základní vlastnosti daného aktiva. Patří mezi ně například model emise, míra decentralizace, podoba white paperu, aktivita vývojářské komunity, vztahy k jiným projektům a celkový vývoj ekosystému. Při tomto hodnocení bývají analyzovány nejen technické aspekty, ale i zapojení uživatelů a vývojářů, protože tyto faktory mohou ovlivňovat dlouhodobý růst a stabilitu daného aktiva. Při rozhodování o zařazení kryptoaktiv do investičního portfolia je tedy potřeba, aby byla provedena jejich důkladná analýza. Od tradičního investování se jednoznačně liší, protože kryptoaktiva nepředstavují společnosti. Jsou to digitální aktiva, jejichž hodnota je určována převážně nabídkou a poptávkou. Přesto je možné využít některé postupy běžné při posuzování firemních akcií, tedy zejména v oblasti základních metrik a struktury hodnocení. Na rozdíl od klasických akciových trhů, kde bývá hodnocení často založeno na účetních výkazech, musí být u kryptoaktiv přístup přizpůsoben jejich odlišnému charakteru. Jejich tvůrci mohou být známi, ale samotné aktivum není společností a není řízeno stejným způsobem. Investoři si proto musí informace sami vyhledat a ověřit. Vzhledem k tomu, že v oblasti kryptoaktiv

zatím neexistuje jednotná metodika hodnocení, je při jejich analýze nutné přistupovat ke každému případu zvlášť. Investoři proto často kombinují prvky fundamentální i technické analýzy. Zatímco ta první pomáhá posoudit, zda má dané aktivum potenciál z dlouhodobého hlediska, technická analýza se soustředí spíše na hledání vhodných momentů pro nákup či prodej na základě vývoje cenových grafů. Proces analýzy bývá časově náročný, protože je nutné zohlednit nejen samotné kryptoaktivum, ale i jeho postavení v širším kontextu. Při zkoumání konkrétního aktiva se doporučuje zaměřit na jeho jedinečné rysy, schopnost řešit praktické problémy a míru přijetí mezi uživateli. Tímto způsobem může být vytvořen ucelený pohled na hodnotu daného kryptoaktiva (Burniske a Tatar 2018)

Dále je hodnota kryptoaktiv ovlivňována kombinací vnitřních a vnějších faktorů. Z vnějších vlivů hraje roli stav globální ekonomiky, zejména inflace, úrokové sazby, zaměstnanost, hospodářský růst a opatření hospodářské politiky. Dopad mají i společenské faktory, jako je popularita daného aktiva, aktivita komunity a vyjádření veřejně známých osobností, zejména influencerů. Ty mohou ovlivnit náladu investorů a tím i cenu. Významným činitelem je také regulační prostředí. Opatření na podporu nebo zákaz kryptoaktiv mívají přímý dopad na jejich hodnotu. Stejně tak i mezinárodní události, jako jsou sankce či konflikty. Dále psychologické vlivy jako strach, očekávání, nebo také známé FOMO (strach z toho, že nám něco uniká). Všechny tyto aspekty formují chování investorů a podporují cenové pohyby. Z uvedeného vyplývá, že při stanovení hodnoty je třeba zohlednit souběh ekonomických, společenských, politických a psychologických vlivů (Anwar et al. 2022).

U nově vydaných kryptoaktiv bývá běžně zaznamenána vysoká volatilita, která je způsobena omezenou likviditou trhu. Ta je charakterizována nízkým počtem aktivních objednávek k nákupu a prodeji, případně malými objemy jednotlivých pokynů. V takovém prostředí může i malá transakce výrazně ovlivnit tržní cenu. Z tohoto důvodu bývá kolísání cen u čerstvě zalistovaných kryptoaktiv časté a prudké. Postupem času, jak je dané aktivum více obchodováno a počet účastníků trhu narůstá, čímž dochází k posílení likvidity. S rostoucím objemem obchodů bývá trh schopen absorbovat větší množství pokynů bez výraznějších cenových výkyvů, čímž dochází ke snižování volatility. Kolísání cen bývá často vyjádřeno pomocí směrodatné odchylky denních procentuálních změn ceny. Vyšší hodnota tohoto ukazatele značí větší riziko, protože odráží míru nejistoty ohledně budoucího vývoje ceny aktiva. Např. u Bitcoinu bylo v minulosti pozorováno, že jeho volatilita převyšovala tradiční akciové tituly, avšak zároveň poskytoval vyšší výnosy. Přesto i v období, kdy došlo k poklesu cenových výkyvů, zůstal Bitcoin z pohledu investičního rizika nadprůměrný. Pro

přesnější vyhodnocení poměru rizika a výnosu bývá využíván tzv. Sharpeho poměr. Tento ukazatel porovnává dosažený výnos s úrovní volatility a umožňuje srovnávat různá aktiva bez ohledu na jejich absolutní výkonnost. V rámci sledovaného období dosahoval Bitcoin vyšších hodnot tohoto poměru než vybrané akcie technologických firem, což signalizovalo, že za podstoupené riziko byla investorům poskytována nadprůměrná odměna. Zároveň bylo zjištěno, že ani nižší výnos nemusí nutně znamenat horší investiční příležitost, pokud je doprovázen nižší volatilitou. Právě díky této kombinaci bylo možné dosáhnout výhodného poměru rizika a výnosu i v obdobích, kdy cenový růst nebyl výrazný. Srovnání s hlavními americkými indexy pak ukázalo, že přestože Bitcoin vykazoval vyšší absolutní výnosy, jeho rizikově očištěné zhodnocení bylo porovnatelné, a v některých letech i vyšší (Burniske a Tatar 2018).

2 PŘEDSTAVENÍ JEDNOTLIVÝCH KRYPTOAKTIV

Tato kapitola se zaměřuje na konkrétní příklady vybraných kryptoaktiv. Jejich podrobnější charakteristika je nezbytná pro pochopení toho, jakým způsobem jednotlivá aktiva technicky fungují, jaké mají vlastnosti a v čem se navzájem liší. Důraz je kladen na ta kryptaaktiva, která jsou v praxi nejčastěji používána nebo technologicky něčím výrazně přispěla k vývoji celého ekosystému. Mezi sledovaná kryptaaktiva patří Bitcoin, Ethereum, Solana, Ripple a stablecoiny.

2.1 Bitcoin

Za první prakticky fungující decentralizované kryptoaktivum je považován Bitcoin, který byl uveden do provozu v roce 2009. Jeho vznik byl inspirován návrhem publikovaným o rok dříve osobou vystupující pod pseudonymem Satoshi Nakamoto. Byla tak navržena nová forma digitální měny nezávislé na centrálních autoritách. Motivací k vytvoření Bitcoinu bylo poskytnutí prostředku elektronické platby bez zapojení bankovního systému. Byla představena peer-to-peer verze elektronické hotovosti, která měla umožnit přímé transakce mezi jednotlivci a zároveň řešit technický problém dvojího utracení, který do té doby vyžadoval centrální dohled. Bitcoin byl navržen jako alternativa k tradičním měnám s potenciálem stát se globálně uznávaným prostředkem směny. Peer-to-peer komunikace je tak princip, kde mají všichni účastníci rovnocenné postavení a data jsou sdílena napřímo. Tento model umožňuje provádění transakcí mezi uživateli bez prostředníků. Účast v síti není nijak podmíněna a může být zahájena kdykoliv pomocí běžného připojení k internetu. Záznam a ověřování transakcí je realizováno pomocí blockchainu, což je distribuovaná databáze, jejíž kopie jsou uloženy na tisících uzlů po celém světě. Transakce jsou shromažďovány do bloků, které jsou po ověření připojovány k již existujícímu řetězci. Tím je zajištěna neměnitelnost dat, jejich veřejná dostupnost i transparentnost celého systému. Za další důležitý aspekt Bitcoinu je považována jeho open-source povaha, která umožňuje veřejný přístup ke zdrojovému kódu. Díky tomu může být systém neustále kontrolován a vylepšován vývojářskou komunitou. Bitcoin je tedy chápán jako decentralizovaná měna a zároveň síťový protokol, jehož fungování je zajištěno prostřednictvím blockchainu a otevřeného vývoje (Sergeenkov 2025).

Bezpečnost bitcoinové sítě je zajištěna díky těžbě, která je postavena na mechanismu Proof of Work. V tomto procesu mezi sebou soutěží tzv. těžaři, tedy uživatelé provozující výpočetní uzly, což jsou prakticky distribuované počítače a jejich cílem je přidání nového

bloku transakcí do bitcoinového blockchainu. K dosažení tohoto cíle musí být vyřešena kryptografická hádanka. Řešení této hádanky je nalezení správného čísla, tzv. nonce. Toto číslo je po zkombinování s časem, seznamem navrhovaných transakcí a identitou předchozího bloku zpracováno prostřednictvím hashovací funkce. Výsledkem je tedy hash, což je výstup, který musí splňovat stanovené požadavky obtížnosti, např. začínat určitým počtem nul. Hashovací funkce zpracovává vstupní data tak, že vytvoří výstup o pevné délce, přičemž i minimální změna ve vstupu způsobí zásadní změnu výsledku. Pokud je nalezen správný výstup, označuje se jako zlatý hash, je tím těžaři umožněno přidat nový blok do blockchainu. Za tuto činnost jsou pak těžaři odměňováni nově vytvořenými bitcoiny prostřednictvím tzv. coinbase transakce, která je vždy uvedena jako první v rámci následujícího nového bloku (Burniske a Tatar 2018).

Jedním ze zásadních principů fungování bitcoinu je jeho omezené celkové množství, které bylo stanoveno na 21 milionů jednotek. Tento počet byl určen tvůrcem bitcoinu a je pevně zakódován v samotném protokolu. Aby bylo zajištěno postupné uvolňování do oběhu, byl zaveden mechanismus zvaný halving, při němž dochází ke snižování odměny pro těžaře přibližně každé čtyři roky. Původní výše odměny činila 50 bitcoinů za jeden blok, přičemž každým halvingem se tato částka zmenšuje na polovinu. V důsledku toho se očekává, že poslední bitcoin bude vytěžen kolem roku 2140. Do té doby budou těžaři odměňováni nejen novými bitcoiny, ale postupně i poplatky za provedené transakce. Právě omezené množství brání neřízenému zvyšování nabídky, jaké může být běžné u tradičních měn. Tento aspekt bývá často srovnáván s vlastnostmi drahých kovů, zejména zlata. Tento princip konečného množství je jedním z hlavních důvodů, proč je bitcoin vnímán jako uchovatel hodnoty (Tapscott a Tapscott 2018).

Pro používání Bitcoinu je nezbytné vlastnit tzv. účet, který tvoří dvojice údajů – veřejná adresa a soukromý klíč. Adresa slouží jako identifikátor pro příjem plateb a může být volně sdílena, zatímco klíč musí zůstat utajen a slouží k autorizaci transakcí. Běžnou praxí je generování nové adresy pro každou jednotlivou platbu s cílem zvýšit soukromí uživatele. Tento přístup je umožněn prakticky neomezeným počtem možných kombinací adres a klíčů. Jejich uchovávání a správa bývá zajištěna prostřednictvím peněženky, která může mít podobu softwarové aplikace nebo specializovaného zařízení. Peněženka umožňuje přehled o zůstatku, který je dán součtem prostředků napříč všemi adresami uživatele. Při odesílání plateb se vytvoří transakce, v níž je uvedeno množství bitcoinů a cílová adresa. Tato transakce je následně předána do sítě prostřednictvím uzlu, na který je peněženka napojena.

Uzel provede kontrolu správnosti transakce, ověří například dostatek prostředků, oprávněnost přístupu k adrese nebo to, zda prostředky nebyly již utraceny. V případě, že je transakce platná, je dále šířena mezi ostatní uzly. Tímto způsobem se informace rychle rozšíří do celé sítě, a to i bez centrální autority, protože každý uzel je propojen s dalšími a opakuje proces ověřování a předávání. Validní transakce jsou uchovávány dočasně v paměti uzlů, dokud nejsou zahrnuty do některého z budoucích bloků (Novák 2023).

U Bitcoinu se často hovoří, že je anonymní. Není zcela anonymní, ale pseudoanonymní. To znamená, že ačkoliv jsou všechny transakce v bitcoinové síti zaznamenány v blockchainu, tak veřejné klíče nejsou přímo spojeny s identitami uživatelů. Díky decentralizaci sítě neexistuje žádná centrální autorita, která by tyto adresy propojovala s reálnými jmény nebo osobními údaji. Transakce probíhají přímo mezi uživatelskými adresami a dokud uživatelé sami nespojí svou identitu s konkrétní adresou (například při registraci na burze), zůstávají jejich transakce v rámci sítě pseudoanonymní. Každá transakce je sice veřejně dohledatelná, ale bez znalosti vlastníků jednotlivých adres je těžké určit, kdo konkrétní transakce provedl (Bouška 2023).

2.2 Ethereum

Myšlenka Etherea byla poprvé prezentována v roce 2014, přičemž první blok byl zapsán v následujícím roce. Za vznikem této platformy stojí Vitalik Buterin a dle tržní kapitalizace se jedná o druhé nejvýznamnější kryptoaktivum. Na rozdíl od Bitcoinu byl systém navržen tak, aby kromě základních funkcí uchovávání a převodu jednotek umožňoval i spouštění programového kódu uloženého přímo na blockchainu. Tento mechanismus, označovaný jako chytré kontrakty (smart contracts), slouží k definování pravidel interakce mezi jednotlivými uživateli a jejich digitálními prostředky. Díky této technologii se Ethereum stalo základem pro vznik dApps, které umožňují přímou interakci mezi uživateli bez potřeby centrální autority. Právě aplikace zaměřené na oblast financí se ukázaly jako nejperspektivnější, což vedlo ke vzniku DeFi. Cílem této oblasti je poskytování finančních služeb, a to s minimálními transakčními náklady a vysokým užitekem pro uživatele. Klíčovým prvkem je zde rovný přístup. Pro využití tohoto systému nezáleží na výši majetku ale pouze na uhrazení pevně stanoveného poplatku. Předpokládá se proto, že řada tradičních finančních služeb může být v budoucnu tímto způsobem nahrazena. Aplikace v rámci DeFi pokrývají základní funkce, kterými jsou směna, půjčování nebo převod hodnoty. Zároveň s

jejich vzájemným kombinováním vzniká dynamické a adaptabilní prostředí, které přitahuje rostoucí počet uživatelů ze standardního finančního sektoru (Harvey et al. 2021).

Spuštěním Etherea přibýlo velké množství dApps. Většina těchto dApps funguje i s vlastními nativními jednotkami, které jsou označovány jako kryptotokeny nebo appcoiny. V rámci Ethereum sítě je využívána jeho jednotka ether, kterou můžeme označit za kryptokomoditu. Proto v případech, kdy dApp využívá svůj kryptotoken, je potřeba pokrytí poplatků za provádění transakcí v rámci sítě právě etherem. Kryptotokeny tedy nemají vlastní blockchain. Jsou pouze využívány v rámci dApps postavených na blockchainu kryptokomodit, jako je právě třeba Ethereum. Můžeme si to představit jako App Store či Google Play, které fungují na příslušných operačních systémech, aniž by vyžadovaly vlastní (Burniske a Tatar 2018).

Od roku 2015 bylo pro dosažení konsenzu v síti Ethereum využíváno Proof of Work. Tento model ale vedl k rozvoji těžebního průmyslu, který se postupně stal doménou specializovaných firem vybavených zařízeními typu ASIC. Vysoká spotřeba energie spojená s těžbou způsobila, že byla vnímána jako environmentálně nevhodná a zároveň se stala běžným uživatelům nedostupnou. Z těchto důvodů bylo rozhodnuto o přechodu na nový mechanismus Proof of Stake. Tento zásadní krok byl uskutečněn v září 2022 v rámci události nazvané „The Merge“. Během této změny se za plného provozu přešlo z těžby na tzv. staking. Energetická náročnost sítě byla snížena přibližně o 99,95 %. Při využívání Proof of Stake je proces dosažení konsenzu založen na účasti validátorů, kteří místo těžby ukládají vlastní prostředky jako záruku správného chování. Výběr validátorů je prováděn na základě vsazených etherů, čímž je umožněna širší účast uživatelů bez nutnosti pořizování technického vybavení. Celý systém tak výrazně snižuje environmentální dopady a zajišťuje vyšší dostupnost potvrzování transakcí v síti. Abychom se stali validátorem, tak je vyžadováno provozování plného uzlu a přihlášení prostřednictvím validátorského klienta. Vklady jsou spravovány pomocí vkladového kontraktu, ve kterém jsou evidovány všechny aktivní validátorské účty. Pro zachování stability sítě byl zaveden pořadník zařazení nových validátorů, aby nebyla síť přetížena. Výše vkladu činí 32 ETH. Tato hodnota je nastavena tak, aby byla zajištěna odolnost vůči tzv. sybil útoku. Tím se zajišťuje, že bez dostatečných nemohou být vytvářeny falešné uzly. V případě pokusu o takový útok by útočník riskoval ztrátu vložených prostředků (Dylan-Ennis 2024).

V blockchainu Ethereum je transakce považována za základní jednotku, na níž je postaveno fungování celé sítě, včetně decentralizovaných financí. Transakcí je rozuměn přenos etheru,

popřípadě kryptotokenu mezi dvěma adresami. Veškeré interakce v rámci sítě Ethereum, včetně těch s chytrými kontrakty, jsou inicializovány právě prostřednictvím transakce, a proto je jejich pochopení zásadní pro porozumění celé síti. Rozlišují se dva hlavní typy adres, a to na adresy uživatelů, tzv. externě vlastněné účty, a adresy přiřazené ke kontraktům. Zatímco přenos etheru je možný pouze mezi externími adresami, tak v případě kontraktních adres je prostřednictvím transakce spouštěn kód uložený v těle smlouvy. Tato interakce může i nemusí být spojena s převodem prostředků. Každá transakce je spouštěna uživatelem z externí adresy a může zahrnovat interakci s více chytrými kontrakty v rámci jedné operace. Proces je zahájen vstupem do prvního kontraktu, který následně definuje jednotlivé kroky, které mají být vykonány. Pokud v průběhu provádění dojde k nesplnění některé podmínky uvedené v kódu smlouvy, tak je celá transakce zneplatněna a všechny předchozí kroky jsou vráceny do počátečního stavu. Tato vlastnost je v blockchainu označována jako atomarita. Ta zajišťuje, že transakce bude provedena celá, nebo vůbec. Tento princip je klíčový pro bezpečnost a předvídatelnost převodů mezi více smlouvami. Každá transakce je spojena s tzv. gas, tedy poplatkem, kde se jeho výše odvíjí od složitosti dané operace. U jednoduchých převodů je poplatek relativně nízký, zatímco u výpočetně náročnějších operací roste. V případě neúspěšného průběhu transakce nebo jejího vypršení platnosti je tento poplatek zcela propadnut, aby byli těžaři chráněni před rizikem neuhrazené práce. O ceně gasu rozhoduje nabídka a poptávka. Vytváří se tak prostředí, ve kterém jsou transakce s vyšší nabídkou upřednostňovány k zařazení do nejbližšího bloku. Před jejich samotným zapsáním jsou transakce dočasně uchovávány v tzv. mempoolu. Každý těžař monitoruje veřejně dostupné transakce, které se následně šíří mezi uzly. V případě, že nabídnutý gas neodpovídá aktuálnímu vytížení sítě, může být transakce přesunuta do pozdějšího bloku (Harvey et al. 2021).

