

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

BAKALÁŘSKÁ PRÁCE

**KRYPTOMĚNY JAKO PROSTŘEDEK K PÁCHÁNÍ
PODVODNÝCH JEDNÁNÍ V ONLINE PROSTORU**

Autor práce: Milada Jahnová, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.

Katedra: Katedra právních oborů a bezpečnostních studií

2025

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Milada Jahnová, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Místo studia: Příbram

Název bakalářské práce: Kryptoměny jako prostředek k páchání podvodných jednání v online prostoru

Název bakalářské práce v anglickém jazyce: Cryptocurrencies as a Means of Committing Fraudulent Acts in the Online Space

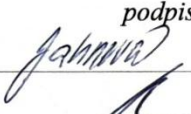
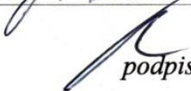
Katedra: Katedra právních oborů a bezpečnostních studií

Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M.

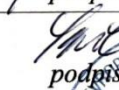
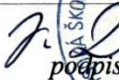
Datum zadání bakalářské práce: listopad 2024

Cíl bakalářské práce:

Hlavním cílem bakalářské práce je zhodnotit využití kryptoměn jako prostředku k páchání podvodných jednání v online prostoru, se zaměřením na identifikaci nejčastějších forem těchto podvodů, jejich dopady na oběti a efektivitu současných právních a technických opatření proti nim. Vedlejším cílem práce je navrhnout doporučení pro zlepšení prevence a detekce těchto trestných činů.

Student: Milada Jahnová, DiS.	datum 7.12.2024	podpis 
Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.	7.12.2024 datum	podpis 

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	12.12.2024 datum	podpis 
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11.12.2024 datum	podpis 
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20.1.2025 datum	podpis 



Prohlašuji, že jsem bakalářskou práci vypracoval(a) 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 vedoucí(ho) 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 JUDr. Milanovi Kocíkovi, MBA, LL.M. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

JAHNOVÁ, M. *Kryptoměny jako prostředek k páchání podvodných jednání v online prostoru*. České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 61 s. Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M.

Bakalářská práce s názvem „*Kryptoměny jako prostředek k páchání podvodných jednání v online prostoru*“ se zaměřuje na problematiku kryptoměn, zejména Bitcoinu. Práce shrnuje důvody vzniku Bitcoinu, popisuje historii peněz, princip jeho fungování a trestné činy spojené s kryptoměnami. Dále se věnuje podvodným jednáním v online prostoru a v neposlední řadě také možnostem prevence.

Klíčová slova: bitcoin, blockchain, budoucnost, kryptoměny, peníze.

ABSTRACT

JAHNOVÁ, M. *Cryptocurrencies as a Means of Committing Fraudulent Acts in the Online Space*. České Budějovice: College of European and Regional Studies, 2025. 61 pages. Bachelor's Thesis Supervisor: JUDr. Milan Kocík, MBA, LL.M.

The bachelor's thesis titled "Cryptocurrencies as a Means of Committing Fraudulent Acts in the Online Space" focuses on the issue of cryptocurrencies, particularly Bitcoin. The thesis outlines the reasons for the creation of Bitcoin, describes the history of money, the principles of its functioning, and the criminal offenses associated with cryptocurrencies. It also addresses fraudulent activities in the online space and, lastly, explores for prevention.

Keywords: bitcoin, blockchain, future, cryptocurrencies, money.

Obsah

Úvod.....	9
1 Cíl a metodika bakalářské práce	11
2 Vymezení kryptoměn	13
2.1 Historie peněz a důvod vzniku Bitcoinu	14
3 Bitcoin	17
3.1 Historie Bitcoinu	17
4 Funkční principy Bitcoinu	19
4.1 Decentralizace	19
4.2 Šifrování (protokol a kryptografie)	20
4.3 Těžba (mining)	20
4.3.1 Půlení odměny za blok (halving)	21
4.4 Struktura databází (blockchain).....	22
5 Pojem kyberkriminalita.....	23
5.1 Trestné činy v prostředí kryptoměn.....	25
6 Nejčastější podvody v online prostoru ve spojitosti s Bitcoinem a dalšími kryptoměnami	27
6.1 Falešné investiční platformy	28
6.2 Phishingové útoky	29
6.3 Pyramidové hry a Ponziho schémata.....	29
6.4 Falešné tokeny a ICO	30
6.5 Podvodné miningové programy	31
6.6 Schémata Pump and Dump	32
7 Současné právní a technický opatření proti kryptokriminalitě	34
7.1 Právní rámec ČR pro kyberprostor a kyberkriminalitu	34
7.2 Technické nástroje a metody	36
8 Oběti trestných činů spojených s kryptoměnami v online prostoru	38

9	Prevence podvodného jednání v online prostoru spojeného s kryptoměnami	
	40	
9.1	Prevence kriminality	40
9.2	Prevence kyberkriminality	41
10	Empirický výzkum	44
10.1	Experiment	44
	Závěr.....	56
	Seznam použitých zdrojů	58
	Seznam tabulek a grafů	61

Úvod

Tato bakalářská práce se zaměřuje na kryptoměny, přičemž větší pozornost bude věnována Bitcoinu, který je nejstarší, nejrozšířenější a nejvíce studovanou kryptoměnou. I když je téma kryptoměn obecně široké, analýza Bitcoinu poskytne konkrétní rámec pro pochopení problémů spojených s tímto novým fenoménem v oblasti online transakcí a podvodů. Bitcoin se stal symbolem kryptoměn a jeho decentralizovaná povaha, anonymita a specifické transakční mechanismy jsou důvody, proč je častým nástrojem pro podvodné aktivity.

Bakalářská práce je rozdělena na teoretickou a empirickou část. V teoretické části se zaměříme na definici kryptoměn a jejich historický vývoj. V podkapitole o historii peněz se zaměříme na dlouhodobý vývoj měnových systémů, který vedl k vytvoření kryptoměn. Dále se budeme věnovat důvodům vzniku Bitcoinu a vysvětlíme, jak tento nový typ měny reagoval na potřebu decentralizovaných a bezpečných transakcí, které by nevyžadovaly zprostředkovatele.

Další část se zaměřuje přímo na Bitcoin. Podrobně prozkoumáme historii Bitcoinu, jeho vznik v roce 2009 a okolnosti, které vedly k jeho vytvoření. Dále analyzujeme, jak Bitcoin ovlivnil svět financí a jak se stal základním kamenem pro rozvoj dalších kryptoměn.

V následující části se soustředíme na funkční principy Bitcoinu. Nejprve se zaměříme na decentralizaci, která je klíčovým prvkem Bitcoinového systému. Dále se věnujeme šifrování, které zajišťuje bezpečnost transakcí, a procesu těžby, nezbytnému pro generování nových jednotek Bitcoinu. V poslední podkapitole se podíváme na strukturu databází, konkrétně na blockchain, který je základem pro uchovávání transakcí v síti.

Další kapitola se věnuje kyberkriminalitě, která zahrnuje trestnou činnost spojenou s využíváním digitálních technologií. Kyberprostor, tvořený propojenými počítačovými systémy, je charakterizován anonymitou, neexistencí hranic a okamžitým globálním dosahem, což z něj činí ideální prostředí pro páčání trestných činů.

Další kapitola analyzuje podvody v online prostoru ve spojitosti s Bitcoinem a dalšími kryptoměnami. Zaměří se na konkrétní příklady podvodů, které se vyskytují

v digitálním prostředí, a na způsoby, jakými jsou kryptoměny zneužívány k nelegálním činnostem.

Následující kapitola se zabývá současnými právními a technickými opatřeními proti kryptokriminalitě. Tato část představuje právní rámec České republiky pro kyberprostor a kyberkriminalitu a zároveň se věnuje technickým nástrojům a metodám využívaným při monitorování a detekci trestné činnosti.

Předposlední kapitola se věnuje dopadům trestných činů spojených s podvodným jednáním v kryptokriminalitě na oběti.

Poslední kapitola zkoumá prevenci podvodného jednání v online prostoru spojeného s kryptoměnami, přičemž nabízí praktické přístupy a doporučení, jak předcházet zneužití kryptoměn k nelegálním účelům.

Pro zpracování empirické části bude zvolen experiment, který se zaměří na reakci na jasně podvodnou nabídku. Cílem bude analyzovat a identifikovat proces podvodu, pochopit jeho mechanismus a vymezit klíčové znaky, pomocí kterých kryptoměny slouží jako nástroj pro páčání podvodů.

Hlavním cílem bakalářské práce je zhodnotit využití kryptoměn jako prostředku k páčání podvodných jednání v online prostoru, se zaměřením na identifikaci nejčastějších forem těchto podvodů, jejich dopady na oběti a efektivitu současných právních a technických opatření proti nim. Vedlejším cílem práce je navrhnout doporučení pro zlepšení prevence a detekce těchto trestných činů.

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce je zhodnotit využití kryptoměn jako prostředku k páchání podvodných jednání v online prostoru, se zaměřením na identifikaci nejčastějších forem těchto podvodů, jejich dopady na oběti a efektivitu současných právních a technických opatření proti nim. Sekundárním cílem je navrhnout doporučení pro zlepšení prevence a detekce těchto trestných činů.

Bakalářská práce je rozdělena na teoretickou a empirickou část a to do deseti hlavních kapitol. V teoretické části práce se zaměřím na definici kryptoměn a jejich historický vývoj. Nejprve se budu věnovat historii peněz a vývoji měnových systémů, které postupně vedly k vzniku kryptoměn. Poté se zaměřím na vznik Bitcoinu, vysvětlím jeho roli jako první decentralizované měny a objasním důvody, které vedly k jeho vytvoření. Následně bude podrobně prozkoumána historie Bitcoinu, jeho funkční principy, včetně decentralizace, šifrování, těžby a konceptu halvingu. Neopomenu ani klíčovou technologii Bitcoinu – blockchain. Další část práce se věnuje kyberkriminalitě a trestným činům v prostředí kryptoměn. Poté se zaměřím na nejčastější podvody spojené s kryptoměnami v online prostoru. Dále se budeme věnovat současným právním a technickým opatřením proti kryptokriminalitě, včetně právního rámce v ČR pro kyberprostor a kyberkriminalitu, a technickým nástrojům a metodám využívaným k jejich monitorování a detekci. Následně se zaměříme na oběti trestných činů spojených s kryptoměnami v online prostoru a na dopady těchto trestných činů na jednotlivce. V poslední kapitole práce se zaměřím na prevenci podvodného jednání v online prostoru a na praktické přístupy a doporučení pro zlepšení ochrany před zneužitím kryptoměn k nelegálním účelům.

Pro teoretickou část bude zpracována rešerše odborné literatury a dalších odborných zdrojů. Kromě toho bude provedena analýza statistických údajů. Pro empirickou část bude zvolen experiment zaměřený na reakci na zjevně podvodnou nabídku. Jeho cílem bude analyzovat a identifikovat podvodný proces, porozumět jeho mechanismu a vymezit klíčové charakteristiky, které umožňují využití kryptoměn jako nástroje pro páchání podvodných aktivit. Experiment bude realizován za použití zcela nové SIM karty, která není vázána na žádné jméno. Telefon použitý v experimentu bude v továrním nastavení a nebude obsahovat žádná osobní data. Dále bude v experimentu použitý tablet, rovněž v továrním nastavení a další mobilní telefon na zaznamenání

hovoru s podvodníkem, aby bylo možné tento hovor následně přepsat do písemné podoby. Experiment bude probíhat až do momentu, kdy by bylo vyžadováno skutečné zaplacení, což by znamenalo reálnou finanční ztrátu. Poté bude sepsán fiktivní rozhovor, který bude inspirován skutečnými podvody, na kterém bude poukázáno na to, jak snadno z Vás podvodník peníze dostane pod zástitou vydělání velké finanční hotovosti a jak by mohl rozhovor probíhat, pokud bychom opravdu naletěli podvodníkovi.

2 Vymezení kryptoměn

Kryptoměna je digitální forma měny, která využívá kryptografii k zabezpečení transakcí v rámci digitálního systému, ve kterém funguje. Je navržena tak, aby fungovala nezávisle jako prostředek směny prostřednictvím počítačové sítě, která nepodléhá žádné centrální autoritě, například vládě nebo centrální bance. Existuje velké množství různých kryptoměn a stejně tak mnoho společností a organizací, které s nimi obchodují nebo je jinak využívají.¹

V této kapitole se seznámíme se základními pojmy a principy, které jsou klíčové pro pochopení kryptoměn. Kryptoměna (cryptocurrency) je systém, který nevyžaduje centrální autoritu a dosahuje shody o svém stavu prostřednictvím distribuovaného mechanismu mezi jednotlivými účastníky. Systém uchovává záznamy o jednotkách kryptoměny a eviduje, kdo je jejich vlastníkem. Vlastnictví těchto jednotek je prokazováno výhradně kryptograficky, což znamená, že se k ověření identity vlastníků používají šifrovací techniky. Systém stanovuje, zda je možné vytvářet nové jednotky kryptoměny. Pokud ano, určuje podmínky jejich vzniku a způsob, jakým je přiděleno vlastnictví těmto novým jednotkám. Systém umožňuje provádění transakcí, které mění vlastnictví jednotek kryptoměny. Transakci může zadat pouze osoba, která prokáže, že dané jednotky skutečně vlastní. Pokud jsou současně zadány dva různé pokyny pro změnu vlastnictví stejných jednotek kryptoměny, systém akceptuje pouze jeden z nich².

Kryptoměnám, které nejsou Bitcoin, se říká altcoiny, což je zkratka vzniklá spojením slov alternativní a (Bit)coin. Lidově se jim často přezdívá shitcoiny nebo memecoiny, což odkazuje na jejich nižší hodnotu nebo spekulativní povahu. Existují jich tisíce. Na webové stránce coinmarketcap.com najdeme přehled většiny z nich, včetně informací o jejich tržní kapitalizaci a vývoji kurzu, pokud jsou obchodovány na některých globálních kryptoměnových burzách. Mnohé z těchto kryptoměn nestojí za větší pozornost, protože jsou často jen upravené verze Bitcoinu nebo jiných starších digitálních

¹ IVANOV, F., KRISTKO, O. CH. *Krypto jednoduše: nejen o bitcoinu pro začátečníky*. Praha: Fisio/Cuddle Inc., 2022. 41 s. ISBN 978-80-908809-0-0.

² LÁNSKÝ, J. *Kryptoměny*. Praha: C.H.Beck, 2018. 3 s. ISBN 978-80-7400-722-4.

měn. Některé mají neobvyklé názvy, inspirované aktuálními trendy nebo veřejně známými osobnostmi, jako například Trumpcoin nebo Putincoin.³

2.1 Historie peněz a důvod vzniku Bitcoinu

Na počátku lidské civilizace a rozvoje svobodné společnosti fungoval výměnný obchod, známý jako barter. Lidé směňovali zboží za zboží nebo služby za zboží, což byl jednoduchý a přímý způsob obchodování. V raných společnostech se jako prostředky směny využívaly například koření, sůl, kožešiny či určité druhy mušlí. Tento systém však měl limity, protože pokud jedna strana nenabízela něco, co druhá potřebovala, obchod nebylo možné uskutečnit. Tento nedostatek omezoval ekonomický rozvoj i zlepšování životní úrovně a ztěžoval spolupráci v širších komunitách. Barter byl vhodný spíše pro malé společenství, například osady, ale nepostačoval pro výměnu mezi vesnicemi nebo mezinárodní obchod. Proto lidé brzy hledali lepší a trvalejší alternativy. Je fascinující, že napříč různými kulturami se jako nejvhodnější prostředky směny přirozeně prosadily zlato a stříbro. Dnes díky našim znalostem chemie je zřejmé, proč zlato i stříbro mají unikátní vlastnosti, které je činí ideálními pro použití jako peníze.

