VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

PODVODNÉ PRAKTIKY V PROSTŘEDÍ KRYPTOMĚN

Autor práce: Filip Kozák, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. et Mgr. Radek Fabian

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Filip Kozák, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Podvodné praktiky v prostředí kryptoměn

Název bakalářské práce v anglickém jazyce: Fraudulent Practices in the Cryptocurrency Market

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: Mgr. et Mgr. Radek Fabian

Datum zadání bakalářské práce: prosinec 2025

Cíl bakalářské práce:
Cílem bakalářské práce je komplexně zhodnotit podvodné jevy v kryptoměnovém prostředí, identifikovat jejich mechanismy a dopady na uživatele a investory a na základě provedeného dotazníkového šetření navrhnout opatření vedoucí ke zvýšení informovanosti a ochrany investorů.

Student: Filip Kozák, DiS.	7.12.2025 *datum*	 *podpis*
Vedoucí práce: Mgr. et Mgr. Radek Fabian	7.12.2025 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	12.1.2026 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	14.1.2026 *datum*	 *podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	7.2.2026 *datum*	 *podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce Mgr. et Mgr. Radku Fabianovi za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

Tato práce se zabývá podvodnými jevy v kryptoměnovém prostředí a zkoumá, jak podvodníci využívají technologických a lidských slabin k dosažení svého cíle. Kryptoměny, jako Bitcoin, přinášejí výhody jako anonymita a nízké transakční náklady, ale zároveň vytvářejí podmínky pro různé formy podvodů, včetně Ponziho schémat, phishingu a falešných ICO. Práce rozebírá techniky sociálního inženýrství, které podvodníci používají, a navrhuje opatření na ochranu investorů, včetně technických a právních nástrojů a zvýšení osvěty mezi uživateli. Cílem je poskytnout přehled o hrozbách a navrhnout způsoby, jak snížit riziko podvodů.

Klíčová slova: kryptoměny, kybernetická bezpečnost, podvody, ochrana před podvody

ABSTRACT

This paper examines fraud phenomena in the cryptocurrency environment and examines how fraudsters exploit technological and human weaknesses to achieve their goals. Cryptocurrencies, such as Bitcoin, offer advantages such as anonymity and low transaction costs, but they also create conditions for various forms of fraud, including Ponzi schemes, phishing, and fake ICOs. The paper analyzes the social engineering techniques used by fraudsters and proposes measures to protect investors, including technical and legal tools and increasing awareness among users. The aim is to provide an overview of the threats and suggest ways to reduce the risk of fraud.

Key words: cryptocurrencies, cyber security, fraud, protection from scams

Obsah

Úvod

V současné době dochází k dynamickému rozvoji digitálních technologií, které zásadním způsobem ovlivňují fungování moderní společnosti. Digitalizace proniká do všech oblastí lidského života, včetně komunikace, vzdělávání, obchodu i finančních služeb. Jedním z nejvýznamnějších projevů této transformace je vznik a rozvoj kryptoměn, které představují inovativní alternativu k tradičním finančním nástrojům. Kryptoměny jsou považovány za významný technologický posun v oblasti financí a platebních systémů, jelikož umožňují realizaci transakcí bez nutnosti zapojení centrální autority, jako jsou banky či jiné finanční instituce.

Od svého vzniku v roce 2009, kdy byl představen Bitcoin jako první decentralizovaná kryptoměna, zaznamenal tento segment prudký rozvoj a získal pozornost nejen technologických nadšenců, ale i široké veřejnosti, investorů a státních institucí. Kryptoměny, založené na technologii blockchain, fungují na principu distribuované databáze, která zajišťuje transparentní a bezpečné zaznamenávání transakcí. Tento decentralizovaný charakter přináší uživatelům řadu výhod, mezi které patří zejména rychlost převodů, nízké transakční náklady, globální dostupnost a relativní nezávislost na tradičních finančních systémech.

Na druhé straně však tyto vlastnosti vytvářejí i prostředí, které je z hlediska bezpečnosti značně specifické. Absence centrální autority, vysoká míra anonymity či pseudonymity a omezená regulace činí kryptoměnové prostředí náchylným k různým formám zneužití. S rostoucí popularitou kryptoměn se tak paralelně rozvíjí i kybernetická kriminalita, která využívá jak technologických nedostatků, tak lidského faktoru. Nedostatečná informovanost uživatelů, jejich důvěra v nové technologie a snaha o rychlé zhodnocení investic často vedou k tomu, že se stávají oběťmi podvodných praktik.

V posledních letech byly v kryptoměnovém prostředí zaznamenány různé formy podvodů, které se neustále vyvíjejí a přizpůsobují aktuálním trendům. Mezi nejčastější patří Ponziho schémata, pyramidové systémy, phishingové útoky, falešné projekty typu Initial Coin Offering (ICO) či další sofistikované metody založené na principech sociálního inženýrství. Tyto podvody často kombinují technologické nástroje s psychologickou manipulací, přičemž jejich cílem je získání finančních prostředků od nic netušících uživatelů.

Významné kauzy, jako například BitConnect nebo OneCoin, poukázaly na rozsah a závažnost tohoto problému. Tyto případy ukázaly, jak snadno mohou být investoři oklamáni prostřednictvím slibů vysokých a rychlých zisků, aniž by si uvědomovali reálná rizika. Oběti těchto podvodů často přicházejí o veškeré investované prostředky, přičemž možnosti jejich navrácení jsou vzhledem k anonymní povaze kryptoměnových transakcí a nedostatečné regulaci velmi omezené.

Problematika podvodů v kryptoměnovém prostředí tak představuje aktuální a významné téma, které vyžaduje hlubší analýzu. S rostoucím významem digitálních aktiv a jejich postupným začleňováním do běžného ekonomického života roste i potřeba zajistit odpovídající úroveň bezpečnosti a ochrany uživatelů. Tato oblast je zároveň charakteristická rychlým vývojem, což klade zvýšené nároky jak na uživatele, tak na regulační orgány.

Cílem této bakalářské práce je komplexně analyzovat podvodné jevy v kryptoměnovém prostředí, identifikovat jejich základní mechanismy a zhodnotit jejich dopady na uživatele. Současně si práce klade za cíl navrhnout konkrétní opatření, která by mohla přispět ke zvýšení bezpečnosti a ochraně investorů. Dílčím cílem je také poukázat na význam vzdělávání a informovanosti veřejnosti jako klíčového faktoru prevence.

Práce se dále zaměřuje na identifikaci hlavních rizikových faktorů, které činí kryptoměny náchylnými k podvodnému jednání. Mezi tyto faktory patří zejména anonymní charakter transakcí, nedostatečně rozvinutý právní rámec, globální dostupnost kryptoměnových trhů a rychlý technologický vývoj. Tyto aspekty společně vytvářejí prostředí, které je obtížně kontrolovatelné a které může být snadno zneužito.

Pozornost je věnována také právnímu rámci kryptoměn a jeho postupnému vývoji. Regulace v této oblasti je stále relativně nová a nejednotná, a to jak na úrovni jednotlivých států, tak i v rámci mezinárodního prostředí. Česká legislativa, stejně jako evropská a globální regulační opatření, se postupně přizpůsobují nově vznikajícím výzvám, avšak jejich implementace často zaostává za rychlostí technologického vývoje. Tento nesoulad vytváří prostor pro aktivity podvodníků a komplikuje vymáhání práva.

V rámci práce budou analyzovány konkrétní případy kryptoměnových podvodů a jejich mechanismy fungování. Důraz bude kladen nejen na technickou stránku těchto podvodů, ale i na behaviorální aspekty, které ovlivňují rozhodování uživatelů. Práce se rovněž zaměří na identifikaci slabých míst v systému a na návrh opatření, která by mohla přispět ke snížení rizik.

Součástí práce bude také návrh preventivních opatření zaměřených na ochranu uživatelů a investorů. Diskutována budou jak technická řešení, například využívání vícefaktorové autentizace, bezpečné uchovávání kryptoměn prostřednictvím hardwarových peněženek či zásady bezpečného chování v online prostředí, tak i opatření legislativního charakteru. Zvláštní důraz bude kladen na význam vzdělávání a zvyšování povědomí veřejnosti, jelikož informovanost je považována za jeden z nejúčinnějších nástrojů prevence.

Kryptoměny lze v současnosti označit za významný fenomén moderní doby, který má potenciál zásadně ovlivnit budoucnost finančních systémů. Vedle svých přínosů však přinášejí i řadu výzev, které nelze opomíjet. Každý uživatel kryptoměn nese odpovědnost za zabezpečení svých digitálních aktiv, což vyžaduje určitou úroveň technických znalostí a obezřetnosti. Bezpečné a efektivní využívání kryptoměn je proto podmíněno nejen technologickým pokrokem, ale i odpovídající regulací a dostatečnou informovaností uživatelů.

Tato bakalářská práce si klade za cíl přispět k lepšímu pochopení problematiky podvodů v kryptoměnovém prostředí a nabídnout ucelený pohled na rizika spojená s tímto dynamicky se rozvíjejícím odvětvím. Získané poznatky mohou být přínosné jak pro běžné uživatele kryptoměn, tak pro odbornou veřejnost či instituce zabývající se problematikou kybernetické bezpečnosti.

1 Cíl a metodika bakalářské práce

Cílem bakalářské práce je komplexně zhodnotit podvodné jevy v kryptoměnovém prostředí, identifikovat jejich mechanismy a dopady na uživatele a investory a na základě provedeného dotazníkového šetření navrhnout opatření vedoucí ke zvýšení informovanosti a ochrany investorů. Práce se zaměřuje na analýzu nejčastějších forem kryptoměnových podvodů, jejich charakteristik, způsobů fungování a rizik, která z nich vyplývají pro jednotlivce i širší společnost.

Pro dosažení stanoveného cíle je bakalářská práce rozdělena na teoretickou a praktickou část. Teoretická část je zaměřena na vymezení a vysvětlení základních pojmů souvisejících s kryptoměnami a technologií blockchain, které tvoří nezbytný základ pro pochopení fungování kryptoměnového ekosystému. Dále se věnuje analýze právního rámce a regulačních přístupů ke kryptoměnám, a to jak na úrovni České republiky, tak i v mezinárodním kontextu. Součástí teoretické části je rovněž identifikace a popis nejrozšířenějších forem podvodů v kryptoměnovém prostředí, mezi které patří zejména Ponziho schémata, pyramidové systémy, falešné ICO a podvodné projekty, phishing, malware a další techniky sociálního inženýrství.

Praktická část bakalářské práce využívá kvantitativní výzkum realizovaný formou dotazníkového šetření jako hlavní výzkumnou metodu. Cílem tohoto šetření je zjistit úroveň informovanosti respondentů o kryptoměnách, jejich osobní zkušenosti s kryptoměnovými investicemi a podvody, stejně jako jejich vnímání rizik spojených s tímto prostředím. Získaná data budou následně statisticky vyhodnocena, analyzována a interpretována v návaznosti na poznatky získané v teoretické části práce.

Na základě výsledků dotazníkového šetření a jejich porovnání s teoretickými poznatky budou v závěrečné části práce formulována doporučení a návrhy opatření zaměřené na zvýšení ochrany investorů a uživatelů kryptoměn. Důraz bude kladen zejména na prevenci podvodů, zvyšování povědomí o rizicích a posílení informovanosti veřejnosti v oblasti bezpečného používání kryptoměnových technologií.

2 Definice kryptoměn a jejich vysvětlení

Kryptoměny jsou digitální nebo virtuální měny, které používají kryptografii k zajištění a ověřování transakcí a k vytváření nových jednotek měny. Na rozdíl od tradičních měn nejsou vydávány nebo kontrolovány žádnou centrální autoritou jako jsou vlády nebo centrální banky, ale jsou založeny na decentralizovaných sítích využívajících technologii blockchain.[1]

Blockchain je distribuovaná databáze, která ukládá informace o transakcích ve formě propojených bloků. Každý blok je propojen s předchozím, což vytváří řetězec tzv. chain, který zajišťuje transparentnost a neměnnost záznamů. Tato technologie je základem fungování kryptoměn a umožňuje transakce, které jsou bezpečné, nezávislé na třetích stranách a odolné vůči manipulaci.[2]

Kryptoměny mohou sloužit nejen jako alternativní platební metoda, ale také jako investiční aktivum. Díky jejich anonymitě a globální povaze jsou kryptoměny využívány v různých kontextech – od mikro plateb až po velké přeshraniční transakce. Mají své výhody ve formě nižších transakčních poplatků a rychlých mezinárodních převodech. Jsou také spojeny s riziky, včetně vysoké volitilita. Volatilita je ukazatel, který hodnotí míru kolísání ceny určitého aktiva (například akcie) v konkrétním časovém období.

Vyšší volatilita znamená, že cena se více mění a tím vytváří širší cenové rozpětí. V rámci obchodování s opcemi rozlišujeme dva základní typy volatility: historickou a implikovanou. Obě hodnoty jsou vyjadřovány v procentech.[3]

Dalšími riziky jsou nedostatek regulací nebo bezpečnostní hrozby, jako jsou hacky či podvody. Kryptoměnové trhy jsou často méně regulované než tradiční finanční systémy, což může vést k vyšší zranitelnosti vůči kybernetickým útokům. Hackerské útoky na kryptoburzy nebo podvodná schémata mohou vést ke ztrátám finančních

[1] LÁNSKÝ, J. *Kryptoměny 1.* vydání. V Praze: C.H. Beck, 2018. 144 stran. ISBN 978- 80-7400-722-4

[2] HADNAGY, C. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.

[3] LYNX. *Historická vs. implikovaná volatilita: Základy obchodování opcí* [online]. [cit. 2025-12-28]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/opce/volatilita/zaklady-obchodovani-opci-9-historicka-vs-implikovana-volatilita/

prostředků investorů. Bezpečnost a ochrana investic proto zůstávají klíčovými faktory při zvažování investic do kryptoměn.[4]

2.1 Kryptoměny

Kryptoměny jsou digitální peníze, které existují pouze online. Na rozdíl od běžných peněz, které používáme každý den (tzv. fiat měna jako je koruna, euro nebo dolar), nejsou kryptoměny kontrolovány vládou ani žádnou bankou. Fiat měna je oficiální měna státu, kterou stát nebo centrální banka vytiskne a kontroluje její množství.

Základem kryptoměn je technologie zvaná blockchain. Blockchain si lze představit jako digitální účetní knihu, kde jsou zaznamenány všechny transakce s kryptoměnou. Každá transakce je zapsaná do bloku, a jakmile je blok plný, přidá se do řetězce dalších bloků. Odtud vychází i pojmenování blockchain neboli řetězec bloků. Díky tomu je historie všech transakcí bezpečně uchovaná a neměnná, což znamená, že nikdo nemůže podvádět nebo transakce zpětně měnit.[5]

Kryptografie je způsob, jakým se informace v kryptoměnách chrání. Lze si to představit jako tajný kód, který zajistí, že transakce je bezpečná a mohou ji vidět jen ti, kteří k ní mají přístup. Díky kryptografii je velmi obtížné, aby někdo ukradl kryptoměnu nebo změnil informace o transakcích.

Kryptoměny jsou také decentralizované, což znamená, že neexistuje žádný centrální orgán, který by je spravoval nebo ovládal (jako např. centrální banka u fiat měn). Místo toho jsou spravovány sítí počítačů po celém světě, které spolupracují a ověřují transakce. Tato decentralizace zaručuje, že kryptoměny jsou odolné vůči vládnímu zásahu nebo manipulaci.

2.1.1 Klíčové vlastnosti kryptoměn

Kryptoměny mají několik důležitých vlastností, které je odlišují od tradičních měn, a právě díky těmto vlastnostem jsou kryptoměny tak specifické. Jednou z nejvýraznějších vlastností kryptoměn je jejich decentralizovaná povaha. Jak je již vysvětleno, na rozdíl od fiat měn, které jsou pod dohledem centrální banky, kryptoměny

[4] HADNAGY, C. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.
[5] MARR, B. *The Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. London: Wiley, 2018. ISBN 9781119467656.

nemají žádného centrálního správce nebo kontrolora. Transakce a jejich ověřování jsou prováděny sítí uživatelů, kteří společně udržují celý systém. Tato decentralizace poskytuje výhodu, že kryptoměny nejsou pod přímým vlivem žádné vlády nebo jiné instituce a jsou odolné vůči cenzuře nebo manipulaci.[6]

Bezpečnost je pro kryptoměny klíčová a je zajištěna díky pokročilé kryptografii. Kryptografie funguje jako šifrování, které zajišťuje, že transakce jsou bezpečné a nemohou být snadno padělány. Každá transakce je šifrována a ověřována tzv. privátními a veřejnými klíči. Přitom veřejný klíč funguje podobně jako adresa, kam může někdo poslat kryptoměnu, a privátní klíč je tajné heslo, kterým je zajištěno, že přístup k těmto prostředkům má jen jejich vlastník.

Většina kryptoměn umožňuje provádět transakce, aniž by bylo nutné odhalit skutečnou identitu uživatele. To znamená, že uživatelé nejsou povinni poskytovat osobní údaje tak jako u bankovních účtů. Nicméně úplná anonymita není u většiny kryptoměn možná – transakce jsou zaznamenány na blockchainu, kde je každá transakce přiřazena k veřejnému klíči. Toto se nazývá pseudonymita, což znamená, že sice nejsou uvedena reálná jména, ale transakce jsou přiřazeny ke konkrétním adresám. Jakmile je transakce s kryptoměnou potvrzena a zapsána do blockchainu, nelze ji vzít zpět. To je velký rozdíl oproti tradičním platebním metodám, kde lze platbu často stornovat nebo reklamovat. V krypto světě, pokud se někdo dopustí chyby (například odešle kryptoměnu na špatnou adresu), neexistuje žádný centrální subjekt, který by mohl platbu vrátit. Tato nevratnost transakcí zvyšuje bezpečnost, ale také klade vyšší odpovědnost na uživatele.[7]

Kryptoměny fungují na internetu. Jsou tedy přístupné komukoliv, kdo má připojení k síti. Neexistují žádné geografické hranice. Kryptoměnu lze posílat komukoliv na světě, a to mnohem rychleji a často i levněji než přes tradiční bankovní systémy. Transakce v kryptoměnách mohou probíhat během několika minut, zatímco mezinárodní bankovní převody mohou trvat i několik dní.[8]

[6] NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Available at: https://bitcoin.org/bitcoin.pdf. [cit. 2025-12-28].
[7] Tamtéž
[8] HARTINGEROVÁ, E. *Lekce 1 - Kryptoměny - Definice a vlastnosti* Zdroj. Online. Itmetwork. 2024, 2024. Dostupné z: https://www.itnetwork.cz/kryptomeny/zaklady-kryptomen. [cit. 2025-12-28].

2.2 Druhy kryptoměn

I když existují tisíce různých kryptoměn, dají se rozdělit na základě jejich účelu a funkcí do několika hlavních kategorií. Každý typ kryptoměny plní trochu jinou roli a má svá specifika.