2.3 Solana

Anatoly Yakovenko, spoluzakladatel Solana blockchainu, během praxe v oblasti distribuovaných systémů zjistil, že implementace mechanismu Proof of History by umožnila výrazné zvýšení rychlosti blockchainové sítě. V roce 2017 společnost Solana Labs zveřejnila white paper ve kterém tuto technologii popsali. Tento přístup umožňuje dosažení konsenzu mezi účastníky blockchainu prostřednictvím ověřování časového sledu jednotlivých událostí. Současně slouží k zaznamenávání průběhu času přímo do blockchainu. V dokumentu bylo dále poukázáno na skutečnost, že tehdejší blockchainové systémy nebyly založeny na jednotném čase. Každý uzel v síti se spoléhal na svůj vlastní lokální čas a neměl

tedy informace o čase ostatních účastníků. Absence důvěryhodného časového standardu tak způsobovala, že rozhodování na základě časového záznamu nemohlo být mezi jednotlivými uzly sjednoceno (Picardo 2024).

Mechanismus Proof of History tedy vytváří sekvenci ověřující průběh času. Tato sekvence je vytvářena prostřednictvím zabezpečeného hashovacího algoritmu, který přijímá jako vstup aktuální transakci a hash předchozí transakce. Výstup hashovací funkce je následně připojen k nové transakci a celý proces se opakuje s každou další transakcí. Na rozdíl od seskupování transakcí běžného u Proof of Work je při využití Proof of History každá transakce hashována samostatně, což umožňuje přesné určení jejího místa v časové posloupnosti. V celém tomto systému je jedním subjektem přijímána odpovědnost za zpracování transakcí. Tento subjekt musí ověřit hash transakce, zjistit, zda je zůstatek účtu dostatečný k pokrytí transakčních poplatků a všechny platné transakce sestavit do sekvence, která slouží jako historický záznam. Tento subjekt je označován jako „PoH Generator“ a i když je jediným subjektem v daném okamžiku, decentralizace systému je zajištěna algoritmem, který po určitém počtu bloků volí nového vůdce. PoH Generator zpracovává transakce na aktuálním stavu uloženém v paměťovém fondu a výsledky spolu s podpisem finálního stavu odesílá uzlům k ověření. Ověřování integrity vůdce je umožněno pomocí paralelizace a díky tomu je tak celá sekvence ověřována rychleji, než je generována. Tento proces je prováděn více jádrovými počítači a podléhá stanoveným časovým omezením. V případě, že nastane situace, kdy dvoutřetinová většina ověřovatelů označí „PoH Generatora“ za škodlivého, je tento subjekt odstraněn a vybere se nový. Solana používá k zápisu do blockchainu jen jeden počítač. To znamená, že celková rychlost sítě a škálovatelnost závisí hlavně na tom, jak rychlý je tento hardware. A protože výpočetní technika se postupně zrychluje, tak podle Moorova zákona se bude i výkon sítě automaticky zlepšovat s novějším hardwarem (Pierro a Tonelli 2022).

Proof of History tedy slouží k časovému označení transakcí a jejich rychlému ověření. K zajištění bezpečnosti, decentralizace a výběru validátorů se používá Proof of Stake. Tento blockchain tak využívá kombinaci dvou konsenzuálních mechanismů. Solana je často porovnávána s platformou Ethereum, která je považována za lídra v oblasti decentralizovaných aplikací. Obě sítě umožňují tvorbu chytrých kontraktů, které hrají klíčovou roli v oblasti decentralizovaných financí i digitálních tokenů (Picardo 2024).

Navzdory technologickým inovacím tohoto rychle rozvíjejícího se blockchainu, je nezbytné zohlednit také rizika, která mohou být s jeho růstem spojena. Skutečnost, že se jedná o

relativně novou síť vede k otázkám ohledně její dlouhodobé bezpečnosti a odolnosti. Doposud nebyla ověřena v takovém rozsahu, jako je tomu u déle fungujících blockchainových systémů. Přestože použitá řešení vykazují výrazný technologický potenciál, mohou současně přinášet i nové bezpečnostní výzvy. V minulosti došlo k několika výpadkům, které vyvolaly pochybnosti o její stabilitě a spolehlivosti.. Jedním z těchto případů byl i výpadek, který trval přibližně pět hodin a krátkodobě ovlivnil cenu tokenu. Zajištění nepřetržitého provozu bude do budoucna zásadní s ohledem na narůstající počet uživatelů a aplikací (Roberts 2024).

2.4 Ostatní

Tato část představuje další významná kryptoaktiva, která se odlišují svým technickým zaměřením nebo specifickým způsobem využití.

2.4.1 Ripple

„Ripple je spíš real-timový platební a zúčtovací systém než příklad klasické kryptoměny.“

Na vývoji této sítě pracuje společnost Ripple labs, kterou v roce 2011 založil Jed McCaleb. Impulsem pro vytvoření tohoto kryptoaktiva bylo navržení decentralizovaného systému, ve kterém by uživatelům bylo umožněno vytvářet a směňovat vlastní digitální prostředky a dluhové závazky obdobné elektronickým směnkám. Transakce v síti Ripple jsou ověřovány pomocí Proof of Correctness. Tento konsenzus je zajišťován skupinou důvěryhodných uzlů. Tím se dosahuje správnosti bez potřeby vysoké výpočetní náročnosti. Na rozdíl od jiných kryptoaktiv tento konsenzuální model spoléhá na důvěru v určité subjekty. Jeho výhodou je naopak rychlost zpracování transakcí, která se pohybuje v řádu sekund. V celé této síti může paralelně existovat více tzv. ledgerů, tedy účetních knih s tím, že každá z nich se chová jako samostatná jednotka. Konečný stav této účetní knihy je určován konsenzem, kterého musí dosáhnout alespoň 80 % uzlů. Každá transakce je považována za návrh na změnu stavu knihy. Pokud se většina uzlů neshodne, tak jsou sporné transakce vyřazeny a proces konsenzu se opakuje, dokud není dosaženo shody (Stroukal a Skalický 2021, s. 429).

Ripple byl vytvořen se záměrem sloužit jako alternativa tradičním přeshraničním platebním systémům, jako je například SWIFT. Při využití pro mezinárodní platby může být ze strany bank přistoupeno buď k využití nativního kryptoaktiva se zkratkou XRP, jako přechodné měny, nebo k využití samotného komunikačního systému pro urychlení převodu tradičních měn. V případě převodu například z dolarů na eura je síť automaticky vyhodnocena

nejvýhodnější cesta. Tedy přímá směna, nebo směna přes XRP jako mezičlánek. Tím může být dosaženo snížení transakčních nákladů, aniž by byla omezena kontrola nad celým procesem. Z hlediska architektury jsou systému přisuzovány tři hlavní výhody – vysoká rychlost, nízké náklady a schopnost škálování. Díky těmto vlastnostem může být Ripple považován za vhodnou alternativu k tradičním bankovním systémům. Transakční poplatky v síti Ripple jsou stanoveny na přibližně 0,00001 XRP, což je výrazně nižší než poplatky spojované s Bitcoinem či klasickými bankovními převody, které mohou dosahovat až několika desítek dolarů. Díky použití sítě RippleNet může být bankám umožněno snížení provozních nákladů až o 60 % (Sergeenkov 2024).

2.4.2 Stablecoiny

Stablecoiny představují specifickou kategorii kryptoaktiv, jejichž hodnota bývá navázána na jiné aktivum, aby si udržely stabilní hodnotu. Obvykle jsou vázány na měny s nízkou volatilitou, případně na komodity, nebo na jiná kryptoaktiva. Hlavním účelem je zmírnění výkyvů v hodnotě, které jsou typické pro běžně obchodovaná kryptoaktiva. Z hlediska způsobu fungování se stablecoiny obvykle rozdělují do čtyř základních typů:

- Stablecoiny kryté fiat měnami – jejich hodnota je zajištěna rezervami v tradičních měnách, přičemž krytí bývá udržováno v poměru 1:1. Příklady zahrnují Tether nebo USD Coin, přičemž správa rezerv bývá svěřena třetím stranám.
- Komoditní stablecoiny – navazují svou hodnotu na tržní cenu fyzické komodity. Například Tether Gold deklaruje krytí skutečnými zlatými zásobami.
- Kryptoměnově zajištěné stablecoiny – využívají jiná kryptoaktiva jako zajištění, které je z důvodu volatility obvykle nadhodnoceno. Například stablecoin DAI funguje tímto způsobem
- Algoritmické stablecoiny – jejich stabilita je udržována prostřednictvím algoritmu, který reguluje nabídku v reakci na změny poptávky. Tento model je však rizikovější, jak ukázal případ kolapsu TerraUSD.

Kvůli rostoucímu významu a šíři využití se stablecoiny dostávají do centra pozornosti regulačních orgánů. Díky svému stabilnímu kurzu a přímému využití v praxi představují stablecoiny důležitý nástroj propojující svět tradičních financí s prostředím kryptoaktiv (Hayes 2024).

3 PROBLEMATIKA PLATEB KRYPROAKTIVY

V souvislosti s kryptoaktivy je důležité zhodnotit nejen technickou proveditelnost transakcí, ale i praktické a systémové překážky, které brání širší adopci jako běžného platebního prostředku. Kapitola se věnuje rizikům, která s sebou využívání kryptoaktiv nese, včetně cenové volatility, regulační nejistoty, bezpečnostních hrozeb či problémům se škálovatelností sítí. Pozornost je dále zaměřena na právní rámec, v němž se kryptoinvestice pohybují, a to jak na mezinárodní, tak na evropské úrovni.

3.1 Rizika a hrozby (volatilita, bezpečnost, technická rizika)

Kryptoinvestice disponují technologií, která se stále vyvíjí a je považována za klíčový prvek jejich budoucího využití. Současně se s ní ale pojí několik potenciálních rizik. Mezi ně tak patří technologické nedostatky, omezení výkonu sítě a hrozby spojené s kybernetickou bezpečností. Jednou zásadní zranitelností bývá označována možnost výpadků. V některých případech bylo způsobeno selhání systému kvůli chybám v kódování, což vedlo ke ztrátě značného množství aktiv. Tyto incidenty ukázaly, že i drobné technické nedostatky mohou vést až k ničivým následkům (Rejeb et al. 2021).

U blockchainů, které využívají konsenzuální mechanismy, je bezpečnost systému podmíněna rovnováhou výpočetního výkonu mezi jednotlivými účastníky. Běžně je nově vytvořený blok připojen k řetězci poté, co byl nalezen účastníkem sítě a potvrzen ostatními. V případě, že by více než polovina celkového výpočetního výkonu byla ovládnuta jedním subjektem, tak by mohla být síť tímto uživatelem manipulována. Taková situace je označována jako 51% útok. V takové situaci by například mohlo být zabráněno potvrzení nových transakcí, zneužití možnosti opětovného použití již utracených prostředků nebo vytváření falešných převodů. Úspěšnost útoku však záleží i na tom, zda je výpočetní výkon udržen po dostatečně dlouhou dobu. V rozsáhlých sítích, jako je třeba Bitcoin, bývá takový útok považován za technicky i ekonomicky velmi náročný (Harvey et al. 2021)

Dalším z rizik může být považována nestabilní hodnota kryptoinvestic. Jelikož u některých z nich, zejména bitcoinu, byl v minulosti zaznamenán takový vývoj, který bývá označován jako cenové bubliny. V obdobích výrazného růstu hodnoty nebývá tento růst vždy podložen odpovídajícím ekonomickým vlivům. Je totiž spíše formován převážně očekáváním cenového růstu investorů. Počáteční zájem bývá následován prudkým nárůstem poptávky, po kterém bývá zaznamenáno náhlé ochlazení trhu, pokles důvěry a s tím i ceny aktiva. Vlivem decentralizované povahy většiny kryptoinvestic nebývají cenové výkyvy řízeny ani

korigovány žádnou externí autoritou. Tato otevřenost bývá považována za faktor, který zvyšuje citlivost systému na vnější vlivy a zároveň pak činí systém zranitelnějším vůči náhlým spekulativním výkyvům. Nestabilita tak bývá připisována nejen tržní nejistotě, ale rovněž technologickému uspořádání, které omezuje možnost přesnější predikce cenového vývoje. Za další faktor podporující spekulace bývá nastavení emise mincí. Například snižování tempa vydávání nových jednotek bývá vnímáno jako možný impuls pro růst jejich ceny. I když může být tento mechanismus technicky odůvodněn, v prostředí finanční spekulace to bývá připodobňováno schématům, která jsou typická pro podvodné investiční struktury. Pokud je k tomu celému ještě připojeno nízké povědomí o fungování těchto technologií, tak spolu s riziky s uchováváním přístupových údajů, bývá vytvářeno prostředí, ve kterém je část uživatelů s menšími znalostmi vystavována zvýšené pravděpodobnosti ztráty (Grujić a Radivojac 2019).

I když jsou kryptoaktiva často prezentována jako bezpečné díky pokročilým šifrovacím technologiím, tak v praxi se ukázalo, že jsou častým cílem kybernetických útoků. Ohrožení vzniká např. při ztrátě nebo neoprávněném sdílení soukromých klíčů, které jsou nezbytné k ověření vlastnictví kryptoaktiv. V minulosti došlo k několika incidentům, při kterých byla dokonce napadena kryptoměnová burza a prostřednictvím odcizených klíčů bylo získáno velké množství aktiv. Další hrozbou jsou škodlivé softwarové kódy, které po infikování zařízení umožňují neoprávněné převody. Zvýšená úroveň anonymity, kterou kryptoaktiva poskytují, může být navíc problematická z hlediska kontroly a vymáhání práva. Tato vlastnost může usnadňovat nelegální jednání a ztěžovat dohled nad zneužitím systému (Rejeb et al. 2021).

3.2 Regulace a legislativní překážky

Mezinárodní organizace jsou v regulaci kryptoaktiv nejednotné, proto se snaží sjednotit jejich regulační rámec. Cílem těchto organizací je tedy zajistit konzistentní přístup k jejich vydávání a oběhu na globální úrovni. Klíčovým aspektem této regulace je kontrola transakcí s kryptoaktivami a stablecoinů. Zároveň je při regulaci nutné přihlídnout ke specifikům jednotlivých aktiv a odlišnou míru rizika spojenou s jejich používáním. Významnou překážkou této snahy je nejen decentralizovaná povaha kryptoaktiv, která ztěžuje jejich dohled a regulaci, ale také rozdílné právní přístupy jednotlivých států. Regulace se proto potýká s nejednotností výkladů a klasifikace kryptoaktiv, což také vede k rozdílným

strategiím jednotlivých jurisdikcí při řízení rizik a samotném vytváření regulačních opatření (Kochergin 2022).

Každá část světa má různé regulační orgány, které přistupují k regulaci kryptoaktiv odlišně. Od přísných pravidel zaměřených na ochranu spotřebitelů a prevenci finanční kriminality až po flexibilnější přístupy podporující inovace v blockchainovém sektoru (Juodis 2024).

Proto je cílem této kapitoly představit hlavní regulační rámce, organizace zodpovědné za jejich tvorbu a porovnat, jak jednotlivé jurisdikce přistupují k právní regulaci kryptoaktiv.

3.2.1 Evropská unie

Nařízení Markets in Crypto-Assets (MiCA) představuje právní rámec Evropské unie pro regulaci kryptoaktiv, jejich vydávání a obchodování. Jeho cílem je zvýšit transparentnost trhu, posílit ochranu spotřebitelů a zajistit stabilitu kryptoměnového sektoru. MiCA stanovuje pravidla pro veřejné nabízení kryptoaktiv a poskytování služeb souvisejících s kryptoaktivy. Současně zavádí opatření proti zneužívání vnitřních informací, manipulaci s trhem a dalším formám nekalého jednání. „*Kryptoaktivem nařízení MiCA rozumí digitální zachycení hodnoty nebo práva, které může být převáděno a ukládáno elektronicky pomocí technologie distribuovaného registru nebo pomocí podobné technologie (dnes typicky pomocí blockchainu)*“ (Novotný 2024).

V rámci nařízení MiCA jsou definovány tři základní typy kryptoaktiv, které podléhají regulaci:

1. Tokeny vázané na aktiva – Jejich hodnota zůstává stabilní díky propojení s více měnami, případně s určitými komoditami nebo jinými kryptoaktivy, či kombinací všech těchto aktiv. Využívají se jak pro platby za zboží a služby, tak i jako prostředek k uchování hodnoty.
2. Elektronické peněžní tokeny – Hodnota těchto tokenů zůstává stabilní díky navázání na jednu jedinou fiat měnu. Funguje tedy jako digitální alternativa hotovosti. Hlavním účelem je jejich využití jako platebního prostředku.
3. Další kryptoaktiva – Do této kategorie patří třeba užitné tokeny nebo i kryptoaktiva jako Bitcoin, Ether a Solana, které jsme si již v 2. kapitole zmínili (Novotný 2024; Rada EU a Evropská rada 2024).