Jak již bylo uvedeno výše, postupně se nejvíce rozšířily mince vyrobené z drahých kovů, jako je zlato a stříbro. Nejstarší známá mince, která byla vyrobena z přírodní směsi zlata a stříbra, pochází z doby před více než 2 700 lety. Jednou z nevýhod používání mincí z drahých kovů je možnost jejich zmenšení ořezáváním, čímž dochází k poklesu jejich hodnoty. Oddělené části lze následně roztavit a použít k ražbě nových mincí, což vede k postupnému zvýšení množství peněz v oběhu a devalvaci hodnoty každé jednotlivé mince. Protože vlády tolerují inflaci pouze tehdy, když ji samy vyvolají, usilovaly o zastavení tohoto neoficiálního znehodnocování. Jedním z těch, kdo se podílel na ochraně hodnoty mincí byl Isaac Newton, slavný fyzik, který v té době působil jako ředitel Královské mincovny. Právě jemu se připisuje zavedení drobných proužků na okraj mincí, které sloužily jako ochrana proti jejich ořezávání. Tímto krokem tak skončila éra snadného znehodnocování mincí.⁴

³ STROUKAL, D., SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing, a.s., 2021. 150 s. ISBN 978-80-271-1043-8.

⁴ GIGI. *21 lekcí: Co mě naučil pád do bitcoinové králičí nory*. Praha: Nakladatelství Braiins Systems, 2022. 68-69 s. ISBN 978-80-908709-01.

První papírové peníze vznikly v Číně v 11. století, ale v amerických koloniích se objevily až v roce 1690. Kolonie Massachusetts, neschopná vyplatit vojáky po neúspěšné vojenské výpravě, vydala poukázky slibující směnu za zlato nebo stříbro. Tento závazek nebyl dodržen, a množství poukázek se výrazně zvýšilo. Myšlenka papírových peněz se rychle rozšířila do dalších kolonií a získala si podporu významných osobností, jako byl Benjamin Franklin. Do konce 50. let 18. století zažily kolonie masivní inflaci – například Rhode Island až 2 300 %. Nakonec tisk peněz vedl k deflaci a ekonomické krizi.⁵

Aby si papírové peníze udržely hodnotu, mnoho států přijalo měnový standard krytý vzácnými kovy, nejčastěji zlatem nebo stříbrem, uloženými v trezorech. Prvním státem, který zavedl moderní zlatý standard, byla Velká Británie v roce 1717 pod vedením Isaaca Newtona. Tento systém významně přispěl k rozvoji britského obchodu a stal se základem ekonomického růstu v celém britském impériu. Velká Británie držela zlatý standard až do roku 1914, s výjimkou napoleonských válek (1797–1821). S každou další zemí, která oficiálně přijala zlatý standard, rostla poptávka po zlatě, což zvyšovalo jeho hodnotu a zároveň motivovalo další státy, aby tento systém zavedly také. Zlatý standard usnadnil obchod tím, že lidé mohli používat bankovky a šeky kryté zlatem, místo aby nosili těžké mince. Tento systém posílil důvěru v měnu a podpořil mezinárodní obchod.⁶

U peněz krytých zlatem stát funguje jako vydavatel a správce bankovek, zároveň dohlíží na celý systém. Nemá však přímou kontrolu nad množstvím zlata v oběhu. Smí vydat pouze tolik bankovek, kolik odpovídá množství zlata uloženého v rezervách. Americký dolar byl navázán na zlato až do roku 1971, kdy prezident Richard Nixon ukončil možnost jeho směny za zlato, čímž zrušil zlatý standard. Od roku 1971, kdy byl zrušen zlatý standard, jsou státní peníze nekryté, tzv. fiat měna. Fiat, z latiny „rozkaz“ nebo „nařízení“, označuje peníze, jejichž hodnotu určuje důvěra ve stát, nikoli krytí zlatem či jinými aktivy. Stát tak může vydávat peníze v libovolném množství, což v některých případech vede k nadměrnému tisku s negativními dopady na ekonomiku, jako je inflace nebo hyperinflace. Historie ukazuje, že nekontrolované navyšování objemu peněz často končí měnovým kolapsem s vážnými důsledky pro společnost.⁷

⁵ TĚTEK, J. *Bitcoin: odluha peněz od státu*. Praha: Grada Publishing, 2022. 44-45 s. ISBN 978-80-907975-8-1.

⁶ AMMOUS, S. *Bitcoinový standard*. Konsensus Network & Braiins, 2022. 33-34 s. ISBN 978-9916-697-24-5.

⁷ PETŘÍK, T. *1 bitcoin za 10 milionů dolarů*. Brno: Tribun EU s.r.o., 2020. 20-21 s. ISBN 978-80-263-1626-8.

Někteří lidé mají potíže s přijetím myšlenky, že současné peníze jsou primárně založené na dluhu a tvoří je především komerční banky, které mají tuto schopnost na základě privilegium uděleného centrální bankou. Když se o tomto tématu hovoří, někteří lidé dokonce tvrdí, že jde o vymyšlené konspirační teorie. Je zajímavé, že realita dnešního peněžního systému je pro mnoho lidí tak nepochopitelná, že se zdráhají ji přijmout. Možná je přesvědčí následující citát z České národní banky. Peníze vznikají obvykle v okamžiku, kdy komerční banka poskytne úvěr klientovi. Na jeho účet připiše částku odpovídající výši úvěru, což okamžitě znamená navýšení peněžní zásoby. Důležité je, že banka nepůjčuje peníze, které by měla uložené jinde, například v centrální bance, a ani nevyužívá již existující vklady. Při poskytování úvěru banka skutečně vytváří nové peníze "tahem pera" nebo kliknutím na klávesnici, které zde dosud nebyly. A v tu chvíli jsou "najednou" k dispozici.⁸

Historie peněz nám připomíná, že svěřit kontrolu nad měnou jediné centrální autoritě je riskantní rozhodnutí. Moc nad tvorbou a správou peněz představuje pokušení, které bývá dříve či později zneužito. Bitcoin nabízí možnost přerušit cyklus neustálých změn měnových pravidel a znehodnocování peněz, pokud se dokážeme poučit z chyb minulosti. 3. ledna 2009 se v budoucnu bude považovat za klíčový den v monetární historii lidstva. Stát, který dlouho využíval kontrolu nad penězi jako svou hlavní mocenskou páku, ji ztrácí. Tento nástroj se vrací zpět do rukou společnosti.⁹

⁸ TĚTEK, J. *Bitcoin: odluka peněz od státu*. Praha: Grada Publishing, 2022. 11, 54 s. ISBN 978-80-907975-8-1.

⁹ TĚTEK, J. *Bitcoin: odluka peněz od státu*. Praha: Grada Publishing, 2022. 11, 37 s. ISBN 978-80-907975-8-1.

3 Bitcoin

Bitcoin je decentralizovaná digitální měna, která umožňuje přímé transakce mezi jednotlivci nebo počítači bez potřeby zprostředkovatele, jako je například banka. Funguje na principu peer-to-peer sítě, což znamená, že všechny transakce a správa měny probíhají prostřednictvím uživatelů a nejsou řízeny žádnou centrální institucí či organizací.¹⁰

Bitcoin se odlišuje od fiat měn (tradiční peníze) a zlata svou pevně danou vzácností a to tím, že jich nikdy nebude existovat více než 21 milionů bitcoinů. Bitcoin lze rozdělit na velmi malé jednotky, přičemž nejmenší z nich, nazývaná satoshi, odpovídá jedné stomiliontině bitcoinu. To umožňuje vlastníkům přesně vědět, jakou část celkové zásoby drží. Například vlastnictví 10 bitcoinů znamená držbu maximálně 0,03 % z celkového objemu, což je limit, kterého se nelze překročit. Zlato je sice považováno za vzácný zdroj, ale jeho nabídka může růst, pokud se objeví nové, efektivnější metody těžby. Naopak fiat měny podléhají inflačním tlakům, protože vlády často zvyšují jejich nabídku k řešení ekonomických problémů. To způsobuje, že hodnota fiat peněz se v čase obvykle snižuje, což ohrožuje úspory jejich držitelů. Bitcoin díky své předem stanovené nabídce funguje jako obrana proti inflaci a uchovatel hodnoty.¹¹

Technologie Bitcoinu má přirozeně deflační charakter. Nejedná se pouze o domněnku, ale o její základní vlastnost. Vzhledem k tomu, že technologie se stává klíčovou součástí stále většího množství oblastí našeho života, směřujeme do éry deflace, která nemá v historii obdoby.¹²

3.1 Historie Bitcoinu

Dějiny Bitcoinu oficiálně začaly v roce 2008. 18. srpna byla registrována doména bitcoin.org, která dnes stále funguje jako hlavní zdroj informací o Bitcoinu. O několik dní později, 31. srpna, zveřejnil Satoshi Nakamoto svou klíčovou práci, známou jako White paper s názvem "Bitcoin: A Peer-to-Peer Electronic Cash System". V tomto dokumentu vysvětlil, proč je důležitý systém umožňující přímé transakce mezi stranami bez potřeby

¹⁰ PRIZKER, Y. *Vynález jménem Bitcoin*. Praha: Nakladatelství Braiins Systems, 2022. 5 s. 978-80-907975-0-5.

¹¹ BOYAPATI, V. *Bitcoin je budoucnost*. Praha: Nakladatelství Braiins Systems, 2023. 42-43 s. 978-80-908709-2-5.

¹² TĚTEK, J. *Bitcoin: Návrat zdravých peněz*. Praha: Nakladatelství Braiins Systems, 2023. 29 s. 978-80-908709-8-7.

třetí osoby, která by je garantovala, a popsal, jak bude fungovat program, který umožní zapojení do bitcoinové sítě, těžbu bitcoinu a provádění transakcí. Ve stejné době Satoshi Nakamoto také vytěžil prvních 50 bitcoinů, které vznikly spolu s tzv. "genesis blokem", tedy prvním blokem blockchainu, což je decentralizovaná účetní kniha, která od té doby zaznamenává všechny transakce. V tomto prvním bloku byla také ukrytá zpráva: "The Times 03/Jan/2009 Chancellor on Brink of Second Bailout for Banks." v překladu "The Times, 3. ledna 2009: Kancléř na pokraji druhého záchranného balíčku pro banky." Tato zpráva, odkazující na článek britského deníku The Times z uvedeného data, se týkala další finanční pomoci bankám během finanční krize a zároveň reflektovala nespokojenost s tradičním finančním systémem, pro který Bitcoin představoval možnou alternativu. Po zveřejnění kódu se kolem Bitcoinu shromáždila skupina nadšenců, kteří začali testovat novou měnu, prováděli transakce a navrhovali vylepšení. V roce 2010 Satoshi Nakamoto prodal své přístupy k doménám a úložištím kódu Gavinu Andresenovi, jednomu z klíčových členů komunity, a poté přestal aktivně zasahovat do vývoje.¹³

Satoshi Nakamoto popisuje Bitcoin jako decentralizovaný systém elektronických peněz, který nevyžaduje centrální autoritu nebo důvěru v třetí strany. Tradiční měny vyžadují velkou míru důvěry, například v centrální banky nebo finanční instituce, které mohou hodnotu měny znehodnotit nebo s ní špatně hospodařit. Na rozdíl od toho Bitcoin eliminuje potřebu důvěry prostřednictvím kryptografických technologií. Problém tradičních bankovních systémů spočívá i v jejich vysokých nákladech a omezené možnosti provádění mikropłateb. Bitcoin tento problém řeší pomocí otevřeného a decentralizovaného systému, kde transakce jsou bezpečně zaznamenány bez potřeby zásahu třetí strany. Tento systém využívá šifrování a technologii blockchainu, která zabezpečuje data a transakce proti neoprávněnému přístupu. Bitcoin také řeší problém dvojího utracení, kdy síť ověřuje každou transakci a zajišťuje, že platba je provedena pouze jednou. Tento inovativní přístup nabízí efektivní a bezpečný způsob, jak provádět finanční transakce bez závislosti na tradičních bankách.¹⁴

¹³ KALINSKÝ, B. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing, 2018. 14 s. 978-80-87383-71-1.

¹⁴ PRIZKER, Y. *Vynález jménem Bitcoin*. Praha: Nakladatelství Braiins Systems, 2022. 8-9 s. 978-80-907975-0-5.

4 Funkční principy Bitcoinu

Následující kapitola se zaměří na analýzu a ekosystém Bitcoinu. Popíše technologie, které tvoří tento systém, jak umožňuje plnit různé funkce, jako je vytváření, přesouvání a uchovávání hodnoty, a jak vlastně celý systém funguje. Pro vytvoření alternativního systému digitálních peněz, který je globální, bezpečný a nezávislý na centrální autoritě (tedy umožňuje přímou komunikaci mezi uživateli), bylo nutné vyřešit problém správného zaznamenávání transakcí, aby bylo zajištěno, že nikdo nebude moci neoprávněně vytvářet nebo krást peníze. Řešení spočívá v kombinaci několika technologií: decentralizované architektury, šifrování, motivačních mechanismů a specifických databázových struktur.¹⁵

4.1 Decentralizace

Decentralizace v bitcoinové síti spočívá v propojení rovnocenných uzlů v peer-to-peer síti bez centrálního bodu kontroly. Na rozdíl od centralizovaných systémů, kde servery řídí připojení klientů, zde žádný uzel nemá nad sítí výhradní moc. Tento model zajišťuje odolnost vůči výpadkům nebo zneužití, protože vyřazení jednoho nebo několika uzlů neohroží celkovou funkčnost. Uzly v síti plní různé funkce. Slouží jako peněženky, které vytvářejí a podepisují transakce pomocí kryptografie. Přijímají transakce, ověřují jejich správnost a předávají je dalším uzlům. Některé uzly se podílejí na těžbě, kdy shromažďují transakce do bloků, které pak přidávají do blockchainu za odměnu v podobě nově vytvořených bitcoinů. Další uzly fungují jako pooly, které rozdělují práci mezi těžaře. Všechny uzly zároveň udržují záznamy blockchainu, čímž zajišťují integritu systému. Síť tvoří tisíce uzlů rozmístěných po celém světě. Tento rozptyl a nízké náklady na provoz nových uzlů zajišťují, že síť je obtížné vyřadit nebo zcela zničit. Na rozdíl od tradičních bankovních systémů nevyžaduje drahou infrastrukturu ani rozsáhlé technické týmy. Nevýhodou tohoto decentralizovaného modelu je nižší efektivita, protože všechny uzly vykonávají stejné úkoly, bez ohledu na aktuální potřeby. Tento přístup však upřednostňuje bezpečnost a stabilitu systému před maximální efektivitou.¹⁶

¹⁵ KALINSKÝ, B. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing, 2018. 37-38 s. 978-80-87383-71-1.

¹⁶ KALINSKÝ, B. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing, 2018. 38 s. 978-80-87383-71-1.