2.2.1 Bitcoin (BTC)

Bitcoin je první a nejznámější kryptoměna, kterou vytvořil anonymní vývojář nebo skupina vývojářů pod pseudonymem Satoshi Nakamoto v roce 2009. Bitcoin je často přirovnáván k „digitálnímu zlatu“, protože je považován za uchovatele hodnoty. Bitcoin byl navržen jako decentralizovaná alternativa k fiat měnám a jeho hlavní výhodou je, že je tzv. deflační, což znamená, že maximální počet bude omezen na 21 milionů mincí, což z něj činí vzácné aktivum. Bitcoin je dnes často používán jako investiční nástroj nebo prostředek pro uchování hodnoty, ale také jako platební metoda, i když omezeně.[9]

2.2.2 Altcoiny

„Altcoin“ je zkratka pro „alternativní mince“, což je označení pro všechny kryptoměny jiné než Bitcoin. Existují tisíce altcoinů, přičemž některé se snaží konkurovat Bitcoinu, zatímco jiné mají zcela odlišné účely. Mezi nejznámější altcoiny patří Ethereum, Litecoin a Ripple.[10]

Ethereum (ETH) se odlišuje od Bitcoinu tím, že není jen měnou, ale i platformou, která umožňuje vytvářet a provozovat decentralizované aplikace (dApps) pomocí chytrých kontraktů. Díky této funkci mohou vývojáři vytvářet různé aplikace na blockchainu, což z něj činí jednu z nejoblíbenějších kryptoměn pro vývojáře.[11]

Litecoin (LTC) byl vytvořen jako „lehčí“ verze Bitcoinu a jeho hlavní výhodou je rychlejší potvrzení transakcí. Často bývá označován jako „stříbro“ v porovnání s „digitálním zlatem“ Bitcoinu.[12]

---

[9] ANTONOPOULOS, A. M. *Mastering Bitcoin*: *Unlocking Digital Cryptocurrencies*. 2nd ed. Sebastopol: O'Reilly Media, 2017. ISBN 9781491954386.
[10] NARAYANAN, A. B. J., FELTEN, E., MILLER, A., GOLDFEDER, S. *Bitcoin and Cryptocurrency Technologies.* Princeton: Princeton University Press, 2016. ISBN 978-0-691-17169-2.
[11] Tamtéž
[12] Tamtéž

Ripple (XRP) je kryptoměna zaměřená na rychlé a levné mezinárodní platby mezi bankami. Na rozdíl od Bitcoinu nesoutěží přímo jako měna pro širokou veřejnost, ale spíše jako nástroj pro banky, který zefektivňuje mezinárodní finanční transakce.[13]

2.2.3 Stablecoiny

Stablecoiny jsou kryptoměny navázané na stabilní aktiva, jako je například fiat měna (např. americký dolar), zlato nebo jiná kryptoměna. Cílem stablecoinů je snížit volatilitu, která je pro kryptoměny typická. Například USDT (Tether) nebo USDC (USD Coin) jsou stablecoiny, které jsou kryté dolarem, což znamená, že jejich hodnota by měla být vždy velmi blízko 1 USD. Stablecoiny jsou oblíbené hlavně proto, že kombinují výhody kryptoměn (rychlé transakce, globální dostupnost) s relativní stabilitou tradičních finančních měn. Často se používají jako prostředek pro obchodování na kryptoměnových burzách nebo jako úložiště hodnoty, když trhy s kryptoměnami zažívají velkou volatilitu.[14]

2.2.4 Tokeny

Tokeny jsou kryptoměny, které jsou založeny na jiné blockchainové síti, často na Ethereu. Na rozdíl od Bitcoinu nebo jiných kryptoměn nemají své vlastní blockchainy, ale jsou vytvářeny prostřednictvím již existujících sítí. Nejznámějším standardem je ERC-20 token, který běží na Ethereum blockchainu. Tokeny mají mnoho různých využití – od prostředků na financování projektů přes tzv. Initial Coin Offering – (ICO) až po přístup ke službám v rámci určitých blockchainových platforem. Také se často používají v decentralizovaných aplikacích (dApps), kde mohou sloužit jako platební prostředky, hlasovací nástroje nebo nástroje pro řízení komunitních projektů. Příkladem je Chainlink (LINK) nebo Uniswap (UNI), které poskytují specifické funkce nad rámec klasických kryptoměn.[15]

2.3 Výhody spojené s používáním kryptoměn

Kryptoměny nabízejí mnoho přínosů, díky nimž jsou pro mnoho lidí zajímavou alternativou k tradičním finančním systémům. Nejsou závislé na žádné centrální bance

[13] TAPSCOTT, D., TAPSCOTT, A. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Penguin, 2016. ISBN 978-1101980132
[14] MCCULLOUGH, J. *Stablecoins: The Future of Money?* Journal of Payments Strategy & Systems, 2020, vol. 14, no. 2, p. 123-130.
[15] NARAYANAN, A. B. J., FELTEN, E., MILLER, A., GOLDFEDER, S. *Bitcoin and Cryptocurrency Technologies.* Princeton: Princeton University Press, 2016. ISBN 978-0-691-17169-2.

nebo vládní instituci, což znamená, že nejsou ovlivňovány politikou nebo ekonomickými změnami v jedné zemi. Transakce mohou být uskutečňovány bez nutnosti zapojení banky, čímž je umožněno lidem bez přístupu k tradičním bankovním službám účastnit se globální ekonomiky. Nízké transakční poplatky a rychlost transakcí, zejména u mezinárodních plateb, jsou považovány za další výhody. Tradiční bankovní systémy bývají pomalé a drahé, zvláště u přeshraničních plateb, kde mohou převody trvat několik dní a zahrnovat vysoké poplatky. Kryptoměny umožňují, aby tyto transakce byly provedeny během několika minut a za nižší náklady.[16]

Ačkoli kryptoměny nejsou zcela anonymní, je poskytována vysoká míra soukromí, protože při transakcích nemusí být poskytovány osobní údaje uživatele, což je odlišuje od tradičních bankovních systémů, kde je identita uživatele vždy součástí procesu. Tím je zajišťována větší kontrola nad osobními údaji a soukromí uživatelů. Bezpečnost transakcí je zajištěna použitím blockchainu, což znamená, že jsou transakce bezpečné a obtížně padělatelné. Jakmile jsou transakce potvrzeny a zaznamenány do blockchainu, nemohou být změněny ani smazány, což snižuje riziko podvodů a zajišťuje důvěru v systém. Transparentnost a neměnnost jsou dále zaručeny tím, že blockchain funguje jako veřejná kniha, která je přístupná všem. Všechny transakce jsou viditelné a ověřitelné, a jakmile jsou zapsány, nelze je změnit ani upravit, čímž je zajišťována neměnnost záznamů a důvěryhodnost systému.[17]

2.4 Nevýhody kryptoměn

Kryptoměny s sebou nesou několik nevýhod, které mohou odradit některé uživatele od jejich používání. Jsou známé svou vysokou volatilitou, což znamená, že jejich ceny se mohou během krátkého časového úseku dramaticky měnit. Tato cenová nestabilita přináší rizika, zejména pro investory, protože může docházet k náhlým a výrazným změnám hodnoty. Zatímco pro některé investory může být volatilita atraktivní díky potenciálně vysokým ziskům, zároveň představuje značné riziko ztrát.

Dalším nevýhodou je omezená akceptace a použitelnost kryptoměn. Navzdory rostoucímu povědomí stále existuje jen omezený počet obchodníků a podniků, které kryptoměny akceptují jako platidlo. I když se situace postupně zlepšuje,

[16] HARTINGEROVÁ, E. *Lekce 1 - Kryptoměny - Definice a vlastnosti* Zdroj. Online. Itmetwork. 2024, 2024. Dostupné z: https://www.itnetwork.cz/kryptomeny/zaklady-kryptomen. [cit. 2025-12-28].
[17] Tamtéž

kryptoměny nejsou běžně používány pro každodenní platby, a uživatelé jsou často nuceni převádět je zpět na fiat měnu. Kromě toho existuje riziko ztráty a krádeží. Kryptoměny jsou digitální aktiva uchovávaná v digitálních peněženkách, a pokud uživatel ztratí přístup ke své peněžence (například ztrátou privátního klíče) nebo pokud dojde k hacknutí peněženky, je téměř nemožné získat prostředky zpět. Na rozdíl od tradičních bank neexistuje žádná instituce, která by mohla poskytnout náhradu nebo pomoc.[18]

Právní nejistota je dalším faktorem spojeným s kryptoměnami, neboť se jedná o relativně nový fenomén, kolem kterého se teprve vyvíjí právní rámec. Různé země mají k regulaci kryptoměn různé přístupy, což vytváří právní nejistotu. Některé státy kryptoměny omezují nebo dokonce zakazují, zatímco jiné se je snaží regulovat, což znamená, že investoři a podnikatelé musí být neustále informováni o právních změnách. Dalším problémem je technická složitost kryptoměn. Pro běžné uživatele může být používání kryptoměn technicky náročné, ať už jde o nastavení peněženek, bezpečné uchovávání privátních klíčů nebo orientaci v krypto světě. Tato složitost může některé uživatele odradit nebo je vystavit riziku ztráty kvůli neznalosti.[19]

[18] LÁNSKÝ, J. *Kryptoměny* 1. vydání. V Praze: C.H. Beck, 2018. 144 stran. ISBN 978- 80-7400-722-4
[19] Tamtéž

3 Právní rámec a regulace

Vzhledem k tomu, že kryptoměny jsou relativně novým fenoménem dnešní doby ve vztahu k problematice kyberbezpečnosti, právní rámec a regulace kolem jsou teprve ve fázi vývoje. Kryptoměnové transakce a obchodování jsou z velké části globální, což znamená, že různé země přistupují k regulacím odlišně. V rámci ochrany investorů, prevence podvodů a zajištění kybernetické bezpečnosti se v mnoha zemích začaly uplatňovat určité regulační zásady, i když přístupy se mohou výrazně lišit.

3.1 Trestní zákoník – podvody a zneužití platebních údajů

V České republice se na kryptoměnové podvody vztahuje zákon č. 40/2009 Sb., trestní zákoník (dále jen „TZ“). Tento zákon definuje různé formy podvodného jednání, které mohou být použity v souvislosti s kryptoměnovými transakcemi, ať už jde o falešná ICO, phishing nebo zneužití platebních údajů.

Podvod

Předmětné ustanovení trestního zákona se zabývá podvodným jednáním, kdy pachatel uvede někoho v omyl s cílem obohatit se na jeho úkor. Kryptoměnové podvody, jako jsou falešné investiční příležitosti (ICO), tedy nabídky prvotního prodeje kryptoměnových tokenů bez reálného projektu či s úmyslem vylákat finanční prostředky od investorů, nebo Ponziho schémata, založená na vyplácení výnosů dřívějším investorům z vkladů nových účastníků bez skutečné ekonomické činnosti, mohou být klasifikovány jako podvod podle § 209 TZ.

Příklad:
Pachatel vytvořil falešné ICO, přesvědčil investory, aby vložili své peníze s příslibem vysokých výnosů, a poté zmizel i s jejich prostředky. Tímto jednáním způsobil investorům škodu a sám se obohatil, což je přesně definováno jako podvod podle § 209 TZ.

Neoprávněný přístup k počítačovému systému a nosiči informací

Phishingové útoky, které zahrnují neoprávněné získání přihlašovacích údajů nebo privátních klíčů k peněženkám, spadají pod tento paragraf. Pokud někdo prostřednictvím phishingu získá přístup k cizímu účtu nebo zařízení, kde jsou uchovávány kryptoměnové prostředky, může být stíhán podle § 230 TZ.

Příklad:
Útočník posílal phishingový e-mail, který přesměroval oběť na falešnou burzovní stránku. Oběť na této stránce zadá své přihlašovací údaje a útočník je následně zneužije ke krádeži kryptoměn. TZ

Zneužití platebního prostředku

Tento paragraf se zabývá neoprávněným použitím platebních údajů, což může být relevantní v případech, kdy jsou zneužity kryptoměnové peněženky nebo burzovní účty k převodům bez vědomí uživatele. Kryptoměnové peněženky fungují podobně jako platební prostředky, a proto může neoprávněný přístup k těmto peněženkám a jejich zneužití spadat pod § 234 TZ.

Příklad:
Pokud někdo získal přístup k peněžence oběti a provedl transakci, při níž převedl prostředky na svůj účet, jedná se o zneužití platebního prostředku podle § 234 TZ.

Tyto paragrafy z trestního zákoníku pokrývají většinu trestných činů spojených s kryptoměnovými podvody a se zneužitím platebních údajů. Právě podvod a neoprávněné získání či použití přístupových údajů k platebním prostředkům jsou v kontextu kryptoměnových investic nejběžnější.

3.2 Zákon o ochraně spotřebitele

V České republice je ochrana spotřebitele regulována zákonem č. 634/1992 Sb., o ochraně spotřebitele, který upravuje práva spotřebitelů a povinnosti podnikatelů. Tento zákon je klíčový i v oblasti kryptoměnových podvodů, zejména pokud jde o falešné investiční projekty, jako jsou podvodná ICO nebo nelegitimní kryptoměnové burzy.

Spotřebitelé jsou v kryptoměnovém prostředí často vystaveni rizikům, protože kryptoměny nejsou vždy jednoznačně regulovány. Zákon o ochraně spotřebitele se však může uplatnit zejména v případech, kdy jsou kryptoměnové projekty nabízeny veřejnosti formou investičních příležitostí, což může být považováno za obchodní činnost. zákona č. 634/1992 Sb., o ochraně spotřebitele (dále jen „ZOS“).

Nekalé obchodní praktiky

Tento paragraf zakazuje používání klamavých a agresivních obchodních praktik. Pokud kryptoměnový projekt slibuje nereálné výnosy nebo poskytuje nepravdivé informace o své podnikatelské činnosti (např. falešná ICO), může být takové jednání klasifikováno jako nekalá obchodní praktika podle § 4 ZOS

Příklad:
ICO slibuje, že jeho tokeny budou mít vysokou budoucí hodnotu a že projekt rychle poroste, přičemž ve skutečnosti neexistuje žádný reálný základ nebo produkt. To je příklad klamavé obchodní praktiky.

Klamavé konání

Tento paragraf se týká přímo situací, kdy podnikatel uvede spotřebitele v omyl ohledně povahy, vlastností nebo účelu produktu. V kontextu kryptoměn by sem mohly spadat případy, kdy podvodníci prezentují falešné produkty nebo služby, které ve skutečnosti neexistují. § 5 ZOS

Příklad:
Kryptoměnový projekt tvrdí, že vyvíjí revoluční technologickou platformu umožňující decentralizované investování, avšak po získání finančních prostředků od spotřebitelů žádnou funkční aplikaci ani technologické řešení neuvede do provozu. Takové jednání by mohlo být posuzováno jako klamavé konání vůči spotřebitelům.

Právo spotřebitele na informace

Podle tohoto paragrafu má spotřebitel právo na jasné a úplné informace o produktu nebo službě, které si kupuje. V oblasti kryptoměn to znamená, že spotřebitel musí být informován o všech rizicích spojených s investicí, včetně volatilních rizik a možnosti ztráty všech prostředků. Pokud spotřebitel není řádně informován o rizicích, lze to považovat za porušení tohoto práva, a to zejména v případě, kdy kryptoměnový projekt záměrně zamlčuje důležité skutečnosti.

Zákon o ochraně spotřebitele je důležitý právní nástroj, který může pomoci chránit investory před podvody a nelegitimními kryptoměnovými projekty. Spotřebitelé mají právo na přesné a pravdivé informace, a pokud jim podnikatel poskytne klamavé nebo

neúplné informace, může čelit právním důsledkům. Tento zákon tak poskytuje důležitou ochranu proti nekalým obchodním praktikám, které jsou v kryptosvětě relativně běžné. § 12 ZOS

4 Regulace v různých zemích

Kryptoměny jsou globálním fenoménem, který není omezen hranicemi jednotlivých států. Nicméně regulace kryptoměn se v jednotlivých zemích výrazně liší. Některé státy se zaměřují na vytvoření jasného a bezpečného regulačního rámce, zatímco jiné se k nim staví s nedůvěrou nebo je dokonce zakazují. Regulace kryptoměn má zásadní význam pro ochranu spotřebitelů, pro boj proti praní špinavých peněz a financování terorismu.[20]

Spojené státy americké

Ve Spojených státech amerických jsou kryptoměny regulovány několika různými federálními agenturami, přičemž každá z nich přistupuje ke kryptoměnám z jiného úhlu. Vzhledem k rozmanitosti právního prostředí a přístupu k regulaci kryptoměn, jsou Spojené státy jednou z nejvýznamnějších zemí, které se snaží zavést jasný regulační rámec pro tento sektor.

Komise pro cenné papíry a burzy

SEC se zaměřuje na regulaci kryptoměnových tokenů, které jsou považovány za cenné papíry (securities). Pokud kryptoměna nebo token spadá do definice cenného papíru, musí se podřídit přísným pravidlům a regulacím, včetně povinnosti registrace a poskytnutí úplných informací investorům. SEC také aktivně zasahuje proti podvodným ICO, které jsou považovány za nelegitimní cenné papíry. Příkladem je několik soudních sporů proti projektům, které prostřednictvím ICO nabízely neregistrované tokeny.[21]

Financial Crimes Enforcement Network (FinCEN)

FinCEN je federální agentura, která se zaměřuje na prevenci praní špinavých peněz a financování terorismu. Kryptoměnové burzy a peněženky v USA spadají pod regulace FinCEN a musí dodržovat pravidla „know your customer“ (KYC) a „anti-money

[20] KUHN, T. R. S., FISCHER L. *Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York: HarperCollins, 2021. ISBN 9780063076628.
[21] GURLEY, J. (2022). *The SEC and Cryptocurrency: A Regulatory Perspective*. In *Cryptocurrency Regulations and Compliance* (pp. 12-27). London: Palgrave Macmillan. ISBN 978-3030927560.

laundering“ (AML), která vyžadují, aby provozovatelé identifikovali své zákazníky a sledovali podezřelé transakce.[22]

Internal Revenue Service (IRS)

IRS se zabývá daňovými aspekty kryptoměn. Kryptoměny jsou ve Spojených státech považovány za majetek (property), což znamená, že jakýkoliv zisk z prodeje nebo směny kryptoměn podléhá zdanění. Uživatelé musí hlásit všechny zisky a ztráty z obchodování s kryptoměnami a zaplatit odpovídající daně. IRS se zaměřuje na prosazování těchto pravidel a v posledních letech zvýšilo počet kontrol zaměřených na držitele kryptoměn.[23]

Commodity Futures Trading Commission (CFTC)

CFTC reguluje deriváty kryptoměn včetně futures kontraktů a dalších finančních nástrojů založených na kryptoměnách. Bitcoin a další kryptoměny jsou podle CFTC považovány za komodity (commodities), což znamená, že podléhají regulacím týkajícím se komoditních trhů. Spojené státy přistupují ke kryptoměnám z několika různých úhlů. Zatímco SEC dohlíží na dodržování pravidel ohledně cenných papírů, FinCEN se zaměřuje na boj proti praní špinavých peněz a IRS na daňové povinnosti spojené s držením kryptoměn. Kryptoměny v USA podléhají silné regulaci, zejména pokud jde o ochranu spotřebitelů a prevenci podvodů.[24]

Evropská unie

Evropská unie (EU) přistupuje k regulaci kryptoměn jako celek, přičemž jednotlivé členské státy implementují evropské směrnice do svých národních právních úprav. EU se zaměřuje na ochranu spotřebitelů, na boj proti praní špinavých peněz (AML) a financování terorismu. V posledních letech došlo k výraznému zpřísnění regulací v této oblasti, zejména prostřednictvím různých směrnic a nařízení.