MiCA stanovuje, že poskytování služeb souvisejících s kryptoaktivy je podmíněno předchozím udělením povolení příslušným národním orgánem členského státu Evropské

unie. Tato povinnost se vztahuje na všechny subjekty označované jako poskytovatelé služeb souvisejících s kryptoaktivy (CASPs). Mezi činnosti, které spadají pod regulaci MiCA, patří především úschova a správa kryptoaktiv na účet třetích osob, provozování obchodních platforem, směna kryptoaktiv za fiat měny nebo jiná kryptoaktiva, provádění pokynů klientů, umístování kryptoaktiv na trh, přijímání a předávání pokynů a rovněž poskytování poradenství v oblasti kryptoaktiv. CASPs jsou dále povinni dodržovat obecné organizační požadavky a pravidla jednání, která zahrnují především povinnost jednat čestně, spravedlivě a profesionálně v nejlepším zájmu svých klientů. Tyto obecné požadavky doplňují specifické povinnosti, které se vztahují k jednotlivým poskytovaným službám. Např. poskytovatelé úschovy kryptoaktiv musí dodržovat přísná pravidla odpovědnosti, včetně bezpečnostních standardů a ochrany majetku klientů, což je oblast, která podléhá zvýšenému dohledu. Cílem tohoto komplexního regulačního rámce je zajistit vysokou úroveň ochrany investorů, podporovat důvěru ve finanční trhy a posilovat integritu trhu s kryptoaktivy v rámci Evropské unie (Hobza a Vondráčková 2021).

3.2.2 USA

Regulace kryptoaktiv ve Spojených státech není jednotná, jelikož do procesu regulace vstupuje více institucí na federální i státní úrovni, přičemž jejich přístupy se často liší a celý vývoj je pomalý (Poynton 2022).

Mezi hlavní regulátory patří Komise pro cenné papíry a burzy (SEC), Komise pro obchodování s komoditními futures kontrakty (CFTC) a Finanční zpravodajská jednotka (FinCEN) spadající pod Ministerstvo financí (Trautman 2018).

FinCEN je federální úřad zaměřený na dohled nad finančními toky s cílem zamezit jejich zneužití k nelegálním účelům, jako je praní špinavých peněz (AML) či financování terorismu. Na základě zákona o bankovním tajemství ukládá povinnost monitorovat transakce a ověřovat identitu zákazníků (KYC), což se od roku 2013 vztahuje i na kryptoaktiva. V tehdy vydaných pokynech FinCEN definovala virtuální měnu jako digitální prostředek směny bez statusu zákonného platidla, čímž podřadila směnárníky a zprostředkovatele těchto transakcí pod režim AML regulace. Výsledkem je široké pojetí dohledu, které umožňuje regulaci většiny kryptoaktiv bez ohledu na jejich konkrétní funkci. SEC, druhý klíčový regulátor, se zaměřuje na ochranu investorů a posuzuje, zda konkrétní kryptoaktivum naplňuje znaky cenného papíru pomocí tzv. Howeyho testu. Pokud jsou splněny podmínky investice, společného podniku a očekávání zisku na základě cizího úsilí,

podléhá aktivum regulačnímu režimu cenných papírů. Zatímco Bitcoin a Ether tímto testem neprošly, u jiných tokenů mohou platit přísné registrační povinnosti a omezení obchodování. Uplatňování testu bývá kritizováno kvůli právní nejistotě a roztříštěné praxi (Jones 2022).

CFTC ve svém přístupu vychází z definice virtuální měny, která je jednotná s pojetím užívaným FinCEN a daňovým úřadem IRS, tedy jako prostředek směny, zúčtovací jednotku nebo uchovatele hodnoty, který plní funkce reálné měny, bez toho aniž by měl status zákonného platidla. Na základě této definice CFTC považuje coinsy a tokeny za komodity. Tento přístup se však liší od postoje FinCEN. Je to z důvodu, že FinCEN považuje firmy směňující kryptoaktiva za převodce peněz, zatímco CFTC je vnímá jako obchodníky s komoditami. Zájem CFTC o oblast kryptoaktiv je kvůli snaze o prevenci podvodů a manipulací na trzích, nad nimiž vykonává dohled. To zahrnuje nejen trhy s futures a deriváty, ale i spotové trhy s komoditami. Přestože CFTC nerozlišuje mezi jednotlivými kryptoaktivami, její přístup zajišťuje regulační dohled a pravomoc k vymáhání práva a to v případech jakýchkoli futures kontraktů či derivátů zahrnujících virtuální měny. Pokud jde o přímé obchodování s těmito aktivy na spotových trzích, tak má CFTC pouze pravomoc zasáhnout při zjištění podvodu nebo manipulace. To ale bez možnosti určovat standardy pro tento typ obchodování (Goforth 2018).

3.2.3 Asie

Čína jako jedna z velmocí asijského kontinentu v roce 2021 zavedla plošný zákaz obchodování a těžby kryptoaktiv. Tento krok byl učiněn na základě obav o udržení finanční stability, omezení finanční kriminality a snižování energetické náročnosti spojené s těžbou. Zároveň byla ze strany čínské vlády zahájena intenzivní podpora vývoje digitální měny centrální banky, známé jako digitální jüan. Tímto opatřením měla být posílena kontrola nad národním měnovým systémem a omezena možná destabilizace, kterou by mohlo způsobit rozšíření soukromých, decentralizovaných kryptoaktiv. Přestože technologie blockchain byla v Číně dříve podporována, v důsledku uvedených zákazů došlo k utlumení jejího rozvoje a řada společností byla nucena přesunout své aktivity do států s příznivější legislativou, jako je například Singapur. Čínský regulační rámec může tak být vnímán jako příklad přístupu, v jehož důsledku dochází k omezení technologického rozvoje a přesunu inovačních aktivit do jurisdikcí s otevřenějším přístupem k digitálním aktivům (Fred a Oluwaseun 2025).

V Ruské federaci je oblast digitálních aktiv upravována samostatně vyvíjeným právním rámcem, jehož základem je specifická terminologie lišící se od běžně používaných pojmů. Namísto označení token bylo zavedeno označení digitální právo, které odkazuje na digitalizovanou formu existujících majetkových práv, nikoli na samostatnou majetkovou kategorii. V rámci této úpravy byly rozlišeny například užitková digitální práva, odpovídající svým charakterem užitkovým tokenům, jejichž právní ochrana je však podmíněna naplněním požadavků stanovených ruskou legislativou. Dále byly vymezeny digitální finanční aktiva, představující formu investičních tokenů, které ztělesňují nároky na plnění či práva spojená s vlastnickými podíly v neveřejných společnostech. Regulace digitálních měn, kam spadají kryptoaktiv, zůstává v Ruské federaci nejednotná. Přestože byly tyto měny právně vymezeny, nebyl dosud vytvořen komplexní právní rámec, který by jejich postavení jednoznačně upravoval. Rozhodovací praxe ruských soudů je v tomto směru nekonzistentní a některá rozhodnutí označila kryptoaktiva za nástroje umožňující praní špinavých peněz, zatímco jiná jim přisoudila status „jiného majetkového práva“, čímž byla zajištěna jejich trestněprávní ochrana. Na vývoj v této oblasti bylo reagováno návrhem zákona „O digitálních měnách“, který byl připraven Ministerstvem financí Ruské federace. Návrh zákona počítá s legalizací kryptoaktiv a jejich využitím v zahraničním obchodě, přičemž má být zavedeno licencování platforem umožňujících jejich obchodování. Sankční mechanismy však zatím návrhem upraveny nebyly. Celkový směr připravované legislativy vykazuje znaky přístupu podobného regulaci trhu s cennými papíry, což naznačuje vysokou míru regulace a dohledu nad daným segmentem digitálních aktiv (Muradyan 2023).

V rámci zbytku zemí Asie je regulace kryptoaktiv v jednotlivých zemích nastavována odlišně, přičemž často bývá zvolena strategie opatrného vyčkávání. V Indii nebyla navzdory původním plánům na zákaz soukromých kryptoaktiv příslušná legislativa přijata a obchodování s těmito aktivy je nadále umožněno. Byla však zavedena daňová opatření, včetně 30% zdanění zisků z těchto aktiv a 1% srážkové daně při transakcích. Ve Vietnamu bylo používání kryptoaktiv jako zákonného platidla označeno za protiprávní, avšak samotné držení a obchodování s těmito aktivy je tolerováno. Regulace v této oblasti zatím zůstává neúplná. V kontrastu k těmto zdrženlivým postojům se nachází Singapur, kde byl vybudován komplexní regulační rámec pod dohledem Měnového úřadu Singapuru. Poskytovatelé služeb digitálních platebních tokenů zde podléhají licenčním požadavkům a přísným pravidlům zaměřeným na prevenci praní špinavých peněz a financování terorismu. Japonsko zvolilo cestu, na níž je dohled nad kryptoměnovým sektorem zčásti delegován na

samoregulační orgán – Japonskou asociaci virtuálních měnových burz. Vysoké daňové zatížení spojené ale přimělo některé subjekty uvažovat o přesunu podnikání do jiných jurisdikcí. Kazachstán zaznamenal výrazný nárůst těžebních aktivit po zavedení restrikcí v Číně, což vedlo k růstu spotřeby energie a následnému zavedení zvláštních daní pro těžaře. Avšak problémy s energetickou infrastrukturou a zvýšené náklady způsobily postupný útlum této činnosti a přesun části těžební kapacity jinam. V Indonésii bylo zakázáno využívat kryptoaktiva jako platební prostředek, nicméně samotné obchodování s nimi zůstává povoleno. Ministerstvo obchodu zde navíc plánuje vytvoření národní kryptoměnové burzy. Z teologického hlediska byly kryptoaktiva prohlášeny Islámskou učenou radou za neslučitelné s právem šaría. Toto stanovisko nemá ale právní závaznost, dokud nebude převzato do oficiální legislativy (Paesano a Siro 2022).

3.2.4 Legalizace plateb kryptoaktivity

El Salvador se stal první zemí, která přijala Bitcoin jako zákonné platidlo. Tato iniciativa byla prosazená prezidentem Nayibem Bukelem a vzbudila celosvětovou pozornost a rozdílné reakce. Hlavním cílem bylo snížit náklady na remittance, které v roce 2020 tvořily 25 % HDP. Dále také posílit finanční začlenění, jelikož až 70 % obyvatel nemělo přístup k bankovním službám. Dále bylo argumentováno možnými úsporami veřejných prostředků díky snížení závislosti na dovozu amerických dolarů. V rámci implementace byl zřízen fond ve výši 150 milionů USD u státní banky BANDESAL, který měl umožnit konverzi bitcoinů na dolary a financovat pobídky, např. jednorázový příspěvek 30 USD v bitcoinech pro každého občana. Pro praktické využití spustila vláda bezpoplatkovou digitální peněženku Chivo a rozsáhlý vzdělávací program. Centrální banka El Salvadoru vydala technické standardy pro konverzní služby, včetně opatření proti praní špinavých peněz a financování terorismu. Projekt čelil řadě problémů, včetně poklesu ceny bitcoinu po státních nákupech a technických obtížích s digitální peněženkou. Mezinárodní měnový fond a Světová banka upozornily na rizika spojená s měnovou a fiskální stabilitou, finanční integritou, ochranou spotřebitelů a vysokou volatilitou bitcoinu. Kritika se zaměřila i na environmentální dopady těžby kryptoaktiv. Reakcí na přijetí bylo i mimo jiné snížení ratingu státního dluhu El Salvadoru. Přestože země slouží jako modelový případ pro adopci kryptoaktiv, tak v národním měnovém systému, projekt provází značné praktické i regulatorní nejistoty a jeho dlouhodobé dopady zůstávají nejasné (Gorjon, 2021).

Kontrastem El Salvadoru je případ mezi již zmíněným regulátorem Spojených států SEC a společností Ripple Labs. V prosinci 2020 bylo mezi nimi zahájeno právní řízení. Hlavní

předmět sporu bylo tvrzení, že společnost stojící za kryptoaktivem XRP neoprávněně distribuovala toto digitální aktivum bez odpovídající registrace, která je dle pravidel pro cenné papíry vyžadována. Ripple Labs toto tvrzení odmítlo a obhájilo se názorem, že XRP představuje formu digitální měny, a nikoliv tedy investiční nástroj, který by podléhal pravidlům SEC. Veřejné oznámení sporu způsobilo výrazný pokles hodnoty XRP, přičemž bylo zaznamenáno snížení tržní ceny o více než polovinu. Současně bylo obchodování s XRP omezeno či zcela přerušeno na několika klíčových kryptoměnových burzách. Navzdory této negativní situaci si Ripple udržela stabilní pozici na trhu díky rozsáhlé spolupráci s více než třemi stovkami finančních institucí. Samotné zahájení řízení bylo vnímáno jako překvapivé, jelikož XRP patřilo v letech 2017 a 2018 mezi nejvýznamnější kryptoaktiva podle velikosti tržní kapitalizace. Ze strany SEC bylo argumentováno, že kontrola Ripple Labs nad významnou částí celkové nabídky XRP a aktivní snaha o růst jeho hodnoty naplňují podmínky Howeyho testu. V březnu 2025 bylo oznámeno, že SEC odvolala svůj záměr pokračovat v soudním sporu, což bylo vnímáno jako důležité vítězství pro Ripple. Právní odborníci však upozornili, že tímto rozhodnutím nebyl vytvořen právně závazný precedent, který by se dal automaticky vztáhnout i na jiné subjekty v rámci tohoto odvětví (Peak 2024).

3.3 Kyberbezpečnost a ochrana uživatelů

Kyberbezpečnost je u kryptoaktiv velmi důležitá, protože jejich hodnota neustále roste a s tím i motivace pro různé podvody a krádeže. Digitální peněženky, směnárny i jednotlivé uživatelské účty jsou často cílem útoků. Bez patřičných opatření nese tato oblast kryptoaktiv potenciální rizika. Hackeři se mohou pokusit získat přístup k privátním klíčům uživatelů, tudíž by se jim umožnilo ukrást prostředky z kryptoměnových peněženek. Z toho vyplývá, že by držitelé kryptoaktiv měli dbát na pečlivé zabezpečení peněženek pomocí silných hesel a bezpečných softwarových nástrojů. Také by měli vyhledávat ověřené a známé směnárny s osvědčenými bezpečnostními protokoly. Uživatelé by si dále měli být vědomi několika běžných kybernetických bezpečnostních problémů. K ochraně před hackery získávajícími přístup k soukromým klíčům nebo heslům by uživatelé měli implementovat vícefaktorové ověřování. Některé směnárny mohou vyžadovat ověření identity, což poskytuje další úroveň zabezpečení. Problém je i nárůst phishingových útoků, které zahrnují zasílání podvodných e-mailů nebo příspěvků na sociálních sítích. Proto je klíčové naučit se rozpoznat známky phishingu a ověřovat platnost zpráv. Dále by si uživatelé měli uvědomovat běžných hrozeb jako škodlivý software a malware. Proto je důležité, aby jejich zařízení byla dostatečně zabezpečena (Logeshwaran et al. 2023).

Za jeden z nejspolehlivějších nástrojů bývá v oblasti zabezpečení kryptoaktiv považována hardwarová peněženka. Tato zařízení jsou navrhována tak, aby soukromé klíče nebyly nikdy vystaveny přímému kontaktu s internetem, ani se zařízením, které by mohlo být napadeno. Veškeré potvrzování transakcí je prováděno přímo na hardwarové peněžence, proto je eliminována možnost zachycení citlivých údajů škodlivým softwarem. Přístup k prostředkům je podmíněn interakcí uživatele prostřednictvím zadání PIN kódu nebo potvrzovacího gesta. Bezpečnostní rozhraní bývá navrhováno tak, aby umožňovalo uživatelsky přívětivou obsluhu a zároveň nemohlo být lehce zneužito. V případě ztráty této peněženky bývá možnost obnovení přístupu pomocí obnovovací fráze, která je vygenerována při prvním nastavení. Tato kombinace izolace, fyzické kontroly a možnosti zálohování činí z hardwarových peněženek preferované řešení pro dlouhodobé uchovávání většího množství kryptoaktiv (Stroukal a Skalický 2021).

3.4 Vliv decentralizace na regulaci a adopci

Decentralizace vytváří prostředí s otevřeným přístupem a nižšími bariérami vstupu. Přestože tento rozvoj je motivován snahou o rozšíření ekonomické účasti, tak hlavním faktorem současné adopce zůstává ve velké míře spekulace. V některých regionech, zejména s nižší důvěrou ve státní měny, je využívání kryptoaktiv podporováno i snahou o obejít stávajícího finančního systému. Díky anonymitě blockchainu je navíc omezena možnost vynucování práva a sankcí za podvodné chování. Z pohledu regulátorů je obtížné zvolit vhodný přístup. Zákaz bývá považován za nežádoucí. Přístup založený na omezení kontaktu mezi tradičním a decentralizovaným sektorem je diskutován jako jedna z možností. Vhodnější variantou se jeví cílená regulace, která zohlední ekonomickou funkci jednotlivých nástrojů a bude schopna identifikovat subjekty vykonávající faktickou kontrolu. Pro dosažení souladu s pravidly může být uvažováno i o technickém řešení v podobě zabudování regulací přímo do chytrých smluv (Aquilina et al. 2025).

4 POTENCIÁL A VÝZVY VYUŽITÍ KRYPTOAKTIV V PLATEBNÍM SYSTÉMU

Kryptoaktiva jsou v současnosti považována za nástroj s významným inovačním potenciálem. Zejména díky možnosti realizace transakcí bez zprostředkovatelů, nízkým nákladům a rychlosti převodů. Současně je však třeba kriticky nahlížet na faktory, které tento rozvoj brzdí. V rámci této kapitoly jsou proto rozebrány nejen výhody, ale i konkrétní výzvy spojené s reálným nasazením kryptoaktiv do běžného ekonomického provozu.