4.2 Šifrování (protokol a kryptografie)

Bitcoin využívá moderní kryptografii, která zahrnuje obrovská čísla, jež jsou pro lidskou intuici téměř nepředstavitelná. Jedním z nejdůležitějších prvků je hashovací funkce SHA-256, která používá 256 bitů k vytvoření bezpečného otisku dat. To, co si běžně představujeme pod 256 bity, není skutečná velikost čísla; ve skutečnosti jde o číslo 2 na 256, což je neuvěřitelně velká hodnota. Konkrétně toto číslo je ohromující, přesahující miliardy miliard a ještě mnohem víc. Pro srovnání, je to mnohem větší než počet atomů v pozorovatelném vesmíru. Tak velká čísla jsou pro nás těžko pochopitelná. Bezpečnost algoritmu SHA-256 spočívá v této obrovské velikosti čísla. Toto číslo má 78 číslic a jeho přesná hodnota je následující: 115 792 089 237 316 195 423 570 985 008 687 907 853 269 984 665 640 564 039 457 584 007 913 129 639 936. Kdyby někdo chtěl tento algoritmus prolomit, musel by provést neuvěřitelně složité výpočty, které by vyžadovaly nesmírně výkonný hardware. To je důvod, proč je Bitcoin zabezpečený: i s dnešními technologiemi je takové číslo prakticky nemožné uhodnout nebo prolomit.¹⁷

4.3 Těžba (mining)

Těžba bitcoinu se výrazně liší od tradiční těžby, protože nesouvisí s těžbou přírodních zdrojů. Bitcoinová těžba spočívá v ověřování transakcí, které probíhají na blockchainu, což je decentralizovaný záznam transakcí. Transakce se shlukují do bloků, které jsou na sebe navázány, což vytváří blockchain. Primárním cílem těžby je ověřování těchto transakcí. Každý blok může obsahovat až 1 MB dat, což odpovídá přibližně 500 transakcím. Průměrný čas pro uzavření jednoho bloku je deset minut. Tento proces je zajištěn mechanismem Proof of Work (důkaz práce), který zaručuje validitu transakcí. Aby byly transakce považovány za definitivní, je nutné počkat na potvrzení několika dalších bloků. Nové bitcoiny vznikají během těžby. Těžaři soutěží o to, kdo jako první úspěšně uzavře blok a potvrdí, že všechny transakce v něm jsou platné. Vítěz získá odměnu v podobě nových bitcoinů. Uzavření bloku zahrnuje použití hashovací funkce, která "smíchá" data o transakcích do unikátní hodnoty nazývané hash. Tento proces zajišťuje integritu a bezpečnost blockchainu. Důležité je také neustálé vylepšování protokolu prostřednictvím BIPů (Bitcoin Improvement Proposals), které zvyšují

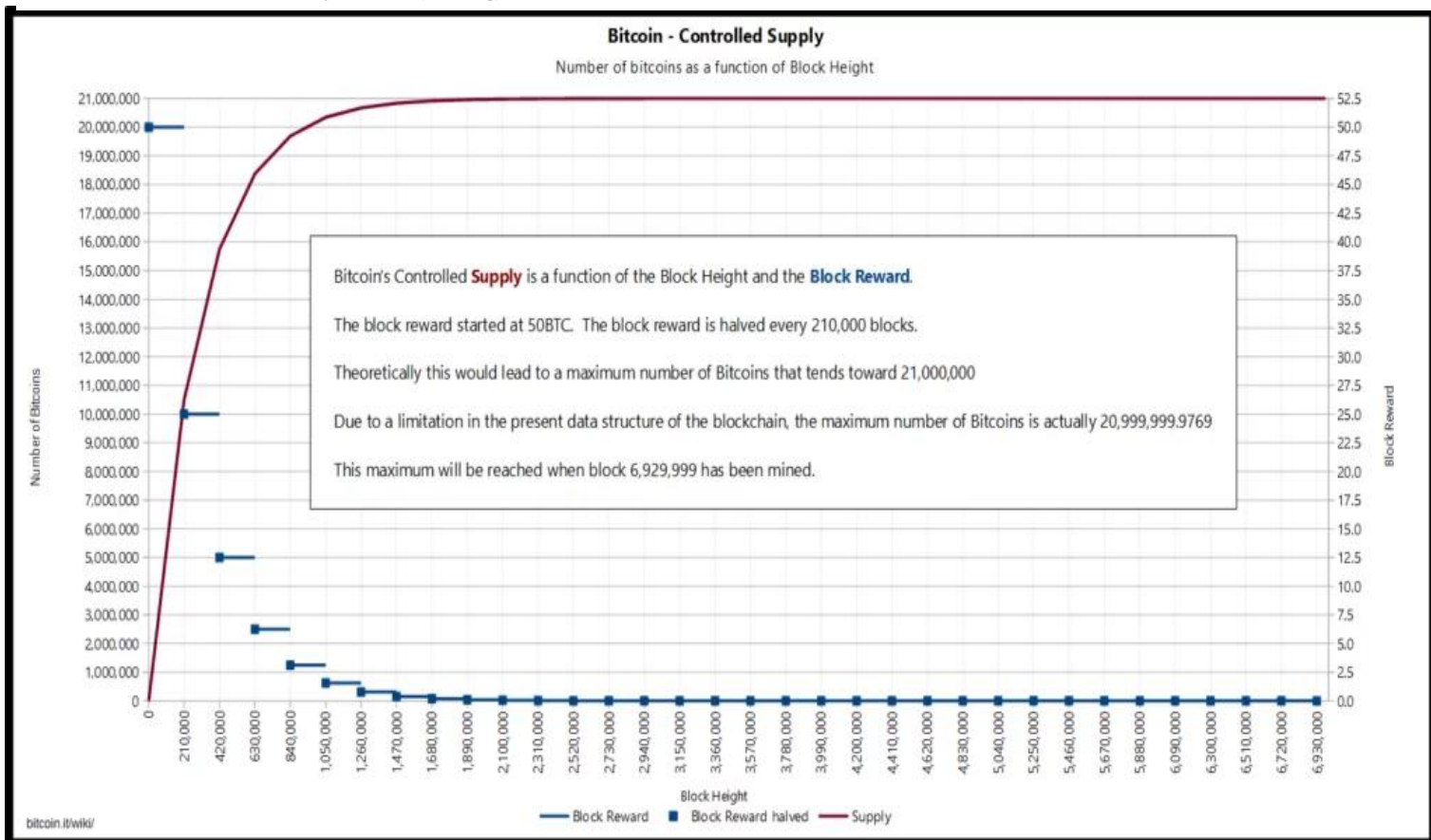
¹⁷GIGI. 21 lekcí: *Co mě naučil pád do bitcoinové králičí nory*. Praha: Nakladatelství Braiins Systems, 2022. 94-95 s. ISBN 978-80-908709-01.

efektivitu a bezpečnost sítě, včetně optimalizace velikosti transakcí a jejich přesouvání mimo hlavní blockchain.¹⁸

4.3.1 Půlení odměny za blok (halving)

Bitcoin vytváří nové mince prostřednictvím těžby, která potvrzuje transakce a zároveň vydává nové bitcoiny. Satoshi Nakamoto chtěl, aby zásoba bitcoinů rostla postupně, ale ne neomezeně, což vedlo k zavedení plánu půlení blokové odměny. Původně byla bloková odměna 50 bitcoinu, ale každé čtyři roky se tato odměna sníží na polovinu. V roce 2012 klesla na 25 bitcoinu, v roce 2016 na 12,5 bitcoinu, a v roce 2020 na 6,25 bitcoinu. Tento proces bude pokračovat až do roku 2140, kdy bude vytěženo všech 21 milionů bitcoinů a těžaři budou odměňováni pouze poplatky za transakce. Tento mechanismus pomáhá zajistit omezenou nabídku bitcoinů a tím zabránit inflaci. Kód Bitcoinu obsahuje pravidla, která automaticky odmítají bloky, jež neodpovídají těmto principům.¹⁹

Obrázek 1 - Graf Půlení odměny za blok (halving)



Zdroj: PRIZKER, Y. Vynález jménem Bitcoin. Praha: Nakladatelství Braiins Systems, 2022. 45 s.978-80-907975-0-5.

¹⁸ NEJESCHLEBA, R. BITCOIN: SEZNAMTE SE! Pochopte bitcoin i bez hlubokých znalostí informatiky či ekonomie. Ve Strážnici: vlastním nákladem, 2022. 33-34 s. ISBN 978-80-11-01333-2.

¹⁹ NEJESCHLEBA, R. BITCOIN: SEZNAMTE SE! Pochopte bitcoin i bez hlubokých znalostí informatiky či ekonomie. Ve Strážnici: vlastním nákladem, 2022. 44-45 s. ISBN 978-80-11-01333-2.

4.4 Struktura databází (blockchain)

Blockchain, tedy řetězec bloků, zajišťuje bezpečnost a neměnnost bitcoinových transakcí. Každý blok obsahuje data o transakcích, hash předchozího bloku a důkaz o vykonané práci. Tímto způsobem jsou všechny bloky propojeny, což vytváří lineární a ověřitelnou historii od prvního bloku (Genesis block) až po současnost. Jakmile je blok přidán do blockchainu, jakákoliv změna v jeho datech by změnila jeho hash. Protože hash bloku je součástí dat následujícího bloku, bylo by nutné přepočítat všechny následující bloky v řetězci. To by vyžadovalo obrovské množství výpočetního výkonu, což činí manipulaci s historií prakticky nemožnou. Důkaz o vykonané práci (Proof of Work) navíc zajišťuje, že vytvoření bloku vyžaduje značné množství energie a času. Tato energetická náročnost funguje jako ochrana proti podvodům. Každý nový blok přidáný do blockchainu zvyšuje zabezpečení předchozích bloků. Čím je blok starší, tím je obtížnější jej změnit, protože by bylo nutné přepočítat všechny následující bloky včetně jejich důkazů práce. Blockchain je distribuovaný. Tisíce uzlů po celém světě uchovávají jeho kopii. Všechny transakce v blockchainu jsou transparentní. Každý uživatel si může ověřit jejich pravost a integritu. To zajišťuje vysokou odolnost vůči podvodům, nátlaku nebo korupci.²⁰

²⁰ PRIZKER, Y. *Vynález jménem Bitcoin*. Praha: Nakladatelství Braiins Systems, 2022. 57-59 s. ISBN 978-80-907975-0-5.

5 Pojem kyberkriminalita

Kybernetická kriminalita představuje formu trestné činnosti, v níž je počítač, jeho technické či programové vybavení, data, nebo jejich propojení v síti zapojeno buď jako předmět útoku, prostředí, ve kterém je trestná činnost páchána, nebo jako nástroj sloužící k jejímu provedení. Do této oblasti nespádají případy, kdy je počítač nebo jeho součásti předmětem útoku výhradně jako movitá věc. Tato trestná činnost zahrnuje široké spektrum jednání, od neoprávněného přístupu k datům až po komplexní útoky na informační infrastruktury.²¹

Kyberprostor je virtuální prostředí tvořené propojenými počítačovými systémy, sítěmi a digitálními zařízeními. Někteří odborníci varují před vnímáním kyberprostoru jako alternativní sféry s odlišnými pravidly, zdůrazňují, že jde o specifickou komunikační síť umožňující spojení lidí a informací. Jiní ho označují za prostor, kde ekonomická hodnota vzniká z myšlenek a jejich virtuálních vyjádření, spíše než z fyzického majetku. Zákon o kybernetické bezpečnosti definuje kyberprostor jako digitální prostředí pro vznik, zpracování a výměnu informací, které je tvořeno informačními systémy a elektronickými komunikačními sítěmi. Klíčovými prvky kyberprostoru jsou virtualita, informace a schopnost vzájemného propojení²².

Kyberprostor je veřejný prostor, který není vlastněn žádnou osobou, úřadem ani státem, a jeho bezpečnostní opatření musí být koordinována mezi různými subjekty. Mezi klíčové charakteristiky kyberprostoru patří anonymita, protože identita uživatelů není snadno prokazatelná. Asymetričnost znamená, že činnost v kyberprostoru může mít dopad na ostatní uživatele bez ohledu na jejich důvěryhodnost. Neexistence hranic znamená, že aktivity nejsou omezeny žádnou jurisdikcí. Okamžitost znamená, že akce mohou mít okamžitý globální dopad. Kyberprostor umožňuje volný vstup i ukončení pobytu, což znamená, že každý může kdykoliv vstoupit nebo vystoupit. Nakonec interakce v kyberprostoru vytvářejí nové znalosti a ovlivňují ostatní uživatele.²³

²¹ KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky v Praze, 2020. 33 s. ISBN 978-80-7251-505-9.

²² RAMEŠOVÁ K. *Právní regulace kybernetické bezpečnosti a její meze*. Praha: Nakladatelství C.H. Beck, 2023. 17 s. ISBN 978-80-7400-931-0.

²³ DOUCEK, P, KONEČNÝ M, NOVÁK L. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. 18-19 s. ISBN 978-80-88260-39-4.

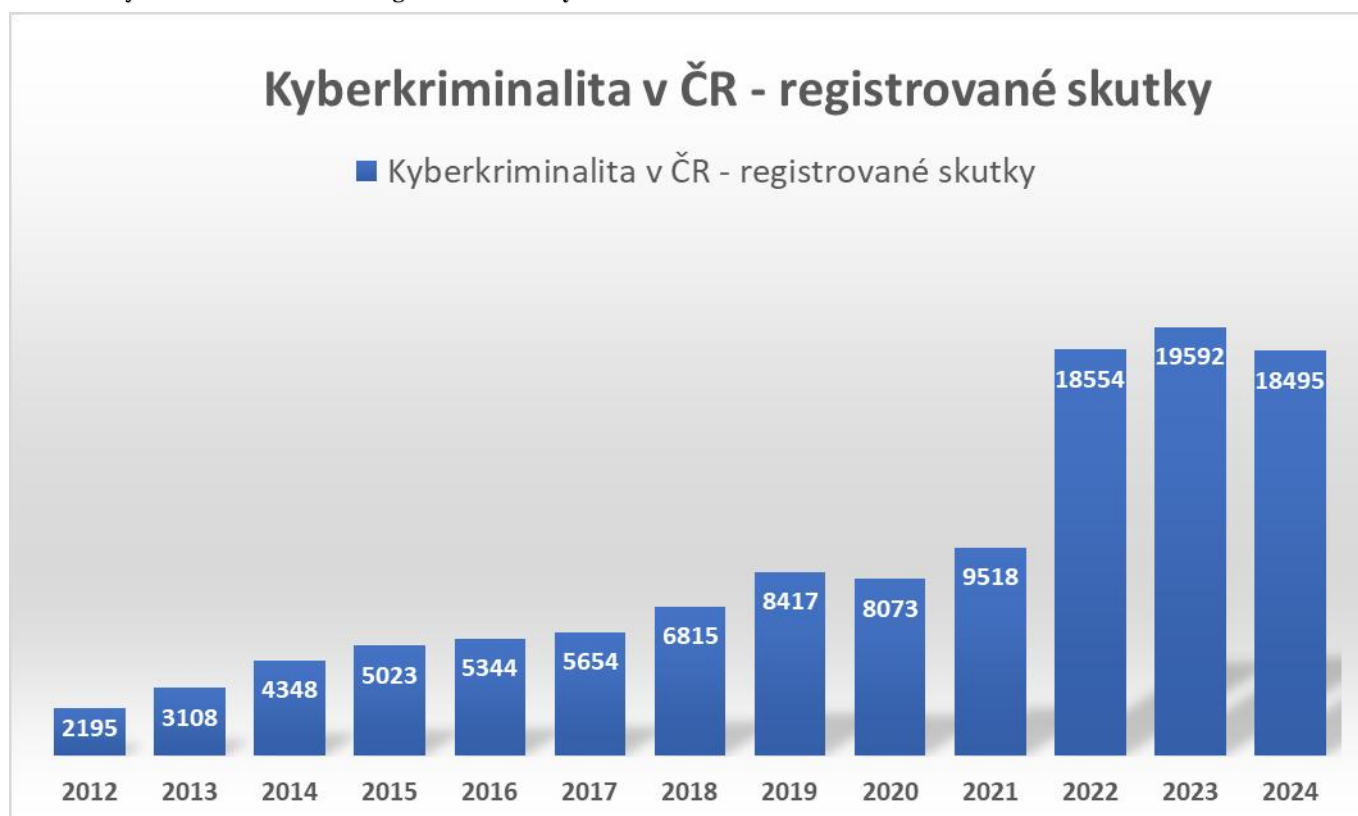
Tabulka 1 - Statistika kyberkriminality v ČR za období 2021-2023

spácháno internetem + ostatními sítěmi (kyberkriminalita) Česká republika, období 1.1. - 31.12.			
	2021	2022	2023
registrované skutky	9518	18554	19592
objasněné skutky	2356	2799	2699
výše způsobené škody celkem	1 458 188 174	3 101 079 286	2 961 974 579

Zdroj: Policie České republiky. Online. Dostupné z: <https://policie.gov.cz/clanek/statistika-kyberkriminality.aspx>. Citováno [2025-02-15].

Kyberkriminalita patří v České republice i celosvětově dlouhodobě k nejstrměji rostoucí trestné činnosti. V roce 2022 tvořila s 18,5 tisíci případy více než 10 % z celkové registrované kriminality v Česku. Meziročně tato kriminalita vzrostla takřka o 100 % (94,9 %). V minulém roce byly nejčastější útoky na přihlašovací údaje k bankovním účtům, přesně cílené ransomware útoky pomocí e-mailu nebo SMS, útoky DoS/DDoS nebo útoky pomocí škodlivých kódů s cílem krádeže dat a účtů uživatelů²⁴.

Graf 1 - Kyberkriminalita v ČR – registrované skutky



Zdroj: Policie České republiky. Online. Dostupné z: <https://policie.gov.cz/clanek/statistika-kyberkriminality.aspx>. Citováno [2025-02-15].

²⁴Ministerstvo vnitra České republiky. [online]. Dostupné z: https://mv.gov.cz/clanek/na-nebezpeci-kyberkriminality-upozorni-den-bezpecnejsiho-internetu.aspx?utm_source=chatgpt.com. Citováno [2025-01-05].