[22] U.S. DEPARTMENT OF THE TREASURY. 2019. A *Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation.* [online]. [cit. 2025-12-22]. Dostupné z: https://home.treasury.gov/system/files/136/FintechReport2019.pdf
[23] GURLEY, J. (2022). *The SEC and Cryptocurrency: A Regulatory Perspective*. In *Cryptocurrency Regulations and Compliance* (pp. 12-27). London: Palgrave Macmillan. ISBN 978-3030927560.
[24] Tamtéž

Směrnice o praní špinavých peněz (AMLD5)

Jedním z klíčových právních rámců EU pro kryptoměny je směrnice Anti-Money Laundering Directive 5 (AMLD5), která vstoupila v platnost v roce 2020. Tato směrnice zavádí povinnosti pro poskytovatele služeb, jako jsou kryptoměnové burzy a poskytovatelé peněženek, aby prováděli identifikaci svých klientů (tzv. „know your customer“ nebo KYC). Tato směrnice vyžaduje, aby kryptoměnové burzy a peněženky sledovaly a hlásily podezřelé transakce. Cílem je zabránit praní špinavých peněz a financování terorismu prostřednictvím kryptoměnových transakcí.[25]

Nařízení Markets in Crypto-Assets (MiCA)

V roce 2020 Evropská komise představila návrh nařízení Markets in Crypto-Assets (MiCA), jehož cílem je zavést jednotný regulační rámec pro kryptoměny v celé EU. MiCA se zaměřuje na ochranu spotřebitelů a regulaci kryptoměnových trhů. Nařízení bude vyžadovat, aby emitenti kryptoměn a poskytovatelé služeb, jako jsou burzy, podléhali regulaci a poskytovali investorům potřebné informace o rizicích. Cílem je vtvořit stabilní a transparentní trh pro kryptoměny a zabránit podvodům.[26]

Evropský orgán pro cenné papíry a trhy (ESMA)

European Securities and Markets Authority (ESMA) dohlíží na to, zda kryptoměny a tokeny splňují kritéria pro cenné papíry podle evropských předpisů. Pokud jsou kryptoměnové tokeny považovány za cenné papíry, podléhají přísné regulaci, včetně registrace a poskytování informací investorům. ESMA také vydává varování před riziky spojenými s investicemi do kryptoměn a upozorňuje spotřebitele na podvodné projekty.[27]

Ochrana spotřebitele

Evropská unie klade důraz na ochranu spotřebitelů, zejména v oblasti kryptoměnových investic, které jsou vysoce rizikové. Regulace se zaměřují na to, aby poskytovatelé služeb informovali spotřebitele o všech rizicích spojených

[25] EUROPEAN PARLIAMENT. *Směrnice (EU) 2018/843 o prevenci používání finančního systému k praní špinavých peněz nebo financování terorismu*. 2018. [online]. [2025-12-18]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32018L0843.
[26] Tamtéž
[27] Tamtéž

s obchodováním s kryptoměnami. To zahrnuje jak volatilitu trhu, tak rizika spojená s podvody a kyberkriminalitou. Evropská unie se postupně zaměřuje na vytvoření komplexního regulačního rámce pro kryptoměny, který bude chránit spotřebitele a zabrání zneužití kryptoměn pro praní špinavých peněz a financování terorismu. Směrnice AMLD5 již zavedla přísné požadavky na burzy a poskytovatele peněženek, zatímco nařízení MiCA slibuje přinést další jednotné regulace napříč celou EU. [28]

Velká Británie

Velká Británie po odchodu z Evropské unie, přistupuje k regulaci kryptoměn samostatně. I když byla součástí implementace některých evropských směrnic, její právní rámec se po brexitu postupně vyvíjí nezávisle na EU. V Británii kryptoměnové trhy podléhají regulaci několika agentur, přičemž důraz je kladen na ochranu spotřebitelů a prevenci praní špinavých peněz.

Financial Conduct Authority (FCA)

FCA je hlavním regulačním orgánem pro finanční trhy ve Velké Británii, včetně kryptoměnového sektoru. V roce 2021 zavedla FCA přísnější pravidla pro poskytovatele kryptoměnových služeb, kteří se musí registrovat u FCA, aby mohli legálně působit na britském trhu. FCA také kontroluje, zda kryptoměnové firmy dodržují pravidla „know your customer“ (KYC) a „anti-money laundering“ (AML), což zahrnuje povinné identifikování klientů a hlášení podezřelých transakcí.[29]

Zákaz kryptoměnových derivátů

V roce 2021 FCA také zakázala maloobchodním investorům ve Velké Británii obchodovat s některými kryptoměnovými deriváty, jako jsou futures a opce. Tento krok byl proveden kvůli vysokému riziku ztrát, které tyto složité finanční nástroje představují

[28] EUROPEAN PARLIAMENT. *Směrnice (EU) 2018/843 o prevenci používání finančního systému k praní špinavých peněz nebo financování terorismu*. 2018. [online]. [2025-12-18]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32018L0843.

[29] GOV.UK. *Statement from UK authorities on Cryptoassets*. 2022. [online]. [cit. 2025-12-18]. Dostupné z:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060448/Statement_from_UK_authorities_on_Cryptoassets_-_March_2022.pdf.

pro běžné investory. FCA uvedla, že tyto produkty jsou příliš rizikové a volatilní a mohou způsobit značné finanční ztráty spotřebitelům.[30]

Kryptoměny a daně

Britská daňová správa, HM Revenue & Customs (HMRC), považuje kryptoměny za majetek (similarly to the US IRS). To znamená, že každý zisk z obchodování s kryptoměnami podléhá kapitálové dani (capital gains tax). Pokud jednotlivec nebo firma drží kryptoměny jako investici a prodává je se ziskem, musí tento zisk nahlásit a zaplatit příslušné daně.[31]

Přístup k Initial Coin Offerings (ICO)

Ve Velké Británii jsou Initial Coin Offerings (ICO) regulovány opatrně. Pokud kryptoměnový token spadá do kategorie cenných papírů, podléhá přísným pravidlům regulace cenných papírů pod dohledem FCA. To znamená, že projekty, které nabízejí tokeny, musí splňovat podmínky transparentnosti a dodržovat pravidla ochrany investorů.[32]

Kybernetická bezpečnost

Velká Británie také klade důraz na kybernetickou bezpečnost a ochranu kryptoměnových burz a uživatelů před kybernetickými útoky. FCA dohlíží na to, aby burzy a peněženky dodržovaly vysoké standardy bezpečnosti a zajišťovaly ochranu osobních údajů a finančních prostředků uživatelů.

Ve Velké Británii je kryptoměnový trh silně regulován především z hlediska ochrany spotřebitelů a prevence praní špinavých peněz. FCA hraje hlavní roli při prosazování těchto regulací a zajišťuje, aby poskytovatelé kryptoměnových služeb plnili své povinnosti. Britské regulace jsou považovány za jedny z nejpřísnějších na světě, což může působit jako prevence před kryptoměnovými podvody.[33]

---

[30] GOV.UK. *Statement from UK authorities on Cryptoassets*. 2022. [online]. [cit. 2025-12-18]. Dostupné z:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060448/Statement_from_UK_authorities_on_Cryptoassets_-_March_2022.pdf.

[31] Tamtéž

[32] HM Revenue & Customs. *Cryptoassets for individuals*. 2021. [online]. [cit. 2025-12-18]. Dostupné z: https://www.gov.uk/government/publications/cryptoassets-for-individuals.

[33] Financial Conduct Authority. *Guidance on Cryptoassets*. 2021. [online]. [cit. 2025-12-18]. Dostupné z: https://www.fca.org.uk/publications/guidance-consultations/guidance-cryptoassets.

Rusko

V Rusku je ke kryptoměnám přistupováno s určitou opatrností a nejasný regulační rámec je stále v procesu vývoje. I když nejsou kryptoměny v Rusku výslovně zakázány, jejich používání je značně omezeno a regulace se stále vyvíjejí. Ruské orgány vyjadřují obavy ohledně praní špinavých peněz, financování terorismu a ochrany státní měny, což vedlo k zavedení restriktivních opatření.

Zákon „O digitálních finančních aktivech“

V roce 2020 Rusko přijalo zákon č. 259-FZ „O digitálních finančních aktivech“, který upravuje používání kryptoměn a dalších digitálních aktiv. Tento zákon legalizuje vydávání a obchodování s digitálními finančními aktivy. Zároveň omezuje používání kryptoměn jako platebního prostředku. Podle tohoto zákona je například zakázáno používat kryptoměny jako náhradu za státní měnu v obchodních transakcích. Tento zákon tak sice umožňuje vlastnit kryptoměny a obchodovat s nimi, ale zároveň stanovuje přísná pravidla pro jejich používání a zakazuje jejich využití jako formu oficiálního platidla.[34]

Postoj Ruska k regulaci kryptoměn

Centrální banka Ruska zastává přísný postoj vůči kryptoměnám a opakovaně varovala před jejich používáním. V zemi navrhla dokonce úplný zákaz těžby a obchodování s kryptoměnami. Tento návrh však zatím nebyl plně schválen. Obavy centrální banky jsou zaměřeny na dopad kryptoměn na finanční stabilitu a možnosti jejich zneužití k nelegálním činnostem. I když jsou kryptoměny v Rusku regulovány, stále podléhají zdanění, což znamená, že jednotlivci a firmy musí hlásit zisky z obchodování s kryptoměnami a zaplatit příslušné daně. Daňové úřady již přijaly opatření k tomu, aby začaly sledovat kryptoměnové transakce a zajistily jejich veškeré zdanění.[35]

Ruské burzy mají omezený přístup k obchodování s kryptoměnami, neboť nejsou plně regulovány. Zákon č. 259-FZ umožňuje vydávání digitálních finančních aktiv, ale Initial Coin Offerings (ICO) a kryptoměnové burzy se stále nacházejí v šedé zóně, bez jasných pravidel a povolení. V praxi to znamená, že ICO a kryptoměnové burzy,

[34] *Financial Conduct Authority. Guidance on Cryptoassets*. 2021. [online]. [cit. 2025-12-18]. Dostupné z: https://www.fca.org.uk/publications/guidance-consultations/guidance-cryptoassets.
[35] REUTERS. *Russia’s central bank calls for blanket ban on cryptocurrencies*. 2021. [online]. [cit. 2025-12-18]. Dostupné z: https://www.reuters.com/technology/russias-central-bank-calls-blanket-ban-cryptocurrencies-2021-01-20/.

které působí na ruském trhu, čelí právní nejistotě. Ruská vláda a regulátoři stále hledají způsoby, jak kontrolovat kryptoměnové aktivity, zejména v oblasti prevence praní špinavých peněz a financování terorismu, což naznačuje, že ačkoliv kryptoměny nejsou v Rusku zakázány, jejich používání je striktně monitorováno a tím je značně omezeno jejich širší využití.[36]

[36] REUTERS. *Russia's central bank calls for blanket ban on cryptocurrencies*. 2021. [online]. [cit. 2025-12-18]. Dostupné z: https://www.reuters.com/technology/russias-central-bank-calls-blanket-ban-cryptocurrencies-2021-01-20/.

5 Ponziho schémata a pyramidové systémy

Ponziho schémata a pyramidové systémy jsou dva typy podvodných finančních modelů, které často slibují vysoké výnosy za krátký čas a přitahují lidi na základě nereálných očekávání. I když se mohou zdát podobné, existují mezi nimi rozdíly. V obou případech však není zisk generován z reálných investic, ale z peněz nově přicházejících účastníků. Ponziho schéma je podvod, při kterém organizátor platí výnosy starším investorům penězi od nových účastníků, místo toho, aby generoval reálný zisk z investic. Tento systém se zhroutí, jakmile přestane přibývat nových investorů.[37]

Pyramidový systém je podobný Ponziho schématu v tom, že je také závislý na neustálém přísunu nových účastníků. Rozdíl spočívá v tom, že každý účastník je odměňován za to, že přivede do systému další účastníky. Každý nově příchozí platí poplatek, který jde těm, kteří jsou nad ním v pyramidě. I tento systém je neudržitelný, protože se nakonec vyčerpá počet lidí ochotných vstoupit do systému.[38]

5.1 Definice Ponziho schématu

Jedná se o finanční podvod, při kterém jsou starším investorům vypláceny zisky z prostředků nově příchozích účastníků, nikoliv z reálných výnosů či zisků investiční činnosti. Tím, že starší investoři obdrží slíbené výnosy, systém vytváří iluzi legitimity a stabilního výnosu, čímž přitahuje další nové investory. Ve skutečnosti ale žádná reálná investice neprobíhá – veškeré peníze cirkulují pouze mezi investory.[39]

Základní princip spočívá v tom, že funguje pouze tak dlouho, dokud je dostatek nových účastníků, kteří do systému vkládají své prostředky. Jakmile se zastaví přísun nových peněz, systém se zhroutí, protože organizátoři nejsou schopni vyplatit výnosy všem dříve zúčastněným investorům. Schéma je pojmenováno po Charlesi Ponzim, který se tímto podvodem proslavil na počátku 20. století, i když podobné systémy existovaly i dříve. Ponzi sliboval investorům vysoké zisky z obchodování s mezinárodními poštovními kupony, ale ve skutečnosti jejich peníze nepoužíval k žádné reálné činnosti. Místo toho je přerozděloval mezi starší investory, čímž vytvořil iluzi

[37] FRANKEL, T. *The Ponzi scheme puzzle: a history and analysis of con artists and victims*. New York, NY: Oxford University Press, 2012. ISBN 0199926611.
[38] Tamtéž
[39] *Introduction to Investing: Ponzi Schemes.* [online]. U.S. Securities and Exchange Commission. Dostupné z: https://www.investor.gov/introduction-investing/investing-basics/glossary/ponzi-schemes [cit. 2025-12-15].

ziskovosti. Hlavním rysem bylo udržování iluze stabilních a vysokých výnosů, které nebyly podloženy skutečnou ekonomickou činností, ale pouze průběžným přísunem nových peněz.[40]

5.1.1 Příklady Ponziho schémat

Ponziho schémata mají dlouhou historii, a i když jejich princip zůstává stejný, přizpůsobují se moderním technologiím a prostředím, jako je například svět kryptoměn. Několik známých příkladů Ponziho schémat, včetně těch v kryptoměnách, ilustruje, jakým způsobem podvodníci využívají důvěry investorů.

BitConnect byl jedním z nejznámějších kryptoměnových Ponziho schémat. Od svého vzniku v roce 2016 lákal investory na slib denních výnosů až 1 % z investice, což vedlo k nereálně vysokým ročním ziskům. BitConnect tvrdil, že jeho výnosy byly generovány „robotickým obchodováním“, které údajně využívalo volatilitu kryptoměnového trhu. Ve skutečnosti však výnosy vyplácel prostřednictvím nových příspěvků od dalších investorů. V roce 2018 se schéma zhroutilo a investoři přišli o miliardy dolarů.[41]

OneCoin je dalším příkladem podvodu, který fungoval na tomto principu. Tvrdil, že vyvíjí revoluční kryptoměnu, která má překonat Bitcoin, a investoři mohli nakupovat vzdělávací balíčky, jež zahrnovaly i tokeny pro těžbu OneCoinu. Žádná skutečná kryptoměna, ale neexistovala a peníze nových investorů byly použity k vyplácení starších členů. Projekt získal miliardy dolarů od investorů po celém světě, než byl podvod odhalen a organizátoři byli zatčeni.[42]

Bernard Madoff provozoval jedno z největších Ponziho schémat v historii, které zasáhlo tisíce investorů, včetně velkých institucí, a trvalo více než dvě desetiletí. Madoff sliboval stabilní výnosy bez ohledu na tržní podmínky, přičemž výnosy vyplácel z peněz

[40] *Introduction to Investing: Ponzi Schemes.* [online]. U.S. Securities and Exchange Commission. Dostupné z: https://www.investor.gov/introduction-investing/investing-basics/glossary/ponzi-schemes [cit. 2025-12-15].
[41] *BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme.* Online. Justice.gov. 2024, 25.2.2022. [cit. 2025-12-15]. Dostupné z: https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.
[42] RASURE, E., PEREZ, Y. *What Happened to OneCoin, the $4 Billion Crypto Ponzi Scheme?* Online. Investopedia. 2024, 9.3.2024. Dostupné z: https://www.investopedia.com/terms/o/onecoin.asp. [cit. 2025-12-15].

nových investorů. Celková výše podvodu se odhaduje na 65 miliard dolarů, což z Madoffova případu činí jeden z největších finančních podvodů v historii.[43]

5.1.2 Varovné signály Ponziho schémat

Ponziho schémata se mohou na první pohled jevit jako atraktivní investiční příležitosti, ale existuje několik charakteristických varovných signálů, které mohou naznačovat, že jdeo podvod. Jedním z nejčastějších znaků jsou nereálně vysoké a stabilní výnosy, které jsou slibovány bez ohledu na tržní podmínky. Legitimní investice vždy zahrnují určitou míru rizika, takže příslib „garantovaných" vysokých zisků v krátkém čase by měl vyvolat podezření. [44]

Dalším varovným signálem je nedostatek informací o tom, jak se s penězi investorů nakládá. Pokud neexistuje jasné vysvětlení, do čeho jsou peníze investovány nebo jakým způsobem generuje projekt zisk, je to další varovný signál. Investoři by měli mít přístup k podrobným informacím o investiční strategii a obchodních modelech projektu. Ponziho schémata také často vytvářejí tlak na přivádění nových investorů, přičemž nabízejí bonusy nebo provize za přivedení nových členů. Pokud je hlavním zdrojem příjmů přísun nových účastníků, pravděpodobně se jedná o podvod. To je také typické pro pyramidové systémy, do nichž účastníci musí přivádět nové lidi, aby vydělali. Varovný signál představuje i anonymita nebo neprůhlednost týmu, který projekt organizuje. U legitimních investičních projektů je běžné, že tým je veřejně známý a má ověřitelnou profesní historii. Naopak, pokud je obtížné zjistit, kdo za projektem stojí, nebo pokud jsou organizátoři anonymní, zvyšuje to riziko podvodu.[45]

Ponziho schémata také často stanovují komplikované nebo nejasné podmínky výběru zisků, například mohou omezovat výběry pouze na určité období nebo nastavovat další překážky. Tímto způsobem organizátoři prodlužují životnost systému a oddalují jeho kolaps. Pokud projekt nastavuje nestandardní pravidla pro výběry, je dobré být obezřetný. V případě, že projekt není regulován nebo podléhá pouze minimálním regulacím, zvyšuje se opět riziko podvodu. Většina legitimních investičních projektů

[43] IACURCI, G. *Ponzi schemes hit highest level in a decade, hinting next 'investor massacre' may be near.* CNBC, 11 Feb. 2020 [cit. 2026-02-20]. Dostupné z: https://www.cnbc.com/2020/02/11/ponzi-schemes-hit-the-highest-level-in-10-years.htm

[44] FRANKEL, T. *The Ponzi scheme puzzle: a history and analysis of con artists and victims*. New York, NY: Oxford University Press, 2012. ISBN 0199926611.