4.1 Adopce kryptoaktiv v platebním styku

Kryptoaktiva v oblasti platebního styku jsou v současnosti vnímána jako oblast s výrazným potenciálem. Díky technologii blockchain mohou být platby realizovány bez zprostředkovatelů, což tedy umožňuje rychlé a levné převody mezi jednotlivými uživateli. Významného uplatnění bývá dosahováno zejména u mezinárodních plateb, kde mohou být prostředky zasílány bez využití bankovního systému, dokonce v řádu minut. V některých případech bývají kryptoaktiva používány i k převodům v oblastech s omezeným přístupem k tradičním finančním službám, čímž může být podpořena finanční inkluze. Ačkoli zatím nedošlo k plošnému zavedení kryptoaktiv jako standardního platebního nástroje, tak jejich praktické využití, jako např. při převodech do rozvojových zemí či při platbách v internetových obchodech, již bylo v praxi úspěšně ověřeno. Potenciál k jejich širšímu uplatnění a postupné adopci se naplní, bude-li podporován rozvojem technologií a vytvořením stabilního regulačního prostředí (Khan et al. 2023)

Ačkoli je kryptoaktivům často přisuzován výrazný potenciál, jejich masové rozšíření mezi běžnými uživateli zatím nenastalo. Brání tomu několik zásadních překážek – nejčastěji zmiňovanými jsou cenová volatilita, neexistence jasného regulačního rámce a nízká míra přijetí ze strany obchodníků. Tyto faktory vzájemně oslabují jak nabídku, tak poptávku. Na druhé straně mohou nízké transakční náklady a důraz na ochranu soukromí přispět k rozšíření používání. Pokud však nejsou splněny základní požadavky na důvěrnost dat, důvěra uživatelů může být snadno narušena. Rozšíření navíc komplikuje nedostatečné povědomí veřejnosti, technické i právní rizika. Důvěra tak zůstává převážně na straně tradičního bankovního systému, což jde proti základnímu principu decentralizace. Pro širší uplatnění kryptoaktiv v běžném platebním styku bude nutné těmto výzvám čelit důsledně a koordinovaně (Hamm 2022).

4.2 Výhody kryptoaktiv oproti tradičním platebním metodám

Tato část se zaměřuje na přehled hlavních výhod, které kryptoaktiva nabízejí v porovnání s tradičními digitálními platebními systémy.

4.2.1 Rychlost a nízká cena transakcí

Transakce prostřednictvím kryptoaktiv bývají charakterizovány nižšími náklady a vyšší rychlostí ve srovnání s tradičními platebními metodami. Díky přímé formě převodu mezi uživateli bez potřeby prostředníka může být výrazně snížena finanční zátěž, která u klasických přeshraničních plateb často zahrnuje vysoké poplatky a dlouhé zpracování. V praxi bylo zaznamenáno, že doba převodu bývá zkrácena na několik minut a náklady tvoří jen zlomek z celkové částky. Tato efektivita byla ověřena například v případech převodů ze zahraničí, kde byla využita blockchainová aplikace namísto služeb typu Western Union. Díky tomu může být kryptoaktivům přisuzována konkurenční výhoda v oblasti mezinárodních plateb, kde je na rychlost a nákladovost kladen důraz. I přesto jsou i určitá rizika, tak samotný mechanismus převodu bývá považován za funkční a efektivní alternativu k tradičním systémům (Grujić a Radivojac 2019)

4.2.2 Absence prostředníků

V modelu tradičního systému plateb je správa transakcí svěřována prostředníkům s pravomocí schvalovat, zdržovat či rušit převody. Tato závislost bývá spojována s omezením některých práv, jako je soukromí, bezpečnost nebo rovný přístup. Zásadní změna nastala s příchodem blockchainové technologie. Pomocí této inovace může být ověřeno vlastnictví a zamezeno problému dvojí útraty. Jakmile je transakce zaznamenána, nemůže být zpětně zrušena nebo upravena třetí stranou. Tím je odstraněna nutnost důvěřovat externím subjektům, tedy prostředníkům. Složitější digitální operace mohou být řízeny prostřednictvím chytrých smluv. Tímto způsobem může být zajištěno plnění podmínek, které by za běžných okolností vyžadovaly zprostředkovatele. Využitím blockchainu je tedy umožněno uchovávání záznamů, které nejsou závislé na existenci jediné autority. I při výpadku služeb, které registraci prováděly, zůstává důkaz o transakci dostupný. Prostřednictvím těchto nástrojů může být snížena potřeba tradičních institucí, a zároveň může být posílena transparentnost a předvídatelnost systému. Zároveň je tím vytvořen prostor pro nové způsoby, jak mohou být práva jednotlivců uplatňována (Tapscott a Tapscott 2018).

4.2.3 Finanční inkluze

Za důležitý přínos blockchainové technologie bývá považována její schopnost podporovat finanční inklusi, a to hlavně ve vztahu k osobám i regionům s omezeným přístupem k tradičním bankovním službám. Díky decentralizované povaze systému a absenci zprostředkovatelů může být umožněno poskytování finančních služeb i tam, kde chybí odpovídající infrastruktura. Tímto způsobem mohou být sníženy náklady na transakce a zároveň může být zajištěna větší bezpečnost a transparentnost pohybů aktiv. Uživatelům bez přístupu k oficiálním dokladům totožnosti může být usnadněn vstup do finančního systému. Kromě toho může být usnadněno poskytování služeb, jako je financování, či spoření. To celé bez závislosti na tradičních finančních institucích. Pomocí chytrých smluv může být zjednodušen a zrychlen průběh těchto operací. To přispívá ke zvýšení důvěry a odstranění některých překážek spojených s nedůvěrou k formálním systémům (Adegbite 2024).

4.2.4 Interoperabilita a přenositelnost

V rámci decentralizovaných financí je interoperabilita považována za jednu ze zásadních vlastností. Je to z důvodu, že umožňuje vzájemné propojení různých protokolů a jejich společné využití. Díky tomu mohou být jednoduché nástroje kombinovány do složitějších celků. Tato schopnost propojení je ve standardním finančním systému značně omezena. Tradiční instituce bývají totiž provozovány odděleně a přechod mezi nimi je často složitý a časově náročný. Přenos dat a aktiv může trvat několik dní a jednotlivé produkty bývá obtížné vzájemně kombinovat. Digitalizace zde pouze zachovala stávající struktury bez zásadní modernizace. V prostředí DeFi je interoperabilita umožněna zejména díky sdílené infrastruktuře a jednotným technickým rozhraním. Pomocí standardů, jako jsou ERC-20, ERC-721 nebo ERC-1155, může být zajištěna kompatibilita různých tokenů. Vývojářům je tak umožněno vytvářet aplikace, které dokážou spolupracovat s širokým výběrem různých aktiv. Součástí tohoto propojení je také tokenizace, která slouží k převodu aktiv do formy tokenů. Tyto tokeny mohou být dále využívány mezi dalšími protokoly. Likvidita je tedy v DeFi sdílena napříč více aplikacemi. Díky této interoperabilitě může být umožněno vytváření nových finančních nástrojů a služeb. Kombinací jednotlivých prvků vznikají inovativní řešení, která by v tradičním systému byla velmi složitá (Harvey et al. 2021).

4.3 Technologie a škálovatelnost

Tato část se zaměřuje na technologické možnosti rozšiřování kapacity blockchainových sítí, které jsou klíčové pro efektivní zpracování plateb. Popsány jsou limity současných řešení a přístupy, které usilují o zvýšení propustnosti, včetně využití doplňkových technologií, jako je Lightning Network. Zmíněn je také koncept škálovatelnostního trilema a kvadrilema.

4.3.1 Škálovatelnost

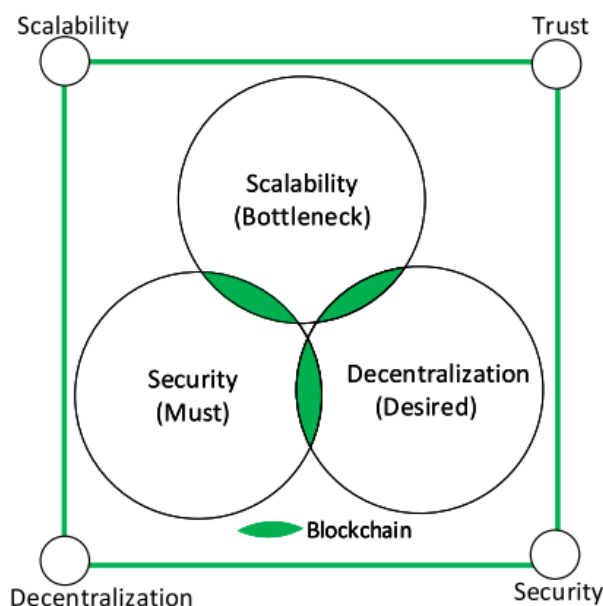
Škálovatelnost je podle Stroukala a Skalického (2021) schopnost systému adekvátně reagovat na zvyšující se zatížení, jako např. zvyšující se počet transakcí, tedy propustnost. Pokud není systém dostatečně škálovatelný a jeho kapacita se při růstu počtu požadavků nezvětšuje, tak to může vést k významným problémům, jako je dlouhá doba čekání na potvrzení transakcí nebo vyšší poplatky. Tyto problémy jsou známy zejména u Bitcoinu a dalších blockchainů patřících do 2. generace.

Pro jednoduchost zůstaňme u Bitcoinu. Novák (2023) ve své knize zmiňuje dvě řešení. První možností je navýšení velikosti jednoho bloku. V současnosti činí velikost bloku 4 MB a udává se, že při tomto nastavení může být zpracováno přibližně 7 transakcí za sekundu. V případě zdvojnásobení velikosti bloku by bylo dosaženo až 20 transakcí za sekundu. Ačkoliv se tímto krokem může zdát problém škálovatelnosti vyřešen, dochází zároveň k jinému nežádoucímu jevu – vyšší míře centralizace. Tato centralizace by byla způsobena nároky na technické vybavení. V případě, že by blok dosahoval velikosti například 1 GB, bylo by pro provoz tzv. uzlu nezbytné disponovat rozsáhlým datovým uložištěm, vysokým výpočetním výkonem a rychlým internetovým připojením. Takové požadavky by splnila pouze omezená skupina uživatelů, čímž by byla síť koncentrována do rukou několika účastníků. Decentralizace, která je základním principem Bitcoinu, by tím byla oslabena. Aktuální velikost bloku 4 MB umožňuje, aby byl uzel provozován i běžnými uživateli, čímž je zachována jak bezpečnost, tak decentralizace sítě. Druhou možností je zkrácení času potřebného k vytěžení jednoho bloku. V současném nastavení je průměrná doba přidání bloku do řetězce přibližně 10 minut. Pokud by byl tento čas zkrácen na jednu minutu, zvýšila by se celková rychlost zpracování transakcí. Zároveň by však vznikl obdobný problém jako při zvětšení bloků. Bylo by nezbytné zajistit vyšší kapacitu pro uložení dat a lepší technické vybavení uzlů. Dále by mohlo docházet ke zpoždění při distribuci bloků mezi uzly po celém světě. V důsledku toho by některé uzly navázaly na starší blok, což by vedlo k častému

větvení blockchainu a nutnosti následné reorganizace. Takovým situacím se síť snaží vyhnout, protože narušují stabilitu a důvěryhodnost systému.

4.3.2 Trilema a kvadrilema škálovatelnosti blockchainu

Z předchozí kapitoly jsme již pochopili, že mezi škálovatelností, decentralizací a bezpečností existuje určitý vztah. Tím se dostáváme k známému trilematu škálovatelnosti blockchainu, který se dnes dokonce prohlubuje i o čtvrtý faktor, tudíž kvadrilema.



Obrázek 1 Trilema a kvadrilema škálovatelnosti blockchainu

(zdroj: Sanka a Cheung 2021)

Obrázek 1 zobrazuje trilema blockchainu, které je původně definováno jako kompromis mezi škálovatelností (Scalability), decentralizací (Decentralization) a bezpečností (Security). Kompromis z toho důvodu, že všechny tyto tři aspekty nemohou být současně plně zachovány. To znamená, že se nám vždy povede mít silné pouze dva aspekty, ten třetí bude slabé místo. Například pokud chci u blockchainu vyšší škálovatelnost a bezpečnost, tak dochází k omezení míry decentralizace. Novější přístup však rozšiřuje tento koncept ještě o čtvrtý klíčový faktor – důvěru (Trust). Tento prvek ukazuje, že škálovatelnost blockchainu není závislá jen na kompromisu mezi decentralizací a bezpečností, ale také na tom, nakolik síť důvěřuje svým validátorům. Blockchainy, které se opírají o důvěryhodné validátory, mohou dosáhnout vyšší škálovatelnosti, protože není nutné mít tak složitý mechanismus pro dosažení konsensu. Zařazení důvěry do kvadrilematu ukazuje, že

blockchainy mohou dosáhnout vyšší škálovatelnosti, pokud akceptují nižší úroveň decentralizace. Decentralizace ale není jediný faktor, který je v tomto vztahu důležitý. Důvěra zde znamená, že uživatelé se spoléhají na určitou skupinu validátorů. Naopak systémy, které se snaží zachovat plnou decentralizaci, musí využívat složitější a výpočetně náročnější mechanismy (např. proof of work) pro dosažení bezpečnosti, což zpomaluje zpracování transakcí. Kvadrilema tedy vyjadřuje vzájemný vztah mezi škálovatelností, decentralizací, bezpečností a důvěrou. Každý blockchainový systém musí najít vhodnou rovnováhu mezi těmito čtyřmi faktory podle toho, jaké jsou jeho cíle a požadavky. (Sanka a Cheung, 2021)

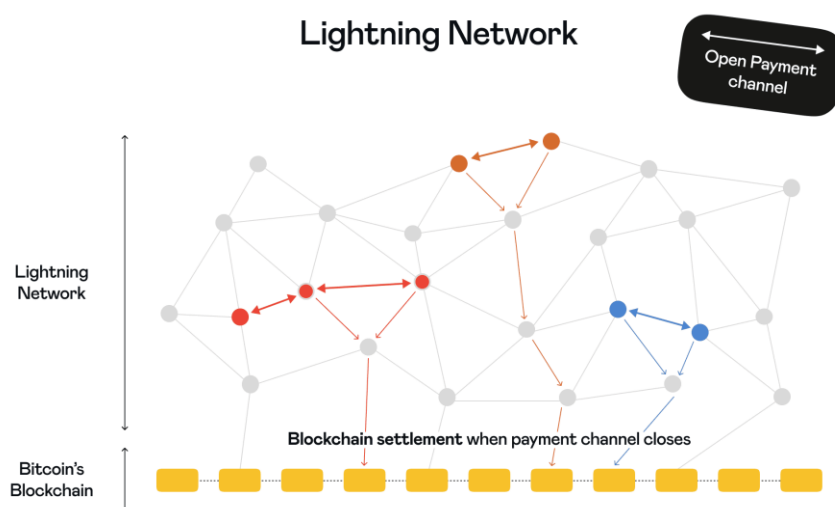
To ale není jediné kvadrilema, se kterým se můžeme v literatuře setkat. Trilema blockchainu, která popisuje kompromis mezi škálovatelností, decentralizací a bezpečností, nevypovídá o jeho praktické využitelnosti. Pokud bychom se soustředili pouze na dosažení rovnováhy mezi těmito třemi faktory, mohli bychom vytvořit fiktivní blockchain, který je formálně bezpečný, škálovatelný a decentralizovaný, avšak zcela nepoužitelný. Představme si systém, který generuje bloky v pevně stanovených intervalech bez jakýchkoli vstupních transakcí. Takový blockchain by teoreticky splňoval požadavky trilematu. Prakticky by ale neměl žádnou reálnou hodnotu pro uživatele. Proto je nezbytné posunout se za hranici trilematu a přidat další klíčový faktor – výpočetní efektivitu. Tento faktor určuje, jak efektivně blockchain dokáže vykonávat užitečné výpočty při přijatelných nákladech. Výpočetní efektivita reflektuje nejen technickou stránku, ale i ekonomické pobídky, například možnost urychlení potvrzování transakcí prostřednictvím vyšších poplatků pro validátory. Kvadrilema blockchainu tak ukazuje, že samotná rovnováha mezi škálovatelností, decentralizací a bezpečností není dostatečná a pro reálné využití blockchainu je nutné zohlednit i jeho výpočetní efektivitu. (Mogavero et al. 2021)

4.3.3 Lightning network

Pro řešení škálovatelnosti blockchainu existují dvě základní cesty. Buď jsou všechny transakce zpracovávány přímo v hlavním řetězci bloků, tzv. on-chain, nebo je část transakcí realizována mimo tento řetězec, tzv. off-chain. On-chain řešení zvyšuje ale nároky na výkon a kapacitu sítě. To tedy může ohrozit celou její decentralizaci. Naopak off-chain přístup odlehčuje hlavní síť tím, že některé transakce probíhají jinde a do blockchainu jsou zapisovány až souhrnně. Typickým příkladem off-chain řešení je Lightning Network, která umožňuje provádění rychlých a levných plateb mezi uživateli a to bez nutnosti záznamu

každé transakce do blockchainu. Tím zvyšuje celkovou propustnost sítě a řeší problém s omezenou kapacitou hlavního řetězce (Stroukal a Skalický 2021).

Lightning Network funguje na základě tzv. platebních kanálů, které umožňují dvěma stranám provádět neomezený počet transakcí mimo hlavní blockchain. Platební kanál funguje jako společný účet, do kterého jedna ze stran vloží určité množství bitcoinů. Tímto krokem se kanál otevře a zapíše do blockchainu jako běžná transakce. Jakmile je kanál otevřen, mohou si obě strany mezi sebou libovolně a okamžitě posílat platby, aniž by každá z těchto transakcí byla zaznamenána do blockchainu. Všechny transakce probíhají rychle a bez poplatků, protože je sledují jen účastníci kanálu. Do blockchainu se zapíše pouze závěrečná transakce, která kanál uzavře a spravedlivě rozdělí zbývající prostředky mezi obě strany. Díky tomu lze uskutečnit tisíce plateb, přitom do blockchainu se uloží pouze dvě – první při otevření kanálu a poslední při jeho uzavření. Hlavní přínos tohoto řešení spočívá v rychlosti, nízkých nákladech a celkovému odlehčení hlavní sítě. Omezením je, že uživatel může utratit pouze tolik prostředků, kolik má ve svém kanálu k dispozici (Novák 2023).



Obrázek 2 Lightning Network

(zdroj: Gerstein 2024)

Pro lepší pochopení slouží Obrázek č. 2. Z obrázku je ale patrné, že platební kanály nejsou pouze mezi dvěma subjekty, ale také se dále propojují. Platební kanál se vyplatí otevřít v případě, kdy se očekává časté využití. Situace, kdy bych někomu chtěl zaplatit pouze jednou by byla zbytečně nákladná, jelikož by šlo pouze o otevření a následné uzavření kanálu (dvě on-chain transakce). Proto byl Lightning Network navržen tak, aby i v situaci, kdy uživatelé

nemají mezi sebou otevřený platební kanál, mohlo dojít k platbě prostřednictvím ostatních účastníků sítě. Jedná se o přesměrování přes jiné uživatele, kteří již mezi sebou kanály otevřené mají. Každý uzel v této cestě pouze přesune část prostředků v rámci svých kanálů a za tuto službu si účtuje drobný poplatek. Prakticky, pokud nemám otevřený kanál s příjemcem platby, ale znám společné propojení přes jiné účastníky sítě, mohu platbu směřovat přes ně. Výsledkem je, že příjemce obdrží požadovanou částku, zatímco prostředníci si ponechají poplatky za zprostředkování (Novák 2023).