5.1 Trestné činy v prostředí kryptoměn

Oblast kryptoměn se v posledních letech stala nejen prostředkem pro inovace a investice, ale také nástrojem, který podvodníci a organizované skupiny zneužívají k nezákonným činnostem. Kryptoměny, díky své anonymitě, decentralizované povaze a globálnímu dosahu, otevírají nové možnosti pro trestnou činnost, která často překračuje hranice států.

Trestné činy spojené s kryptoměnami lze zařadit pod ustanovení zákona č. 40/2009 Sb., trestní zákoník, a to konkrétně do Hlavy V – Trestné činy proti majetku a Hlavy VI – Trestné činy hospodářské, Díl 1 - Trestné činy proti měně a platebním prostředkům. Mezi nejčastější delikty patří:

Podvod – znění zákona trestní čin Podvodu §209 zákon č. 40/2009 Sb., trestní zákoník. *„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“*²⁵

Legalizace výnosů z trestné činnosti – znění zákona trestný čin Legalizace výnosů z trestné činnosti §216 Sb., trestní zákoník. *„Kdo ukryje, na sebe nebo na jiného převede, přechovává nebo užívá věci, která je výnosem z trestné činnosti spáchané na území České republiky nebo v cizině jinou osobou, nebo kdo takovou věc přemění v úmyslu umožnit jiné osobě, aby unikla trestnímu stíhání, trestu nebo ochrannému opatření nebo jejich výkonu, nebo kdo se ke spáchání takového trestného činu spolčí, bude potrestán odnětím svobody až na čtyři léta, peněžitým trestem, zákazem činnosti nebo propadnutím věci.“*²⁶

Legalizace výnosů z trestné činnosti z nedbalosti – znění zákona trestný čin Legalizace výnosů z trestné činnosti z nedbalosti § 217 Sb., trestní zákoník. *„Kdo jinému z nedbalosti umožní zastřít původ nebo zjištění původu větší hodnoty, která je výnosem*

²⁵ ČESKO. *Zákony II : úplná znění zákonů a souvisejících předpisů z oblasti trestní zákoník, trestní řád, zákon o odpovědnosti za přestupky a řízení o nich.* Český Těšín: PORADCE, s. r. o., 2020. 49 s. ISBN 1802-8330.

²⁶ ČESKO. *Zákony II : úplná znění zákonů a souvisejících předpisů z oblasti trestní zákoník, trestní řád, zákon o odpovědnosti za přestupky a řízení o nich.* Český Těšín: PORADCE, s. r. o., 2020. 51 s. ISBN 1802-8330.

z trestné činnosti spáchaná na území České republiky nebo v cizině, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci.“²⁷

Porušení povinnosti při správě cizího majetku – znění zákona trestný čin Porušení povinnosti při správě cizího majetku § 220 Sb., trestní zákoník. „*Kdo poruší podle zákona mu uloženou nebo smluvně převzatou povinnost opatrovat nebo spravovat cizí majetek, a tím jinému způsobí škodu nikoli malou, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.*”²⁸

Neoprávněný přístup k počítačovému systému a nosiči informací – znění zákona trestný čin Neoprávněný přístup k počítačovému systému a nosiči informací §230 zákon. č. 40/2009 Sb., trestní zákoník. „*Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.*“²⁹

Zkrácení daně, poplatku a podobné povinné platby – znění zákona trestný čin Zkrácení daně, poplatku a podobné povinné platby §240 zákon č. 40/2009 Sb., trestní zákoník. „*Kdo ve větším rozsahu zkrátí daň, clo, pojistné na sociálním zabezpečení, příspěvek na státní politiku zaměstnanosti, pojistné na úrazové pojištění, pojistné na zdravotní pojištění, poplatek nebo jinou podobnou povinnou platbu anebo vyláká výhodu na některé z těchto povinných plateb, bude potrestán odnětím svobody na šest až tři léta nebo zákazem činnosti.*“³⁰

²⁷ ČESKO. *Zákony II : úplná znění zákonů a souvisejících předpisů z oblasti trestní zákoník, trestní řád, zákon o odpovědnosti za přestupky a řízení o nich.* Český Těšín: PORADCE, s. r. o., 2020. 51 s. ISBN 1802-8330.

²⁸ ČESKO. *Zákony II : úplná znění zákonů a souvisejících předpisů z oblasti trestní zákoník, trestní řád, zákon o odpovědnosti za přestupky a řízení o nich.* Český Těšín: PORADCE, s. r. o., 2020. 53 s. ISBN 1802-8330.

²⁹ ČESKO. *Zákony II : úplná znění zákonů a souvisejících předpisů z oblasti trestní zákoník, trestní řád, zákon o odpovědnosti za přestupky a řízení o nich.* Český Těšín: PORADCE, s. r. o., 2020. 54 s. ISBN 1802-8330.

³⁰ ČESKO. *Zákony II : úplná znění zákonů a souvisejících předpisů z oblasti trestní zákoník, trestní řád, zákon o odpovědnosti za přestupky a řízení o nich.* Český Těšín: PORADCE, s. r. o., 2020. 56 s. ISBN 1802-8330.

6 Nejčastější podvody v online prostoru ve spojitosti s Bitcoinem a dalšími kryptoměny

Ekosystém digitálních měn, jehož hodnota dosáhla až 1,8 bilionu dolarů, připomíná „Divoký západ“ – technologie a inovace překonávají regulace, které za nimi značně zaostávají. V důsledku toho vzniká prostor pro zločinecké aktivity, včetně podvodů, hackerských útoků, krádeží, únosů a vydírání. Podvodné systémy, jako Ponziho schémata, se staly běžnou součástí tohoto světa. V tomto kontextu kryptoměny a jejich ekosystém jsou častým cílem pro podvodníky, mafii a oportunisty, kteří se zaměřují na vysoké zisky a manipulaci s informacemi. Zakladatel kryptoměny Litecoin, Charlie Lee, to trefně shrnul v proslulém tweetu: „Když něco vypadá jako kachna, plave jako kachna a kváká jako kachna, je to Ponziho schéma.“ Tento svět je bohužel místem, kde podvody a nelegální činnosti jsou téměř na denním pořádku.³¹

Bitcoin bývá často spojován s nelegální činností kvůli představě, že je zcela anonymní. To však není pravda, bitcoin je pseudonymní. Veřejný blockchain uchovává všechny transakce, které kdy proběhly, a kdokoliv si je může prohlédnout, přičemž záznamy nelze zpětně smazat. Místo konkrétních jmen obsahuje blockchain bitcoinové adresy (směsici písmen a čísel). Bitcoinové transakce jsou velmi snadno trasovatelné, což komplikuje jeho využití k nelegálním aktivitám. Specializované firmy se zabývají trasováním transakcí a často spolupracují se státními složkami. Díky otevřenosti blockchainu mohou orgány činné v trestním řízení získat informace o pohybu a množství bitcoinů, což výrazně usnadňuje odhalování nelegálních aktivit.³²

Kryptoměny se staly populární alternativou k tradičním měnám, přičemž jejich atraktivitu zvyšuje potenciál vysokých zisků. I přes jejich proměnlivou hodnotu zájem o kryptoměny roste, zejména díky snadné dostupnosti aplikací umožňujících jejich nákup a správu. Tato oblíbenost však přitahuje i podvodníky, kteří hledají způsoby, jak využít kryptoměny k vlastnímu obohacení, zejména vzhledem k jejich anonymní povaze. Bitcoin, jako jedna z nejznámějších kryptoměn, je obzvláště lákadlem, a podvodníci často

³¹ STANFORD E. *Cryptowars*. London: Kogan Page Ltd, 2021. 9 s. ISBN 978-13-9860-068-3.

³² NOVÁK M. *Bitcoin: Revoluce, nebo podvod?* Praha: Nakladatelství Braiins Systems, 2024. 73-74 s. ISBN 978-80-908709-9-4.

cílí na uživatele, kteří v kryptoměnách vidí příležitost k rychlému zisku, ale nemusí být dostatečně obeznámeni s riziky spojenými s touto investicí.³³

6.1 Falešné investiční platformy

Podvodníci často využívají kryptoměnové trhy k vytvoření falešných burz nebo investičních platforem, které na první pohled vypadají jako legitimní a spolehlivé. S pomocí atraktivních reklam, slibů vysokých výnosů a odborných analýz lákají oběti, aby investovaly své peníze. Tyto platformy často slibují rychlé a bezpečné zisky z obchodování s kryptoměnami nebo poskytnutí exkluzivních investičních příležitostí. Jakmile uživatelé odešlou své prostředky na účet platformy, pachatelé přestanou komunikovat a zmizí. Platforma je často zrušena, nebo je zcela blokována přístup k účtům uživatelů, čímž zůstávají jejich investice nenávratně ztraceny. Tento typ podvodu je obzvláště nebezpečný, protože oběti často nemají možnost své prostředky získat zpět, a to kvůli anonymitě kryptoměn a absenci efektivní regulace v tomto sektoru.

Podvodníci často lákají své oběti na velmi výhodné nabídky, které se objevují například ve formě internetové reklamy. Kromě investičních příležitostí různých typů nabízejí také pomoc s nákupem kryptoměn, obvykle s příslibem vysokých výnosů. Komunikace mezi podvodníky a obětí bývá dlouhodobá. Oběť je neustále ujišťována, že vše probíhá podle plánu, například prostřednictvím přístupu k falešnému investičnímu portfoliu nebo virtuální peněženice na podvodných webových stránkách. Pro zvýšení důvěryhodnosti bývají vyžadovány pravidelné vklady, přičemž výplata výnosů je podmíněna dlouhodobějším setrváním v systému. Poškozený se tak o podvodu často dozví až po delší době, kdy už investoval značné finanční prostředky. Podvodné organizace jsou velmi dobře organizované a působí profesionálně. Mívají několik úrovní „pracovníků“, mezi které patří operátoři, investiční poradci, technici či manažeři. Jejich podvodné scénáře jsou pečlivě propracované s cílem maximalizovat zisky. Pokud se oběť pokusí získat své investované peníze zpět, podvodníci přecházejí ke strategii komplikací. Tvrdí například, že je potřeba provést ještě jednu poslední platbu, po které již budou slíbené peníze vyplaceny. Tento typ psychické manipulace se označuje jako efekt utopených nákladů (sunk cost fallacy) – oběť si říká: „Už jsem do toho investoval tolik, teď přece nemůžu přestat, když jsem tak blízko!“ Oběti často podvodníkům dobrovolně

³³Policie České republiky. Online. Dostupné z: <https://policie.gov.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx>. Citováno [2025-01-08].

poskytují citlivé osobní údaje, kopie dokladů totožnosti, platebních karet nebo dokonce umožňují vzdálený přístup ke svému počítači. Tím se vystavují riziku zneužití svých financí i identity, což může vést k úplnému vyprázdnění jejich bankovního účtu.³⁴

6.2 Phishingové útoky

Phishing je podvodná činnost, při které pachatel vydává sám sebe za důvěryhodnou osobu nebo instituci, aby získal citlivé informace, jako jsou přihlašovací údaje, čísla sociálního pojištění nebo bankovní detaily. Útočníci často využívají falešné webové stránky nebo e-maily, které napodobují legitimní služby, a pomocí manipulace přesvědčí oběti k zadání svých údajů. Součástí tohoto podvodu může být i odkaz obsahující škodlivý software, který oběť nevědomky aktivuje.³⁵

Phishing je nejrozšířenější typ kybernetického útoku, jehož cílem je získat citlivé údaje, jako jsou čísla kreditních karet, hesla nebo jiné důvěrné informace. Útočníci se vydávají za důvěryhodné instituce a snaží se přesvědčit oběti, aby jim tyto údaje dobrovolně poskytly. Bohužel, mnoho lidí na tyto podvody stále naletí. S rozvojem technologií phishing nabývá i sofistikovanějších forem. Útočníci například vytvářejí falešné verze aplikací používaných pro nákup a prodej kryptoměn. V takovém případě vás přímo nekontaktují, ale podstrčí vám podvodný software, který se vydává za legitimní aplikaci. Pokud jej nic netušící uživatel použije, může nevědomky udělit útočníkovi přístup ke svým finančním prostředkům.³⁶

6.3 Pyramidové hry a Ponziho schémata

Pyramidové schéma je podvodný model, který funguje na principu hierarchické struktury. Účastníci na nižších úrovních finančně podporují ty na vyšších úrovních, přičemž jejich příjmy závisí na získávání nových členů do systému. Noví členové se poté zařazují na nižší úroveň a poskytují prostředky těm, kteří jsou v hierarchii nad nimi. Tento

³⁴Policie České republiky. Online. Dostupné z: <https://policie.gov.cz/clanek/prevence-kraj-kryptomeny-v-rukou-podvodniku.aspx>. Citováno [2025-01-29].

³⁵IVANOV, F., KRISTKO, O. CH. *Krypto jednoduše: nejen o bitcoinu pro začátečníky*. Praha: Fisio/Cuddle Inc., 2022. 69 s. ISBN 978-80-908809-0-0.

³⁶ČESKO. Finex. Online. Dostupné z: <https://finex.cz/phishing-kryptomeny/>. Citováno [2025-01-29].

cyklus pokračuje, dokud nepřestane přibývat dostatek nových účastníků, což vede ke kolapsu schématu.³⁷

Americká Komise pro cenné papíry (SEC) odhalila nelegální činnost skupiny osob stojících za projektem Forsage, který fungoval jako pyramidové schéma. Od investorů po celém světě podvodně získali více než 300 milionů dolarů. Podle žaloby SEC spustili Vladimír Okhotnikov, Michail Sergejev, Sergej Maslakov a další v roce 2020 web Forsage.io, který se prezentoval jako decentralizovaná platforma pro smart kontrakty na blockchainech Ethereum, Tron a Binance. Ve skutečnosti však šlo o podvodné schéma, kde jediným způsobem výdělku bylo získávání nových účastníků. Forsage bylo opakovaně terčem regulačních zásahů, protože v roce 2020 proti němu zasáhla filipínská Komise pro cenné papíry, v roce 2021 pak regulátor v Montaně. Navzdory tomu obžalovaní v propagaci pokračovali. SEC v žalobě označila Forsage za učebnicový příklad pyramidového a Ponziho schématu, které bylo agresivně propagováno na sociálních sítích a dalších investičních platformách. Podle vyšetřovatelů neprodávalo žádný skutečný produkt, a investoři mohli vydělat pouze zapojením nových členů. Kromě čtyř hlavních zakladatelů SEC obvinila také tři organizátory v USA, kteří schéma aktivně propagovali, včetně na platformách jako YouTube. Mezi obviněnými jsou i osoby, které vedly největší propagační skupinu Forsage na území USA. Forsage je dalším příkladem podvodných projektů v oblasti kryptoměn, kdy se pachatelé snaží obejít federální zákony o cenných papírech tím, že se odvolávají na blockchainové technologie a smart kontrakty.³⁸

6.4 Falešné tokeny a ICO

Podvodníci často využívají popularitu kryptoměn k vytvoření falešného projektu nebo tokenu, který prezentují jako slibnou investiční příležitost. Prostřednictvím procesu nazývaného Initial Coin Offering (ICO) lákají investory na nereálné přísliby vysokých výnosů či revoluční technologie. Na základě dobře zpracovaného marketingu a zdánlivě profesionální prezentace získají od důvěřivých investorů finanční prostředky. Jakmile obdrží požadované investice, projekt náhle ukončí, zmizí z trhu a investoři přijdou o své

³⁷IVANOV, F., KRISTKO, O. CH. *Krypto jednoduše: nejen o bitcoinu pro začátečníky*. Praha: Fisio/Cuddle Inc., 2022. 72 s. ISBN 978-80-908809-0-0.

³⁸Seznam zprávy. Online. Dostupné z: <https://www.seznamzpravy.cz/clanek/ekonomika-finance-byznys-meny-kryptomeny-lakali-na-slova-jako-krypto-nebo-blockchain-slo-o-obri-pyramidovy-podvod-210669>. Citováno [2025-01-29].

peníze. Tito podvodníci často zneužívají nedostatečné znalosti uživatelů a nedokonalou regulaci kryptoměnového trhu.