[45] Tamtéž

podléhá regulačnímu dohledu, což poskytuje určitou míru ochrany investorům. Neregulované projekty, zejména v oblasti kryptoměn, mohou podvodníci snadno využít kvůli nedostatku dohledu. Upozornění na tyto varovné signály může pomoci investorům rozpoznat potenciální podvody a chránit své investice.[46]

[46] FRANKEL, T. *The Ponzi scheme puzzle: a history and analysis of con artists and victims*. New York, NY: Oxford University Press, 2012. ISBN 0199926611.

6 Falešné ICO a podvodné projekty

Initial Coin Offerings (ICO) neboli falešná ICO jsou jednou z metod, jak podvodníci lákají peníze od lidí, kteří chtějí investovat do nových kryptoměn. ICO je způsob, jakým projekty získávají finance na svůj rozvoj. Funguje to tak, že lidé vloží své peníze do projektu výměnou za nově vytvořené tokeny nebo kryptoměny s nadějí, že jejich hodnota v budoucnu vzroste. Tento proces se dá přirovnat ke sbírce peněz, kdy projekt od lidí získává prostředky na svůj rozvoj. Problém je, že některá ICO jsou falešná a žádný skutečný projekt za nimi neexistuje. Podvodníci slibují velké výnosy a průlomové technologie, ale jakmile vyberou dostatek peněz, zmizí a investoři o své prostředky přijdou. [47]

Falešná ICO a jejich fungování

Falešná ICO fungují na principu přilákání co největšího množství investorů. Projekt slibuje revoluční technologie, vysoké výnosy nebo jiné benefity. Obvykle začíná tím, že vytvoří atraktivní a profesionálně vypadající webové stránky, na kterých vytvořený projekt prezentuje svůj plán. Často nabízí takzvaný „whitepaper“ (technický dokument), který popisuje jejich cíle, plány a způsob fungování. Vše bývá navrženo tak, aby projekt působil seriózně a důvěryhodně. Ve skutečnosti však za tímto projektem často nestojí žádný reálný produkt ani technologie. Podvodníci vyzívají investory, aby vložili své peníze výměnou za tokeny nebo kryptoměnu, u které slibují růst a budoucí zisky. Investoři následně posílají do projektu své prostředky, obvykle ve formě kryptoměn jako Bitcoin nebo Ethereum, s vidinou zisku, ale žádné zisky se nedostaví, protože podvodníci se všemi prostředky zmizí.[48]

Tyto falešné projekty mohou trvat různě dlouho. Některé z nich sbírají peníze měsíce a působí dojmem serióznosti, jelikož pravidelně komunikují s investory, zatímco jiné zmizí hned po získání dostatečného množství prostředků. Tyto podvody jsou často označovány jako tzv. exit scam. Po dosažení cíle podvodníci náhle zmizí, zruší webové stránky a přestanou komunikovat. Falešná ICO často využívají rychlosti a anonymní

[47] HENNIGAN. R. (2021*). "Initial Coin Offerings: The Good, the Bad, and the Ugly."* Investopedia. [online] Dostupné z: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp [cit. 2025-12-17].
[48] Tamtéž

povahy kryptoměnových transakcí, což jim umožňuje rychle zmizet beze stopy. Investoři nemají možnost je vyhledat ani donutit přijmout odpovědnost.

6.1 Příklady podvodných projektů

V historii kryptoměn existuje několik notoricky známých falešných ICO, které přilákaly tisíce investorů a v konečném důsledku způsobily značné ztráty. Tyto podvody byly často dobře promyšleny a využívaly především důvěry investorů, kteří se těšili na velké výnosy.

Pincoin a iFan

Toto jsou dva propojené kryptoměnové podvody, které v roce 2018 společně přilákaly od investorů zhruba 660 milionů dolarů. Obě ICO byla organizována stejnou vietnamskou společností Modern Tech a slibovala obrovské výnosy. Pincoin tvrdil, že jde o investici s vysokými zisky, zatímco iFan byl prezentován jako sociální síť. Po úspěšném vybrání prostředků firma zmizela a investoři zůstali bez jakýchkoli prostředků či vysvětlení.[49]

Centra Tech

Centra Tech je dalším známým příkladem falešného ICO, které získalo asi 32 milionů dolarů. Projekt měl podporu známých osobností, jako například boxera Floyda Mayweathera, a tvrdil, že nabízí debetní karty, které umožní uživatelům provádět platby kryptoměnami. Později se ukázalo, že projekt neměl žádné reálné produkty a organizátoři byli obviněni z podvodu.[50]

OneCoin

I když OneCoin nebyl přesně klasickým ICO, šlo o významný kryptoměnový podvod, který přilákal miliardy dolarů. Projekt tvrdil, že vyvíjí revoluční kryptoměnu, která předčí Bitcoin, ale ve skutečnosti šlo o Ponziho schéma. Investoři mohli nakupovat vzdělávací balíčky, které údajně zahrnovaly OneCoin tokeny, ale žádná kryptoměna

[49] XIAO, Y., ZHANG, N., LIU, Y. *Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites*. arXiv. 2020.

[50] U.S. SECURITIES AND EXCHANGE COMMISSION. *SEC Charges Centra Tech Co-Founders in Fraudulent ICO* [online]. 2018 [cit. 2026-01-03]. Dostupné z: https://www.sec.gov/news/press-release/2018-53

neexistovala. Zakladatelé projektu zmizeli s obrovským množstvím peněz, než byl podvod odhalen.[51]

Tyto příklady ukázaly, jak dobře mohou být podvodné projekty propracovány a jak snadno mohou oklamat i zkušené investory například příslibem vysokých zisků, inovativních technologií, podporou známých osobností, jednoduše vším, co přitahuje důvěru veřejnosti.

6.2 Varovné signály falešných ICO

Rozpoznání podvodných projektů před investováním peněz je klíčové pro ochranu financí. I když mohou na první pohled vypadat seriózně a přitažlivě, existují určité varovné příznaky, které mohou signalizovat, že se jedná o podvod. Jedním z nejzřetelnějších varovných signálů je příslib extrémně vysokých výnosů v krátkém časovém období. Kryptoměnové trhy jsou velmi volatilní, a proto žádný seriózní projekt nemůže garantovat stabilní zisky, zvláště ve výši stovek nebo tisíců procent. Pokud projekt slibuje jisté a vysoké výnosy, je to důvod k obezřetnosti. Varovným signálem je nedostatek transparentnosti ohledně týmu, který za projektem stojí. Podvodné ICO často skrývají identitu svých zakladatelů a týmu, což může naznačovat, že se podvodníci snaží uniknout zodpovědnosti. Ověřitelný tým s profesionálním zázemím je jedním ze základních ukazatelů důvěryhodného projektu. Skutečný projekt by měl mít jasně definovaný produkt nebo službu, na které pracuje. Podvodná ICO však často nabízejí pouze sliby a vize bez jakéhokoli funkčního prototypu nebo reálné ukázky technologie. Pokud projekt nemá žádné hmatatelné výsledky a prezentuje pouze nejasné plány do budoucna, je třeba být na pozoru.[52]

Dalším důležitým faktorem je kvalita whitepaperu. Tento technický dokument by měl podrobně vysvětlovat, jak projekt funguje, jaké má cíle a jakými prostředky hodlá těchto cílů dosáhnout. U falešných ICO bývá whitepaper často plný obecných frází, technického žargonu a slibů, které nelze podložit reálnými důkazy. Absence regulace nebo neregulované prostředí také může naznačovat potenciální podvod. Falešná ICO často působí v jurisdikcích, kde není žádná nebo jen minimální regulace. Naopak legitimní projekty se zpravidla snaží pracovat v souladu s právními předpisy,

[51] XIAO, Y., ZHANG, N., LIU, Y. *Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites.* arXiv. 2020.
[52] BURNISKE, C., TATAR, J**.** *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond.* New York: McGraw-Hill Education, 2017. ISBN 978-1260026672.

což poskytuje určitou úroveň ochrany investorů. Pokud projekt otevřeně ignoruje nebo se vyhýbá regulacím, zvyšuje to riziko podvodu.

Agresivní marketingové strategie a tlak na rychlé investice mohou být dalším varovným signálem. Falešná ICO často používají klamavé reklamy a snaží se přimět investory k rychlému rozhodnutí pomocí omezených časových nabídek, které vytvářejí pocit naléhavosti. Tento tlak na rychlou investici je dalším důvodem k obezřetnosti. Pokud investor narazí na kterýkoli z těchto varovných příznaků, měl by být velmi opatrný a důkladně prozkoumat projekt předtím, než se rozhodne investovat.[53]

[53] BURNISKE, C., TATAR, J**.** *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond.* New York: McGraw-Hill Education, 2017. ISBN 978-1260026672.

7 Phishing a malware

Phishing a malware jsou dvě z nejběžnějších technik, které kyberzločinci používají k získání přístupu k osobním údajům a kryptoměnovým prostředkům investorů. V kryptoměnovém světě jsou tyto techniky často cíleny na uživatele, kteří nevěnují dostatečnou pozornost zabezpečení svých účtů a peněženek. Phishing zahrnuje oklamání uživatele s cílem odhalit jeho přihlašovací údaje nebo privátní klíče. Malware je škodlivý software, který může infikovat zařízení oběti a získat přístup k citlivým informacím.

Obě techniky jsou záludné v tom, že je obtížné je rozpoznat, zvláště pokud útočníci napodobují legitimní služby a používají sofistikované techniky. Tento typ podvodu má většinou devastující dopad, protože útočníci získají přístup ke kryptoměnové peněžence a mohou snadno převést všechny prostředky a uživatel je prakticky bez šance získat je zpět.[54]

Způsob fungování phishingu

Phishing je forma kybernetického útoku, při kterém se útočník snaží obelstít oběť a získat citlivá data, jako jsou přihlašovací údaje, hesla nebo privátní klíče ke kryptoměnovým peněženkám. Útoky v kryptoměnovém světě jsou velmi nebezpečné, protože pokud útočník získá přístup k privátním klíčům nebo účtům na kryptoměnových burzách, může rychle a nevratně převést všechny prostředky na svůj účet.[55]

Tyto podvody se často provádějí prostřednictvím e-mailů. Útočníci posílají zprávy, které vypadají jako zprávy od důvěryhodných zdrojů, například kryptoměnových burz nebo peněženek. E-maily často obsahují odkazy na falešné webové stránky, které se tváří jako legitimní, ale jejich cílem je získat přihlašovací údaje oběti. Další variantou těchto útoků jsou falešné webové stránky. Útočníci vytvářejí kopie skutečných webů kryptoměnových burz nebo peněženek. Pokud se oběť na takovou stránku přihlásí, poskytne útočníkům své přihlašovací údaje, které jsou následně zneužity.

Útočníci v současné době také využívají sociální sítě a různou formu falešné zákaznické podpory. Napodobují zákaznickou podporu na sociálních sítích a předstírají,

[54] CHECK POINT RESEARCH. *The Rising Threat of Phishing Attacks with Crypto Drainers* [online]. 2023 [cit. 2025-12-17]. Dostupné z: https://research.checkpoint.com/the-rising-threat-of-phishing-attacks-with-crypto-drainers/.
[55] *Phishing*. Online. Eset. 2024, 2024. Dostupné z: https://www.eset.com/cz/phishing/. [cit. 2025-12-15].

že pomáhají uživatelům vyřešit jejich problémy. Během této „pomoci“ získávají citlivé informace. V některých případech mohou vytvářet falešné aplikace pro správu kryptoměnových peněženek nebo burz, které mají za cíl získat přihlašovací údaje od uživatele.[56] Tyto útoky jsou značně nebezpečné, protože se velmi dobře maskují jako legitimní komunikace. Oběti si často neuvědomí, že byly podvedeny, dokud už není příliš pozdě a jejich kryptoměnové prostředky jsou pryč.

7.1 Typy malwaru

Malware představuje škodlivý software, který útočníci využívají k nelegálnímu přístupu k počítačům nebo k jiným digitálním zařízením obětí. V kryptoměnovém prostředí může malware sloužit k odcizení privátních klíčů, přihlašovacích údajů nebo k těžbě kryptoměn na zařízeních obětí bez jejich vědomí.[57] Existuje několik typů malwaru, které jsou specificky zaměřeny na kryptoměny.

Keylogger je typ malwaru, který zaznamenává veškeré úhozy na klávesnici oběti. Útočníci pak mohou tyto záznamy analyzovat s cílem získat přihlašovací údaje ke kryptoměnovým burzám nebo peněženkám. Keylogger může být na zařízení nainstalován, aniž by si toho oběť všimla, například prostřednictvím škodlivé přílohy v e-mailu nebo falešné aktualizace softwaru. [58]

Dalším významným typem je **ransomware**, což je malware, který zašifruje data na zařízení oběti a vyžaduje výkupné, obvykle v kryptoměnách, výměnou za dešifrovací klíč. Tento typ útoku může být devastující, protože oběti nemají přístup ke svým datům, dokud nezaplatí útočníkům. Ransomware útoky se často zaměřují na organizace, ale mohou být použity i proti jednotlivcům.[59]

Cryptojacking je další forma malwaru, která využívá výpočetní výkon zařízení oběti k těžbě kryptoměn, aniž by o tom uživatel věděl. Tento typ útoku většinou způsobí

[56] CHECK POINT RESEARCH. *The Rising Threat of Phishing Attacks with Crypto Drainers* [online]. 2023 [cit. 2025-12-17]. Dostupné z: https://research.checkpoint.com/the-rising-threat-of-phishing-attacks-with-crypto-drainers/.
[57] ABDELHAMID, N., AISSANI, D., BENMOUSSA, F. *Mitigation strategies against phishing attacks: A comprehensive review.* Computers & Security. 2023. DOI: 10.1016/j.cose.2023.103392.
[58] VERMA, R. DAS, A. *Malicious URL detection using machine learning: A survey*. arXiv. 2017
[59] YLI-HUMMO, J. KO, D., CHOI, S., PARK, S., SMOLANDER, K. *Security of cryptocurrencies: A systematic literature review*. IEEE Access. 2023.

zpomalení výkonu počítače nebo mobilního zařízení, protože veškerý jeho výkon je skrytě používán k těžbě kryptoměn pro útočníka.[60]

Trojan neboli **trojský kůň**, je software, který se tváří jako legitimní aplikace, ale po instalaci na zařízení umožňuje útočníkům vzdálený přístup. V kryptoměnovém světě může být Trojan použit k získání přístupu k peněženkám nebo burzovním účtům. Útočníci mohou okamžitě převést kryptoměnu pryč bez vědomí oběti.[61]

Clipboard malware je specifický typ malwaru, který sleduje, co uživatel kopíruje do schránky. Pokud uživatel zkopíruje adresu kryptoměnové peněženky, malware ji může zaměnit za adresu peněženky útočníka, což znamená, že když uživatel vloží tuto adresu při odesílání kryptoměn, prostředky budou poslány na adresu podvodníka. Malware tedy představuje zákeřnou hrozbu, neboť často pracuje na pozadí bez vědomí uživatele, a způsobuje značné škody, pokud si uživatel neuvědomí, že jeho zařízení bylo infikováno.[62]

Strategie prevence a eliminace rizik phishingu a malwaru

Zabezpečení v rámci kryptoměnového ekosystému je v odborném diskurzu definováno jako prioritní determinant ochrany digitálních aktiv. Vzhledem k faktu, že kompromitace privátních klíčů či autentizačních údajů vede k ireverzibilní (nenávratné) ztrátě prostředků, jsou tyto hrozby klasifikovány jako kritická bezpečnostní rizika. Odborná literatura v této souvislosti akcentuje význam synergie technických a organizačních opatření, která je považována za klíčový faktor pro signifikantní snížení pravděpodobnosti úspěšné realizace kybernetického útoku. [63]

7.2 Mechanismy prevence a eliminace rizik phishingových útoků

Phishingové útoky jsou v odborné literatuře identifikovány jako jeden z primárních vektorů kybernetické kriminality, směřující k nelegálnímu získávání autentizačních údajů a privátních klíčů v prostředí digitálních aktiv. Dostupné studie

[60] RICO, J. *What is Cryptojacking*? [online]. 2024 [cit. 2025-12-17]. Dostupné z: https://www.cybersecurityguide.org/cryptojacking/
[61] WEBGLOBE. *Co je Trojský kůň (Trojan virus) a co v počítači způsobuje?* [online]. [cit. 2025-12-17]. Dostupné z: https://www.webglobe.cz/co-je-trojski-kun-trojan-virus-a-co-v-pocitaci-zpusobuje
[62] SAHOO, D., LIU, C., HOI, S. C. H. *High accuracy phishing detection based on convolutional neural networks*. arXiv. 2020.
[63] HADNAGY, C. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.

v této souvislosti definují verifikaci URL adres a kontrolu šifrovaného HTTPS spojení jako základní parametry pro posouzení integrity webových rozhraní. Vzhledem k častému využívání technik typu typosquatting (registrace domén s vizuálně podobným názvem) je systematická analýza adresního řádku v teoretických modelech bezpečnosti považována za nezbytný prvek preventivní strategie.[64]

Elektronická pošta představuje klíčový distribuční kanál pro phishingové kampaně a šíření škodlivého kódu. Schopnost identifikace anomálií v nevyžádaných zprávách a eliminace interakce s neověřeným obsahem jsou literaturou označovány za kritické komponenty individuální prevence. Součástí komplexního bezpečnostního rámce je dekonstrukce principů sociálního inženýrství, které tvoří psychologický fundament pro manipulativní techniky využívané k extrakci citlivých dat. [65]

Integrace technických instrumentů s organizačními postupy, především pak s edukací uživatelů, vede k prokazatelnému posílení celkové odolnosti proti kybernetickým hrozbám. Současný stav poznání potvrzuje, že tato multidimenzionální strategie představuje vysoce efektivní nástroj pro mitigaci rizik a ochranu finančních prostředků v kryptoměnovém ekosystému.[66]

7.3 Technické a softwarové nástroje pro zmírňování malwarových hrozeb

Antivirový software je v odborném kontextu definován jako elementární instrumentárium určené k detekci a eliminaci různorodých forem škodlivého kódu, zejména keyloggerů a trojských koňů. Výzkumné poznatky potvrzují, že systematická aktualizace bezpečnostních programů, operačních systémů a aplikačního vybavení signifikantně zvyšuje detekční schopnosti systémů a minimalizuje riziko kompromitace datové integrity.[67]

V kontextu hrozeb typu ransomware je jako vysoce efektivní preventivní mechanismus identifikováno pravidelné zálohování dat, přičemž separace záložních kopií

[64]SEZNAM.CZ. *Protokol HTTPS* [online]. [cit. 2025-12-28]. Dostupné z: https://napoveda.seznam.cz/cz/fulltext-hledani-v-internetu/protokol-https/
[65] HADNAGY, C. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.
[66]SEZNAM.CZ. *Protokol HTTPS* [online]. [cit. 2025-12-28]. Dostupné z: https://napoveda.seznam.cz/cz/fulltext-hledani-v-internetu/protokol-https/
[67] *Mitigation strategies against the phishing attacks.* ScienceDirect [online], 2023 [cit. 2026-03-06]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167404823002973

od primárního zařízení snižuje pravděpodobnost ireverzibilní ztráty informací v důsledku kryptografického útoku. Teoretické rámce zdůrazňují, že integrace procesů zálohování s aktivní antivirovou ochranou představuje klíčový pilíř komplexní strategie zajištění dat před malwarovými hrozbami.