Tento proces je na obrázku č.2 znázorněn jako cesta navazujících šipek, které vedou napříč uzly a samotné vypořádání probíhá až po uzavření kanálu v hlavním blockchainu.

5 SHRNUÍ TEORETICKÉ ČÁSTI

Teoretická část práce poskytla podrobný přehled o vývoji, vlastnostech a funkcích kryptoaktiv ve vztahu k jejich využitelnosti jako platebního prostředku. Z historického vývoje vyplynulo, že současné kryptoaktiva vznikla jako reakce na omezení tradičních finančních systémů, přičemž klíčovým přelomem bylo zavedení Bitcoinu a později i Etherea. Tyto projekty položily základy pro vznik decentralizovaných aplikací a otevřely prostor pro rozvoj sektoru decentralizovaných financí.

Byly rozebrány základní funkce a vlastnosti peněz, přičemž největší důraz byl kladen na funkci všeobecného prostředku směny. Ukázalo se, že některé technické vlastnosti kryptoaktiv, tedy zejména dělitelnost a přenositelnost, odpovídají požadavkům kladeným na peněžní prostředek. Naopak klíčovou slabinou zůstává nízká míra akceptace a nedostatečná stabilita hodnoty, které zatím brání širšímu použití v běžném platebním styku. V práci je také upozorněno, že vlastnosti jako decentralizace nebo pseudonymita nejsou klasickými ekonomickými funkcemi peněz, ale představují významný technologický přínos, který zvyšuje uživatelskou autonomii.

Zvláštní pozornost byla věnována decentralizaci a jejím dopadům na regulaci, transparentnost a důvěru. Popsané případy ukazují, že absence centrální autority přináší výhody v podobě nezávislosti na prostřednících, ale zároveň komplikuje právní vymahatelnost, prosazování pravidel a ochranu uživatelů. Tato problematika se projevuje zejména při srovnání regulačních přístupů v USA, Evropě a Asii, kde je možné sledovat různou míru restrikce nebo podpory kryptoaktiv.

V technologické části teorie byl detailně rozebrán problém škálovatelnosti a popsána trilema i kvadrilema blockchainu, která ukazují, že mezi bezpečností, decentralizací, výkonností a důvěrou musí být vždy dosaženo určité rovnováhy. Na základě tohoto teoretického rámce byly představeny technické přístupy ke zvýšení kapacity sítě, zejména Lightning Network jako příklad off-chain řešení umožňujícího rychlé a levné transakce mimo hlavní blockchain. Praktická použitelnost tohoto přístupu však závisí na kvalitní infrastruktuře a ochotě uživatelů přizpůsobit své chování.

Celkově lze shrnout, že kryptoaktiva mají potenciál plnit platební funkce, ale jejich využití v běžném ekonomickém prostředí naráží na technologické, regulatorní i uživatelské limity. Teoretické poznatky tak vytvořily rámec pro praktické porovnání s tradičními digitálními platebními systémy, které bude předmětem další části práce.

II PRAKTICKÁ ČÁST

6 PLATEBNÍ FUNKCE KRYPTOAKTIV VE SROVNÁNÍ S TRADIČNÍMI SYSTÉMY

Platební funkce představuje jednu z nejčastěji diskutovaných oblastí praktického využití kryptoaktiv. Aby mohly kryptoaktiva v reálném prostředí plnit roli efektivního platebního nástroje, musí být schopna konkurovat zavedeným digitálním metodám, jako jsou karetní sítě. V této kapitole je proto provedeno porovnání vybraných kryptoaktiv s tradičními platebními systémy.

6.1 Rychlost platebních systémů

Rychlost zpracování transakcí je klíčovým faktorem pro platební funkci kryptoaktiv. Pokud mají kryptoaktiva v praxi konkurovat tradičním platebním metodám, musí být schopny zpracovávat transakce rychle a efektivně. Cílem této kapitoly je analyzovat rychlost transakcí u různých blockchainů a tradičních platebních systémů. V rámci tohoto srovnání budeme analyzovat rychlost transakcí u Bitcoinu, Etherea, Solany a tradičních platebních systémů Visa a Mastercard. Pro analýzu jsme si zvolili následující ukazatele:

1. TPS (Transactions per Second) – kolik transakcí dokáže síť zpracovat za sekundu
2. TPS Max – maximální teoretický počet transakcí za sekundu
3. Latence – jak dlouho trvá potvrzení transakce
4. Finalita transakce – za jak dlouho je transakce považována za definitivně potvrzenou a nevratnou

Pro účely této analýzy jsme využili údaje z veřejně dostupného portálu Chainspect.app, který zobrazuje reálné statistiky o propustnosti blockchainových sítí. Data jsme čerpali ke dni 13. května 2025 a pracujeme s průměrnou hodnotou TPS, TPS Max, latencí a finalitou. Hodnota TPS v daný den odráží běžné zatížení sítě a umožňuje objektivní posouzení její výkonnosti v praktickém provozu.

6.1.1 Bitcoin

U Bitcoin on-chain bývá uváděna maximální teoretická propustnost 7 TPS (viz kapitola 4.3.1). Z portálu Chainspect.app jsme zjistili, že průměrná hodnota TPS činila 3,92. Latence odpovídá délce vytěžení jednoho bloku, tedy přibližně 10 minut. Finalita je běžně považována za dosaženou po šesti potvrzeních, což odpovídá přibližně 60 minutám. Teprve

po této době je riziko případné reorganizace řetězce zanedbatelné a transakce může být považována za neodvolatelnou (Chainspect 2025).

Off-chain vrstva Lightning Network teoreticky umožňuje dosažení až 1 000 000 TPS díky paralelnímu zpracování v mnoha platebních kanálech. Finalita je v tomto případě dosažena prakticky okamžitě. Transakce jsou potvrzovány v řádu milisekund až jednotek sekund, tedy téměř instantně (Rodrigues 2022). Vzhledem k povaze Lightning Network nelze přesně stanovit hodnoty TPS dosažené v konkrétním období, jelikož tyto transakce nejsou zapisovány do blockchainu, ale probíhají pouze v rámci jednotlivých platebních kanálů (viz kapitola 4.3.3). Vypořádání na hlavním Bitcoin blockchainu pak podléhá opět standardní bitcoinové finalitě, avšak jednotlivé off-chain platby jsou realizovány okamžitě.

6.1.2 Ethereum

U Ethereum on-chain je podle údajů z portálu Chainspect.app uváděna průměrná propustnost 16,11 TPS, přičemž maximální teoretická hodnota činí 119 TPS. Průměrná latence bloků dosahuje přibližně 12,08 sekundy, avšak konečné potvrzení transakce nastává zhruba po 16 minutách (Chainspect 2025).

V rámci off-chain řešení na síti Ethereum je v praxi nejrozšířenějším přístupem využití tzv. optimistic rollup sítí. Mezi nejvýznamnější z nich patří Arbitrum, která implementuje vlastní fraud-proof systém a zpracovává denně stovky tisíc transakcí. Díky své škálovatelnosti, nízkým poplatkům a integraci s aplikacemi v oblasti DeFi je Arbitrum považována za nejpoužívanější síť tohoto typu (Barchat 2025). Arbitrum dosahuje svých teoretických maxim na hodnotě 40 000 TPS Max. V běžném provozu dosahuje síť průměrné propustnosti přibližně 28,98 TPS, latence činí 0,25 sekundy a finalita odpovídá přibližně 16 minutám, tedy obdobně jako u on-chain vrstvy (Chainspect 2025).

6.1.3 Solana

Solana je příkladem vysoce výkonného on-chain blockchainu. Deklarovaná maximální teoretická propustnost dosahuje až 65 000 TPS. Podle dat činila průměrná hodnota 1 267 TPS, což výrazně převyšuje hodnoty zaznamenané u ostatních on-chain sítí. Solana navíc dosahuje velmi nízké latence, přibližně 0,39 sekundy, přičemž finalita je obvykle dosažena do 12,8 sekundy (Chainspect 2025).

6.1.4 Visa

Společnost Visa zpracovala v roce 2024 přibližně 233,8 miliardy transakcí prostřednictvím své globální platební sítě (Visa 2025).

$$\frac{233\,800\,000\,000}{(365 \times 24 \times 60 \times 60)} = 7\,413,75$$

Po přepočtu na počet sekund v roce to odpovídá průměrnému výkonu přibližně 7 414 TPS. Jedná se o dosaženou průměrnou hodnotu, která dobře ilustruje vysokou škálovatelnost tradičních platebních systémů. U společnosti Visa se uvádí, že její síť je navržena tak, aby zvládla až 65 000 TPS ve špičce, což je považováno za TPS Max (Visa 2017).

6.1.5 Mastercard

Mastercard zpracoval v roce 2024 celkem 159,4 miliardy transakcí, které prošly jeho vlastní platební sítí (Mastercard 2025).

$$\frac{159\,400\,000\,000}{(365 \times 24 \times 60 \times 60)} = 5\,054,54$$

Tento objem odpovídá průměrné propustnosti 5 055 TPS. Jedná se o průměrnou hodnotu dosaženou v průběhu celého roku 2024. V kontextu této analýzy je důležité upozornit, že běžně citovaná teoretická kapacita sítě Mastercard činí 5 000 TPS (Okhaifo 2025). To znamená, že Mastercard v roce 2024 prakticky dosáhla hranice uváděné maximální propustnosti své sítě. Tato hodnota bývá zmiňována i ve starších zdrojích (Craig 2021), což může naznačovat, že síť byla buď technicky vylepšena, nebo skutečně operovala na hranici své výkonové kapacity. Aktuálnější technické údaje o infrastruktuře Mastercard však nejsou veřejně dostupné.

6.1.6 Komparativní analýza rychlosti platebních systémů

Tabulka 1 Srovnávací přehled rychlosti platebních systémů

Platební systém	TPS (tx/s)	TPS Max (tx/s)	Latence	Finalita
Bitcoin (on-chain)	4,75	7	10 min	60 min
Bitcoin (off-chain)	-	1 000 000	<1 s	Okamžitě
Ethereum (on-chain)	16,11	119,1	12 s	16 min
Ethereum (off-chain)	28,98	40 000	0,25 s	16 min
Solana	1 267	65 000	0,39 s	12,8 s
Visa	7 414	65 000	0,15 - 5 s	1–2 dny
Mastercard	5 055	5 000	0,15 - 5 s	1–2 dny

(zdroj: vlastní zpracování)

Rychlost transakcí je zásadním parametrem, který určuje reálnou využitelnost kryptoaktiv v každodenním platebním styku. Pokud mají kryptoaktiva naplno plnit svou platební funkci a konkurovat tradičním systémům, musí kromě vysoké transakční propustnosti zajistit také nízkou latenci a dostatečně rychlou a důvěryhodnou finalizaci transakcí.

Z výsledků analýzy vyplývá, že základní on-chain vrstvy, jako je Bitcoin či Ethereum, mají v oblasti rychlosti svá technologická omezení. Propustnost těchto sítí zůstává relativně nízká a latence i finalita transakcí jsou z pohledu běžných plateb spíše nevýhodné. Tato omezení však byla zásadně zmírněna s nástupem off-chain řešení, jako Lightning Network pro Bitcoin nebo optimistic rollupy, v našem případě Arbitrum na Ethereumu. Tato řešení umožňují zpracovávat transakce v řádu milisekund, s minimálními náklady a s okamžitou nebo velmi rychlou finalitou. Lightning Network navíc teoreticky dosahuje až milionu transakcí za sekundu, což je hodnota nesrovnatelně vyšší než u tradičních platebních systémů.

Zajímavým případem v rámci on-chain sítí je Solana, která v porovnání s Bitcoinem a Ethereumem vykazuje výrazně vyšší výkon, jak v oblasti propustnosti, tak i z hlediska latence a finality.

Tradiční karetní síť, jako jsou Visa a Mastercard, zůstávají v praxi nadále nejrozšířenějšími platebními systémy s mimořádnou škálovatelností. Jejich výhodou je velmi nízká latence, uváděná v hodnotách 0,15 až 5 sekundách (OpenFare © 2025) a stabilní infrastruktura. Z pohledu obchodníka je však důležité vnímat i specifické pojetí finality, jelikož je sice transakce zákazníkovi okamžitě autorizována ale obchodník obvykle obdrží prostředky až po 1–2 pracovních dnech (Škop 2024).

Lze tedy konstatovat, že off-chain řešení kryptoaktiv dokáží v mnoha případech nabídnout vyšší transakční výkon, nižší latenci a rychlejší finalitu než zavedené platební infrastruktury.

Z hlediska platební funkce tak představují reálnou alternativu k tradičním systémům, a to zejména tam, kde je důležitá okamžitá nevratnost transakcí, nižší závislost na zprostředkovateli a decentralizovaná kontrola.

6.2 Transakční poplatky

Výše transakčních poplatků je jedním z hlavních faktorů, které ovlivňují rozhodování uživatelů při výběru platební metody. Tato část se zaměřuje na porovnání nákladovosti tradičních platebních systémů (Visa, Mastercard) s vybranými kryptoaktivy (Bitcoin, Ethereum, Solana).

6.2.1 Transakční poplatky kryptoaktiv

Jak již bylo uvedeno, kryptoaktiva se vyznačují vysokou volatilitou, a to nejen z hlediska tržní ceny, ale také z pohledu transakčních poplatků. Ty se mohou v závislosti na vytíženosti sítě, typu transakce či konkurenci v mempoolu výrazně lišit, přičemž extrémní hodnoty při síťových špičkách mají potenciál statisticky zkreslit průměrné výsledky. V rámci této analýzy pracujeme s mediánovou hodnotou transakčních poplatků k datu 13. května 2025. Tento přístup umožňuje zachytit typickou uživatelskou zkušenost při běžném provozu dané sítě. Uvědomujeme si, že transakční poplatky v blockchainových sítích jsou proměnlivé a citlivé na aktuální síťovou zátěž, avšak právě mediánová hodnota představuje stabilnější a lépe interpretovatelnou metriku než průměr ovlivněný extrémními hodnotami.

Bitcoin

V rámci bitcoinové sítě se výše transakčních poplatků výrazně liší v závislosti na použité vrstvě. Při standardní on-chain transakci, jsou poplatky určovány tržně, tedy uživatel si stanovuje částku, kterou je ochoten zaplatit za zařazení své transakce do bloku. V době průměrné vytíženosti sítě se mediánový poplatek za běžnou bitcoinovou transakci pohybuje přibližně kolem 0,728 USD (BitInfoCharts 2025a).

Naproti tomu u Lightning Network je poplatek za takovou platbu obvykle tvořen dvěma komponentami:

- Fixní základní poplatek – ten činí typicky 1 satoshi
- Směrovací poplatek – jeho výše se pohybuje kolem 0,000066 satoshi na jeden převáděný satoshi, tedy 66 ppm (0,0066 %). Tato sazba je procentuálně invariantní (IML © 2025).

Ethereum

Na základní vrstvě sítě Ethereum (off-chain) se transakční poplatky odvíjí se od výpočetního nákladu transakce, tedy gasu (viz kapitola 2.2). V praxi mohou být poplatky při vysoké síťové zátěži značně vysoké, stejně jako u bitcoinu. Z dat jsme zjistili, že mediánový poplatek vychází na 0,517 USD (BitInfoCharts 2025b).

Naproti tomu off-chain řešení Arbitrum představuje výrazně levnější alternativu k on-chain transakcím na síti Ethereum. Pro ilustraci výše poplatků v síti Arbitrum byla využita data z portálu Arbiscan.io ke dni 13. května 2025. V tento den činil celkový objem zaplacených poplatků 17,564 ETH při celkovém počtu 2 628 226 transakcí (Arbiscan © 2025). Při průměrné tržní ceně 1 ETH = 2 680 USD (Kurzy.cz © 2025) lze vypočítat průměrný transakční poplatek následujícím způsobem:

$$\frac{17,564}{2\,628\,226} \times 2\,680 = 0,0179$$

Z toho vyplývá, že průměrný poplatek za jednu transakci v síti Arbitrum činil v daný den 0,0179 USD, což z tohoto řešení činí vysoce nákladově efektivní variantu pro každodenní transakce.

Solana

Solana je často uváděna jako příklad extrémně škálovatelné a nákladově efektivní blockchainové platformy vhodné pro každodenní platby. Na rozdíl od sítí typu Ethereum nebo Bitcoin zde neexistuje poplatková aukce, která by při vyšší zátěži zvyšovala ceny, tedy uživatel platí vždy jen fixní zlomkovou část SOL bez ohledu na převáděnou částku. Její transakční poplatky jsou extrémně nízké – za duben 2025 činil tento průměrný poplatek za běžnou transakci přibližně 0,00335 USD (Token Terminal 2025).

6.2.2 Transakční poplatky u platebních karet

Pokud se rozhodneme zaplatit platební kartou, obchodník pro tohle zpracování potřebuje platební terminál. Společnosti, které platební terminály provozují si za provedené transakce také účtují poplatky. Na základě evropské legislativy vznikl model MIF++ a vyznačuje se povinným uplatňováním jednotného rozdělení poplatků mezi více stran.

Z každé karetní transakce je účtována celková částka složená z několika samostatných složek:

- Mezibankovní poplatek (interchange fee)
- Poplatek karetním společenstvem (scheme fee)
- Poplatek za zpracování (acquirer fee)

První složka představuje **mezibankovní poplatek**, který je odváděn bance, která kartu vydala. U spotřebitelských karet vydaných v rámci Evropského hospodářského prostoru (EHP) je jeho výše stanovena na 0,2 % u debetních a 0,3 % u kreditních karet. Většina transakcí tedy spadá pod evropskou regulaci (Comgate © 2025).

Druhou složkou je **poplatek karetním společenstvem**. Mezi ně patří například Visa nebo Mastercard. Jeho výše se může lišit mimo jiné v závislosti na typu karty, či způsobu platby (Comgate 2025). Přehled poplatků účtovaných karetními společnostmi Mastercard a Visa v rámci domácích transakcí v České republice k dubnu 2025 uvádí Tabulka 2. Údaje vycházejí z dokumentu zveřejněného společností Worldline, který shrnuje oficiální sazby karetních společností platné pro tuzemský trh (Worldline 2025).