Ve studii zaměřené na ICO projekty uskutečněné v roce 2017 bylo zjištěno, že až 80 % z nich mělo podvodný charakter. Mezi nejznámější případy patřil projekt Confido, který v listopadu 2017 získal 375 000 dolarů, než jeho tvůrci zmizeli. Po zveřejnění této skutečnosti cena tokenu prudce klesla z 0,60 USD na 0,10 USD během několika hodin a nadále ztrácela hodnotu. Dalším rozsáhlým podvodným ICO bylo Centra, které získalo 32 milionů dolarů a využilo ke své propagaci známé osobnosti, například Floyda Mayweathera a DJ Khaleda. V dubnu 2018 byli dva zakladatelé projektu zatčeni a token následně ztratil téměř veškerou hodnotu. Podvodná ICO často zneužívají falešné informace o svých vývojových týmech nebo poradcích. Tvůrci těchto projektů se snaží vzbudit důvěru tím, že uvádějí fiktivní odborníky s údajným napojením na významné instituce nebo veřejně známé osobnosti. Fotografie těchto členů týmů bývají snadno dohledatelné na internetu, což může pomoci odhalit podvodné záměry projektu. Dalším častým trikem je nabízení tokenů na sociálních sítích. Podvodníci se často vydávají za významné osobnosti kryptoměnového světa, například Vitalika Buterina nebo Elona Muska, a slibují uživatelům, že jim zdarma poskytnou tokeny. Běžnou taktikou je výzva typu: „Pošlete 1 ETH na tuto adresu a obdržíte zpět větší množství kryptoměny.“ Takové nabídky jsou vždy podvodné, protože kryptoměny představují finanční hodnotu, a nikdo je nerozdává zdarma³⁹.

6.5 Podvodné miningové programy

Podvodníci využívají oblíbenosti těžby kryptoměn a vytvářejí falešné nabídky softwaru nebo cloudových služeb, které údajně umožňují těžit kryptoměny s vysokými zisky. Tyto služby lákají na jednoduchost použití a zaručený pasivní příjem bez velkých investic, přičemž slibují vysoké výnosy z efektivního těžebního procesu. Jakmile uživatelé zakoupí přístup, zjistí, že buď nefungují vůbec, nebo jsou navrženy tak, aby tajně těžily kryptoměny pro podvodníky. V některých případech programy obsahují skrytý kód, který využívá výpočetní výkon zařízení uživatele pro těžbu bez jeho vědomí. Tento typ podvodu je obzvlášť nebezpečný, protože nezanechává viditelné stopy a oběti se obtížně domáhají náhrady škod. Podvodníci také často vytvářejí webové stránky, které

³⁹Binance square. Online. Dostupné z: <https://www.binance.com/en/square/post/147556/>. Citováno [2025-01-30].

napodobují oficiální platformy pro cloudovou těžbu. Mohou zkopírovat logo známé společnosti nebo vytvořit podobné a použít doménu, která vypadá jako ta pravá, ale s malou změnou. Jiné podvody se zaměřují na jednodušší weby, které cílí na lidi, kteří nejsou dostatečně obeznámeni s kryptoměnami a nepoznají falešnou stránku. Dříve existovaly i aplikace, které slibovaly využití výkonu zařízení pro těžbu kryptoměn, jako je Monero. Tyto aplikace, často implementované pomocí pluginů, těžily kryptoměny na počítačích uživatelů bez jejich vědomí a způsobovaly přetížení systémů. Hackeri ovládali počítačové sítě a instalovali těžební software, z něhož výnosy směřovaly do jejich peněženek. I když většina těchto aplikací již nefunguje, stále existují podvodníci, kteří vytvářejí falešné aplikace, které vypadají důvěryhodně, ale nemají žádnou skutečnou těžební schopnost. Jejich cílem je přimět uživatele k utrácení peněz nebo klikání na reklamy, z nichž podvodníci získávají příjmy. Některé aplikace napodobují skutečné platformy pro cloudovou těžbu, ale ve skutečnosti nenabízejí žádnou funkční službu.⁴⁰

6.6 Schémata Pump and Dump

Pump and Dump je strategie v kryptoměnách, při které skupina investorů koordinovaně manipuluje s cenou určitého aktiva, často u projektů s nízkou tržní kapitalizací a nízkou likviditou. Tento proces zahrnuje umělé zvýšení ceny následované jejím rychlým poklesem, což může vést k finančním ztrátám pro nezkušené investory. Tato strategie je považována za neetickou a potenciálně nelegální, protože využívá manipulace trhu k dosažení zisku na úkor ostatních účastníků⁴¹.

V mnoha zemích, včetně České republiky, roste počet tvůrců digitálního obsahu zaměřených na finance, známých jako „finfluenceri“. Tito jednotlivci působí na sociálních sítích a jiných digitálních platformách, kde se věnují tématům osobních financí, investování a dalším finančním otázkám, a poskytují rady, názory nebo informace v těchto oblastech. Mezi finfluencery mohou být jak odborníci v oblasti financí, tak i lidé, kteří čerpají ze svých osobních zkušeností. Někteří finfluenceri mohou pozitivně přispět k finanční gramotnosti tím, že dokážou srozumitelně vysvětlit složité finanční koncepty, zatímco jiní mohou poskytovat rady, které nejsou vždy v nejlepším zájmu investorů. Důvody mohou být různé, například nedostatečné odborné znalosti nebo

⁴⁰Crypto adviser. Online. Dostupné z: <https://thecryptoadviser.co.uk/fake-bitcoin-miner-app-cloud-platform/>. Citováno [2025-01-30].

⁴¹IVANOV, F., KRISTKO, O. CH. *Krypto jednoduše: nejen o bitcoinu pro začátečníky*. Praha: Fisio/Cuddle Inc., 2022. 72 s. ISBN 978-80-908809-0-0.

snaha o osobní zisk na úkor těch, kteří se jejich radami řídí. Česká národní banka proto doporučuje, aby investoři přistupovali k radám od finfluencerů s opatrností a nepovažovali je za jediný základ pro svá investiční rozhodnutí.⁴²

Telegram a Discord jsou populární platformy, které uživatelům umožňují sdílet zprávy, obrázky, videa a další soubory s jednotlivci nebo skupinami. Tyto služby se staly hlavním nástrojem pro kryptoměnové pumpovací schémata, která byla využívána k manipulaci s cenami kryptoměn. V roce 2018 měly Telegram a Discord přes 200 milionů a 130 milionů aktivních uživatelů. Podvodné skupiny na těchto platformách často zveřejňovaly signály pro manipulaci s trhem, což vedlo k rychlému zvýšení cen některých kryptoměn. Studie, která analyzovala více než 4 800 pumpovacích signálů z Telegramu a Discordu, zjistila, že 10 % těchto signálů vedlo k nárůstu ceny kryptoměny o více než 18 % během pěti minut. Tato schémata se zaměřovala zejména na kryptoměny s nízkou kapitalizací, u kterých byla vyšší pravděpodobnost manipulace díky nižší likviditě. Tento typ podvodu byl výnosnější u méně známých kryptoměn než u dominantních měn na trhu. Studie upozorňuje na rizika, která s sebou přináší tato praxe, a vyzývá investory, aby byli opatrní při investování do kryptoměn, zejména těch s nízkou kapitalizací. Také apeluje na regulátory a organizace v kryptoměnovém sektoru, aby podnikli kroky k eliminaci těchto podvodů, protože trh s kryptoměnami je náchylný k manipulacím.⁴³

⁴²Česká Národní banka. Online. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Upozorneni-Ceske-narodni-banky-pro-investory-sledujici-tzv.-finfluencery/>. Citováno [2025-01-30].

⁴³ČESKO. Kurzycz. Online. Dostupné z: <https://zpravy.kurzy.cz/480221-vikendar-zlodejna-na-kryptomenach-vynasi-vysoke-zisky/>. Citováno [2025-01-30].

7 Současné právní a technický opatření proti kryptokriminalitě

Efektivita současných právních a technických opatření proti kryptokriminalitě je stále kladeno pod drobnohled, zejména vzhledem k rychlému rozvoji kryptoměnového trhu a jeho technologií. Kryptoměny, díky své decentralizované povaze a možnosti anonymních transakcí, se staly nástrojem pro páchaní různých trestných činů, včetně podvodů, praní špinavých peněz či financování terorismu. Právní rámce a regulace v mnoha zemích stále zaostávají za technologickým pokrokem, což vytváří značné výzvy v oblasti vymáhání práva. Technologické nástroje, jako jsou blockchainové analýzy a pokročilé monitorovací systémy, se sice vyvíjejí, avšak i přesto zůstávají neúplné v detekci složitějších, anonymních transakcí. Zároveň tyto technologie nedokážou zcela eliminovat výzvy, které s sebou kryptoměny přinášejí, například v oblasti anonymizace nebo cross-border transakcí. Tato kapitola se zaměří na hodnocení efektivity aktuálních právních a technických nástrojů v boji proti kryptokriminalitě.

7.1 Právní rámec ČR pro kyberprostor a kyberkriminalitu

Při uplatňování právních norem v kyberprostoru se stát setkává s výzvami spojenými s regulací internetu, který je v podstatě řízen samotnými uživateli, čímž zůstává stát omezen v tradičních prostorových hranicích své jurisdikce. Tento faktor výrazně komplikuje efektivní vymáhání práva v online prostředí. V oblasti trestního práva se pro kyberprostor uplatňuje zásada místní působnosti, která je v tomto kontextu specifická, protože kyberprostor nemá jasně vymezené hranice, což činí právní působnost odlišnou od té, která platí v klasickém fyzickém prostoru. V této bakalářské práci jsem se proto zaměřila převážně na tyto dvě klíčové právní normy: Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a Zákon č. 40/2009 Sb., trestní zákoník, které se vztahují na problematiku kybernetické bezpečnosti a kriminality v online prostoru.

Zákon o kybernetické bezpečnosti upravuje práva a povinnosti jednotlivců a organizací v oblasti kybernetické bezpečnosti a kyberprostoru, stejně jako pravomoci orgánů veřejné moci v této oblasti. Tento právní rámec byl zaveden především v reakci na rychlý rozvoj internetových technologií a integraci kritické infrastruktury do kyberprostoru, což vyžadovalo specifickou právní regulaci pro její ochranu. S rostoucím přenosem ekonomických aktivit do online prostředí se také zvýšila závislost na

bezpečném a stabilním fungování institucí a jejich systémů v kyberprostoru, což má přímý vliv na ekonomiku, včetně hrubého domácího produktu. Zákon se také zaměřuje na ochranu běžných uživatelů před riziky zneužití informačních technologií. Hlavním orgánem odpovědným za kybernetickou bezpečnost v České republice je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který koordinuje oblast kybernetické a informační bezpečnosti. Tento úřad se podílí na vytváření legislativy, včetně návrhu certifikačních schémat, a hraje klíčovou roli v ochraně kritické informační infrastruktury a významných informačních systémů. Zákon o kybernetické bezpečnosti nenavrhuje konkrétní ochranu proti cíleným kyberútokům, což je odpovědnost jednotlivých subjektů, které spravují kritickou infrastrukturu.⁴⁴

Druhým klíčovým právním předpisem pro praktické uplatnění problematiky kybernetických trestných činů je zákon č. 40/2009 Sb., trestní zákoník. Tento zákon reaguje na výzvy spojené s kybernetickými trestnými činy a zavádí pojmy specifické pro kyberprostor, jako jsou data, počítačové systémy, nosiče informací, počítačové vybavení a další. Tímto způsobem trestní zákoník umožňuje právní postih trestné činnosti, která se odehrává v online prostředí, a poskytuje nástroje pro adekvátní právní řešení této problematiky.

V České republice je regulace kryptoměnových služeb v oblasti boje proti praní špinavých peněz (AML) upravena v souladu s evropskými předpisy. Nařízení EU o boji proti praní špinavých peněz (AMLD) bylo implementováno v roce 2017 a stanovuje povinnosti pro subjekty zapojené do obchodování s kryptoměnami, aby zajistily, že jejich služby nebudou zneužity k praní špinavých peněz. Dne 1. ledna 2017 byla novelou zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, zavedena povinnost pro osoby poskytující služby spojené s virtuálními měnami, jako jsou kryptoměnové burzy a směnárny, aby vedly evidenci o svých klientech. V praxi to znamená, že kryptoměnové burzy a směnárny v České republice musí provádět důkladnou kontrolu (due diligence) svých klientů, monitorovat transakce a hlásit podezřelé aktivity příslušným orgánům. Tyto subjekty také musí zajistit dodržování standardů zabezpečení dat a implementaci opatření proti praní špinavých

⁴⁴Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Online. Dostupné z: <https://nukib.gov.cz/cs/o-nukib/organizacni-struktura-uradu/>. [2025-02-14].

peněz. Kryptoměnové směnárny a poskytovatelé služeb spojených s kryptoměnami jsou povinni implementovat opatření proti praní špinavých peněz (AML), která zahrnují identifikaci a ověřování uživatelů (Know Your Customer, KYC). Tato opatření zahrnují shromažďování a ověřování osobních údajů klientů, monitorování transakcí a hlášení podezřelých aktivit příslušným orgánům. Cílem je zajistit transparentnost a zabránit zneužívání kryptoměnových služeb pro nelegální činnosti, jako je praní špinavých peněz nebo financování terorismu.⁴⁵

7.2 Technické nástroje a metody

Ačkoliv se kryptoměny často považují za anonymní, ve skutečnosti jsou pouze pseudonymní, protože každá transakce je zaznamenána na blockchainu, kde ji lze zpětně dohledat. Trasování transakcí v kryptoprostoru se opírá o on-chain analýzu, která umožňuje sledovat pohyb prostředků mezi jednotlivými adresami a odhalovat podezřelé aktivity, jako je praní špinavých peněz, podvody nebo financování nelegálních činností. Díky transparentní povaze blockchainu lze identifikovat adresy spojené s kryptoměnovými burzami, darknetovými tržišti nebo velkými investory takzvanými velrybami, kterým lze doslova vidět pod ruce. Moderní analytické platformy, jako jsou Chainalysis, Elliptic nebo CipherTrace, využívají pokročilé algoritmy k mapování transakčních toků a propojení blockchainových adres s konkrétními burzami, službami nebo dokonce osobami. To znamená, že pokud pachatel převede ukradené prostředky na burzu, která vyžaduje ověření identity prostřednictvím systému KYC neboli Know Your Customer, jeho totožnost může být snadno odhalena. Kromě toho se dá pomocí analýzy vzorců chování určit, zda konkrétní adresa patří velkým hráčům, podvodníkům, hackerům nebo například tržištím na darknetu, kde probíhá obchodování s nelegálním zbožím a službami. K odhalení pachatele nejčastěji dochází ve chvíli, kdy se snaží nelegálně získané prostředky přeměnit na běžnou fiat měnu. To se obvykle děje při převodu kryptoměn na centralizované burze, při výběru hotovosti prostřednictvím kryptoměnového bankomatu nebo při snaze využít některou z finančních služeb, které vyžadují ověření identity. Právě v těchto momentech mohou regulační orgány a právní složky zasáhnout a propojit konkrétní transakce s reálnou osobou. Díky neustálému

⁴⁵Finanční analytický úřad. Online. Dostupné z: <https://fau.gov.cz/files/kryptomeny-a-legalizace-vynosu-z-trestne-cinnosti.pdf>. [2025-14-02].

vývoji v oblasti blockchainové analytiky se stává trasování kryptoměnových toků stále efektivnějším nástrojem v boji proti kryptokriminalitě.⁴⁶

Monitorování a detekce transakcí v kryptoměnovém prostoru využívá různé pokročilé metody, které umožňují sledování podezřelých aktivit v reálném čase. Mezi hlavní techniky patří on-chain analýza, která sleduje transakce na blockchainu a umožňuje trasování prostředků mezi adresami. Moderní nástroje jako umělá inteligence a strojové učení pomáhají analyzovat velké množství transakčních dat, hledat neobvyklé vzory chování a identifikovat možné podvody nebo praní špinavých peněz. Systémy také využívají behaviorální analýzu transakcí, kdy sledují chování jednotlivých adres a porovnávají je se známými modely podvodného jednání, například podezřelým nárůstem transakcí nebo využíváním anonymizačních služeb. Další metodou je sledování blacklistů a rizikových adres, což umožňuje rychle detekovat transakce mezi adresami spojenými s nelegálními aktivitami, jako je hacking nebo obchodování na darknetu. Geolokační analýza a IP tracking doplňují ochranu tím, že pomáhají identifikovat podezřelé transakce, zejména pokud se přihlášení k účtu děje z neobvyklých geografických oblastí. Clustering zase umožňuje spojování adres patřících stejné osobě nebo organizaci, čímž se odhalují organizované podvodné aktivity. Mezi nejznámější analytické nástroje patří Chainalysis, Elliptic, CipherTrace nebo Crystal Blockchain, které využívají tyto metody k monitorování kryptoměnových transakcí a detekci podezřelých aktivit, čímž pomáhají minimalizovat riziko zneužití kryptoměn pro nelegální činnosti.