Pro správu a uchovávání kryptoměnových aktiv jsou v odborné literatuře hardwarová úložiště (tzv. cold wallets) klasifikována jako bezpečnější alternativa k softwarovým řešením. Tato distinkce vyplývá z principu offline uchovávání privátních klíčů, což zásadně limituje možnosti neoprávněné exfiltrace citlivých údajů v případě infikace hostitelského zařízení malwarem. [68]

Nedílnou součástí robustní bezpečnostní strategie je rovněž validace provenience (původu) softwaru a instalovaných aplikací. Distribuce a stahování programů z neověřených zdrojů je identifikována jako kritický vektor pro šíření malwaru, který může ohrozit technickou integritu zařízení i bezpečnost kryptoměnových účtů. Dostupná literatura potvrzuje, že teprve synergie aktivní antivirové ochrany, důsledného ověřování zdrojů a využití hardwarových prvků pro správu klíčů tvoří základ komplexní ochrany aktiv v digitálním prostředí. [69]

[68] *Mitigation strategies against the phishing attacks*. ScienceDirect [online], 2023 [cit. 2026-03-06]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167404823002973
[69] Tamtéž

8 Sociální inženýrství a manipulace

Sociální inženýrství a manipulace jsou techniky, které jsou kyberzločinci využívány k tomu, aby podvedli vytipované oběti a přiměli je k tomu, aby jim samy poskytly citlivé informace, popřípadě udělaly to, co zločinci potřebují. V kryptoměnovém světě jsou tyto praktiky obzvlášť nebezpečné, protože mohou vést ke ztrátě peněženek, přihlašovacích údajů nebo přímému převodu kryptoměn bez možnosti jejich vrácení.

Sociální inženýrství zahrnuje různé formy manipulace, které často využívají důvěru, nevědomost nebo psychologické slabiny oběti. Útočníci mohou například předstírat, že jsou pracovníci technické podpory, přátelé nebo legitimní autority, aby oběti přesvědčili k provedení určitých akcí.[70]

Definice sociálního inženýrství

Sociální inženýrství je forma podvodu, při které útočník zmanipuluje oběť tak, aby mu dobrovolně poskytla citlivé informace, provedla určitou akci nebo otevřela přístup k zabezpečeným systémům. Místo využití technických zranitelností se útočníci zaměřují na lidský faktor, protože je často snadnější podvést člověka než prolomit technickou bezpečnost.

V kryptoměnovém světě to znamená, že útočník může například oběť přesvědčit, aby mu poskytla privátní klíče ke své kryptoměnové peněžence, přihlašovací údaje k burzám nebo dokonce přímo odeslala kryptoměny na účet podvodníka. Sociální inženýrství je obzvláště účinné, protože většina uživatelů nemusí být dostatečně obezřetná nebo technicky zdatná, aby rozpoznala pokus o manipulaci. Zatímco technické útoky (např. hacking) jsou založené na využití slabin v softwaru nebo hardwaru, sociální inženýrství pracuje s lidskými emocemi a důvěrou. Útočník často vystupuje jako někdo důvěryhodný nebo autoritativní, aby získal přístup k citlivým informacím.[71]

8.1 Hlavní techniky sociálního inženýrství

Útočníci využívající sociální inženýrství mají k dispozici různé metody, jak manipulovat své oběti. V kryptoměnovém prostředí tyto techniky často zahrnují

[70] HADNAGY, C. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.
[71] Tamtéž

získávání přihlašovacích údajů, privátních klíčů nebo přímou manipulaci obětí k odeslání kryptoměn. Níže jsou uvedeny nejčastěji používané techniky sociálního inženýrství.

Phishing je jednou z nejběžnějších forem sociálního inženýrství, při které jsou citlivé údaje, jako jsou přihlašovací informace, čísla platebních karet nebo privátní klíče, podvodně získávány útočníky. Často jsou rozesílány falešné e-maily, které se tváří jako legitimní zprávy od kryptoměnových burz, peněženek nebo jiných důvěryhodných zdrojů. Oběti jsou následně přesměrovány na falešné webové stránky, na kterých jsou požadovány jejich citlivé informace, a ty jsou následně zneužívány. V případě cílenější formy phishingu, označované jako spear phishing, jsou e-maily a komunikace přizpůsobeny přímo na konkrétní oběti nebo organizaci. Na rozdíl od běžného phishingu je zde často využíváno podvržení identity známé osoby nebo kolegy, což zvyšuje pravděpodobnost úspěchu podvodu.[72]

Další technikou je **pretexting**. Jedná se o vytvoření falešného příběhu s cílem získat důvěru oběti. Útočníci předstírají, že jsou zaměstnanci burzy nebo technické podpory a žádají o potvrzení totožnosti či přístupových údajů, aby byl obnoven přístup k účtu. Tento falešný scénář přiměje oběť k poskytnutí citlivých informací.

Vishing, neboli hlasový phishing, je další technika, při níž jsou oběti telefonicky kontaktovány útočníky, kteří se vydávají za zástupce kryptoměnové burzy nebo peněženky. Bývá požadována například aktualizace hesla nebo potvrzení přihlašovacích údajů, přičemž telefonní hovor často působí naléhavěji než e-mailová komunikace.[73]

V případě **baitingu** je obětem nabídnuto něco lákavého, například „bonus“ nebo „dárek“ ve formě kryptoměn, pokud splní určitou akci. Tyto nabídky často zahrnují falešné investiční příležitosti nebo podvodné „giveaways“. Oběti jsou přesvědčeny, aby odeslaly kryptoměny s příslibem vyššího zisku.[74]

Tailgating je technika využívaná ve fyzickém prostoru. Útočníkovi je umožněn přístup do zabezpečených míst, například do kanceláře, kde jsou uloženy citlivé údaje. I když tato metoda není v kryptoměnovém světě tak častá, může být použita k získání přístupu na pracoviště kryptoměnových burz. Ve všech těchto případech jsou lidská

[72] HADNAGY, C. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.
[73] Tamtéž
[74] Tamtéž

důvěra a nevědomost zneužívány k tomu, aby oběti poskytly útočníkům citlivé informace nebo provedly kroky vedoucí ke ztrátě kryptoměn či přístupu k účtům.[75]

8.1.1 Psychologické principy

Úspěch sociálního inženýrství závisí na manipulaci s lidskými emocemi a chováním. Útočníci využívají několik klíčových psychologických principů, které zvyšují pravděpodobnost, že oběť udělá to, co útočník potřebuje. Tyto principy jsou často založeny na rychlém rozhodování, důvěře nebo strachu. Lidé mají přirozený sklon poslouchat autority, což je často zneužíváno útočníky, kteří se vydávají za zástupce důvěryhodných institucí, jako jsou banky, kryptoměnové burzy nebo dokonce vláda. Pokud je předstírán status autority, je pravděpodobné, že budou získány citlivé údaje. Příkladem může být situace, kdy je oběť kontaktována osobou vydávající se za pracovníka zákaznické podpory kryptoměnové burzy a žádá o přihlašovací údaje k ověření účtu. V tomto případě se oběť podvolí, protože vnímá útočníka jako autoritu.[76]

Útočníky je často vytvářen pocit naléhavosti nebo strachu, což vede oběť k rychlému jednání bez přemýšlení. Bývá tvrzeno, že pokud není okamžitě provedena požadovaná akce, může dojít k uzamčení účtu nebo ztrátě prostředků. Tento pocit naléhavosti vede k tomu, že oběť jedná impulzivně, například když obdrží e-mail s varováním, že její kryptoměnový účet byl napaden, a je požádána, aby okamžitě změnila heslo. Strach ze ztráty způsobí, že oběť zadá své údaje právě na falešné stránce.[77]

Důvěra je dalším psychologickým faktorem, který útočníci využívají. Často se snaží získat důvěru oběti tím, že se vydávají za přátele, kolegy nebo důvěryhodné známé. Když si oběť myslí, že komunikuje s někým, komu může věřit, je ochotnější poskytnout citlivé informace. Příkladem je situace, kdy útočník skrze sociální sítě naváže kontakt s obětí, postupně si získá její důvěru, a nakonec požádá o peníze nebo kryptoměny pod záminkou „bezpečné investice."

Princip reciprocity je další technikou, kterou útočníci využívají. Lidé mají přirozenou tendenci oplácet laskavosti, a proto mohou být nabízeny falešné „bonusy"

[75] HADNAGY, C. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.
[76] Tamtéž
[77] MITNICK, K. D. & SIMON, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security.* Wiley. ISBN 978-0764518482.

nebo výhodné nabídky výměnou za přístup k citlivým informacím. Útočník může například nabídnout zázračný investiční nástroj zdarma, ale před jeho poskytnutím požádá o přihlašovací údaje nebo o zaslání malé částky kryptoměn.[78]

K manipulaci je často využíván také zvyk a rutina. Útočníci se mohou pokusit o útok v okamžiku, kdy oběť vykonává běžné činnosti, aby situace vypadala normálně. Příkladem může být e-mail, který se tváří jako běžné oznámení o transakci z burzy, kterou oběť pravidelně používá. Protože tento krok odpovídá rutině, oběť klikne na odkaz a zadá své údaje. Útočníci se snaží zneužít základní psychologické principy, jako jsou autorita, důvěra, strach, reciprocita a rutina, aby oběť zmanipulovali k rychlému a nekritickému rozhodování, což často vede ke ztrátě citlivých údajů nebo kryptoměn.[79]

8.2 Mechanismy a strategie eliminace rizik sociálního inženýrství

Prevence proti praktikám sociálního inženýrství je v odborném kontextu podmíněna synergií zvýšené ostražitosti, kritického myšlení a systematického přístupu k nakládání s citlivými údaji. Úspěšnost útoků je v literatuře často dávána do souvislosti s exploatací impulzivního chování nebo kognitivní nepozornosti uživatelů, což tvoří fundament pro úspěšnou realizaci útočných kampaní. [80]

Teoretické modely bezpečnosti identifikují jako primární pilíř ochrany kritickou evaluaci příchozích informací a důslednou verifikaci legitimity požadavků na sdílení citlivých dat. Standardizované procesy v rámci legitimizovaných organizací, včetně kryptoměnových platforem, striktně vylučují vyžadování autentizačních údajů či privátních klíčů mimo zabezpečené a ověřené kanály.[81]

Dvoufaktorová autentizace (2FA) představuje jednu z nejefektivnějších metod aktivní obrany, neboť i v případě kompromitace primárního hesla zůstává integrita účtu chráněna druhým faktorem, například jednorázovým kódem či hardwarovým tokenem. Odborné zdroje v tomto směru preferují využití specializovaných autentizačních aplikací

[78] MITNICK, K. D. & SIMON, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security.* Wiley. ISBN 978-0764518482.
[79] Tamtéž
[80] Tamtéž
[81] KOVÁŘ, P. *Zabezpečení online účtů: Moderní přístupy a technologie*. 1. vyd. Praha: XYZ Publishing, 2022. ISBN 978-80-123-4567-8.

(např. Google Authenticator) před SMS zprávami, které vykazují vyšší zranitelnost vůči útokům typu SIM swap.

Sociální sítě jsou identifikovány jako významný vektor pro manipulativní techniky, včetně impersonace (napodobování) známých osobností či autoritativních subjektů. Komunikace prostřednictvím neověřených platforem představuje riziko zneužití dat útočníky imitujícími oficiální podporu burz či poskytovatelů služeb, což v analytických studiích vede k doporučení striktní verifikace komunikačních zdrojů.[82]

Vizuální věrohodnost phishingových stránek, které jsou často k nerozeznání od legitimních rozhraní, zvyšuje nároky na technologickou ostražitost. Kontrola doménového jména a přítomnost šifrovaného spojení (HTTPS) jsou klasifikovány jako klíčové indikátory validity webové prezentace. Výzkumy potvrzují, že kombinace validace URL adres a zabezpečené komunikace signifikantně redukuje pravděpodobnost kompromitace přístupových údajů.[83]

Psychologický tlak vyvolaný pocitem naléhavosti je běžně využívaným nástrojem k vynucení nekritického jednání uživatelů. Analýza chování legitimizovaných služeb ukazuje, že tyto subjekty nevyužívají nátlakové techniky k okamžitému získávání dat či převodu aktiv, a tudíž je každý takový požadavek v bezpečnostních rámcích považován za rizikový indikátor.

Technická integrita koncových zařízení, zajištěná pravidelnou aktualizací operačních systémů a bezpečnostního softwaru, tvoří elementární technologickou bariéru. Exploatace neopravených zranitelností (vulnerabilit) v zastaralém softwaru je totiž v literatuře popsána jako standardní metoda pro instalaci škodlivého kódu a následnou exfiltraci dat.[84]

Celkově lze konstatovat, že integrace zvýšené ostražitosti, pokročilých autentizačních metod a důsledné verifikace online komunikace představuje komplexní strategii pro mitigaci rizik sociálního inženýrství. Hlubší porozumění metodice útočníků

[82] FURNELL, S. (2002). *Cybercrime: Vandalizing the information society*. Addison-Wesley. ISBN 978-0201721591.
[83] KOVÁŘ, P. *Zabezpečení online účtů: Moderní přístupy a technologie*. 1. vyd. Praha: XYZ Publishing, 2022. ISBN 978-80-123-4567-8.
[84] FURNELL, S. (2002). *Cybercrime: Vandalizing the information society*. Addison-Wesley. ISBN 978-0201721591.

a analytické hodnocení neověřených požadavků jsou vnímány jako klíčové determinanty bezpečnosti v digitálním prostředí.[85]

[85] FURNELL, S. (2002). *Cybercrime: Vandalizing the information society*. Addison-Wesley. ISBN 978-0201721591.

9 Návrhy opatření pro ochranu investorů

Vzhledem k tomu, že kryptoměnové trhy představují relativně nový a dynamicky se rozvíjející sektor, je nezbytné navrhnout účinná opatření pro ochranu investorů před podvody, zneužitím a ztrátou prostředků. Kryptoměnové podvody mohou mít závažné dopady na investory, kteří často nedisponují dostatečnými znalostmi pro identifikaci rizik spojených s tímto typem investic. Opatření zaměřená na zvýšení bezpečnosti kryptoměnových investorů zahrnují vzdělávací aktivity, posílení právní ochrany a implementaci technických řešení. [86]

Zvyšování povědomí a vzdělávání

Regulační orgány, kryptoměnové burzy a další poskytovatelé služeb mohou prostřednictvím osvětových kampaní vysvětlovat základní principy kryptoměn, rizika spojená s investicemi a varovné signály podvodů. Vzdělávací materiály by měly být koncipovány tak, aby byly srozumitelné jak pro začátečníky, tak pro zkušené investory, a poskytovaly informace o ochraně investorů, například o rozpoznávání falešných ICO, bezpečném uchovávání kryptoměnových peněženek a doporučených bezpečnostních postupech.[87]

Kromě tištěných či digitálních materiálů mohou kryptoměnové burzy pořádat školení a webináře, které účastníkům poskytují znalosti o bezpečném uložení privátních klíčů, používání hardwarových peněženek, nastavení dvoufaktorové autentizace a dalších klíčových bezpečnostních opatřeních. Vzdělávání by mělo zahrnovat i informace o právních předpisech a regulacích, aby investoři byli informováni o dostupných nástrojích ochrany svých práv.[88]

Podpora spolupráce mezi veřejným a soukromým sektorem je rovněž doporučována. Centrální banky, finanční úřady a kryptoměnové burzy mohou společně

[86] KEENAN, J. (2020). *Understanding cryptocurrency and its potential for financial fraud*. New York: Springer. ISBN 978-3030361232.
[87] KHAN, M. A. & ALI, F. (2023*). Cybersecurity in Cryptocurrency: Protecting Investors from Fraud. In Advancements in Cybersecurity and Digital Forensics* (pp. 33-50). New York: Springer. ISBN 978-i.cz/cs/1992-634
[88] ZOHAR, A., SIVAN, A. (2021). *Cryptocurrency and its regulatory implications: The impact on investors' rights and fraud prevention. In Advances in Digital Economy and E-Business* (pp. 45-62). London: Academic Press. ISBN 978-0128142237

zajišťovat aktuální a ověřené informace o investičních rizicích a bezpečnostních opatřeních, čímž se zvyšuje celková informovanost investorů.[89]

Zvyšování povědomí a vzdělávání se tak jeví jako zásadní nástroj ochrany investorů před podvody, protože znalosti o fungování kryptoměnových trhů a o preventivních opatřeních umožňují investorům lépe se chránit proti podvodným praktikám.[90]

9.1 Právní ochrana investorů

Právní ochrana je klíčovým mechanismem boje proti kryptoměnovým podvodům, zejména vzhledem k tomu, že kryptoměny a blockchainové technologie nejsou ve většině jurisdikcí plně regulovány, což komplikuje uplatnění práv investorů v případě podvodu. Postupně vznikají právní rámce a regulace zaměřené na zajištění transparentnosti kryptoměnových transakcí a zvýšení odpovědnosti poskytovatelů služeb.[91]

V mnoha zemích se uplatňují regulace typu „know your customer“ (KYC) a „anti-money laundering“ (AML), které vyžadují identifikaci investorů a monitorování podezřelých transakcí. Tato opatření snižují anonymitu podvodníků a umožňují efektivnější stíhání podvodných aktivit.[92]

Na úrovni mezinárodních regulací lze uvést například Markets in Crypto-Assets (MiCA) v Evropské unii nebo regulace SEC ve Spojených státech, jejichž cílem je zvýšit transparentnost kryptoměnových projektů a burz a tím minimalizovat riziko podvodů. Právní rámce také umožňují soudní postih podvodníků, ačkoli globální charakter kryptoměnových transakcí a anonymita útočníků mohou tento proces komplikovat. Přesto mezinárodní spolupráce a nové právní předpisy zvyšují pravděpodobnost dopadení a postihu pachatelů.