Tabulka 2 Přehled poplatků Visa a Mastercard za zpracování transakcí

Poplatek	Visa	Mastercard
za zúčtování a vypořádání transakce	€0.005	€0.0005 – €0.0425 (dle částky)
za autorizaci transakce	€0.0032	0.0090 %
za ochranu proti kybernetickým hrozbám	€0.00045	–
na inovace a rozvoj trhu	0.0800 %	0.0900 %
za netransakční náklady	0.0036 %	0.0125 %
z objemu transakcí	–	0.0570 %
Paušální poplatek za transakci	–	€0.0070
Celkový poplatek	€0,00865 + 0.0836 %	€0.0565 + 0.3295 %

(zdroj: vlastní zpracování)

Tabulka znázorňuje pouze základní poplatky, které jsou účtovány z každé transakce. Můžeme tedy tento celkový poplatek z tabulky x označit jako minimální. Samozřejmě záleží na podmínkách a okolnostech jednotlivých transakcí, např. při platbě pomocí Apple Pay nebo Google Pay, by se u karty společnosti Mastercard zvýšil celkový poplatek o 0,01 %,

kvůli tokenizaci platby. Poplatky se takto mohou na základě stanovených sazeb dostat až přes 2 % (Worldline © 2025).

Poslední složkou je **poplatek za zpracování transakce**, který je účtován poskytovatelem terminálu nebo platební brány. Tento poplatek pokrývá náklady spojené s technickým zabezpečením transakcí a bývá stanoven kombinací procentní a fixní části (Comgate 2025). Je těžké určit kolik si v průměru společnosti poskytující platební terminály účtují tento poplatek, jelikož je tato sazba určována každému obchodníkovi individuálně a sazby bývají obchodním tajemstvím, tudíž nejsou veřejně dohledatelné.

6.2.3 Komparativní analýza poplatků platebních systémů

Tabulka 3 Srovnání výše poplatků platebních systémů

Platební systém	Poplatek
Bitcoin (on-chain)	0,728 USD
Bitcoin (off-chain)	0,0066 % + 1 satoshi
Ethereum (on-chain)	0,517 USD
Ethereum (off-chain)	0,0179 USD
Solana	0,00335 USD
Visa	0,00865 EUR + 0,0836 %
Mastercard	0,0565 EUR + 0,3295 %

(zdroj: vlastní zpracování)

Na základě výše uvedené analýzy lze učinit několik zásadních závěrů týkajících se nákladovosti jednotlivých platebních systémů. Srovnání ukazuje, že výše transakčních poplatků se mezi jednotlivými platformami výrazně liší, a to nejen mezi tradičními karetními systémy a blockchainovými sítěmi, ale i uvnitř samotného ekosystému kryptoaktiv, tedy mezi on-chain a off-chain vrstvami.

Nejnižší transakční poplatky dlouhodobě vykazuje blockchain Solana, u kterého se průměrná výše poplatku pohybuje v hodnotách 0,00335 USD. Velmi příznivě vychází i off-chain řešení jako Lightning Network (0,0066 % + 1 satoshi) a Arbitrum jakožto zástupce škálovatelných druhých vrstev na síti Ethereum, kde byla zjištěna hodnota přibližně 0,0179 USD za transakci. Tato řešení ukazují vysoký potenciál pro každodenní mikrotransakce, kde je nízká nákladovost klíčová.

Naopak on-chain transakce na sítích Bitcoin a Ethereum se vyznačují podstatně vyššími poplatky. V době sběru dat činil medián poplatku na bitcoinu 0,728 USD,

u etherea 0,517 USD, což z těchto plateb činí méně vhodné nástroje pro nízkonákladové platby v běžném provozu. Tato výše poplatků je silně ovlivněna vytížeností sítě a často vykazuje značnou volatilitu, což snižuje předvídatelnost nákladů.

Tradiční karetní systémy Visa a Mastercard pak vykazují střední úroveň nákladovosti. V absolutních číslech se mohou jevit jako levnější (např. Visa: €0,00865 + 0,0836 %), nicméně kvůli procentní části poplatku se při vyšších částkách poplatky rychle navyšují. Mastercard dosahuje ještě vyšší sazby (€0,0565 + 0,3295 %), a to ještě bez započtení dodatečných nákladů (např. tokenizace). Celkové náklady na transakci se tak mohou vyšplhat až nad 2 % z hodnoty platby, zejména u malých obchodníků nebo při přeshraničních transakcích. Nevýhodou je rovněž složitá a málo transparentní struktura poplatků.

Z hlediska uživatelské nákladovosti tak vycházejí nejlépe škálovatelné blockchainové sítě nové generace a off-chain řešení, které nabízejí extrémně nízké poplatky při zachování vysoké rychlosti a decentralizace. Je však třeba dodat, že výběr vhodného platebního nástroje nezávisí pouze na výši poplatků, ale také na rychlosti zpracování, míře adopce, regulaci, bezpečnosti a dalších faktorech.

7 PRAKTICKÉ VYUŽITÍ KRYPTOAKTIV V PLATEBNÍM STYKU

7.1 Možnosti získání a nákupu kryptoaktiv

V rámci této kapitoly jsou představeny hlavní cesty, jak mohou být kryptoaktiva získána. Nejedná se pouze o nákup na burze. Jsou také další způsoby, které uživatelům umožňují vstup do světa těchto digitálních aktiv. Zde jsou vybrané způsoby:

- Centralizované kryptoměnové burzy
- Kryptoměnové automaty (kryptomaty)
- Peer-to-peer směnárny a platformy
- Decentralizované burzy (DEX)
- Alternativní způsoby získávání kryptoaktiv (bez nákupu)

Centralizované kryptoměnové burzy jsou nejčastější forma při nákupu kryptoaktiv. Uživatelům je umožněna výměna tradičních státních měn za různé druhy kryptoaktiv. Nákup je umožněn pomocí platebních metod včetně bankovních převodů nebo plateb kartou. Vzhledem k centralizované povaze je běžně požadováno ověření identity dle pravidel KYC. Burzy zpravidla nabízejí i další služby v podobě různých investičních nástrojů, staking nebo spořicí programy. Poplatky zde bývají nižší než u směnáren. Mezi centralizované burzy patří např. známé společnosti jako Binance a Coinbase, které se řadí mezi světově největší a spolehlivé burzy. Českým představitelem centralizované burzy je společnost Coinmate (Vondrák a Machek 2024).

Další možností je využití **kryptoměnových automatů**, někdy také zkráceně označovaných jako kryptomaty. Umožňují nákup kryptoaktiv za hotovost nebo platební kartou, a to bez nutnosti registrace (Mrázková 2022). V České republice je provozováno několik sítí, např. Kvakomat (viz Obrázek 8), Bitcoinmat.sk. V zahraničí je rozšířen například provozovatel General Bytes nebo Bitcoin Depot. Informace o dostupnosti konkrétních automatů jsou dohledatelné na platformě CoinATMradar (2025).

Transakce mohou být prováděny i bez zprostředkovatele, přímo mezi uživateli, prostřednictvím **peer-to-peer směnáren**. Tyto platformy jako je Vexl.it, HodlHodl, Bisq nebo PeachBitcoin, zprostředkovávají obchodní kontakt mezi kupujícím a prodávajícím. Některé z nich využívají úschovu prostředků (escrow) a kryptografické smlouvy, aby byla transakce zabezpečena bez nutnosti centrální autority (Carnimeo 2024).

Kryptoaktiva lze získat i přes **decentralizované burzy**, které fungují bez provozovatele. Uživatelé zde obchodují napřímo prostřednictvím chytrých kontraktů. Připojení probíhá přes kryptoměnovou peněženku, tedy bez nutnosti registrace. Mezi nejznámější DEX patří Uniswap (Ethereum), PancakeSwap (BNB Chain), SushiSwap nebo Curve. Obchodování na těchto platformách je však spojeno s vyššími nároky na znalosti a uživatelskou zodpovědnost (Wimmer 2025).

Alternativní způsoby získávání kryptoaktiv bez přímého nákupu lze např. těžbou, stakingem (viz kapitola 2) nebo prostřednictvím různých aplikací a programů. Odměny lze získávat i za používání určitých nástrojů, např. webový prohlížeč Brave vyplácí uživatelům tokeny BAT (Hayes 2023). Vznikají i projekty, jako např. Helium, které motivují uživatele k provozování zařízení v síti internetu věcí (IoT) výměnou za tokenové odměny (Miah 2025).

7.2 Možnosti platby kryptoaktivy

S rostoucím technologickým pokrokem a rozšiřujícím se povědomím veřejnosti začaly být kryptoaktiva čím dál více využívány jako prostředek směny, nikoliv tedy pouze jako investiční spekulace, jak je často zmiňováno. V rámci této kapitoly bude poskytnut přehled, kde se v současnosti kryptoplatby podporují. Existují tři hlavní způsoby využití – přímé, nepřímé a zprostředkované platby

7.2.1 Přímá platba obchodníkovi

Přímá platba znamená, že zákazník uhradí zboží nebo službu přímo kryptoaktivem, kterou obchodník akceptuje, bez nutnosti její konverze do tradiční měny (Kibet 2025).

Webová platforma BTCmap.org mapuje podniky po celém světě, které akceptují bitcoin jako formu platby. Ke květnu 2025 je na mapě evidováno 15 511 obchodních míst celosvětově, z toho 1 064 lokalit se nachází v České republice. V praxi se s přímými kryptoplatbami lze setkat zejména v oblasti pohostinství, typicky u kaváren, restaurací či barů, ale také v různorodé škále služeb. Podle dostupných dat z platformy BTCmap.org akceptují kryptoaktiva rovněž kadeřnické salony, ubytovací zařízení a často také zdravotnická zařízení, zejména zubní lékaři. Tato diverzifikace napříč sektory naznačuje postupné rozšiřování praktického využití kryptoaktiv mimo technologickou komunitu i do běžného spotřebitelského prostředí. Česká republika tak patří mezi aktivnější státy v oblasti přijetí

kryptoaktiv, zejména ve větších městech jako Praha, Brno či Ostrava, kde je koncentrace těchto podniků nejvyšší (BTC Map © 2022-2025).

Významným příkladem v rámci České republiky i střední Evropy je společnost Alza.cz, která patří mezi největší internetové prodejce v regionu. Tento e-shop umožňuje platbu bitcoinem již od roku 2017 a od roku 2023 rozšířil své možnosti i o podporu Lightning Network, což umožňuje téměř okamžité a nízkonákladové transakce, čímž významně zvyšuje uživatelský komfort a efektivitu platebních operací (Alza.cz © 2023).

Kryptoaktiva nacházejí své uplatnění i v oblasti realit, která je tradičně spojena s vysokými částkami a složitým právním rámcem. Podle poskytovatele platebních služeb BitPay (2025) akceptuje přímé kryptoplatby několik realitních společností a zprostředkovatelů nemovitostí, především ve Spojených státech. Tento vývoj ukazuje, že využití kryptoaktiv se začíná prosazovat i v oblastech, které byly vyhrazeny výhradně tradičním bankovním metodám.

7.2.2 Nepřímá platba

Nepřímé využití kryptoaktiv jako platebního prostředku lze pomocí nákupu dárkových poukazů, které můžeme následně uplatnit u běžných maloobchodních prodejců (Kibet 2025). Tento přístup umožňuje spotřebitelům využívat kryptoaktiva i v případech, kdy obchodník nepřijímá kryptoplatby přímo. Slouží na to platformy jako Bitrefill, BitPay, eGifter a Gyft nabízejí širokou škálu poukazů pro různé značky a regiony.

Na českém trhu je nabídka dárkových poukazů dostupná zejména prostřednictvím platformy Bitrefill, která umožňuje nákup poukazů do populárních obchodů a služeb, jako jsou Alza, Kaufland, Zalando, OMV, H&M, Slevomat, Xbox, PlayStation Store, Steam, Vivantis či Ticketmaster. Americký trh nabízí ještě širší výběr, včetně značek jako Amazon, Starbucks, Walmart, Apple či Netflix, které patří mezi nejčastěji využívané (Bitrefill © 2025).

Tento přístup umožňuje využití kryptoaktiv v běžné spotřebě bez nutnosti jejich konverze do tradičních měn. Představuje uživatelsky přívětivé řešení a zároveň obchází některá regulatorní nebo technická omezení přímých kryptoplateb.

7.2.3 Platba přes zprostředkovatele

I v případech, kdy obchodník kryptoaktiva nepřijímá přímo, existují způsoby, jak lze kryptoaktiva použít k úhradě zboží či služeb prostřednictvím zprostředkovatelů (Kibet 2025).

Uvedeme si dvě časté řešení:

- platební brány
- platební karty

Platební brána funguje jako prostředník mezi zákazníkem platícím kryptoaktivem a obchodníkem, který přijímá tradiční měnu. Zákazník zaplatí např. v BTC nebo ETH, ale obchodník obdrží částku v korunách, eurech nebo dolarech. Brána transakci technicky zpracuje, ověří na blockchainu a v reálném čase konvertuje na požadovanou měnu. Tento model je tak výhodný pro obchodníky, kteří nechtějí řešit volatilitu kryptoaktiv ani správu peněženek. Z pohledu uživatele jde o běžnou kryptoplatbu, jen je zprostředkována třetí stranou (Machek a Redakce Finex 2024).

V Česku tuto možnost aktuálně nabízí např. GoPay, které integruje kryptoplatby do svého systému a umožňuje zákazníkům platit i přes Lightning síť (GoPay © 2024). Mezi další mezinárodní brány patří například BitPay, CoinGate, Confirmito.

Tyto služby se postupně integrují i do restaurací přes platformy jako např. Qerko v rámci českého trhu (Václavík 2023).

Platební karty také patří mezi velmi populární řešení, které fungují většinou v rámci sítí Visa nebo Mastercard. Uživatel platí kartou fyzicky či online a v okamžiku platby dochází k automatické konverzi kryptoaktiva na tradiční měnu. Pro obchodníka je platba zcela běžná, uživatel však čerpá přímo ze své kryptoměnové peněženky. Tento přístup je velmi komfortní pro každodenní použití, protože nevyžaduje podporu kryptoaktiv ze strany obchodníka. Platbu lze provést kdekoliv, kde je akceptována daná karetní značka. Mezi známé poskytovatele patří např. Crypto.com, Coinbase nebo Binance (Machek a Redakce Finex 2024).

7.3 Využití kryptoplateb při běžném platebním styku

Cílem této kapitoly je na základě praktických ukázek a konkrétních výpočtů porovnat možnosti plateb pomocí kryptoaktiv, konkrétně prostřednictvím Lightning Network, s běžně používanými platebními metodami. Nejprve se zaměříme na výběr a charakteristiku peněženek podporujících Lightning Network, poté popíšeme praktickou realizaci platby v reálném prostředí a následně analyzujeme, jak by se lišila stejná transakce v případě použití platební karty.

7.3.1 Lightning peněženky

Chceme-li v praxi platit přes Lightning Network, budeme na to potřebovat kryptoměnovou peněženku, která tuto funkci podporuje. Mezi oblíbené a běžně používané Lightning peněženky například patří:

- BlueWallet: <https://bluewallet.io/>
- Wallet of Satoshi: <https://www.walletofsatoshi.com/>
- Breez Wallet: <https://breez.technology/>
- Phoenix Wallet: <https://phoenix.acinq.co/>
- Muun Wallet: <https://muun.com/>
- Zeus: <https://zeusln.app/>

I mezi těmito peněženkami existují rozdíly. Základním rozlišením je, zda se jedná o typ custodial nebo non-custodial.

- Typ custodial znamená, že soukromé klíče a správu drží třetí strana. Uživatel tak důvěřuje poskytovateli služby a nemá přímou kontrolu nad svými prostředky.
- Typ non-custodial naopak uživatel drží a spravuje své vlastní privátní klíče, což přináší vyšší bezpečnost a soukromí, ale i větší odpovědnost.

Bezpečnost je tedy velmi důležitým aspektem. Non-custodial peněženky jsou obecně považovány za bezpečnější, protože soukromé klíče neopustí zařízení uživatele. Na druhou stranu mohou být náročnější na používání pro běžného uživatele. Pro začátečníky může být tedy vhodnější začít s typem custodial. Jedním z faktorů je i poplatek za vytvoření platebního kanálu (viz kapitola 4.3.3). Většinou se jedná o peněženky typu non-custodial, kde musíte napojit svůj uzel (Novák 2023).

7.3.2 Praktická ukázka platby přes Lightning Network

V této části si ukážeme, jak probíhá platba prostřednictvím sítě Lightning Network v praxi. Pro demonstraci jsme zvolili peněženku Phoenix Wallet, a to z důvodu, že se jedná o typ non-custodial, která zároveň nabízí uživatelsky přívětivé prostředí.

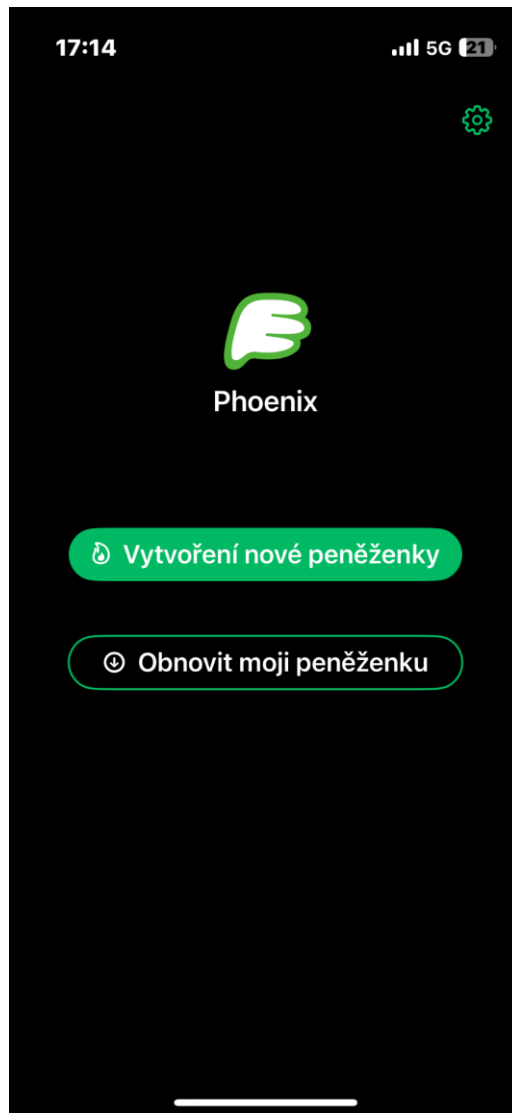
1. Nejprve jsem si aplikaci Phoenix Wallet nainstalovali do mobilního zařízení a spustili ji. Na úvodní obrazovce nás aplikace přivítala sdělením „Váš klíč, vaše bitcoiny“, čímž byla zdůrazněna zodpovědnost za privátní klíče a vlastněná aktiva. Peněženka je v tomto smyslu označována jako „Self-Custody“ a zároveň jsme byli upozorněni na to, že přebíráme plnou kontrolu nad svými prostředky (viz Obrázek 3).