Nástroje jako Chainalysis, Elliptic a CipherTrace jsou klíčové platformy pro monitorování kryptoměnových transakcí a identifikaci podezřelých aktivit. Využívají pokročilou on-chain analýzu, algoritmy umělé inteligence a strojového učení k analýze transakčních vzorců a odhalování spojitostí mezi blockchainovými adresami. Cílem je propojit transakce s reálnými osobami při převodu prostředků na platformy vyžadující ověření totožnosti. Díky těmto nástrojům mohou vyšetřovatelé efektivně sledovat pohyb prostředků a reagovat na pokusy o praní špinavých peněz a jiné nelegální činnosti.

⁴⁶TRADECZ. Online. Dostupné z: <https://www.tradecz.cz/co-je-on-chain-analyza-a-co-je-to-blockchain-jak-analyzovat-bitcoin-a-ethereum/>. Citováno [2025-02-16].

8 Oběti trestných činů spojených s kryptoměnami v online prostoru

Definice oběti trestného činu znění zákona §2 odst. 2 zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů). „Obětí se rozumí fyzická osoba, které bylo nebo mělo být trestným činem ublíženo na zdraví, způsobena škoda nebo nemajetková újma nebo na jejíž úkor se pachatel trestným činem obohatil nebo měl obohatit.“⁴⁷

Oběťmi trestné činnosti spojené s kryptoměnami mohou být jednotlivci, firmy i instituce zapojené do kryptoměnového ekosystému. Mezi nejčastější oběti patří individuální investoři, kteří se stávají terčem podvodů, jako jsou falešné investiční projekty nebo phishingové útoky. Starší osoby, které nejsou obeznámeny s digitálními technologiemi, mohou být manipulovány podvodníky, kteří využívají jejich nižší digitální gramotnost. Malé firmy, které přijímají kryptoměny jako platební prostředek, mohou čelit útokům typu ransomware nebo phishing, což vede k finančním ztrátám a poškození reputace. Zprostředkovatelé a směnárny kryptoměn mohou být napadeny hackery, což má za následek ztrátu prostředků zákazníků. Technologičtí nováčci a lidé poprvé zapojující se do kryptoměn mohou snadno naletět na podvodné webové stránky nebo e-maily. Vlády a státní instituce se mohou stát oběťmi praní špinavých peněz nebo daňových úniků. Investiční poradci a makléři se zase mohou ocitnout v právních problémech v důsledku zneužívání jejich reputace v podvodných schématech. Vzhledem k rychlému rozvoji kryptoměn se oběťmi mohou stát prakticky všichni, kdo se pohybují v tomto prostoru.

Trestná činnost spojená s kryptoměnami má pro oběti závažné a často dlouhodobé dopady, které nejsou pouze ekonomické, ale zasahují i do psychické, sociální a právní sféry jejich života. S rostoucí popularitou kryptoměn a jejich čím dál širším využíváním se tento fenomén stává magnetem pro různé formy podvodů, krádeží a jiných trestných činností. Vzhledem k tomu, že kryptoměny představují relativně novou technologii, která stále není dostatečně regulována a má své specifické nástrahy, počet obětí těchto

⁴⁷Ministerstvo vnitra České republiky. Online. Dostupné z: <https://www.e-sbirka.cz/sb/2013/45?zalozka=text>. Citováno [2025-02-15].

trestných činů rapidně roste. Finanční ztráty spojené s podvody mohou mít devastující účinky, přičemž oběti často přicházejí o značné částky peněz, které investovaly v dobré víře. Některé oběti si dokonce berou půjčky nebo investují své úspory s cílem získat zisk z kryptoměn, avšak místo toho čelí úplné ztrátě investice, což může vést k zadlužení a vážným finančním problémům. Tento ekonomický dopad je často spojen s výrazným psychologickým stresem, frustrací a pocity viny, jelikož oběti často cítí, že jejich důvěřivost nebo neznalost vedla k jejich ztrátám. Pocity viny a studu jsou časté a mohou vést k dlouhodobým psychickým problémům, včetně úzkostí, depresí a ztráty sebevědomí. Kromě toho, že finanční ztráty ovlivňují osobní život obětí, mohou mít i sociální důsledky, jako je narušení rodinných vztahů, napětí v přátelských nebo pracovní sféře, a dokonce i sociální izolace, kdy se oběti stydí sdílet svou zkušenost a stáhnou se do sebe. Právní a institucionální aspekty, jako je obtížné vymáhání práva a nedostatečná regulace v oblasti kryptoměn, ještě zhoršují situaci obětí, jelikož často nemají přístup k efektivním mechanismům ochrany svých práv, což komplikuje jak samotné vyšetřování trestné činnosti, tak i nápravu vzniklých škod.

Rozdělení dopadů trestných činů spojených s kryptoměnami:

- **Ekonomické dopady:** finanční ztráty a zadlužení,
- **Psychologické a emoční dopady:** stres a frustrace, pocity viny a studu,
- **Sociální dopady:** narušení rodinných vztahů, společenská izolace,
- **Právní a institucionální aspekty:** obtížné vymáhání práva, nedostatečné regulace.

9 Prevence podvodného jednání v online prostoru spojeného s kryptoměnami

9.1 Prevence kriminality

Prevence kriminality představuje soubor opatření zaměřených na předcházení páčání trestných činů, snižování kriminality a eliminaci jejích negativních dopadů na společnost. Definice prevence kriminality podle Ministerstva vnitra ČR: *“Prevence kriminality zahrnuje soubor nerepresivních opatření, tedy veškeré aktivity vyvíjené státními, veřejnoprávními i soukromoprávními subjekty směřující k předcházení páčání kriminality a snižování obav z ní. Patří sem opatření, jejichž cílem či důsledkem je zmenšování rozsahu a závažnosti kriminality a jejích následků, ať již prostřednictvím omezení kriminogenních příležitostí, nebo působením na potenciální pachatele a oběti trestných činů. Jedná se o opatření sociální prevence, situační prevence, včetně informování veřejnosti o možnostech ochrany před trestnou činností a pomoci obětem trestných činů. Prevence kriminality úzce souvisí s prevencí dalších sociálně patologických jevů, z nichž k nejzávažnějším patří nejrůznější formy závislostí.”*⁴⁸

Prevence kriminality se dělí podle dvou základních hledisek:

1. Dle adresátů:

- a) Primární prevence – zaměřena na celou populaci s cílem předcházet vzniku kriminality (osvěta, vzdělávání, právní povědomí).
- b) Sekundární prevence – cílená na rizikové skupiny, které mají zvýšenou pravděpodobnost páčání trestné činnosti (např. sociálně vyloučené skupiny, osoby s kriminální minulostí).
- c) Terciární prevence – zaměřena na pachatele trestné činnosti s cílem jejich resocializace a zabránění recidivě.

⁴⁸ Ministerstvo vnitra České republiky. Online. Dostupné z: <https://mv.gov.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?>. Citováno [2025-03-16].

2. Dle obsahu a zaměření:

- a) Sociální prevence – soustředí se na odstranění příčin kriminality prostřednictvím sociálních programů (vzdělávání, integrace, podpora rodin).
- b) Situační prevence – cílem je snížit příležitosti k páčání trestné činnosti prostřednictvím technických a organizačních opatření (kamerové systémy, zabezpečení majetku).
- c) Viktimologická prevence – zaměřena na ochranu potenciálních obětí kriminality (zvýšení informovanosti, sebeobrana, bezpečné chování v online prostředí).

9.2 Prevence kyberkriminality

V kontextu digitálního světa se čím dál více do popředí dostává prevence kyberkriminality, jejímž cílem je minimalizovat rizika spojená s využíváním moderních technologií a internetu. Účinná prevence v oblasti kybernetické kriminality může zahrnovat několik opatření, jako jsou například:

Neslibujte si rychlé zbohatnutí – Podvodníci často lákají oběti na vidinu rychlého a snadného zisku, slibují nereálně vysoké výnosy bez jakéhokoliv rizika. Tyto nabídky bývají prezentovány jako „jedinečná investiční příležitost“, která se už nebude opakovat, čímž vytvářejí tlak na rychlé rozhodnutí. Ve skutečnosti jde často o Ponziho schémata nebo jiné podvodné investice, kde noví investoři financují zisky těch předchozích, dokud se systém nezhroutí. Skutečné investování vždy zahrnuje riziko, a pokud někdo slibuje jistý a vysoký výnos, je důvod k ostražitosti. Nejlepší obranou je důkladné ověření zdroje, skeptický přístup a konzultace s odborníky.

Ověřujte společnosti – Před jakoukoli investicí je důležité pečlivě prověřit společnost nebo platformu, se kterou chcete spolupracovat. Podvodníci často oslovují potenciální oběti přes sociální sítě, e-maily nebo telefonáty a vydávají se za investiční poradce či zástupce známých firem. Místo důvěry k nevyžádaným nabídkám je lepší sami aktivně vyhledat a ověřit důvěryhodnou investiční společnost. Pomoci mohou recenze, zkušenosti ostatních uživatelů, licence od regulačních úřadů a transparentní historie

firmy. Pokud firma působí podezřele nebo nemá žádné dohledatelné informace, je lepší se jí vyhnout.⁴⁹

Neposílejte peníze neznámým lidem – Nikdy neposílejte peníze neznámým osobám, i když vám slibují vysoké zisky nebo výplatu z minulých investic. Podvodníci často tvrdí, že k uvolnění výdělků je potřeba nejprve zaplatit „poplatek“ nebo „daň“, čímž se snaží z obětí vylákat další finance. Ve skutečnosti se jedná o taktiku známou jako „advance-fee scam“, kde žádné výnosy neexistují a podvodníci si ponechají vše, co jim pošlete. Navíc peníze, které obdržíte od podezřelých zdrojů, mohou pocházet z jiných podvedených osob, čímž se můžete nevědomky zaplést do praní špinavých peněz. Nejlepší obranou je vždy pečlivá kontrola, komu své finance svěřujete, a zásada, že pokud něco zní příliš dobře na to, aby to byla pravda, pravděpodobně to pravda není. Kryptoburzy vám nikdy nevolají, aby vás přesvědčily k investicím nebo platbám, proto jakákoli podobná nabídka je okamžitým varovným signálem.

Zpozorněte pro aplikace pro vzdálený přístup – Podvodníci často využívají aplikace pro vzdálený přístup, jako jsou AnyDesk, TeamViewer nebo UltraViewer, aby získali kontrolu nad vaším zařízením a ukradli vaše finance. Obvykle vás kontaktují s falešnou záminkou – například jako „technická podpora“, „zákaznický servis investiční platformy“ nebo „zástupce banky“ – a přesvědčí vás, abyste si program nainstalovali. Jakmile jim udělíte přístup, mohou manipulovat s vašimi účty, přesměrovat transakce nebo získat citlivé údaje, jako jsou přihlašovací údaje k burzám a kryptopeněženkám. Nikdy nikomu neznámému neumožňujte vzdálený přístup k vašemu zařízení a pokud vás někdo k instalaci takového programu přemlouvá, je to téměř jistě podvod.

Poproste o radu ve svém okolí či vyhledejte odborníky na danou problematiku – Pokud máte jakékoli pochybnosti o podezřelé nabídce nebo neznámé investici, nebojte se obrátit na své blízké nebo někoho z vašeho okolí, kdo má zkušenosti s kryptoměnami a online bezpečností. Konzultace s důvěryhodnou osobou může pomoci odhalit potenciální podvod, na který byste sami nemuseli přijít. Mnozí lidé, kteří se pohybují v oblasti investic a kryptoměn, jsou schopni rozpoznat varovné signály a nabídnout vám cenné rady. Odborné poradenství nebo i jen názor někoho, kdo se

⁴⁹Bezpečná Příbram. Online. Dostupné z: <https://www.bezpecnapribram.cz/258-reverzni-inzertni-podvody>. Citováno [2025-02-18].

problematikou zabývá, může být klíčové při ochraně vašich financí. Nezapomeňte, že podvodníci využívají osamělosti a snahy rychle zbohatnout, takže je vždy lepší požádat o názor někoho, kdo se na věc dívá z nadhledu.

Mějte své prostředky na své hardwarové peněženke – Uchovávání kryptoměn přímo na burze představuje velké bezpečnostní riziko, protože burzy mohou být terčem hackerských útoků, podvodů nebo mohou zkrachovat, čímž můžete o své prostředky přijít. Nejbezpečnějším způsobem ukládání kryptoměn je použití hardwarové peněženky, která uchovává privátní klíče offline, a tím znemožňuje jejich zcizení hackery. Mezi nejznámější a nejdůvěryhodnější hardwarové peněženky patří Trezor, vyvinutý českou firmou SatoshiLabs, který nabízí vysokou úroveň zabezpečení a snadné ovládání. Použití hardwarové peněženky chrání vaše kryptoměny nejen před online útoky, ale i před rizikem krachu burzy nebo podvodného jednání třetích stran. Držet kryptoměny mimo burzu je zásadní pravidlo bezpečného investování.

10 Empirický výzkum

Empirická část této práce bude zaměřena na experimentální analýzu reakce na jasně podvodnou nabídku v oblasti kryptoměn. Cílem experimentu je podrobně prozkoumat a identifikovat proces podvodu, který se často vyskytuje v souvislosti s kryptoměnami, a to jak v kontextu jejich využívání k nelegálním aktivitám, tak i v širším rámci finančních podvodů. Během experimentu budou analyzovány konkrétní mechanismy, které podvody v této oblasti umožňují, a klíčové charakteristiky podvodných nabídek. Výstupy experimentu poslouží k lepšímu pochopení rizik spojených s kryptoměnami a k definování znaků, které mohou sloužit k identifikaci podvodných aktivit v této sféře. Empirická část poskytne cenné údaje a poznatky, které mohou přispět k prevenci podvodů a k rozvoji efektivních opatření pro jejich odhalování a eliminaci.

10.1 Experiment

Pro účely této práce byl proveden experiment, jehož cílem bylo analyzovat taktiky podvodníků při telefonických podvodech spojených s údajnými investicemi do bitcoinu. Během tohoto experimentu bylo úmyslně reagováno na podvodný telefonát a následně byl sledován průběh komunikace, včetně pokusů podvodníka o získání citlivých informací či přístupu k bankovnímu účtu.

Hovor probíhal tak, že volající tvrdil, že jsem vlastníkem bitcoinu a že se mnou potřebuje projednat důležité kroky ohledně mého údajného účtu. Po celou dobu rozhovoru byl patrný manipulační tón a snaha podvodníka vyvolat dojem naléhavosti. Řídila jsem se pokyny volajícího až do okamžiku, kdy mě instruoval k instalaci aplikace Anydesk, která umožňuje vzdálený přístup k zařízení. I když jsem aplikaci nainstalovala, z bezpečnostních důvodů jsem její funkce omezila tak, aby podvodník nemohl ovládat myš, klávesnici ani kameru mého zařízení. V okamžiku, kdy podvodník požadoval sdělení PIN k bankovnímu účtu, došlo k odmítnutí tohoto požadavku, načež hovor rychle ukončil. Očekávala jsem, že se pokusí vylákat finanční prostředky nebo získat přístup k bankovnímu účtu sofistikovanějším způsobem, avšak k tomu nakonec nedošlo. Celý průběh hovoru ukázal, že podvodník spoléhal na rychlé jednání oběti a byl připraven přejít k dalším krokům pouze v případě, že by jeho instrukce byly bez odporu následovány.