Například v USA Komise pro cenné papíry a burzy (SEC) podnikla právní kroky proti několika podvodným ICO projektům a burzám, které nedodržely zákonné

[89] KEENAN, J. (2020). *Understanding cryptocurrency and its potential for financial fraud*. New York: Springer. ISBN 978-3030361232.
[90] KHAN, M. A. & ALI, F. (2023). *Cybersecurity in Cryptocurrency: Protecting Investors from Fraud. In Advancements in Cybersecurity and Digital Forensics* (pp. 33-50). New York: Springer. ISBN 978-i.cz/cs/1992-634
[91] ZOHAR, A., SIVAN, A. (2021). *Cryptocurrency and its regulatory implications: The impact on investors' rights and fraud prevention. In Advances in Digital Economy and E-Business* (pp. 45-62). London: Academic Press. ISBN 978-0128142237
[92] Tamtéž

povinnosti. Vedle právní ochrany se v některých jurisdikcích objevují i pojišťovací produkty pro kryptoměnové investory, které poskytují kompenzaci v případě krádeže prostředků nebo podvodu. Kryptoměnové burzy a poskytovatelé peněženek mohou tyto produkty využít k doplnění ochrany investorů.[93]

V České republice hraje významnou roli zákon č. 634/1992 Sb., o ochraně spotřebitele, který umožňuje stíhat nekalé obchodní praktiky včetně klamavých aktivit kryptoměnových projektů. Tento právní nástroj zajišťuje, že spotřebitelé mají možnost uplatnit svá práva při podezření na podvod. ZOS

Celkově se právní rámce a regulace postupně zlepšují, což zvyšuje transparentnost a odpovědnost kryptoměnových projektů. I přes tyto pokroky je stále nezbytné, aby investoři disponovali znalostmi o rizicích a přijímali opatření pro ochranu svých prostředků. [94]

9.1.1 Analýza technologických instrumentů pro zabezpečení digitálních aktiv

Technologické instrumenty a ochranné mechanismy jsou v odborném diskurzu definovány jako klíčový prvek prevence kryptoměnových podvodů a zajištění integrity aktiv. Vzhledem k digitální povaze kryptoměn je technické zabezpečení považováno za fundamentální pro ochranu osobních údajů, autentizačních údajů a privátních klíčů. Implementace preventivních opatření umožňuje signifikantní minimalizaci rizik spojených s neoprávněnou exfiltrací prostředků.[95]

V rámci bezpečnostních standardů jsou hardwarová úložiště (tzv. cold wallets) identifikována jako vysoce efektivní metoda ochrany, neboť princip fyzické izolace privátních klíčů od sítě internetu zásadně redukuje povrch útoku. Technická řešení, jako jsou například zařízení Trezor nebo Ledger, neumožňují síťový přístup k citlivým údajům, čímž je v teoretických modelech bezpečnosti eliminována možnost kompromitace aktiv i v případě napadení hostitelského zařízení malwarem.

---

[93] ZOHAR, A., SIVAN, A. (2021). *Cryptocurrency and its regulatory implications: The impact on investors' rights and fraud prevention. In Advances in Digital Economy and E-Business* (pp. 45-62). London: Academic Press. ISBN 978-0128142237

[94] KEENAN, J. (2020). *Understanding cryptocurrency and its potential for financial fraud*. New York: Springer. ISBN 978-3030361232.

[95] KHAN, M. A. & ALI, F. (2023). *Cybersecurity in Cryptocurrency: Protecting Investors from Fraud. In Advancements in Cybersecurity and Digital Forensics* (pp. 33-50). New York: Springer. ISBN 978-i.cz/cs/1992-634

Významnou roli v rámci víceúrovňové ochrany hraje dvoufaktorová autentizace (2FA), která statisticky snižuje pravděpodobnost neoprávněného přístupu k uživatelským účtům. Tento mechanismus, vyžadující kromě statického hesla i sekundární dynamický faktor (např. kód z aplikace typu Google Authenticator nebo hardwarový token), představuje bariéru, která zůstává účinná i v případě prolomení primárních přihlašovacích údajů.[96]

Integrita přenosu informací je v kybernetickém prostoru podmíněna využitím šifrované komunikace, zejména při interakci s burzovními rozhraními či digitálními peněženkami. Protokoly jako HTTPS jsou v literatuře popsány jako nezbytný standard pro prevenci interceptingu (zachycení) citlivých dat během jejich tranzitu sítí.

Pokročilé metody zabezpečení, jako jsou multi-signature peněženky, představují další vrstvu ochrany založenou na distribuci odpovědnosti. Požadavek na verifikaci transakce více nezávislými klíči znamená, že kompromitace jediného privátního klíče není dostačující pro provedení nelegitimního převodu prostředků. Tento mechanismus je v odborných kruzích identifikován jako vysoce efektivní zejména pro subjekty s potřebou institucionální úrovně zabezpečení.[97]

Proces zajištění kontinuity a obnovitelnosti přístupu k aktivům je v teoretických rámcích úzce spojen s pravidelným zálohováním privátních klíčů a tzv. obnovovacích frází (seedů). Odborná rešerše zdůrazňuje nezbytnost offline uchovávání těchto záloh na fyzicky bezpečných místech pro eliminaci rizik spojených s kybernetickými útoky. Mnoho hardwarových řešení implementuje standardizované mechanismy obnovy, které umožňují rekonstrukci peněženky i v případě ztráty či poškození primárního hardwaru.[98]

Kritickou komponentou technologické obrany je systematická aktualizace softwarového vybavení. Kontinuální vývoj kryptoměnových platforem a burz zahrnuje pravidelné odstraňování bezpečnostních vulnerabilit (zranitelností). Teoretické modely předpokládají využívání aktuálních verzí softwaru i operačních systémů jako základní předpoklad funkční ochrany. V tomto kontextu je rovněž akcentován význam

[96] KHAN, M. A. & ALI, F. (2023). Cybersecurity in Cryptocurrency: Protecting Investors from Fraud. In Advancements in Cybersecurity and Digital Forensics (pp. 33-50). New York: Springer. ISBN 978-i.cz/cs/1992-634
[97] Tamtéž
[98] Tamtéž

antivirových programů a firewallů, které plní detekční funkci vůči malwaru či keyloggerům.[99]

Závěrem lze konstatovat, že integrace technologických instrumentů, jako jsou hardwarová úložiště, vícefaktorová autentizace, šifrování a distribuované potvrzování transakcí, vede k prokazatelnému snížení rizik krádeže digitálních aktiv. Komplexní přístup k těmto opatřením signifikantně zvyšuje rezistenci investic vůči dynamicky se vyvíjejícím hrozbám v kybernetickém prostoru. [100]

[99] KHAN, M. A. & ALI, F. (2023). *Cybersecurity in Cryptocurrency: Protecting Investors from Fraud*. In *Advancements in Cybersecurity and Digital Forensics* (pp. 33-50). New York: Springer. ISBN 978-3031290467

[100] Tamtéž

10 Průzkum a dotazníkové šetření

Dotazníkové šetření bylo zvoleno jako metoda sběru dat, protože nabízí efektivní způsob, jak získat cenné informace od většího počtu respondentů v relativně krátkém čase. Tato metoda umožňuje snadnou standardizaci otázek, což usnadňuje analýzu výsledků a porovnání odpovědí mezi různými skupinami. Dotazníky mohou být distribuovány online, což zvyšuje dostupnost a pohodlí pro respondenty a tím zvyšuje míru odpovědí. Tímto způsobem mohou být získány rozmanité názory a zkušenosti, což umožní lepší porozumění zkoumané problematiky a formulaci relevantních závěrů.

10.1 Analýza získaných dat

Získaná data byla analyzována na základě odpovědí celkem 207 respondentů, kteří vyplnili dotazník zaměřený na problematiku kryptoměn, jejich rizik a podvodných praktik v tomto prostředí. Odpovědi respondentů byly následně zpracovány pomocí tabulkového procesoru Microsoft Excel, kde byly vytvořeny souhrnné tabulky a grafické znázornění jednotlivých výsledků.

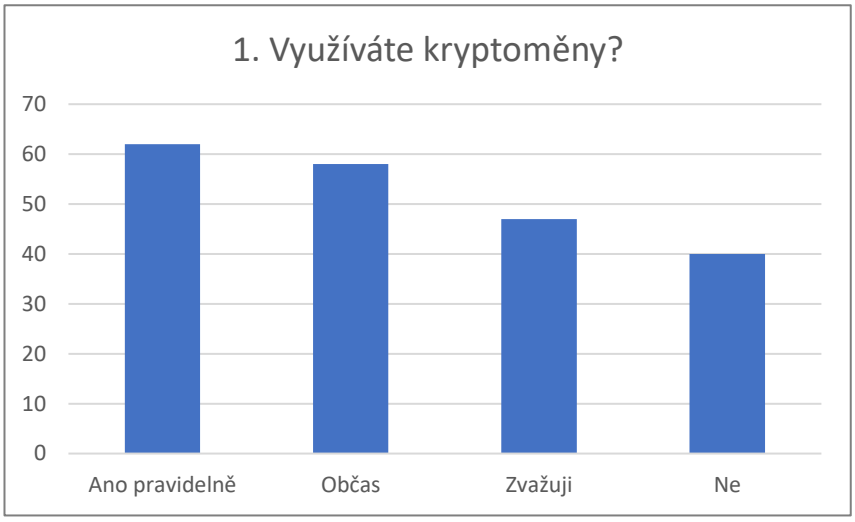
Analýza se zaměřila především na míru využívání kryptoměn mezi respondenty, jejich povědomí o rizicích investování, zkušenosti s podvodnými praktikami a úroveň znalostí v oblasti kybernetické bezpečnosti. Důležitou součástí analýzy bylo také zjištění, zda si respondenti uvědomují existenci regulace kryptoměn a jaký význam jí přisuzují z hlediska ochrany investorů.

Z výsledků vyplývá, že většina respondentů má alespoň základní povědomí o kryptoměnách a část z nich s nimi má i praktickou zkušenost v podobě investování. Současně však respondenti ve velké míře vnímají investování do kryptoměn jako rizikové. Analýza rovněž ukázala, že někteří respondenti se již setkali s phishingovými útoky nebo s nabídkami, které mohly vykazovat znaky podvodných investičních schémat.

Výsledky také naznačují, že respondenti považují za důležitou především větší informovanost veřejnosti, vzdělávání v oblasti kybernetické bezpečnosti a zavedení vhodných regulačních opatření. Tyto faktory mohou podle respondentů přispět ke snížení počtu podvodných aktivit v oblasti kryptoměn.

Otázka č. 1 – Využíváte kryptoměny v běžném životě (např. investice, platby, obchodování)?

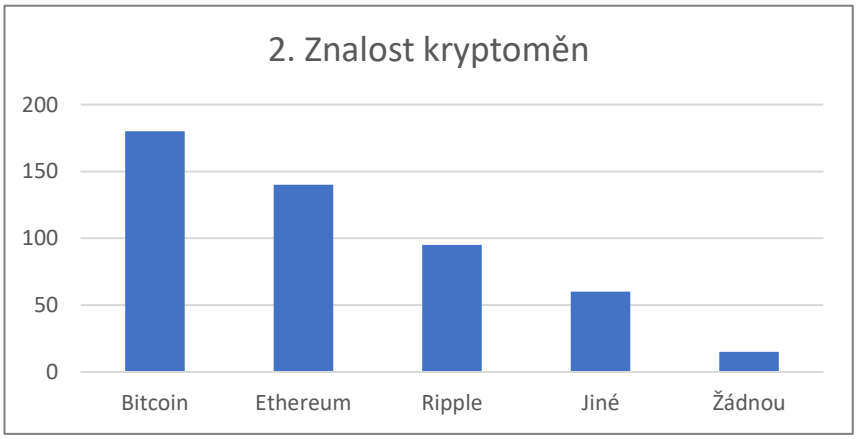
Výsledky ukazují, že významná část respondentů kryptoměny používá pravidelně nebo alespoň občas. Menší část respondentů kryptoměny nepoužívá nebo o jejich využití zatím pouze uvažuje.



Graf 1 Využívání kryptoměn
Zdroj: vlastní zpracování

Otázka č. 2 – Jaké kryptoměny znáte nebo vlastníte? (možno označit více odpovědí)

Nejznámější kryptoměnou mezi respondenty je Bitcoin, následovaný kryptoměnou Ethereum. Menší část respondentů uvedla také Ripple nebo jiné kryptoměny.

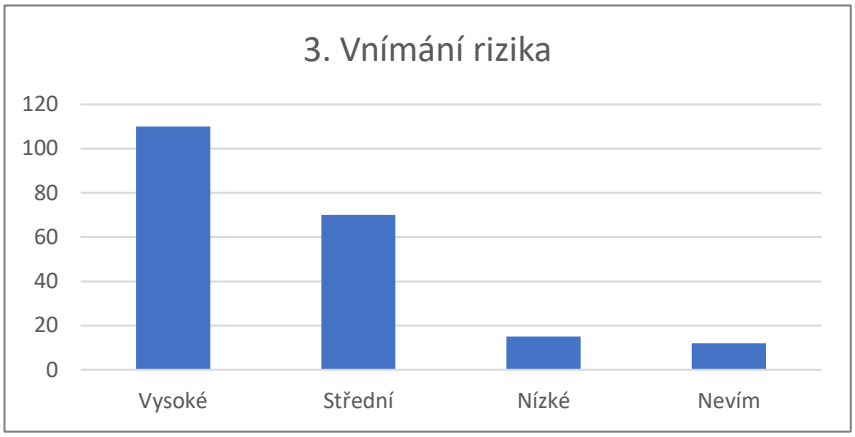


Graf 2 Znalost kryptoměn

Zdroj: vlastní zpracování

Otázka č. 3 – Jak vnímáte riziko investování do kryptoměn?

Většina respondentů považuje investování do kryptoměn za vysoce rizikové. Menší část respondentů vnímá riziko jako střední nebo nízké.

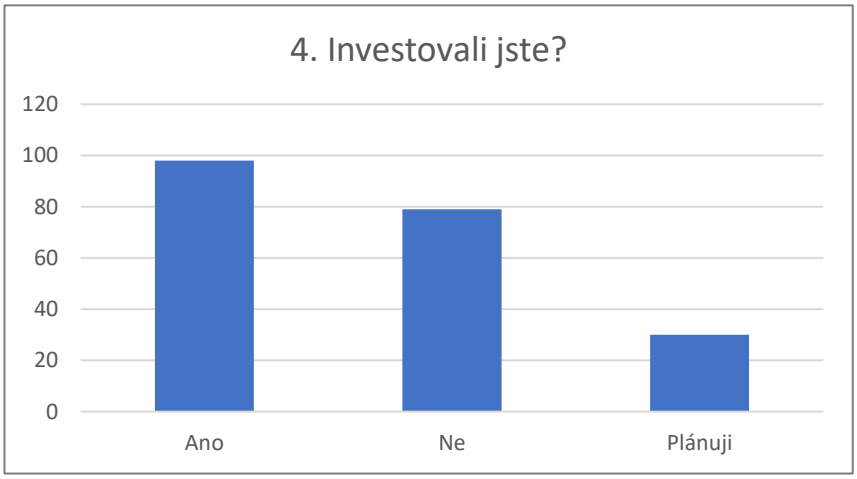


Graf 3 Vnímání rizika

Zdroj: vlastní zpracování

Otázka č. 4 – Investovali jste někdy do kryptoměn?

Přibližně polovina respondentů již někdy investovala do kryptoměn. Zbytek respondentů buď zatím neinvestoval, nebo investici teprve zvažuje.

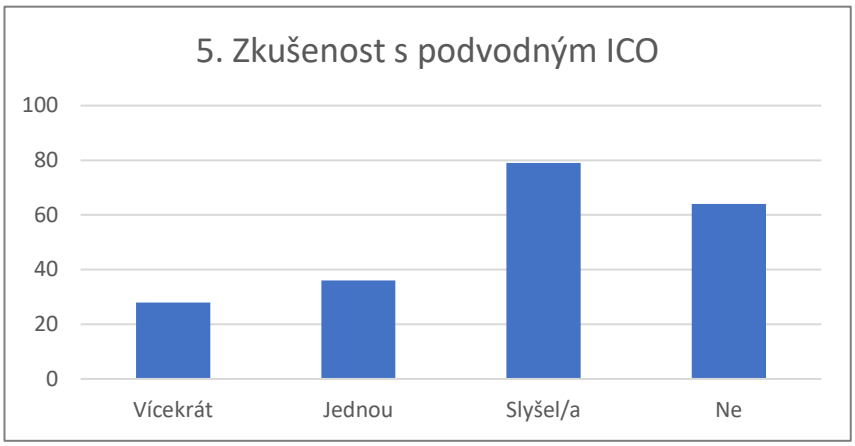


Graf 4 Investování

Zdroj: vlastní zpracování

Otázka č. 5 – Setkali jste se někdy s nabídkou investovat do nově vznikající kryptoměny (tzv. ICO), u které se později ukázalo, že šlo o podvod (např. autoři projektu po vybrání peněz zmizeli)?

Část respondentů uvedla, že se již setkala s podvodnými ICO projekty nebo o nich alespoň slyšela. Významná skupina respondentů však uvedla, že se s tímto typem podvodu nesetkala.

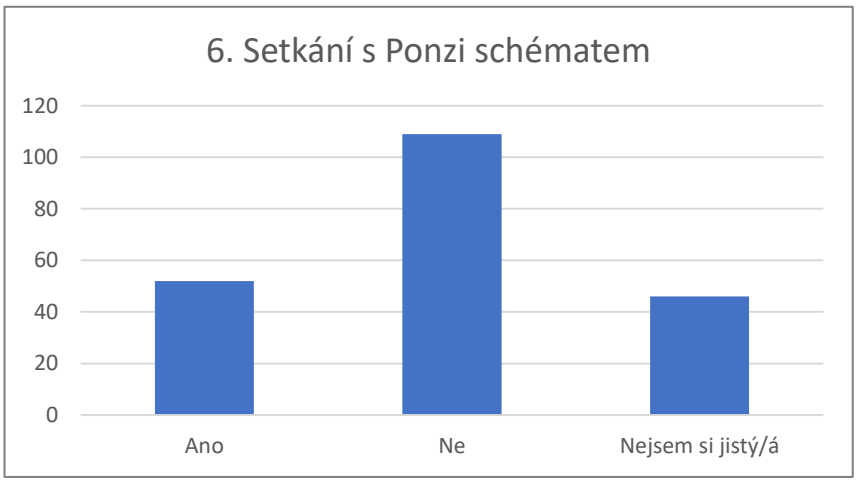


Graf 5 Zkušenost s podvodným ICO

Zdroj: vlastní zpracování

Otázka č. 6 – Byla Vám někdy nabízena investice, jejíž ziskovost byla podmíněna náborem dalších účastníků nebo kde byly slibovány vysoké výnosy bez jasného zdroje příjmů (typické znaky Ponziho schématu či pyramidy)?

Menší část respondentů uvedla osobní zkušenost s podobnou nabídkou. Většina respondentů však uvedla, že se s takovou situací nesetkala.

