

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

BAKALÁŘSKÁ PRÁCE

**KRYPTOMĚNY, JEJICH PRINCIP A UPLATNĚNÍ
V NELEGÁLNÍM OBCHODU S OMAMNÝMI A
PSYCHOTROPNÍMI LÁTKAMI**

Autor práce: Jan Berkovský, DiS.

Studijní obor: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Milan Kocík, MBA

Katedra: Katedra právních oborů a bezpečnostních studií

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Jan Berkovský, DiS.

Studijní program: Bezpečnostně právní činnost

Studijní obor: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Místo studia: Příbram

Název bakalářské práce: Kryptoměny, jejich princip a uplatnění v nelegálním obchodu s omamnými a psychotropními látkami.

Název bakalářské práce v anglickém jazyce: Cryptocurrencies, their principle and application in the illegal trade in narcotics and psychotropic substances.

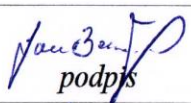

Katedra: Katedra právních oborů a bezpečnostních studií

Vedoucí bakalářské práce: Mgr. Milan Kocík, MBA

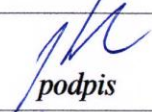
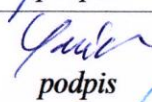
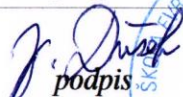
Datum zadání bakalářské práce: listopad 2021

Cíl bakalářské práce: Prioritní cíle bakalářské práce jsou stanoveny dva. Prvním je zjistit, jaký je aktuální trend a vývoj nákupu omamných a psychotropních látek na tzv. Dark Webu pomocí výzkumné metody sběr a analýza statistických dat. Druhým cílem je poté zjistit připravenost Policie České republiky se s tímto fenoménem plně konfrontovat. Hlavní výzkumnou metodou zde bude metoda rozhovoru s policisty ze specializovaných oddělení PČR, kteří se touto problematikou aktivně zabývají.

Jako sekundární cíl si bakalářská práce klade definovat fenomén kryptoměn, jejich anonymitu jako platebního prostředku a jejich další směřování v blízké budoucnosti, definování kyberprostoru a hlavně jeho, většinou běžných uživatelů skrytý, Dark Web a tržiště, kde se provádí nelegální činnost.

Student: Jan Berkovský, DiS.	20.11.2021 datum	 podpis
Vedoucí práce: Mgr. Milan Kocík, MBA	30.11.2021 datum	 podpis

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	6.12.2021 datum	 podpis
Prorektorka pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	9.12.2021 datum	 podpis
Rektor: doc. Ing. Jiří Dušek, Ph.D.	14.12.2021 datum	 podpis



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

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

.....

Děkuji vedoucímu bakalářské práce Mgr. Milanu Kocíkovi, MBA, za cenné rady, připomínky a metodické vedení práce. Děkuji své partnerce za cenné rady, připomínky k bakalářské práci a za trpělivost.

ABSTRAKT

BERKOVSKÝ, J. *Kryptoměny, jejich princip a uplatnění v nelegálním obchodu s omamnými a psychotropními látkami: bakalářská práce*. České Budějovice : Vysoká škola evropských a regionálních studií, 2022. 59 s. Vedoucí bakalářské práce : Mgr. Milan Kocík, MBA

Klíčová slova: Kryptoměny, Bitcoin, Ethereum, Monero, altcoin, Blockchain, Clear Web, Deep Web, Darknet, Dark Web, tržiště, drogy, omamné a psychotropní látky, ilegální obchod.

Souhrn

Tato práce se zabývá problematikou kryptoměn, jejich principem a uplatněním v nelegálním obchodu s omamnými a psychotropními látkami.

Teoretická část popisuje fenomén kryptoměn, jejich princip a využití. V této části je podrobně popsána první a nejvýznamnější digitální měna Bitcoin a dále jsou popsány od něj odvozené alternativní měny. Dále je zde podrobně popsán a definován kyberprostor, doplněn o platnou legislativu. Taktéž je v této části popsána i temná, skrytá část internetu, která je následně doplněná o fenomén temných tržišť a s ním úzce spojenou drogovou kriminalitou. V poslední části je popsán boj proti drogové kriminalitě v České republice.

V praktické části jsou empirickou metodou zkoumány řízené rozhovory policistů ze specializovaných pracovišť Policie České republiky a na jejich podkladě jsou vypracovány myšlenkové mapy, které poskytují ucelený pohled na zkoumanou problematiku. V této části je dále zpracována SWOT analýza, která zkoumá připravenost orgánu Policie České republiky se s tímto fenoménem plně konfrontovat.

ABSTRACT

BERKOVSKÝ, J. *Cryptocurrencies, their principle and application in the illegal trade in narcotics and psychotropic substance: Bachelor Thesis*. České Budějovice : The College of European and Regional Studies, 2022. 59 p. Supervisor : Mgr. Milan Kocík, MBA

Key words: Cryptocurrencies, Bitcoin, Ethereum, Moero, Altcoin, Blockchain, Clear Web, Deep Web, Darknet, Dark Web, Marketplace, Drugs, Narcotics and psychotropics substances, illegal trade.

Summary

This work deals with the issue of cryptocurrencies, their principle and application in the illegal trade in narcotic and psychotropic substances.

The theoretical part describes the phenomenon of cryptocurrencies, their principle and use. This section describes in detail the first and most important digital currency Bitcoin and the alternative currencies derived from it. Furthermore, cyberspace is described and defined in detail, supplemented by current legislation. This section also describes the dark, hidden part of the Internet, which is then supplemented by the phenomenon of dark markets and closely related drug crime. The last part describes the fight against drug crime in the Czech Republic.