Experiment byl zahájen dne 15.2.2025 v 13:30 hodin, kdy byla na internetové platformě nalezena reklama na inzerát nabízející možnost investování do kryptoměn s garantovaným vysokým zhodnocením. Inzerát působil profesionálně, obsahoval logo domnělé investiční společnosti a odkaz na webovou stránku s formulářem pro registraci. Po vyplnění základních údajů, jako je jméno a telefonní číslo, přišla první odpověď od podvodníka přibližně za 10 minut, kdy mě kontaktoval prostřednictvím telefonního hovoru. První podvodník hovor ukončil do několika minut. Druhý podvodník se představil jako Dvořák, údajný zaměstnanec investiční společnosti, a tvrdil, že mám u nich evidovanou investici ve výši 0,38 bitcoinu, což při aktuálním kurzu odpovídá přibližně 35 000 dolarům (cca 840 000 Kč). Tvrdil, že se jedná o částku, kterou mám k dispozici na svém investičním účtu, a že si ji mohu okamžitě vybrat. Jedinou podmínkou pro provedení výběru bylo stažení programu AnyDesk, který umožňuje vzdálený přístup k zařízení. Podvodník instruoval, že po instalaci programu se připojím ke „klientskému účtu“, kde mě provede procesem výběru. Komunikace probíhala jak přes veřejnou WiFi síť, tak i přes mobilní data z předplacené SIM karty. Pro minimalizaci rizika ohrožení osobních údajů a bezpečnosti jiných zařízení byl použit mobilní telefon v továrním nastavení s předplacenou SIM kartou. Tablet, který byl součástí experimentu, byl rovněž v továrním nastavení a nebyl připojen k žádnému mobilnímu operátorovi. Záznam hovoru byl proveden prostřednictvím druhého telefonu, který sloužil výhradně k dokumentaci experimentu. Po skončení hovoru byl celý rozhovor přepsán do písemné podoby pro následnou analýzu. Po celou dobu interakce byla použita smyšlená identita, přičemž jsem se podvodníkovi představila jako Jana Nováková. V případě dalších dotazů ohledně osobních údajů jsem měla připravené smyšlené odpovědi, avšak podvodník kromě jména a příjmení žádné další informace nepožadoval.

Experiment trval přibližně 1 den, během kterého proběhlo několik telefonických hovorů a výměn zpráv. Telefonát, který je přepsán níže trval 50 minut.

Celý experiment vyžadoval pouze minimální finanční investici, konkrétně nákup předplacené SIM karty za 155 Kč, kterou jsem si zakoupila přes mobilní aplikaci Vinted. Veškeré ostatní vybavení bylo k dispozici a nebylo nutné pořizovat žádné další technické prostředky. Během hovoru byl patrný východoevropský přízvuk volajícího, přičemž lze předpokládat, že se jednalo o přízvuk ukrajinský nebo ruský.

Níže je uveden podrobný přepis rozhovoru.

Podvodník: Dobrý den paní Kovářová, tady Dvořák, zaměstnanec investiční společnosti, kdy Vám volám na základě toho, že u nás máte evidovanou investici 0,38 bitcoinu, kdy je to celkem 35.000 dolarů (při dnešním kurzu to je cca 840.000,- Kč).

Já: Dobrý den, vážně? Tak to je super. Ale já se jmenuji Jana Nováková. Není to omyl?

Podvodník: Omlouvám se, to je moje chyba paní Nováková. Samozřejmě to není omyl. Ještě jednou se omlouvám.

Já: Dobře nic se neděje.

Podvodník: Máte tedy u nás paní Nováková tu investici. Chcete to tedy vybrat nebo dále investovat, aby jste měla ještě více peněz?

Já: Tolik peněz? Určitě to chci vybrat, protože se peníze vždycky hodí.

Podvodník: No tak to musíme nainstalovat program Anydesk.

Já: Anydesk jo?

Podvodník: Máte u sebe počítač nebo nějaký tablet?

Já: Mám u sebe momentálně jenom tablet.

Podvodník: Tak na tabletu to taky můžeme udělat to není problém.

Já: Výborně, tak já ho jdu zapnout. Jak to teda uděláme?

Podvodník: Počkejte chvíli, já si to tady připravím.

Já: Dobře, počkám.

Podvodník: Máte nějaké číslo na tabletu? Abych Vám na něj poslal SMS zprávu?

Já: Ne nemám v tabletu žádnou SIM kartu.

Podvodník: Nevadí, chtěl jsem Vám poslat odkaz přes SMS zprávu. Máte nainstalovaný Anydesk na tom tabletu?

Já: Ne nemám. Mám si ho stáhnout?

Podvodník: Ano, je zapotřebí, aby jste měla stáhnutý Anydesk, aby jsme mohli pokračovat.

Já: A nejde to bez něj? Že by jste mi ty peníze poslali na účet?

Podvodník: Musíte si to stáhnout, já se tam jinak nedostanu, potřebujeme ten Anydesk.

Já: Tak mě navigujte co mám tedy dělat. Když to jinak nejde.

Podvodník: Já právě u Vás mám jen to, že máte těch 0,38 bitcoinu a Vaše jméno, příjmení a více informací u vás nevidím, proto musíte stáhnout ten Anydesk, aby jsme to viděli. A abych Vám pomohl s ovládáním.

Já: Jak tedy to mám stáhnout do toho tabletu?

Podvodník: Musíme to tam dostat do toho tabletu. Máte tedy Android nebo iPad? Jde to pouze přes Android.

Já: No mám Android. Jak to tam tedy dostanu? Aby jste to tedy ovládal a viděl více informací?

Podvodník: Musíte si stáhnout Anydesk, aby jsme se dostali do toho účtu.

Já: Tak jsem si ho stáhla přes GooglePlay a mám tady nějaké číslo na obrazovce.

Podvodník: Tak mi nadiktujte to číslo. Aby jsme se připojili.

Já: Dobře, vydržte. To číslo je tedy 480.

Podvodník: Dobře a teď dole klikněte na zelené tlačítko.

Já: Vidím ho tady tak na něj mám tedy kliknout?

Podvodník: Ano musíte to zmáčknout, aby jsme Vám ty peníze převedli.

Já: Zmáčkla jsem ho, jste tady, ale nic se neděje.

Podvodník: Pošlu Vám tam tedy odkaz, na něj klikněte. Musím se na to podívat.

Já: Nic tu nemám, žádný odkaz tu není. Co mám tedy dělat, abych dostala ty peníze?

Podvodník: Vydržte chvíli, hned Vám ho tam pošlu, jen musím něco vyřídit.

Já: Já tu stále nic nevidím, kde je ten odkaz?

Podvodník: Máte ho tam v tom Anydesku. Poslal jsem Vám ho, měla by jste to vidět na obrazovce.

Já: Ano, už to vidím a na to mám kliknout?

Podvodník: Musíte to zkopírovat do prohlížeče.

Já: Dobře jdu to zkopírovat do prohlížeče. Je to hotové. A teď to vyberu jak, ty peníze?

Podvodník: Teď to můžete vybrat, ale můžete to nechat klidně na tom účtu, protože když to vyberete teď'...

Já: Ale já to chci vybrat teď' hned ty peníze teda.

Podvodník: Počkejte chvíli. Takže když to chcete vybrat hned, musíte mi dát číslo účtu, SWIFT k účtu a PIN k účtu.

Já: Tak já Vám nadiktuju to číslo účtu.

Podvodník: Číslo účtu, SWIFT k účtu a PIN k účtu. Musíte mi nadiktovat všechno.

Já: A na co potřebujete PIN k účtu, k posláni peněz přece stačí jen číslo účtu.

Podvodník: Aby jsme převedli ty peníze, tak to musíte právě potvrdit a přihlásit se. Tak to převedeme ty peníze k Vám.

Já: Ale to nemusíte mít můj PIN přece, aby jsme převedli ty peníze.

Podvodník: K tomu, aby jsme to převedli tak musíme mít všechno, bez toho to nepřevedeme ty peníze. Vy snad nechcete ty peníze vybrat? Takhle ty peníze propadnout a nedostanete se k nim.

Já: Ale to by mělo jít. Já ty peníze samozřejmě chci.

Podvodník: Musíte to přes internetové bankovníctví s námi potvrdit, jinak to nejde. Jinak to ztratíte tedy ty peníze, když to neuděláte. Přijdete o všechno jinak.

Já: Já o to nechci přijít, tak mi to pošlete na účet.

Podvodník: To nepůjde poslat, když nám to neřeknete. Musíte nám dát všechny informace, jinak ty peníze nedostanete.

Já: Ale tak mi to pošlete na účet, to by mělo jít bez problémů. Nebudu Vám posílat PIN k mému účtu.

Podvodník: Musíte to poslat jinak o všechno přijdete. Máte tady hodně peněz.

Já: Já Vám to ale nepošlu.

Podvodník: Zavěsil.

Poté jsem se pokusila zavolat zpět na číslo ze kterého podvodník volal, ale zvedl to opravdový majitel telefonního čísla, který o ničem nevěděl. Hovor z toho čísla byl totiž přesměrovaný.

Podvod probíhal v několika fázích: nejprve podvodník vytvořil důvěru tvrzením o mé investici v bitcoinech, následně mě manipuloval sliby rychlého zisku a tlakem na okamžité jednání. Klíčovým krokem byl požadavek na instalaci aplikace Anydesk, která by mu umožnila vzdálený přístup k mému zařízení. Poté chtěl číslo účtu a SWIFT kód, ale hlavním cílem bylo získání PIN kódu k internetovému bankovníctví. Když jsem ho odmítla sdělit, hovor ukončil.

Podvodníci kombinují psychologickou manipulaci, technické prostředky a anonymitu kryptoměn, které umožňují nevratné transakce a ztěžují odhalení pachatele. Podvodné praktiky často zahrnují falešné investice či podvodné kryptopeněženky. Obrana spočívá v informovanosti, opatrnosti a dodržování zásady, že seriózní instituce nikdy nepožaduje přístup k zařízení ani citlivé údaje přes telefon.

Tabulka 2 – Tabulka shrnující průběh experimentu

Tabulka shrnující průběh experimentu	
Časový údaj	Průběh experimentu
15.2.2025 v 13:30 hodin	Zahájení experimentu – vyhledání inzerátu na webových stránkách.
15.2.2025 v 13:35 hodin	Vyplnění základních údajů přes odkaz na webové stránce investiční společnosti s formulářem pro registraci.
15.2.2025 v 13:45 hodin	První kontaktování od podvodníka – obdržení telefonátu. Podvodník tvrdil, že volá z investiční společnosti a informoval o údajné investici do bitcoinu, kdy do několika minut zavěsil.
15.2.2025 v 14:08 hodin	Druhé kontaktování od podvodníka – obdržení telefonátu. Podvodník také tvrdil, že volá z investiční společnosti a informoval o údajné investici do bitcoinu.
15.2.2025, 14:08 – 14:58 hodin	Telefonická komunikace s podvodníkem. Podvodník se snažil přesvědčit k instalaci programu AnyDesk pod záminkou výběru investovaných prostředků. Během hovoru opakovaně žádal o sdělení citlivých údajů, včetně čísla účtu a PIN k internetovému bankovníctví. Podvodník naléhal na zadání údajů do aplikace a přihlášení k bankovnímu účtu. Po odmítnutí poskytování citlivých informací podvodník reagoval nátlakem a nakonec ukončil hovor.
15.2.2025 v 15:00 hodin	Ukončení experimentu, vyhodnocení komunikace a zpracování výsledků.

Zdroj: Vlastní zpracování

Abych experiment dále rozšířila a lépe porozuměla metodám podvodníků, rozhodla jsem se vytvořit simulaci situace, ve které bych podvodníkovi poskytla plný vzdálený přístup k počítači či tabletu. Tento scénář vychází ze skutečných podvodů popisovaných v médiích a odborných článcích, stejně jako z volně dostupných videí na platformě YouTube.

V této části experimentu tedy popíšu, jak by situace probíhala, pokud bych podvodníkovi umožnila plně ovládat mé zařízení. Začnu tam, kde jsem v prvním experimentu odmítla poskytnout plný vzdálený přístup. Nyní mu však přístup umožním a budu zaznamenávat, jakými prostředky se mě snaží manipulovat, jaké techniky používá a jaké následky by takový postup mohl mít. Na závěr shrnu celý průběh simulovaného podvodu a vyhodnotím jeho rizika.

Podvodník: Tak když máte Anydesk otevřený, tak je tam číslo, které budu potřebovat, abyste mi ho nadiktoval.

Já: Ano to číslo vidím, je to číslo 589.

Podvodník: Já se tedy připojím a vyskočí Vám tabulka, tu potvrďte.

Já: Potvrzeno.

Podvodník: Ted' Vám otevřu naši stránku, na které uvidíte kolik bitcoinu máte a můžete se rozmyslet co s tím tedy budeme dělat.

Já: Dobře. Tak jestli mi to ukážete, abych se potom rozhodla.

Podvodník: Dobře ukážu Vám tedy, jak se to dělá a co se bude dít s penězi, které nám pošlete nebo které pošleme my Vám.

Já: To zní skvěle.

Podvodník: Zkopírujte si odkaz, který jsem Vám poslal do svého prohlížeče a klikněte na otevřít účet.

Já: Mám to otevřené.

Podvodník: Máte před sebou platformu, kde vidíte nejvyšší kurz. Kde vidíte, jak to jde nahoru a dolu. A kde jsou již Vaše bitcoiny, které u nás máte.

Já: Dobře a kdy mám tedy nakupovat?

Podvodník: Ted' Vám to ukážu.

Já: Aha a můžu to i vybrat kdy budu chtít?

Podvodník: Ano, kliknete zde a takhle si peníze snadno vyberete.

Já: Aha, rozumím.

Podvodník: Tak ted' jestli se přihlásíte do svého internetového bankovníctví, abychom tedy poslali ty peníze na Váš účet.

Já: Dobře. Přihlásím se.

Podvodník: Ted' tedy bude potřeba, abyste poslala nějaké peníze na náš zahraniční účet, abychom mohli dále obchodovat a vydělávat Vám peníze.

Já: Super, to zní lákavě.

Podvodník: Nelekněte se, podívám se sám na Vaše limity, zda máte tyto platby na zahraniční účet povolené. Většinou je tam limit a nemuselo by nás to pustit ty peníze poslat.

Já: Ano vidím to, jak tam klikáte.

Podvodník: Vidíte, že nedělám nic špatného. Jenom nastavíme ty limity. Vidím tedy, že máte na účtu 300.000,-Kč. Nechcete tedy investovat více peněz, aby se Vám to vyplatilo?

Já: No chtěla jsem investovat pouze půlku.

Podvodník: Aha, ale pokud zainvestujete větší obnos peněz, můžete využít naši dnešní nabídku, kdy se Vám ty peníze lépe zhodnotí a vy tak vyděláte více. Tato nabídka platí ale pouze jen pro dnešek. Normálně je tato nabídka pouze pro VIP klienty. Ty peníze si můžete vybrat klidně za dva dny. Nebudou tam muset být nějak dlouho a stejně se Vám zhodnotí.

Já: Nechtěla jsem tam posílat tolik peněz, ale promyslím to.

Podvodník: Jak jsem říkal, peníze bude moci vybrat klidně za dva dny a tím, že jich pošlete více budete mít lepší zhodnocení. Jde o Vaše peníze, rozhodněte se, jak chcete, ale takhle byste vydělala víc.

Já: Tak dobře, chci vydělat víc.

Podvodník: Tak zainvestujete všechny?

Já: Ano chci vydělat co nejvíc peněz. A když říkáte, že si ty peníze mohu vybrat i za třeba dva dny, tak to asi není problém.

Podvodník: Tak vyplníme platbu? Platba bude směřovat na účet u Revolutu, který je na jméno Havlíček, přičemž se jedná o našeho účetního, který peníze ihned převede na investiční platformu, kde již investujete.

Já: Takže mohu začít ihned?

Podvodník: Jakmile peníze odejdou z Vašeho účtu. Může Vám totiž volat banka, ale té řekněte, že to posíláte třeba kamarádovi, protože nechtějí, abyste posílala větší obnos peněz jinam a vydělávala jinde.

Já: Aha a proč to tak je, to musím lhát?

Podvodník: Nebudete tak úplně lhát, ale banka nechce o peníze přijít, a proto je lepší, když jim řekněte něco jiného než, že chce vydělávat jinde.

Já: Tak to tedy jdeme poslat?

Podvodník: Dobře vyplním tedy číslo účtu, jak jsem říkal napíšu tam jméno našeho účetního a také že je to tedy pro něj jako kamaráda.

Já: Dobře rozumím.

Podvodník: Teď potvrďte platbu na telefonu, aby proběhla.

Já: Potvrzeno.