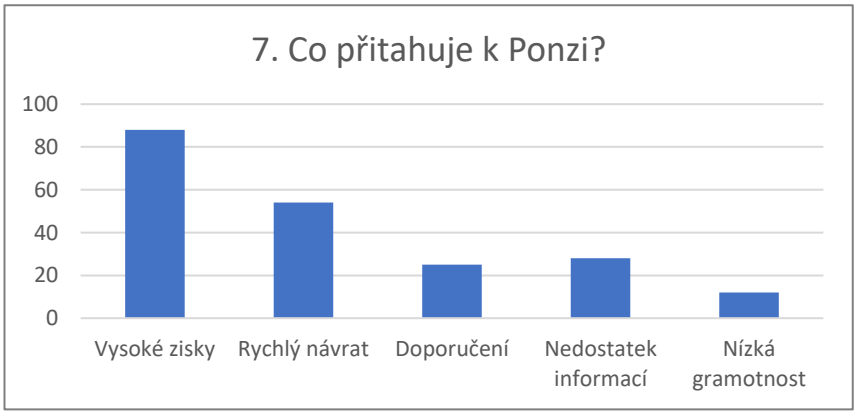


Graf 6 Setkání s Ponzi schématem

Zdroj: vlastní zpracování

Otázka č. 7 – Co podle vás nejčastěji přitahuje lidi k Ponziho schématům?

Respondenti nejčastěji uváděli jako hlavní motivaci slibované vysoké zisky a rychlý návrat investice. Dalšími faktory jsou nedostatek informací o rizicích nebo doporučení známých.

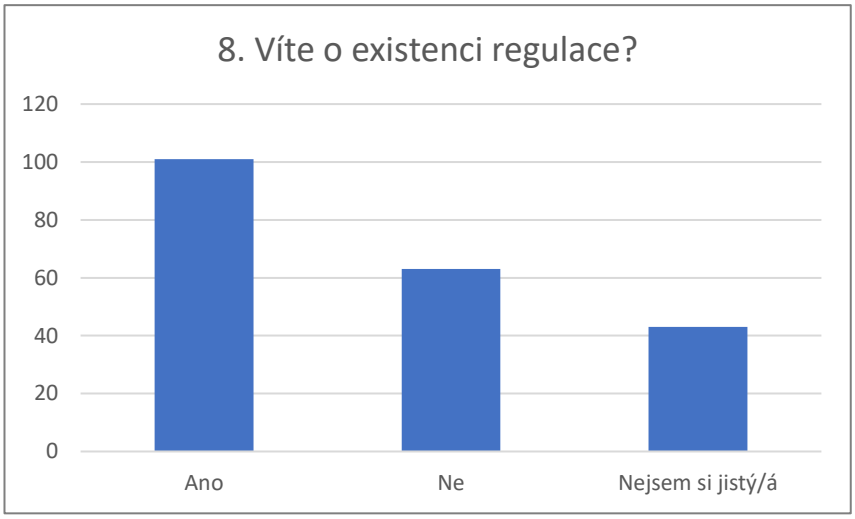


Graf 7 Co přitahuje k Ponzi

Zdroj: vlastní zpracování

Otázka č. 8 – Víte, že kryptoměny podléhají v některých zemích státní regulaci?

Přibližně polovina respondentů uvedla, že si je existence regulace kryptoměn vědoma. Zbytek respondentů o regulaci buď neví, nebo si není jistý.

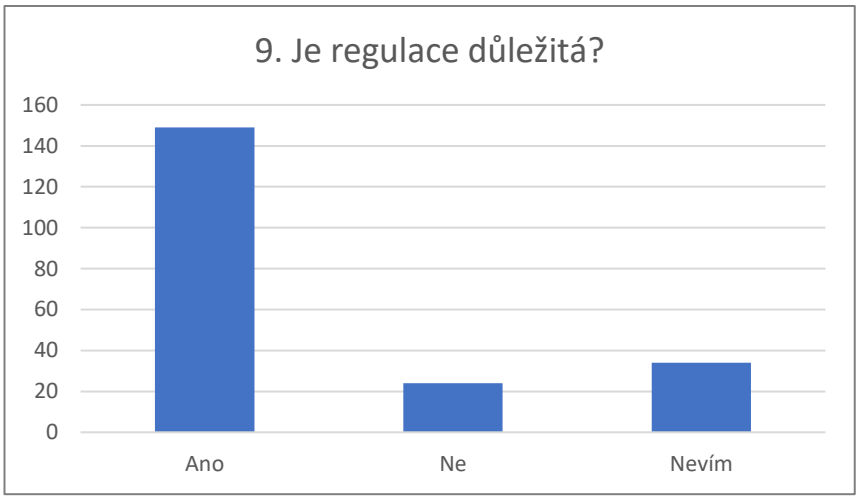


Graf 8 Existence regulace

Zdroj: vlastní zpracování

Otázka č. 9 – Vnímáte regulaci kryptoměn jako důležitou pro ochranu investorů?

Většina respondentů považuje regulaci kryptoměn za důležitý nástroj ochrany investorů. Pouze menší část respondentů regulaci nepovažuje za potřebnou.

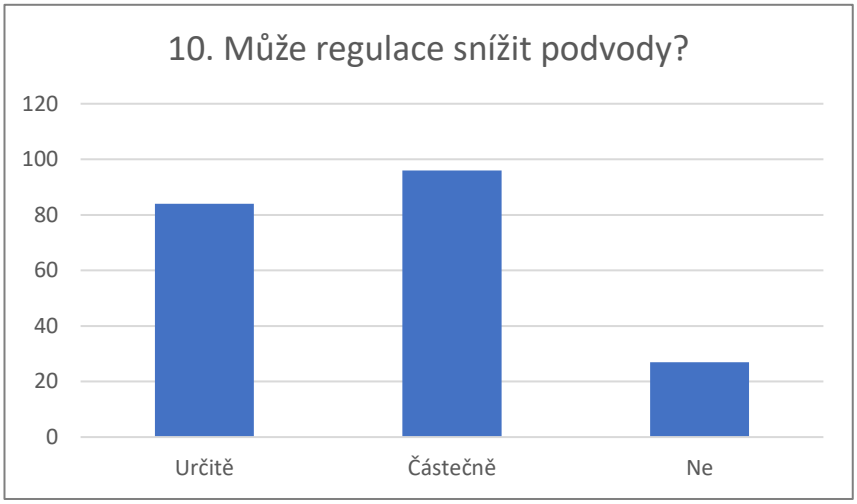


Graf 9 Je regulace důležitá?

Zdroj: vlastní zpracování

Otázka č. 10 – Myslíte si, že státní regulace kryptoměn může snížit podvodné aktivity v této oblasti?

Respondenti nejčastěji uváděli, že regulace může podvodné aktivity snížit alespoň částečně. Menší část respondentů se domnívá, že regulace může problém vyřešit výrazněji nebo naopak nepomůže.

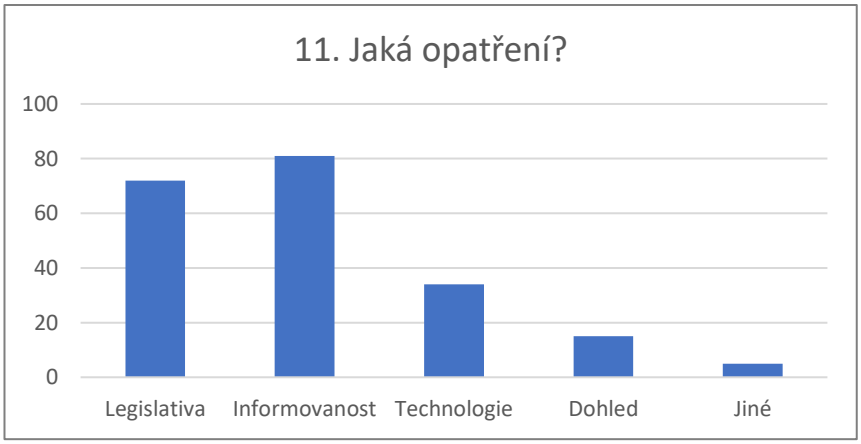


Graf 10 Může reegulace snížit podvody?

Zdroj: vlastní zpracování

Otázka č. 11 – Jaká opatření by podle vás měla být přijata, aby se zabránilo podvodům v kryptoměnovém prostředí?

Nejčastěji respondenti uváděli potřebu větší informovanosti veřejnosti a přísnější legislativy. Další možností podle respondentů je zlepšení bezpečnostních technologií.

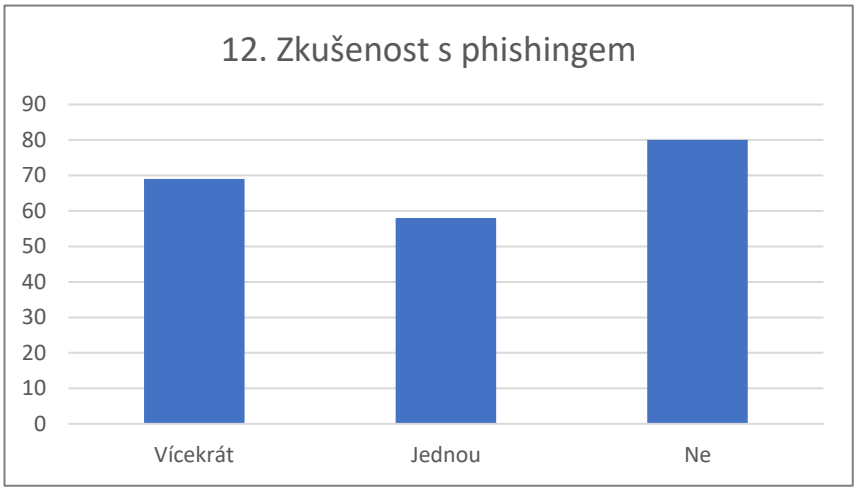


Graf 11 Opatření

Zdroj: vlastní zpracování

Otázka č. 12 – Máte zkušenosti s phishingovými útoky (např. podvodné e-maily, falešné investiční nabídky, podvodné zprávy)?

Výsledky ukazují, že značná část respondentů se již s phishingovým útokem setkala. Přibližně třetina respondentů uvedla, že s phishingem zatím zkušenost nemá.

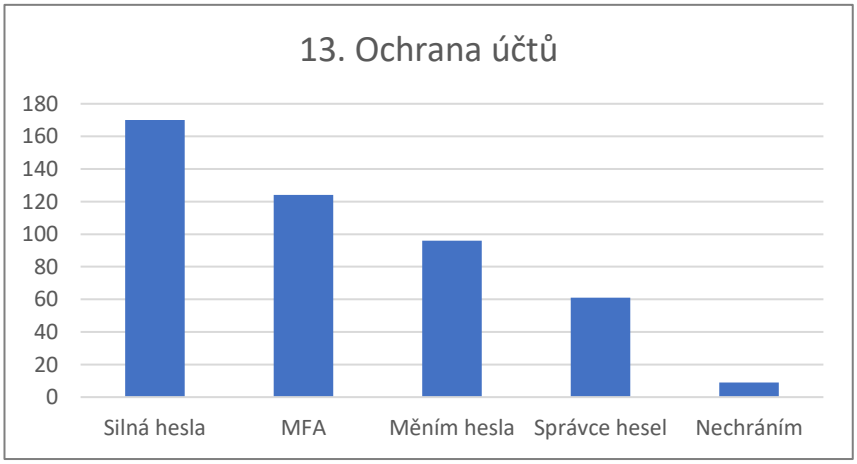


Graf 12 Zkušenost s phisingem

Zdroj: vlastní zpracování

Otázka č. 13 – Jakým způsobem chráníte své online účty a citlivé údaje? (možno označit více odpovědí)

Nejčastěji respondenti používají silná hesla a vícefaktorové ověřování. Pouze malá část respondentů uvedla, že své účty nechrání žádným zvláštním způsobem.

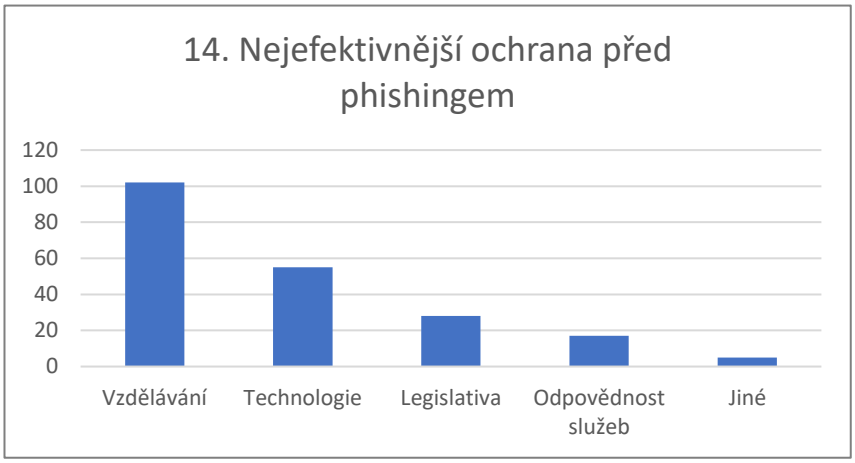


Graf 13 Ochrana účtu

Zdroj: vlastní zpracování

Otázka č. 14 – Co by podle vás bylo nejefektivnějším způsobem ochrany před phishingem?

Respondenti nejčastěji označili vzdělávání uživatelů jako nejúčinnější způsob ochrany. Další možností je podle nich využívání moderních bezpečnostních technologií.

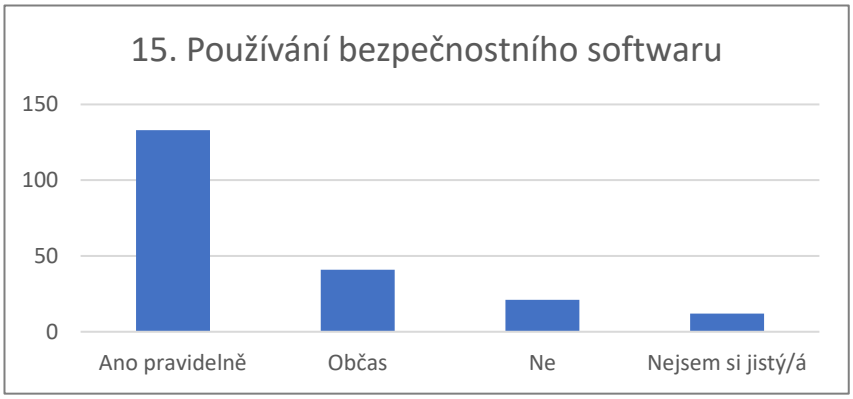


Graf 14 Nejefektivnější ochrana

Zdroj: vlastní zpracování

Otázka č. 15 – Používáte na svých zařízeních (PC, mobil, tablet) nějaký bezpečnostní software nebo antivirový program (např. ESET, Avast, Windows Defender)?

Většina respondentů uvedla, že používá antivirový program nebo jiný bezpečnostní software pravidelně. Menší část respondentů jej používá pouze občas nebo vůbec.

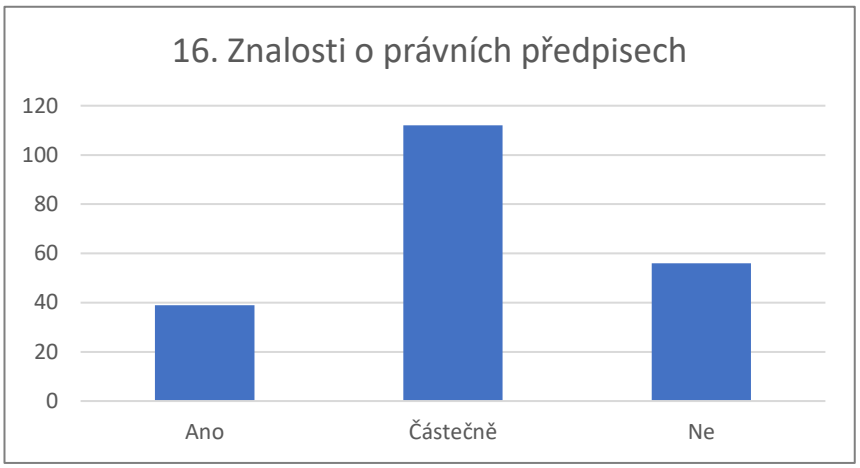


Graf 15 Ochrana proti malwaru

Zdroj: vlastní zpracování

Otázka č. 16 – Máte dostatečné znalosti o právních předpisech týkajících se kryptoměn a internetové bezpečnosti?

Pouze menší část respondentů uvedla, že má dostatečné znalosti o právní regulaci kryptoměn. Většina respondentů se domnívá, že má pouze částečné nebo žádné znalosti.



Graf 16 Znalost právních předpisů

Zdroj: vlastní zpracování

10.1 Shrnutí výsledku průzkumu

Na základě dotazníkového šetření, kterého se zúčastnilo celkem 207 respondentů, bylo zjištěno, že většina respondentů má alespoň základní povědomí o kryptoměnách a část z nich je také aktivně využívá, zejména za účelem investování. Nejznámější kryptoměnou mezi respondenty je Bitcoin, následovaný kryptoměnou Ethereum. Zároveň většina respondentů vnímá investování do kryptoměn jako rizikové, což souvisí především s jejich vysokou volatilitou a možností výskytu podvodných praktik.

Výsledky průzkumu dále ukázaly, že část respondentů se již setkala s informacemi o podvodných projektech typu ICO nebo s nabídkami, které mohou vykazovat znaky Ponziho schématu. Poměrně velké množství respondentů má také zkušenost s phishingovými útoky, což potvrzuje, že kybernetická kriminalita je v online prostředí poměrně častým jevem. Respondenti zároveň uváděli, že hlavním důvodem, proč lidé investují do podvodných schémat, jsou především sliby vysokých a rychlých zisků.

Dalším důležitým zjištěním je, že většina respondentů považuje regulaci kryptoměn za důležitou z hlediska ochrany investorů a omezení podvodných aktivit. Respondenti zároveň zdůrazňovali význam větší informovanosti veřejnosti, vzdělávání uživatelů a využívání bezpečnostních technologií jako účinných nástrojů prevence. Výsledky také naznačují, že přestože řada respondentů využívá základní bezpečnostní opatření, jejich znalosti o právní regulaci kryptoměn a kybernetické bezpečnosti jsou často pouze částečné.

Závěr

Virtuální prostředí a dynamický rozvoj digitálních technologií zásadním způsobem ovlivňují fungování současné společnosti. Digitalizace přináší nové možnosti v oblasti komunikace, podnikání i financí, přičemž kryptoměny představují jeden z nejvýznamnějších projevů této transformace. Vedle nesporných přínosů však tento vývoj současně vytváří i nové bezpečnostní výzvy, které jsou úzce spjaty s nárůstem kybernetické kriminality. Právě problematika podvodných praktik v kryptoměnovém prostředí byla hlavním předmětem této bakalářské práce.

Hlavním cílem práce bylo komplexně zhodnotit podvodné jevy v kryptoměnovém prostředí, identifikovat jejich mechanismy a analyzovat jejich dopady na uživatele. Současně bylo cílem navrhnout konkrétní opatření vedoucí ke zvýšení ochrany investorů. Na základě provedené analýzy teoretických východisek a výsledků empirického šetření lze konstatovat, že stanovený cíl práce byl naplněn. Práce poskytla ucelený přehled o nejčastějších formách podvodů, vysvětlila jejich principy fungování a zároveň formulovala doporučení směřující k minimalizaci rizik.