Obrázek 3 Úvodní obrazovka aplikace Phoenix Wallet

(zdroj: ACINQ 2025)

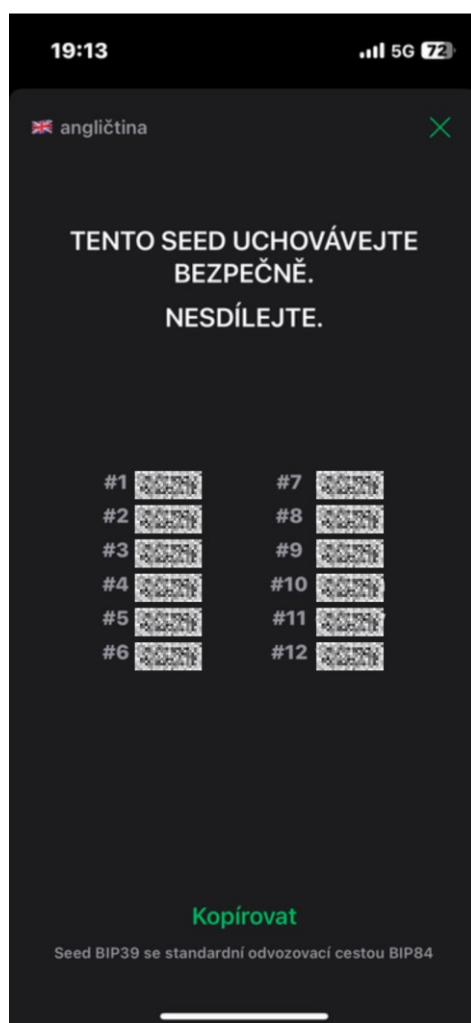
2. Následně jsme byli vyzváni k výběru mezi obnovením stávající peněženky nebo vytvořením nové. Pro účely této ukázky jsme zvolili možnost vytvořit novou peněženku (viz Obrázek 4).



Obrázek 4 Volba vytvoření nebo obnovení peněženky

(zdroj: ACINQ 2025)

3. Po jejím vytvoření bylo možné začít využívat všechny funkce aplikace. Z bezpečnostního hlediska jsme přešli do nastavení, kde jsme byli upozorněni žlutým vykřičníkem u položky „obnovovací fráze“. Na Obrázku 5 je zobrazena podoba této fráze, tzv. seedu. Dle pokynu aplikace jsme všech 12 tajných slov kvůli bezpečnosti zakryli. Zároveň je potřeba upozornit, že snímek obrazovky této fráze, tak jak jsme to udělali z důvodu demonstrace, není považován za bezpečný způsob uschování seedu.



Obrázek 5 Zobrazení seedu

(zdroj: ACINQ 2025)

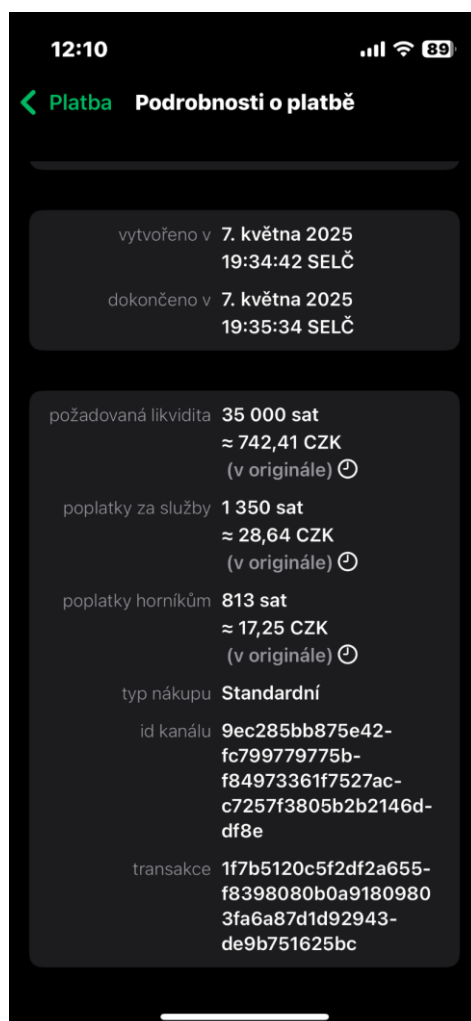
4. Následoval krok, kdy jsme do peněženky nabyli prostředky. Rozhodli jsme se pro nákup přes kryptoměnový bankomat provozovaný společností Kvakomat (viz kapitola 7.1). Zvolen byl konkrétní bankomat umístěný v pohostinském podniku Bar No. 7 (viz Obrázek 6), kde jsme současně plánovali provést samotnou platbu.



Obrázek 6 Kvakomat umožňující nákup kryptoaktiv

(zdroj: vlastní)

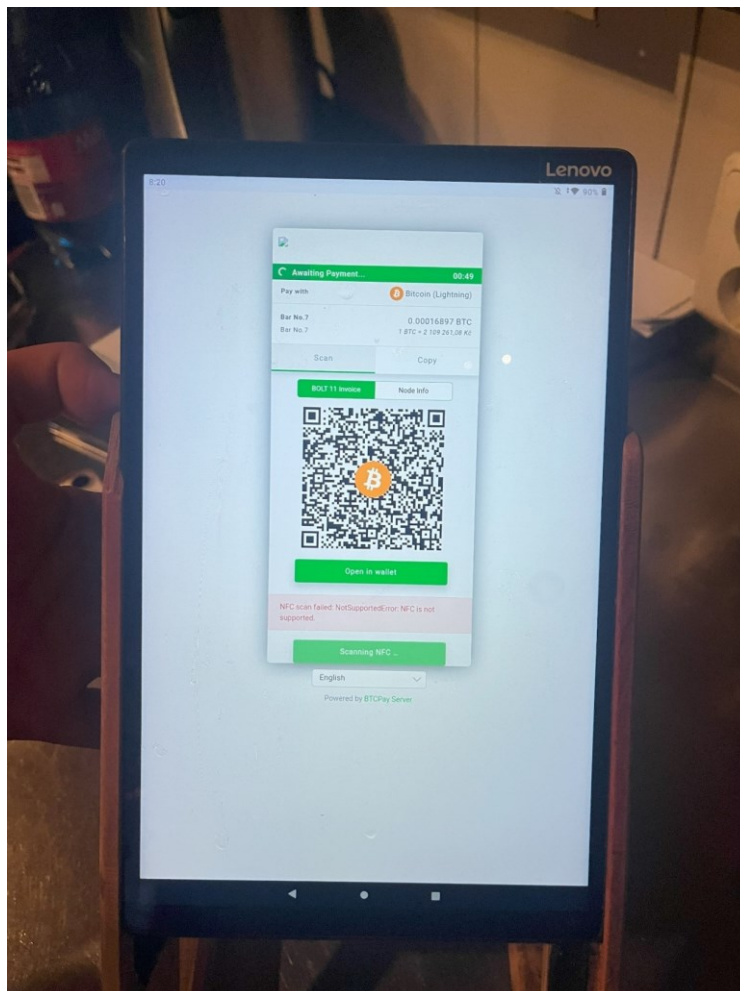
5. Na peněženku nám bylo odesláno 0,00035 BTC, tedy 35 000 satoshi. Z detailů transakce (viz Obrázek 7) je patrné, že část prostředků byla využita na poplatek za službu a těžařům. Tímto úkonem došlo k otevření platebního kanálu v síti Lightning Network, což znamená, že budoucí platby mohou být realizovány s minimálními náklady.



Obrázek 7 Podrobnosti o platbě

(zdroj: ACINQ 2025)

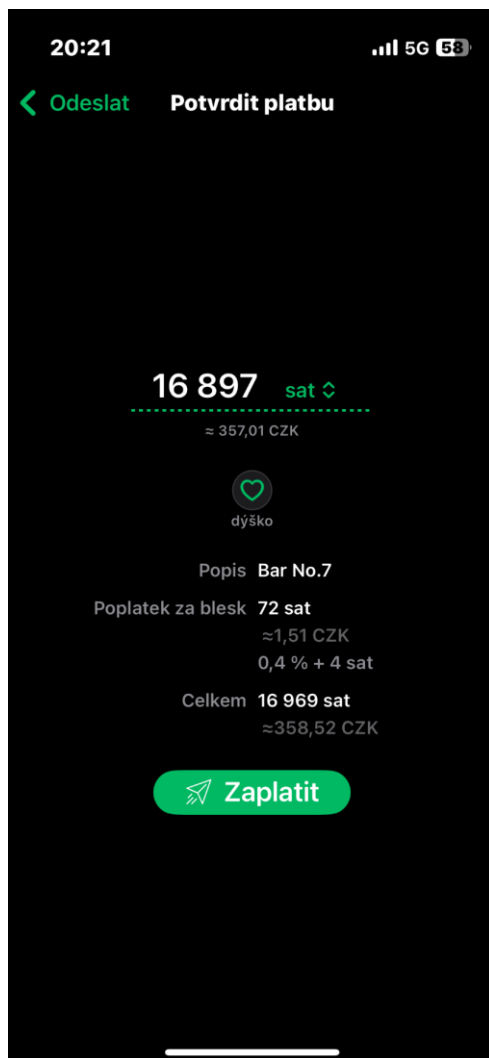
6. Po připsání částky jsme disponovali zůstatkem 32 837 satoshi. V podniku jsme požádali o možnost úhrady prostřednictvím Lightning Network a byl nám předložen QR kód označován jako tzv. faktura (viz Obrázek 8).



Obrázek 8 QR kód určený k úhradě transakce

(zdroj: vlastní)

7. V aplikaci jsme následně zvolili možnost „Odeslat“, naskenovali QR kód a potvrdili platbu tlačítkem „Zaplatit“ (viz Obrázek 9). Transakce proběhla úspěšně a bez jakýchkoli komplikací.



Obrázek 9 Potvrzení platby

(zdroj: ACINQ 2025)

V rámci tohoto návodu byl představen celý proces od instalace aplikace Phoenix Wallet, přes vytvoření nové peněženky, její zabezpečení a nabití prostředků, až po samotnou platbu pomocí Lightning Network. Celý postup byl z naší perspektivy intuitivní, uživatelsky přívětivý, probíhal rychle a bez jakýchkoliv komplikací. Za otevření platebního kanálu a nabití bitcoinů do peněženky byly účtovány poplatky ve výši 28,64 Kč (1 350 satoshi) za služby a 17,25 Kč (813 satoshi) těžařům, celkově 45,89 Kč (2 163 satoshi). Samotná platba pomocí sítě byla realizována s poplatkem 1,51 Kč (71,588 satoshi) a potvrzena během 928 milisekund. Uvedené částky vycházejí z ceny bitcoinu v den platby, tedy přibližně 2 115 441 Kč za 1 BTC.

7.3.3 Porovnání Lightning Network a platební karty Visa

Pro porovnání následně vypočítáme hypotetickou výši poplatků, které by vznikly při zaplacení stejné částky prostřednictvím platební karty Visa. Výpočet vychází z regulovaných i neregulovaných složek nákladů dle evropského modelu MIF++ a veřejně dostupných sazeb, které jsem uvedl v kapitole x.

Tabulka 4 Výpočet hypotetického poplatku při platbě Visa kartou

Složka poplatku	Sazba / částka	Výpočet	Poplatek
Mezibankovní poplatek	0,20 %	$0,002 \times 358,52$	0,717 Kč
Poplatek karetní společnosti (Visa)	€0,00865 + 0,0836 %	$(0,0836 \% \times 358,52) +$ $0,00865 \text{ € } (\approx 0,212 \text{ Kč})$	0,511 Kč
Poplatek za zpracování transakce	~1 %	$0,01 \times 358,52$	3,585 Kč
Celkem (odhad)	-	-	~4,81 Kč

(zdroj: vlastní zpracování)

Uvedený odhad 1 % za poplatek za zpracování transakce vychází z příkladu společnosti Global Payments (2025). Ačkoli konkrétní výše tohoto poplatku závisí na individuálních smluvních podmínkách a nabídkách, které nejsou veřejně dohledatelné.

Při přímém porovnání vychází transakce prostřednictvím Lightning Network na přibližně 1,51 Kč, což vychází na třetinu nákladů platby kartou Visa. Přesto je vhodné

připomenout, že uvedené poplatky za Visa transakci představují pouze minimální odhad. Ve skutečnosti mohou být celkové náklady vyšší v závislosti na konkrétních okolnostech, jako je typ terminálu, využití platební brány, způsob platby, či individuální dohoda mezi obchodníkem a poskytovatelem služeb.

Další významnou výhodou platby prostřednictvím Lightning Network je rychlost zúčtování z pohledu obchodníka. V našem případě mohl obchodník disponovat přijatými prostředky prakticky okamžitě po potvrzení transakce, tedy do několika sekund. Naproti tomu při využití tradičního platebního terminálu prostřednictvím karetní společnosti bývají prostředky obchodníkovi připsány až s časovým odstupem 1 až 3 pracovních dnů.

Z provedeného srovnání tedy vyplývá, že z hlediska čistě transakčních nákladů se Lightning Network v daném případě jeví jako efektivnější platební metoda než tradiční karetní schéma. Současně nabízí velmi rychlé zpracování transakce a funguje nezávisle na bankovní infrastruktuře.

ZÁVĚR

Tato bakalářská práce se zaměřila na posouzení, zda a jak kryptoaktiva naplňují platební funkci, a porovnala jejich vlastnosti s tradičními digitálními platebními metodami, jako jsou Visa a Mastercard. V rámci teoretické části byla popsána ekonomická definice peněz, technologické principy fungování kryptoaktiv a překážky spojené s jejich využíváním v běžném platebním styku.

Praktická část ukázala, že off-chain řešení jako Lightning Network nebo Arbitrum dokáží nabídnout velmi nízké poplatky, rychlé zpracování transakcí a okamžitou finalitu. V určitých parametrech tak kryptoaktiva dokáží konkurovat nebo dokonce překonat tradiční systémy typu Visa a Mastercard. I přesto je využití těchto technologií oproti tradičním metodám stále v jisté míře omezené, existují náznaky postupného rozšiřování praktického využití. Alternativy, které byly v praktické části představeny, ukazují, že kryptoaktiva již nejsou doménou úzké technologické komunity, ale postupně se více stávají součástí běžného placení.

Závěrem lze konstatovat, že kryptoaktiva vykazují potenciál stát se součástí moderního platebního systému, avšak jejich širší využití bude záviset na odstranění technologických, legislativních i uživatelských překážek. Ačkoliv práce nebyla zaměřena na předpověď vývoje, na základě zjištěných technických parametrů a současného stavu využití kryptoaktiv lze uvažovat o tom, že jejich budoucí role v platebním systému by mohla spočívat ve funkčním doplnění tradičních metod.

SEZNAM POUŽITÉ LITERATURY

IML, 2025. *Lightning Network Statistics* | *IML – Lightning Network Search and Analysis Engine – Bitcoin mainnet* [online] [cit. 2025-05-18]. Dostupné z: <https://1ml.com/statistics>

ACINQ, 2025. Phoenix Wallet [software]. 8. duben 2025. [cit. 2025-05-07]. Dostupné z: <https://apps.apple.com/cz/app/phoenix-wallet/id1544097028>

ADEGBITE, Ayodeji, 2024. *The Role Of Blockchain Technology In Enhancing Financial Inclusion* [online]. Dostupné z: <https://doi.org/10.9790/5933-1505071928>

ALZA, 2023. *Na Alze teď zaplatíte bitcoinem také přes Lightning Network* | *Alza.cz* [online] [cit. 2025-05-14]. Dostupné z: <https://www.alza.cz/platba-bitcoinem-pres-lightning-network-alza>

ANWAR, Andi Faisal, Baso IWANG, Hasbiullah HASBIULLAH a Ahmad KAFRAWI, 2022. Fundamental Analysis of Cryptocurrency Price Fluctuations; A Socio-Economic, Political and Psychological Approach [online]. 12(7), 1466–1473 [cit. 2025-04-30]. ISSN 2169-8767. Dostupné z: <https://doi.org/10.46254/AU01.20220336>

AQUILINA, Matteo, Giulio CORNELLI, Jon FROST a Leonardo GAMBACORTA, 2025. Cryptocurrencies and decentralised finance: functions and financial stability implications [online]. [cit. 2025-05-04]. Dostupné z: <https://www.bis.org/publ/bppdf/bispap156.htm>

ARBISCAN, 2025. *Arbitrum One Charts and Statistics* | *Arbitrum One* [online] [cit. 2025-05-20]. Dostupné z: <https://arbiscan.io/charts>

BARCHAT, Corey, 2025. *What are Optimistic Rollups and how do they work?* | *MoonPay* [online] [cit. 2025-05-20]. Dostupné z: <https://www.moonpay.com/learn/blockchain/what-are-optimistic-rollups>

BITINFOCHARTS, 2025a. *Bitcoin (BTC) statistics – Price, Blocks Count, Difficulty, Hashrate, Value* [online] [cit. 2025-05-18]. Dostupné z: <https://bitinfocharts.com/bitcoin/>

BITINFOCHARTS, 2025b. *Ethereum / Ether (ETH) statistics – Price, Blocks Count, Difficulty, Hashrate, Value* [online] [cit. 2025-05-20]. Dostupné z: <https://bitinfocharts.com/ethereum/>

BITPAY, 2025. *Who Accepts Crypto? 250+ Stores Where You Can Spend Bitcoin + Crypto* | *BitPay* [online] [cit. 2025-05-22]. Dostupné z: <https://www.bitpay.com/directory>

BITREFILL, 2025. *Bitrefill (Czech Republic) - Buy Gift Cards, eSIM & Airtime with Bitcoin or Crypto – Bitrefill* [online] [cit. 2025-05-14]. Dostupné z: <https://www.bitrefill.com/cz/en/gift-cards/>

BOUŠKA, Kamil, 2023. *Velká kniha o Bitcoinu a kryptoměnách aneb Finanční gramotnost pro každého*. Praha: Braiins Publishing. ISBN 978-80-908709-5-6.