Podvodník: Teď počkáme do dalšího dne, až peníze přijdou a já se Vám zítra ozvu, abychom podepsali smlouvu.

Já: Dobře moc Vám děkuji.

V druhém rozhovoru, který fiktivně probíhal mezi mnou a podvodníkem, bylo zjevné, jak podvodník využíval různé techniky manipulace, aby mě přesvědčil k tomu, abych mu poslala peníze. Nejprve se snažil vytvořit dojem, že investice do bitcoinu byla velmi výhodná, a že zisk je téměř zaručený. Představil mi fiktivní platformu, která údajně zprostředkovávala obchodování s kryptoměnami, a tvrdil, že můžu snadno a rychle vydělat.

Podvodník se mě pokusil přesvědčit, že když investuji větší částku, mohu využít „exkluzivní nabídky“ s lepšími podmínkami pro zhodnocení. Tlak na rychlé rozhodování, přičemž jsem měla pocit, že nabídka je časově omezená, byl součástí manipulace, která měla za cíl urychlit mou reakci a rozhodnutí bez důkladného přemýšlení. Podvodník mi navrhl, abych pro zajištění transakce použila aplikaci Anydesk, což byla klíčová technika, která mu umožnila vzdálený přístup k mému zařízení.

Ve chvíli, kdy jsem byla na platformě a obdržela instrukce k platbě, podvodník mě přesvědčil, že musí poslat peníze na zahraniční účet, aby transakce proběhla správně. Tvrdil, že platba je potřebná k tomu, aby investice začala růst, a přitom se mě snažil ujistit, že peníze mohu vybrat v krátkém čase. Celý rozhovor se zaměřil na to, abych co nejrychleji poslala peníze na účet podvodníka. Tento proces byl podpořen tlakem, že pokud peníze nepošlu okamžitě, nabídka zanikne.

Po několika manipulačních krocích a mých obavách, abych nezmeškala šanci na rychlý zisk, jsem nakonec souhlasila a peníze byly odeslány na účet podvodníka. Jakmile peníze opustily můj účet, podvodník přestal komunikovat a já byla bez šance získat zpět své finanční prostředky. Podvodník mi také slíbil, že se druhý den ozve, jakmile platba proběhne, a že podepíšeme smlouvu. Nicméně druhý den se vůbec neozval, jak sliboval, a smlouvu také neposlal. Peníze z mého účtu byly odeslány a podvodník přestal s veškerou komunikací.

Tento rozhovor ukazuje, jak podvodníci využívají kombinaci technických nástrojů (vzdálený přístup přes Anydesk), psychologické manipulace a iluzí o rychlém zisku k tomu, aby přiměli oběť k okamžité platbě. Jakmile byly peníze odeslány na zahraniční účet, podvodník už neměl žádný zájem o další komunikaci. Zneužívání kryptoměn jako nástroje pro takové podvody je obzvlášť nebezpečné, protože transakce jsou nevratné a těžko dohledatelné. Tato zkušenost ukazuje, jak důležité je mít na paměti zásady bezpečnosti a nikdy nesdílet přístupové údaje nebo provádět finanční transakce na základě telefonních nebo online kontaktů, které nejsou ověřeny.

Tabulka 3 – Tabulka manipulačních technik

Tabulka manipulačních technik	
Manipulační technika	Popis manipulační techniky
<u>Autorita a důvěryhodnost</u>	Podvodník se vydává za pracovníka investiční společnosti a tím vytváří iluzi důvěryhodnosti, což oběti pomáhá věřit v legitimitu nabídky.
<u>Lákavá nabídka</u>	Oběti je nabídnuto výhodné zhodnocení investice a možnost okamžitého zisku, což vytváří dojem výhodnosti obchodu.
<u>Vytváření naléhavosti</u>	Nabídky jsou prezentovány jako časově omezené nebo výjimečné, což tlačí oběť k rychlému rozhodnutí bez dostatečného zvážení.
<u>Nabídka výhod (přetvářka vzájemného jednání)</u>	Podvodník vytváří dojem, že oběti poskytuje výhodu (např. zisk nebo bonus), aby ji motivoval k dalším krokům, které budou pro něj výhodné.
<u>Psychologický nátlak</u>	Podvodník používá pozitivní posílení a opakovaně vyzdvihuje výhody rychlého jednání, čímž podporuje oběť v rozhodnutí investovat více peněz.
<u>Sociální tlak</u>	Oběť je tlačena k rozhodnutí, aby nepropásla „unikátní příležitostí“, což vytváří tlak na rychlou akci.
<u>Technická manipulace</u>	Použití AnyDesk k manipulaci s technikou oběti a usměrňování jejích akcí v průběhu procesu, což má oběť přimět k dalším krokům, které by jinak nebyla ochotná podniknout.
<u>Nátlak a strach</u>	Podvodník vyvolává strach z propadnutí peněz a ztráty příležitosti, což přiměje oběť k riskantnímu jednání.
<u>Postupné stupňování požadavků</u>	Podvodník začíná s menšími požadavky (např. poskytnutí údajů k účtu), které postupně eskalují až k větším částkám a osobním informacím.

Zdroj: Vlastní zpracování

Tabulka ukazuje, jak manipulační techniky používané v podvodech slouží k ovlivnění rozhodování obětí, čímž je podvodník přiměje k jednání, které by za normálních okolností neprovedly.

Závěr

Tato bakalářská práce se zaměřila na analýzu kryptoměn, přičemž hlavní pozornost byla věnována Bitcoinu jako nejstarší a nejrozšířenější kryptoměně. Bitcoin se stal, díky své decentralizované povaze, anonymitě a specifickým transakčním mechanismům, často využívaným nástrojem pro podvodné aktivity v online prostoru. V teoretické části práce jsem se věnovala historickému vývoji peněz a okolnostem vedoucím k vytvoření Bitcoinu, přičemž jsem prozkoumala, jak tento nový typ měny reagoval na potřebu bezpečných, decentralizovaných transakcí, které nevyžadovaly zprostředkovatele. Dále jsem podrobně prozkoumala principy fungování Bitcoinu, včetně jeho decentralizace, šifrování, těžby a blockchainu, které tvoří základ pro bezpečné provádění transakcí v síti.

Další část práce se soustředila na kyberkriminalitu a podvody v online prostoru, zejména ty spojené s kryptoměnami. Kryptoměny, a zejména Bitcoin, se staly nástrojem pro různé nelegální činnosti, přičemž jejich anonymita a nevratnost transakcí usnadňují podvodné jednání. Byly analyzovány konkrétní příklady podvodů a metody zneužívání kryptoměn k páchání trestné činnosti. V této souvislosti jsem se věnovala současným právním a technickým opatřením proti kyberkriminalitě a vyhodnotila jejich efektivitu v boji proti těmto podvodům. Zkoumána byla také problematika obětí trestných činů spojených s kryptoměnami v online prostoru, přičemž zvláštní důraz byl kladen na preventivní opatření zaměřená na snižování rizika podvodného jednání v online prostoru, a to jak v rámci obecné prevence kriminality, tak specifické prevence kyberkriminality.

Empirická část práce přinesla praktický pohled na proces podvodu v oblasti kryptoměn. Experiment, který jsem provedla, spočíval v reakci na podvodný telefonát, který měl za cíl přesvědčit mě k investici do bitcoinu. Během experimentu jsem analyzovala manipulační techniky, které podvodníci používají k vytvoření důvěry a k přesvědčení oběti, aby odeslala své peníze. Podvodník využíval sliby rychlého zisku a tlačil na okamžité rozhodování, čímž se snažil vyvolat tlak na rychlou reakci bez dostatečného přemýšlení. Klíčovým momentem bylo využití aplikace Anydesk, která umožnila podvodníkovi získat vzdálený přístup k zařízení. Nakonec v druhém nahraném rozhovoru byly peníze odeslány a podvodník přestal komunikovat, což potvrzuje nevratnost kryptoměnových transakcí a důležitost opatrnosti při komunikaci s neověřenými subjekty.

Výsledek empirické části potvrdil, že kryptoměny, zejména Bitcoin, jsou účinným nástrojem pro páchaní podvodných aktivit, a to především díky své anonymitě, decentralizovanosti a nevratnosti transakcí. Experiment ukázal konkrétní metody manipulace a technické nástroje, které podvodníci používají k tomu, aby oběti přiměli k okamžitému odeslání peněz. Podvodníci se zaměřují na vytváření iluze rychlého zisku a využívají psychologických technik, které oběť přesvědčí k rychlému rozhodování.

Hlavním cílem této bakalářské práce bylo zhodnotit využití kryptoměn, především Bitcoinu, k páchaní podvodů v online prostoru, se zaměřením na identifikaci nejčastějších forem těchto podvodů, jejich dopady na oběti a empirická část poskytla konkrétní příklad, jak tento proces vypadá v praxi. Práce rovněž prozkoumala efektivitu současných právních a technických opatření proti kyberkriminalitě, přičemž ukázala, že je potřeba zlepšit preventivní a detekční mechanismy, aby se minimalizovalo riziko podvodů. Sekundárním cílem bylo navrhnout doporučení pro zlepšení prevence a detekce těchto trestných činů. Na základě výsledků experimentu lze doporučit další vzdělávání veřejnosti o bezpečnosti při používání kryptoměn, rozvoj lepších kontrolních mechanismů a spolupráci mezi institucemi na globální úrovni, která by pomohla odhalit a eliminovat kryptoměnové podvody.

Ve světle těchto poznatků se ukazuje, jak důležité je rozumět nejen technologickým aspektům kryptoměn, ale i jejich využívání v nelegálních aktivitách. Předcházení kryptoměnovým podvodům si vyžaduje soustavnou osvětu a implementaci efektivních bezpečnostních opatření na všech úrovních. Jak ukazuje analýza manipulačních technik, podvodníci využívají různé psychologické taktiky k ovlivnění obětí, což zdůrazňuje potřebu nejen technologické ochrany, ale také vzdělávání veřejnosti o těchto metodách a schopnosti rozpoznat varovné signály podvodného jednání.

Seznam použitých zdrojů

Literární zdroje

1. AMMOUS, S. *Bitcoinový standard*. Konsensus Network & Braiins, 2022. 332 s. ISBN 978-9916-697-24-5.
2. BOYAPATI, V. *Bitcoin je budoucnost*. Praha: Nakladatelství Braiins Systems, 2023. 124 s. ISBN 978-80-908709-2-5.
3. ČESKO. *Zákony II: úplná znění zákonů a souvisejících předpisů z oblasti trestní zákoník, trestní řád, zákon o odpovědnosti za přestupky a řízení o nich*. Český Těšín: PORADCE, s. r. o., 2020. 160 s. ISBN 1802-8330.
4. DOUCEK, P., KONEČNÝ, M., NOVÁK, L. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. 272 s. ISBN 978-80-88260-39-4.
5. GIGI. *21 lekcí: Co mě naučil pád do bitcoinové králičí nory*. Praha: Nakladatelství Braiins Systems, 2022. 152 s. ISBN 978-80-908709-01.
6. IVANOV, F., KRISTKO, O. CH. *Krypto jednoduše: nejen o bitcoinu pro začátečníky*. Praha: Fisio/Cuddle Inc., 2022. 176 s. ISBN 978-80-908809-0-0.
7. KALINSKÝ, B. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing, 2018. 136 s. ISBN 978-80-87383-71-1.
8. KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky v Praze, 2020. 328 s. ISBN 978-80-7251-505-9.
9. LÁNSKÝ, J. *Kryptoměny*. Praha: C.H. Beck, 2018. 160 s. ISBN 978-80-7400-722-4.
10. NEJESCHLEBA, R. *BITCOIN: SEZNAMTE SE! Pochopte bitcoin i bez hlubokých znalostí informatiky či ekonomie*. Ve Strážnici: vlastním nákladem, 2022. 173 s. ISBN 978-80-11-01333-2.
11. NOVÁK, M. *Bitcoin: Revoluce, nebo podvod?* Praha: Nakladatelství Braiins Systems, 2024. 128 s. ISBN 978-80-908709-9-4.

12. PETŘÍK, T. *1 bitcoin za 10 milionů dolarů*. Brno: Tribun EU s.r.o., 2020. 157 s. ISBN 978-80-263-1626-8.
13. PRIZKER, Y. *Vynález jménem Bitcoin*. Praha: Nakladatelství Braiins Systems, 2022. 114 s. ISBN 978-80-907975-0-5.
14. RAMEŠOVÁ, K. *Právní regulace kybernetické bezpečnosti a její meze*. Praha: Nakladatelství C.H. Beck, 2023. 268 s. ISBN 978-80-7400-931-0.
15. STANFORD, E. *Cryptowars*. London: Kogan Page Ltd, 2021. 264 s. ISBN 978-13-9860-068-3.
16. STROUKAL, D., SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing, a.s., 2021. 289 s. ISBN 978-80-271-1043-8.
17. TĚTEK, J. *Bitcoin: odluka peněz od státu*. Praha: Grada Publishing, 2022. 116 s. ISBN 978-80-907975-8-1.
18. TĚTEK, J. *Bitcoin: Návrat zdravých peněz*. Praha: Nakladatelství Braiins Systems, 2023. 184 s. ISBN 978-80-908709-8-7.

Elektronické zdroje

1. Bezpečná Příbram. Online. Dostupné z: <https://www.bezpecnapribram.cz/258-reverzni-inzertni-podvody>. Citováno [2025-02-18].
2. Binance square. Online. Dostupné z: <https://www.binance.com/en/square/post/147556/>. Citováno [2025-01-30].
3. Česká Národní banka. Online. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Upozorneni-Ceske-narodni-banky-pro-investory-sledujici-tzv.-finfluency/>. Citováno [2025-01-30].
4. ČESKO. Finex. Online. Dostupné z: <https://finex.cz/phishing-kryptomeny/>. Citováno [2025-01-29].
5. ČESKO. Kurzycz. Online. Dostupné z: <https://zpravy.kurzy.cz/480221-vikendar-zlodejna-na-kryptomenach-vynasi-vysoke-zisky/>. Citováno [2025-01-30].
6. Crypto adviser. Online. Dostupné z: <https://thecryptoadviser.co.uk/fake-bitcoin-miner-app-cloud-platform/>. Citováno [2025-01-30].

7. Finanční analytický úřad. Online. Dostupné z: <https://fau.gov.cz/files/kryptomeny-a-legalizace-vynosu-z-trestne-cinnosti.pdf>. Citováno [2025-02-14].
8. Ministerstvo vnitra České republiky. Online. Dostupné z: https://mv.gov.cz/clanek/na-nebezpeci-kyberkriminality-upozorni-den-bezpecnejsiho-internetu.aspx?utm_source=chatgpt.com. Citováno [2025-01-05].
9. Ministerstvo vnitra České republiky. Online. Dostupné z: <https://mv.gov.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?>. Citováno [2025-03-16].
10. Ministerstvo vnitra České republiky. Online. Dostupné z: <https://www.e-sbirka.cz/sb/2013/45?zalozka=text>. Citováno [2025-02-15].
11. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Online. Dostupné z: <https://nukib.gov.cz/cs/o-nukib/organizacni-struktura-uradu/>. Citováno [2025-02-14].
12. Policie České republiky. Online. Dostupné z: <https://policie.gov.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx>. Citováno [2025-01-08].
13. Policie České republiky. Online. Dostupné z: <https://policie.gov.cz/clanek/prevence-kraj-kryptomeny-v-rukou-podvodniku.aspx>. Citováno [2025-01-29].
14. Seznam zprávy. Online. Dostupné z: <https://www.seznamzpravy.cz/clanek/ekonomika-finance-byznys-meny-kryptomeny-lakali-na-slova-jako-krypto-nebo-blockchain-slo-o-obri-pyramidovy-podvod-210669>. Citováno [2025-01-29].
15. TRADECZ. Online. Dostupné z: <https://www.tradecz.cz/co-je-on-chain-analyza-a-co-je-to-blockchain-jak-analyzovat-bitcoin-a-ethereum/>. Citováno [2025-02-16].

Seznam tabulek a grafů

Obrázek 1 - Graf Půlení odměny za blok (halving)	21
Tabulka 1 - Statistika kyberkriminality v ČR za období 2021-2023.....	24
Tabulka 2 – Tabulka shrnující průběh experimentu.....	50
Tabulka 3 – Tabulka manipulačních technik	55
Graf 1 - Kyberkriminalita v ČR – registrované skutky	24