Teoretická část práce poukázala na specifické vlastnosti kryptoměn, zejména decentralizaci, pseudonymitu a absenci centrální autority. Tyto charakteristiky byly identifikovány jako zásadní faktory, které významně ovlivňují bezpečnost celého systému. Na jedné straně umožňují vyšší míru svobody a nezávislosti uživatelů, na straně druhé však ztěžují kontrolu a regulaci, což vytváří příznivé podmínky pro vznik a rozvoj podvodných aktivit. Analýza dále ukázala, že podvodné praktiky v kryptoměnovém prostředí se neustále vyvíjejí a přizpůsobují aktuálním trendům a technologiím.

Za klíčové formy podvodného jednání byly označeny zejména Ponziho schémata, pyramidové systémy, falešné investiční projekty a techniky sociálního inženýrství. Společným znakem těchto aktivit je kombinace technologických nástrojů a cílené manipulace lidského chování. Podvodníci často využívají nedostatečné informovanosti uživatelů, jejich důvěry či snahy o rychlé zhodnocení investic. Práce tak potvrdila, že významnou roli v oblasti kybernetické bezpečnosti hraje nejen technologie, ale především lidský faktor.

Významným přínosem práce byla praktická část založená na dotazníkovém šetření, kterého se zúčastnilo 207 respondentů. Získaná data poskytla cenný vhled do vnímání rizik a chování uživatelů v kryptoměnovém prostředí. Výsledky ukázaly, že většina respondentů si uvědomuje rizikovost investic do kryptoměn, což lze hodnotit jako pozitivní zjištění. Přesto se však značná část z nich setkala s konkrétními pokusy o podvodné jednání, což poukazuje na přetrvávající vysokou míru ohrožení.

Za zvláště důležité zjištění lze považovat rozpor mezi deklarovanou opatrností a reálnou zkušeností s podvody. Tento fakt naznačuje, že samotné povědomí o existenci rizik není dostatečné k jejich efektivnímu předcházení. Uživatelé sice rizika vnímají, avšak často nedisponují dostatečnými znalostmi nebo dovednostmi, které by jim umožnily těmto hrozbám účinně čelit.

Dalším významným zjištěním byla nízká úroveň znalostí v oblasti právní regulace kryptoměn. Většina respondentů uvedla, že má pouze omezené nebo žádné informace o legislativním rámci. Tento nedostatek může vést k podcenění rizik a k vyšší zranitelnosti vůči podvodným praktikám. Z tohoto pohledu se ukazuje jako nezbytné posílit informovanost veřejnosti nejen v oblasti technologií, ale i právních aspektů digitálních financí.

Na základě provedené analýzy byla formulována řada doporučení zaměřených na zvýšení bezpečnosti uživatelů. Mezi nejdůležitější patří využívání technických bezpečnostních opatření, jako je vícefaktorová autentizace, používání silných hesel a bezpečné uchovávání kryptoměn prostřednictvím hardwarových peněženek. Důležitá je rovněž obezřetnost při investování a schopnost kriticky posuzovat důvěryhodnost jednotlivých projektů.

Zásadním závěrem práce je však skutečnost, že technická opatření sama o sobě nejsou dostačující. Klíčovou roli hraje především vzdělávání a zvyšování digitální gramotnosti uživatelů. Informovaný uživatel je schopen lépe rozpoznat podvodné jednání, vyhodnotit rizika a přijímat odpovědná rozhodnutí. Tento závěr byl potvrzen i výsledky dotazníkového šetření, ve kterém respondenti označili vzdělávání za nejefektivnější nástroj prevence.

V širším kontextu lze konstatovat, že problematika podvodů v kryptoměnovém prostředí přesahuje rámec jednotlivých uživatelů a představuje významnou výzvu pro celou společnost. S rostoucím významem digitálních aktiv bude nezbytné rozvíjet odpovídající regulační mechanismy, které zajistí ochranu investorů a zároveň nebudou brzdit technologické inovace. Důležitá je také mezinárodní spolupráce, jelikož kybernetická kriminalita nemá geografické hranice.

Pro budoucí výzkum se nabízí řada možných směrů. Vhodné by bylo zaměřit se například na detailní analýzu konkrétních případů podvodů, jejich ekonomické dopady nebo na efektivitu preventivních opatření. Další oblastí zájmu může být i studium chování uživatelů v digitálním prostředí a faktorů, které ovlivňují jejich rozhodování.

Závěrem lze shrnout, že kryptoměnové prostředí představuje dynamicky se rozvíjející oblast, která s sebou nese jak významné příležitosti, tak i značná rizika. Kyberkriminalita v této oblasti bude pravděpodobně i nadále narůstat, a proto je nezbytné věnovat této problematice zvýšenou pozornost. Tato bakalářská práce přispívá k lepšímu pochopení dané problematiky a nabízí konkrétní doporučení, která mohou napomoci ke zvýšení bezpečnosti uživatelů v digitálním prostředí.

Seznam použitých zdrojů

Literární zdroje

1. ABDELHAMID, N., AISSANI, D., BENMOUSSA, F. *Mitigation strategies against phishing attacks: A comprehensive review. Computers & Security*. 2023. DOI: 10.1016/j.cose.2023.103392.

2. ANTONOPOULOS, A. M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* 2nd ed. Sebastopol: O'Reilly Media, 2017. ISBN 9781491954386.

3. BURNISKE, C., TATAR, J**.** *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond.* New York: McGraw-Hill Education, 2017. ISBN 978-1260026672.

4. FRANKEL, T. *The Ponzi scheme puzzle: a history and analysis of con artists and victims*. New York, NY: Oxford University Press, 2012. ISBN 0199926611.

5. FURNELL, S. (2002). *Cybercrime: Vandalizing the information society*. Addison-Wesley. ISBN 978-0201721591.

6. GURLEY, J. (2022). *The SEC and Cryptocurrency: A Regulatory Perspective*. In *Cryptocurrency Regulations and Compliance* (pp. 12-27). London: Palgrave Macmillan. ISBN 978-3030927560.

7. HADNAGY, C. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, [2018]. ISBN 978-1-119-43338-5.

8. KEENAN, J. (2020). *Understanding cryptocurrency and its potential for financial fraud*. New York: Springer. ISBN 978-3030361232.

9. KHAN, M. A., ALI, F. (2023). *Cybersecurity in Cryptocurrency: Protecting Investors from Fraud*. In *Advancements in Cybersecurity and Digital Forensics* (pp. 33-50). New York: Springer. ISBN 978-3031290467

10. KOVÁŘ, P. *Zabezpečení online účtů*: *Moderní přístupy a technologie.* 1. vyd. Praha: XYZ Publishing, 2022. ISBN 978-80-123-4567-8.

11. KUHN, T. R. S., FISCHER L. *Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York: HarperCollins, 2021. ISBN 9780063076628.

12. LÁNSKÝ, J. *Kryptoměny* 1. vydání. V Praze: C.H. Beck, 2018. 144 stran. ISBN 978- 80-7400-722-4

13. MARR, B. *The Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. London: Wiley, 2018. ISBN 9781119467656.

14. MCCULLOUGH, J. *Stablecoins: The Future of Money? Journal of Payments Strategy & Systems*, 2020, vol. 14, no. 2, p. 123-130.

15. MITNICK, K. D., SIMON, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security.* Wiley. ISBN 978-0764518482.

16. NARAYANAN, A., BONNEAU, J., EDWARD, F., MILLER, A., GOLDFEDER, S. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, [2016]. ISBN 978-0-691-17169-2.

17. SAHOO, D., LIU, C., HOI, S. C. H. *High accuracy phishing detection based on convolutional neural networks*. *arXiv*. 2020.

18. TAPSCOTT, D., TAPSCOTT, A. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Penguin, 2016. ISBN 978-1101980132

19. Trozze, A., et al. *Cryptocurrencies and future financial crime. Crime Science*. 2022, roč. 11, č. 1, s. 1–35. DOI: 10.1186/s40163-021-00163-8.

20. VERMA, R., DAS, A. *Malicious URL detection using machine learning: A survey*. *arXiv*. 2017.

21. XIAO, Y., ZHANG, N., LIU, Y**.** *Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites. arXiv*. 2020.

22. YLI-HUMMO, J., KO, D., CHOI, S., PARK, S., SMOLANDER, K. *Security of cryptocurrencies: A systematic literature review*. *IEEE Access*. 202

23. ZOHAR, A., SIVAN, A. (2021). *Cryptocurrency and its regulatory implications: The impact on investors' rights and fraud prevention*. In *Advances in Digital Economy and E-Business* (pp. 45-62). London: Academic Press. ISBN 978-0128142237.

Elektronické zdroje

1. *BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme.* Online. Justice.gov. 2024, 25.2.2022. [cit. 2025-12-15]. Dostupné z: https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

2. CHECK POINT RESEARCH. *The Rising Threat of Phishing Attacks with Crypto Drainers* [online]. 2023 [cit. 2025-12-17]. Dostupné z: https://research.checkpoint.com/the-rising-threat-of-phishing-attacks-with-crypto-drainers/.

3. FINANCIAL CONDUCT AUTHORITY. *Guidance on Cryptoassets*. 2021. [online]. [cit. 2025-12-18]. Dostupné z: https://www.fca.org.uk/publications/guidance-consultations/guidance-cryptoassets.

4. GOV.UK. *Statement from UK authorities on Cryptoassets*. 2022. [online]. [cit. 2025-12-18]. Dostupné z:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060448/Statement_from_UK_authorities_on_Cryptoassets_-_March_2022.pdf.

5. HARTINGEROVÁ, E. *Lekce 1 - Kryptoměny - Definice a vlastnosti* Zdroj. Online. Itmetwork. 2024, 2024. Dostupné z: https://www.itnetwork.cz/kryptomeny/zaklady-kryptomen. [cit. 2025-12-28].

6. HAYYES, A., BERNIE M. *Who He Was and How His Ponzi Scheme Worked.* Online. Investopedia. 2024. Dostupné z: https://www.investopedia.com/terms/b/bernard-madoff.asp. [cit. 2025-12-15].

7. HENNIGAN, R. (2021). *"Initial Coin Offerings: The Good, the Bad, and the Ugly."* Investopedia. [online] Dostupné z: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp [cit. 2025-12-17].

8. HM Revenue & Customs. *Cryptoassets for individuals*. 2021. [online]. [cit. 2025-12-18]. Dostupné z: https://www.gov.uk/government/publications/cryptoassets-for-individuals.

9. *Introduction to Investing: Ponzi Schemes*. [online]. U.S. Securities and Exchange Commission. Dostupné z: https://www.investor.gov/introduction-investing/investing-basics/glossary/ponzi-schemes [cit. 2025-12-15].

10. IACURCI, Greg. *Ponzi schemes hit highest level in a decade, hinting next 'investor massacre' may be near.* CNBC, 11 Feb. 2020 [cit. 2026-02-20]. Dostupné z: https://www.cnbc.com/2020/02/11/ponzi-schemes-hit-the-highest-level-in-10-years.htm

11. *Jak poznat podvod a jak se mu vyhnout.* Online. Kryyptobezpečně. 2024. Dostupné z: https://www.kryptobezpecne.cz/blog/jak-poznat-podvod-a-jak-se-mu-vyhnout. [cit. 2025-12-15].

12. LYNX. *Historická vs. implikovaná volatilita: Základy obchodování opcí* [online]. [cit. 2025-12-28]. Dostupné z: https://www.lynxbroker.cz/investovani/burzovni-trhy/opce/volatilita/zaklady-obchodovani-opci-9-historicka-vs-implikovana-volatilita/

13. MORABITOX**.** *Upozornění na rizika a varování: Vaše osobní údaje a kryptoměny mohou být v důsledku těchto problémů ztraceny nebo odcizeny.* Morabitox. [online]. [cit. 2026-02-20]. Dostupné z: https://www.morabitox.com/cz/Risk-Disclosure

14. NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Available at: https://bitcoin.org/bitcoin.pdf. [cit. 2025-12-28].

15. *Phishing*. Online. Eset. 2024, 2024. Dostupné z: https://www.eset.com/cz/phishing/. [cit. 2025-12-15].

16. RASURE, E., PEREZ, Y. *What Happened to OneCoin, the $4 Billion Crypto Ponzi Scheme?* Online. Investopedia. 2024, 9.3.2024. Dostupné z: https://www.investopedia.com/terms/o/onecoin.asp. [cit. 2025-12-15].

17. REUTERS. *Russia's central bank calls for blanket ban on cryptocurrencies*. 2021. [online]. [cit. 2025-12-18]. Dostupné z: https://www.reuters.com/technology/russias-central-bank-calls-blanket-ban-cryptocurrencies-2021-01-20/.

18. RICO, J. *What is Cryptojacking?* [online]. 2024 [cit. 2025-12-17]. Dostupné z: https://www.cybersecurityguide.org/cryptojacking/

19. SEZNAM.CZ. *Protokol HTTPS* [online]. [cit. 2025-12-28]. Dostupné z: https://napoveda.seznam.cz/cz/fulltext-hledani-v-internetu/protok ol-https/

20. U.S. DEPARTMENT OF THE TREASURY. 2019. *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation.* [online]. [cit. 2025-12-22]. Dostupné z: https://home.treasury.gov/system/files/136/FintechReport2019.pdf

21. U.S. SECURITIES AND EXCHANGE COMMISSION. *SEC Charges Centra Tech Co-Founders in Fraudulent ICO* [online]. 2018 [cit. 2026-01-03]. Dostupné z: https://www.sec.gov/news/press-release/2018-53

22. WEBGLOBE. *Co je Trojský kůň (Trojan virus) a co v počítači způsobuje?* [online]. [cit. 2025-12-17]. Dostupné z: https://www.webglobe.cz/co-je-trojski-kun-trojan-virus-a-co-v-pocitaci-zpusobuje

Legislativní dokumenty

1. Česká republika. Zákon č. 40/2009 Sb., trestní zákoník. Sbírka zákonů České republiky, 2009.

2. Zákon č. 634/1992 Sb., o ochraně spotřebitele. Sbírka zákonů, 1992. Dostupné z: https://www.zakonyprolidi.cz/cs/1992-634

3. EUROPEAN PARLIAMENT. *Směrnice (EU) 2018/843 o prevenci používání finančního systému k praní špinavých peněz nebo financování terorismu.* 2018. [online]. [2025-12-18]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32018L0843.

Seznam zkratek

2FA	Two-Factor Authentication
AMLD5	Anti-Money Laundering Directive 5
AML	Anti-Money Laundering
CFTC	Commodity Futures Trading Commission
dApps	Decentralized Applications
ESMA	European Securities and Markets Authority
ETH	Ethereum
EU	Evropská unie
FCA	Financial Conduct Authority
FinCEN	Financial Crimes Enforcement Network
HMRC	HM Revenue & Customs
HTTPS	Hypertext Transfer Protocol Secure
ICO	Initial Coin Offering
IRS	Internal Revenue Service
KYC	Know Your Customer
LINK	Chainlink
LTC	Litecoin
MiCA	Markets in Crypto-Assets
SEC	Securities and Exchange Commission
TZ	Trestní zákoník
UNI	Uniswap

URL	Uniform Resource Locator
USDC	USD Coin
USDT	Tether
USA	United States of America
XRP	Ripple
ZOS	Zákon o ochraně spotřebitele

Seznam tabulek a grafů

Seznam příloh

Přílohy

Příloha A: Dotazník pro empirický výzkum

1. Využíváte kryptoměny v běžném životě (např. investice, platby, obchodování)?

a) Ano, pravidelně

b) Občas

c) Zatím ne, ale zvažuji

d) Ne, a neplánuji to

2. Jaké kryptoměny znáte nebo vlastníte? (možno označit více odpovědí)

a) Bitcoin

b) Ethereum

c) Ripple

d) Jiná

e) Žádnou neznám

3. Jak vnímáte riziko investování do kryptoměn?

a) Vysoké

b) Střední

c) Nízké

d) Nevím

4. Investovali jste někdy do kryptoměn?

a) Ano

b) Ne

c) Plánuji

5. Setkali jste se někdy s nabídkou investovat do nově vznikající kryptoměny (tzv. ICO), u které se později ukázalo, že šlo o podvod (např. autoři projektu po vybrání peněz zmizeli)?

(např. projekt sliboval vysoké zisky, ale po vybrání peněz zmizel)

a) Ano, vícekrát

b) Ano, jednou

c) Slyšel/a jsem o tom, ale osobně jsem se nesetkal/a

d) Ne

6. Byla Vám někdy nabízena investice, jejíž ziskovost byla podmíněna náborem dalších účastníků nebo kde byly slibovány vysoké výnosy bez jasného zdroje příjmů (typické znaky Ponziho schématu či pyramidy)?

a) Ano

b) Ne

c) Nejsem si jistý/á

7. Co podle vás nejčastěji přitahuje lidi k Ponziho schématům?

a) Slíbené vysoké zisky

b) Rychlý návrat investice

c) Doporučení známých

d) Nedostatek informací o rizicích

e) Nízká finanční gramotnost

8. Víte, že kryptoměny podléhají v některých zemích státní regulaci?

a) Ano

b) Ne

c) Nejsem si jistý/á

9. Vnímáte regulaci kryptoměn jako důležitou pro ochranu investorů?

a) Ano

b) Ne

c) Nevím

10. Myslíte si, že státní regulace kryptoměn může snížit podvodné aktivity v této oblasti?

a) Ano, určitě

b) Ano, ale jen částečně

c) Ne, regulace nic nezmění

11. Jaká opatření by podle vás měla být přijata, aby se zabránilo podvodům v kryptoměnovém prostředí?

a) Přísnější legislativa

b) Větší informovanost veřejnosti

c) Lepší bezpečnostní technologie

d) Přísnější dohled nad burzami

e) Jiná

12. Máte zkušenosti s phishingovými útoky (např. podvodné e-maily, falešné investiční nabídky, podvodné zprávy)?

a) Ano, několikrát

b) Ano, jednou

c) Ne

13. Jakým způsobem chráníte své online účty a citlivé údaje? (možno označit více odpovědí)

a) Používám silná hesla

b) Využívám vícefaktorové ověřování (MFA)

c) Pravidelně měním hesla

d) Používám správce hesel

e) Nechráním je nijak zvlášť

14. Co by podle vás bylo nejefektivnějším způsobem ochrany před phishingem?

a) Vzdělávání uživatelů

b) Lepší detekční technologie

c) Přísnější legislativa

d) Zvýšení odpovědnosti poskytovatelů služeb

e) Jiné

15. Používáte na svých zařízeních (PC, mobil, tablet) nějaký bezpečnostní software nebo antivirový program (např. ESET, Avast, Windows Defender)?

a) Ano, pravidelně (např. antivirový program, firewall, bezpečnostní balíček)

b) Občas

c) Ne, nepoužívám

d) Nejsem si jistý/á

16. Máte dostatečné znalosti o právních předpisech týkajících se kryptoměn a internetové bezpečnosti?

a) Ano

b) Částečně

c) Ne, vůbec