BTC MAP, 2025. *Czechia – BTC Map Country* [online] [cit. 2025-05-14]. Dostupné z: <https://btcmap.org/country/cz>

BURNISKE, Chris a Jack TATAR, 2018. *Cryptoassets: the innovative investor's guide to bitcoin and beyond*. New York: McGraw-Hill. ISBN 978-1-260-02667-2.

CARNIMEO, Andrea, 2024. *11 Best Bitcoin-Only Exchanges And Apps Of 2025* [online] [cit. 2025-05-22]. Dostupné z: <https://blockdyor.com/best-bitcoin-only-exchanges/>

COINATMRADAR, 2025. *Bitcoin ATM Map – Find Bitcoin ATM, Online Rates* [online] [cit. 2025-05-22]. Dostupné z: <https://coinatmradar.com/>

COMGATE, 2025. *Jak porovnat ceníky konkurence* [online] [cit. 2025-05-19]. Dostupné z: <https://help.comgate.cz/docs/jak-porovnat-ceniky-konkurence>

CRAIG, Jeffrey, 2021. *How many transaction per second can Bitcoin process? Scalability Problem – Phemex Blog* [online] [cit. 2025-05-22]. Dostupné z: <https://phemex.com/blogs/what-is-transactions-per-second-tps>

DYLAN-ENNIS, Paul, 2024. Absolute Essentials of Ethereum. *Absolute Essentials of Ethereum* [online]. 1–98 [cit. 2025-04-01]. Dostupné z: <https://doi.org/10.4324/9781003319603>

FRED, Tommy a Iseoluwa OLUWASEUN, 2025. The Legal Status of Digital Assets and Cryptocurrencies: Adaptive Regulatory Models.

GERSTEIN, Julia, 2024. *Blockchain Breakdown: What is a Layer 2?* [online] [cit. 2025-03-18]. Dostupné z: <https://volet.com/blog/post/blockchain-breakdown-what-is-a-layer-2-01je1vkvv6ctjysv8m6cgvhc9d>

GLOBAL PAYMENTS, 2025. *Kompletní průvodce schématem MIF++: Kolik zaplatíte?* [online] [cit. 2025-05-19]. Dostupné z: <https://www.globalpayments.cz/cs-cz/podpora/mif>

GOFORTH, Carol R., 2018. U.S. Law: Crypto is Money, Property, a Commodity, and a Security, all at the Same Time [online]. [cit. 2025-03-17]. Dostupné z: <https://papers.ssrn.com/abstract=3272975>

GOODELL, Geoff a Tomaso ASTE, 2019. Can Cryptocurrencies Preserve Privacy and Comply With Regulations? *Frontiers in Blockchain* [online]. 2. Dostupné z: <https://doi.org/10.3389/fbloc.2019.00004>

GOPAY, 2024. *Rozšiřujeme podporu kryptoměn a zavádíme Bitcoin Lightning* | GoPay blog [online] [cit. 2025-05-17]. Dostupné z: <https://www.gopay.com/blog/rozsirujeme-podporu-kryptomen-a-zavadime-bitcoin-lightning/>

GORJON, Sergio, 2021. The Role of Cryptoassets as Legal Tender: The Example of El Salvador [online]. [cit. 2025-03-18]. Dostupné z: <https://papers.ssrn.com/abstract=3944765>

GRUJIĆ, Miloš a Goran RADIVOJAC, 2019. FUTURE OF CRYPTOCURRENCIES AND BLOCKCHAIN TECHNOLOGY IN FINANCIAL MARKETS [online]. 1, 56–75. Dostupné z: <https://doi.org/10.7251/JOCE1901056R>

HAMM, Peter, 2022. Acceptance Factors for Cryptocurrencies as Payment Systems. In: [online]. Dostupné z: <https://doi.org/10.24251/HICSS.2022.729>

HARVEY, Campbell R., Ashwin RAMACHANDRAN a Joey SANTORO, 2021. *DeFi and the future of finance*. New Jersey: Wiley. ISBN 978-1-119-83601-8.

HAYES, Adam, 2023. *What Is a Basic Attention Token (BAT)? How It Tracks Consumers* [online] [cit. 2025-05-22]. Dostupné z: <https://www.investopedia.com/terms/b/basic-attention-token.asp>

HAYES, Adam, 2024. *Stablecoins: Definition, How They Work, and Types* [online] [cit. 2025-05-21]. Dostupné z: <https://www.investopedia.com/terms/s/stablecoin.asp>

HOBZA, Martin a Aneta VONDRÁČKOVÁ, 2021. Crypto-Asset Services under the Draft MiCA Regulation. *SSRN Electronic Journal* [online]. [cit. 2025-03-17]. Dostupné z: <https://doi.org/10.2139/SSRN.3984355>

CHAINSPECT, 2025. *Fastest Blockchains by TPS [2025] | Chainspect* [online] [cit. 2025-05-13]. Dostupné z: <https://chainspect.app/dashboard>

JONES, Lindsay Sain, 2022. Beyond the Hype: A Practical Approach to CryptoReg. *SSRN Electronic Journal* [online]. [cit. 2025-03-17]. Dostupné z: <https://doi.org/10.2139/SSRN.3874133>

JUODIS, Andrius, 2024. *Cryptocurrency Regulations Around the World - iDenfy* [online] [cit. 2025-03-14]. Dostupné z: <https://www.idenfy.com/blog/cryptocurrency-regulations-around-the-world/>

KHAN, Ruby; DHALIWAL, Navdeep; DEORARI, Rajesh; ANOOSHA, P.; HUSSEIN, Ali et al. The way to implement Cryptocurrency for International Payments and Remittances. Online. In: 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, 2023, s. 226-229. ISBN 979-8-3503-9926-4. Dostupné z: <https://doi.org/10.1109/ICACITE57410.2023.10183323>. [cit. 2025-05-22].

KIBET, Lydia, 2025. *7 Ways To Use Cryptocurrency for Everyday Purchases | Nasdaq* [online] [cit. 2025-05-22]. Dostupné z: <https://www.nasdaq.com/articles/7-ways-use-cryptocurrency-everyday-purchases>

KOCHERGIN, Dmitry, 2022. Crypto-assets: Economic nature, classification and regulation of turnover. *iorj.hse.ru* [online]. 17(3), 75–130 [cit. 2025-03-14]. Dostupné z: <https://doi.org/10.17323/1996-7845-2022-03-04>

KURZY.CZ, 2025. *Ethereum - aktuální a historické ceny kryptoměny Ethereum, graf vývoje ceny kryptoměny Ethereum - 3 měsíce - měna USD | Kurzy.cz* [online] [cit. 2025-05-20]. Dostupné z: <https://www.kurzy.cz/komodity/ethereum-graf-vyvoje-ceny/usd-3-mesice>

LOGESHWARAN, J, Venkata Ashok K GORANTLA, Venkataramaiah GUDE a Bhargavi GORANTLA, 2023. The Smart Performance Analysis of Cyber Security Issues in Crypto Currency Using Blockchain. In: 2023 6th International Conference on Contemporary

Computing and Informatics (IC3I) [online]. s. 2235–2241. Dostupné z: <https://doi.org/10.1109/IC3I59117.2023.10397950>

MACHEK, Vojtěch a REDAKCE FINEX, 2024. *Kryptoměnové karty | Srovnání kryptokaret [2025]* » *Finex.cz* [online] [cit. 2025-05-17]. Dostupné z: <https://finex.cz/rubrika/kryptomeny/krypto-karty/>

MASTERCARD, 2025. MASTERCARD INCORPORATED FISCAL YEAR 2024 FORM 10-K ANNUAL REPORT [online]. 6 [cit. 2025-05-19]. Dostupné z: https://s25.q4cdn.com/479285134/files/doc_financials/2024/ar/MA-12-31-2024-10-K-as-filed-with-exhibits.pdf

MIAH, Sal, 2025. *What Is Helium Mining? Earn HNT With a Helium Miner* [online] [cit. 2025-05-22]. Dostupné z: <https://www.webopedia.com/crypto/learn/what-is-helium-mining-hnt>

MISHKIN, Frederic S., 2022. *The economics of money, banking and financial markets*. Thirteenth edition. Harlow: Pearson. ISBN 978-1-292-40948-1.

MOGAVERO, Francesco, Ivan VISCONTI, Andrea VITALETTI a Marco ZECCHINI, 2021. The Blockchain Quadrilemma: When Also Computational Effectiveness Matters. *Proceedings - IEEE Symposium on Computers and Communications* [online]. [cit. 2025-03-10]. ISSN 15301346. Dostupné z: <https://doi.org/10.1109/ISCC53001.2021.9631511>

MRÁZKOVÁ, Anna, 2022. *Bitcoinový bankomat: Jak funguje a jak jej používat?* | *Blog | iMore.cz* [online] [cit. 2025-05-22]. Dostupné z: <https://www.imore.cz/clanek/14512-bitcoinovy-bankomat-jak-funguje-a-jak-jej-pouzivat?srsltid=AfmBOop-HM8h09boHGGiLSGqXjm8OiDpQNBQCED-jgIduPSfaNycEcUg>

MURADYAN, S, 2023. Digital Assets: Legal Regulation and Estimation of Risks. *Journal of Digital Technologies and Law* [online]. 1, 123–151. Dostupné z: <https://doi.org/10.21202/jdtl.2023.5>

NOVÁK, Michal, 2023. *Lightning network: platby budoucnosti*. Praha: Braiins Publishing. ISBN 978-80-908709-4-9.

NOVOTNÝ, Martin, 2024. *MiCA: Základní přehled* [online] [cit. 2025-03-15]. Dostupné z: <https://akschejbal.cz/mica-zakladni-prehled>

OKHAIFO, Godwin, 2025. *Understanding TPS: Which Blockchains Are the Fastest?* [online] [cit. 2025-05-19]. Dostupné z: <https://hashlock.com/blog/understanding-tps-which-blockchains-are-the-fastest>

OPENFARE, 2025. *Tap Latency Explained – World Wide OpenFare* [online] [cit. 2025-05-21]. Dostupné z: <https://wwopenfare.com/tap-latency-explained/>

PAESANO, Federico a Dorothy SIRON, 2022. Working Paper 38: Cryptocurrencies in Asia and beyond: law, regulation and enforcement. *Basel Institute on Governance Working Papers* [online]. 1–69. Dostupné z: <https://doi.org/10.12685/bigwp.2022.38.1-69>

PEAK, Bradley, 2024. *The SEC vs. Ripple lawsuit: Everything you need to know* [online] [cit. 2025-03-22]. Dostupné z: <https://cointelegraph.com/learn/articles/the-sec-vs-ripple-lawsuit-everything-you-need-to-know>

PICARDO, Elvis, 2024. *What Is Solana (SOL) and How Does SOL Crypto Work?* [online] [cit. 2025-04-14]. Dostupné z: <https://www.investopedia.com/solana-5210472>

PIERRO, Giuseppe Antonio a TONELLI, Roberto. Can Solana be the Solution to the Blockchain Scalability Problem? Online. In: 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). IEEE, 2022, s. 1219-1226. ISBN 978-1-6654-3786-8. Dostupné z: <https://doi.org/10.1109/SANER53432.2022.00144>. [cit. 2025-05-22].

POYNTON, Aaron, 2022. U.S. Cryptocurrency Regulation: A Slowly Evolving State of Affairs. *SSRN Electronic Journal* [online]. [cit. 2025-03-17]. Dostupné z: <https://doi.org/10.2139/SSRN.4204063>

QAROUSH, Zaer, Shadi ZAKARNEH a Ammar DAWABSHEH, 2022. Cryptocurrencies Advantages and Disadvantages: A Review [online]. **4**, 1–20. Dostupné z: <https://doi.org/10.24071/ijasst.v4i1.4610>

RADA EU A EVROPSKÁ RADA, 2024. *Trhy kryptoaktiv a jejich regulace v EU* [online] [cit. 2025-03-17]. Dostupné z: <https://www.consilium.europa.eu/cs/policies/crypto-assets-how-the-eu-is-regulating-markets/>

REIFF, Nathan, 2024. *What Was the First Cryptocurrency?* [online] [cit. 2025-03-28]. Dostupné z: <https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/>

REJEB, Abderahman, Karim REJEB a John KEOGH, 2021. Cryptocurrencies in Modern Finance: A Literature Review. *ETIKONOMI* [online]. **20**, 93–118. Dostupné z: <https://doi.org/10.15408/etk.v20i1.169111>

ROBERTS, Ben, 2024. *Exploring Solana: a next-generation blockchain platform | Independent Reserve* [online] [cit. 2025-04-17]. Dostupné z: <https://www.independentreserve.com/blog/knowledge-base/exploring-solana-a-next-generation-blockchain-platform>

SANKA, Abdurrashid Ibrahim a Ray C.C. CHEUNG, 2021. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications* [online]. **195**, 103232 [cit. 2025-03-10]. ISSN 1084-8045. Dostupné z: <https://doi.org/10.1016/J.JNCA.2021.103232>

SERGEENKOV, Andrey, 2024. *What Is Ripple (XRP)? A Guide for Investors in April 2025* [online] [cit. 2025-04-22]. Dostupné z: <https://www.forbes.com/sites/digital-assets/article/what-is-ripple-xrp/>

SERGEENKOV, Andrey, 2025. *What Is Bitcoin? A Beginner's Guide to Bitcoin Mining, Halving, and Real-World Uses* [online] [cit. 2025-03-29]. Dostupné z: <https://www.coindesk.com/learn/what-is-bitcoin>

STROUKAL, Dominik a Jan SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 3. rozšířené vydání. Praha: Grada Publishing. ISBN 978-80-271-1043-8.

ŠKOP, Luděk, 2024. *Platební terminály 2025 - Velké nezávislé srovnání poskytovatelů* [online] [cit. 2025-05-22]. Dostupné z: <https://blog.inspirum.cz/platebni-terminaly-2024-velke-nezavisle-srovnani-poskytovatelu-cr/>

TAPSCOTT, Don a Alex TAPSCOTT, 2018. *Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world*. London: Portfolio/Penguin. ISBN 978-0-241-23786-1.

TOKEN TERMINAL, 2025. *Solana Average transaction fee | Token Terminal* [online] [cit. 2025-05-19]. Dostupné z: <https://tokenterminal.com/explorer/projects/solana/metrics/transaction-fee-average>

TRAUTMAN, Lawrence J., 2018. Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace. *SSRN Electronic Journal* [online]. [cit. 2025-03-17]. Dostupné z: <https://doi.org/10.2139/SSRN.3182867>

VÁCLAVÍK, Lukáš, 2023. *Bitcoinem už zaplatíte i za pivo a oběd. Querko zavedlo podporu kryptoměn* – Živě.cz [online] [cit. 2025-05-17]. Dostupné z: <https://www.zive.cz/clanky/bitcoinem-uz-zaplatite-i-za-pivo-a-obed-querko-zavedlo-podporu-kryptomen/sc-3-a-222715/default.aspx>

VISA, 2017. *Visa Fact Sheet* [online] [cit. 2025-05-21]. Dostupné z: <https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf>

VISA, 2025. *Visa Annual Report 2024* [online]. [cit. 2025-05-19]. Dostupné z: <https://annualreport.visa.com/home/default.aspx>

VONDRÁK, Matouš a Vojtěch MACHEK, 2024. *Kryptoměnové burzy | Kde obchodovat? Velké srovnání 2025* » Finex.cz [online] [cit. 2025-05-12]. Dostupné z: <https://finex.cz/rubrika/kryptomeny/burzy/>

WĄTOREK, Marcin, Stanisław DROŻDŻ, Jarosław KWAPIEŃ, Ludovico MINATI, Paweł OŚWIECIMKA a Marek STANUSZEK, 2021. Multiscale characteristics of the emerging global cryptocurrency market. *Physics Reports* [online]. **901**, 1–82 [cit. 2025-05-04]. ISSN 0370-1573. Dostupné z: <https://doi.org/10.1016/J.PHYSREP.2020.10.005>

WIMMER, Florian, 2025. *What Is a DEX? Pros and Cons Explained [2025]* [online] [cit. 2025-05-22]. Dostupné z: <https://www.blockpit.io/en-us/blog/what-is-a-dex>

WORLDLINE, 2025. *Indicative Card Scheme Fee Rates as of April 2025 Czech Republic* [online] [cit. 2025-05-13]. Dostupné z: <https://worldline.com/content/dam/worldline/global/documents/brochures/scheme-fees-czech-republic.pdf>

SEZNAM OBRÁZKŮ

Obrázek 1 Trilema a kvadrilema škálovatelnosti blockchainu	42
Obrázek 2 Lightning Network	44
Obrázek 3 Úvodní obrazovka aplikace Phoenix Wallet	62
Obrázek 4 Volba vytvoření nebo obnovení peněženky	63
Obrázek 5 Zobrazení seedu.....	64
Obrázek 6 Kvakomat umožňující nákup kryptoaktiv	65
Obrázek 7 Podrobnosti o platbě.....	66
Obrázek 8 QR kód určený k úhradě transakce	67
Obrázek 9 Potvrzení platby.....	68

SEZNAM TABULEK

Tabulka 1 Srovnávací přehled rychlosti platebních systémů.....	51
Tabulka 2 Přehled poplatků Visa a Mastercard za zpracování transakcí.....	54
Tabulka 3 Srovnání výše poplatků platebních systémů	55
Tabulka 4 Výpočet hypotetického poplatku při platbě Visa kartou.....	69

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BTC Bitcoin

ETH Ethereum

SOL Solana

DeFi Decentralizované finance (Decentralized Finance)

dApps Decentralizované aplikace (Decentralized Applications)

SEC Komise pro cenné papíry a burzy USA (U.S. Securities and Exchange Commission)

MiCA Nařízení o trzích s kryptoaktivy (Markets in Crypto-Assets Regulation)

KYC Ověření totožnosti zákazníka (Know Your Customer)

AML Opatření proti praní špinavých peněz (Anti-Money Laundering)

TPS Počet transakcí za sekundu (Transactions Per Second)