In the practical part, the interviews of police officers from specialized workplace of the Police of the Czech Republic are examined by an empirical method, and mind maps are developed on their basis, which provide a comprehensive view of the researched issues. In this part, a SWOT analysis is further elaborated, which examines readiness of the Police of the Czech Republic to fully confront this phenomenon.

Obsah

Úvod.....	10
1 Cíl a metodika bakalářské práce	12
2 Kryptoměny a jejich legální využití.....	13
2.1 Peer-to-peer	13
2.2 Kryptografie	13
2.3 Digitální otisk - Hash	14
2.4 Blok a systém PoW / PoS.....	14
2.5 Blockchain.....	15
3 Bitcoin.....	16
3.1 Co je to Bitcoin a jak funguje.....	17
3.2 Bitcoin, jako měna budoucnosti?	17
3.3 Bitcoinová adresa	20
3.4 Bitcoinové peněženky	21
3.4.1 Softwarová peněženka	21
3.4.2 Hardwarová peněženka	22
3.5 Bitcoin a WikiLeaks	22
4 Altcoiny, jejich princip a využití.....	23
4.1 Altcoiny a jejich neomezené možnosti.....	25
4.1.1 Monero - plně anonymní digitální měna.....	26
5 Kyberkriminalita	27
5.1 Legislativa	27
5.2 Temná síť internetu	29
5.2.1 Surface web.....	29
5.2.2 Deep web.....	29
5.2.3 Darknet.....	30
5.2.4 Dark Web	30
5.2.5 Prohlížeč TOR.....	32

5.3	Temná tržiště	33
5.3.1	Silk Road.....	33
5.3.2	AlphaBay	35
5.3.3	Hansa Market	37
5.3.4	Sheep Marketplace	38
5.3.5	Hydra Market	39
5.3.6	Temná tržiště v době pandemické.....	40
5.4	Odhalování a vyšetřování kybernetické kriminality	42
5.4.1	Pachatel kybernetické kriminality a jeho motiv.....	42
5.4.2	Kriminalistické stopy	45
5.4.3	Počítačové stopy a jejich kategorie	45
5.4.4	Účetní stopy	46
5.4.5	Paměťové stopy.....	47
5.4.6	Odhalování kybernetické kriminality.....	47
6	Drogová kriminalita v České republice.....	50
6.1	Drogy na internetu i mimo něj	50
6.2	Základní dělení drog.....	51
6.2.1	Látky stimulující centrální nervový systém	51
6.2.2	Látky tlumící centrální nervový systém.....	52
6.2.3	Látky ovlivňující vnímání	53
6.3	Boj proti drogové kriminalitě v České republice	54
6.3.1	Obchod s metamfetaminem.....	54
6.3.2	Obchod s konopnými látkami	55
6.3.3	Obchod s MDMA.....	56
7	Vyhodnocení výzkumu	57
7.1	Víte, jaký je aktuální vývojový trend nákupu OPL v internetovém prostředí?	58
7.2	Jaká je dle Vás připravenost orgánu PČR se s tímto fenoménem plně konfrontovat?	59

7.3	Na jaké úrovni je dle Vás současná situace v rámci edukace policistů v oblasti kyberkriminality?	60
7.4	Jakými školeními či kurzy jste si v rámci této problematiky prošel, případně víte i o nějakých dalších?	61
7.5	Pokud můžete srovnat vývoj nákupu OPL před pandemií COVID-19 a situaci v následujících pandemických letech, došlo v této problematice k nějakému vývoji a rozšíření?	62
7.6	Jaké kryptoměny se dle Vás používají k nákupu OPL na Darknetu?.....	63
7.7	SWOT analýza	64
	Závěr	67
	Seznam použitých zdrojů	69
	Seznam zkratk	73
	Seznam tabulek a grafů	75

Úvod

Téma bakalářské práce „Kryptoměny, jejich princip a uplatnění v nelegálním obchodu s omamnými a psychotropními látkami“ jsem si zvolil, protože mě téma kryptoměn a obecně kybernetické kriminality v poslední době velice zajímá. Navíc se s touto problematikou jakožto policista setkávám stále častěji a téma bakalářské práce tak беру i jako možnost k rozvoji svých dosavadních znalostí. Úvodem bych chtěl citovat myšlenku od E. O. Wilsona: „*Máme paleolitické emoce, středověké instituce a nadpozemskou technologii.*“ O kryptoměny jsem se začal aktivně zajímat až v roce 2021. Předtím jsem věděl, že existuje Bitcoin a další kryptoměny, tušil jsem, jak fungují, ale nevěnoval jsem tomu příliš velkou pozornost. Má první zkušenost s kryptoměnou byla ve formě investování do Bitcoinu na burze, jakožto ochrana před působením vnějších vlivů, jako je například inflace. Ze začátku jsem sledoval edukační videa a četl si odborné články, abych věděl, jak se v tomto fenoménu orientovat, jak začít investovat a diverzifikovat si své portfolio. Po nabytí určitých vědomostí jsem se připojil k několika skupinám na sociální síti Facebook a ke skupinám na komunikační službě Telegram, kde se aktivně hovoří o situaci na kryptotrhu a sdílejí se zde aktuální informace ze světa kryptoměn. Ve svém zaměstnání řeším primárně spisy na úrovni přestupků, které se týkají kybernetické kriminality. Jedná se zejména o různá podvodná jednání. Téma bakalářské práce, které jsem zvolil, mi poskytlo ucelený pohled na problematiku kryptoměn a jejich použití k legálním i ilegálním aktivitám. Tato práce mi poskytla mnoho užitečných informací, které jistě aplikuji ve svém profesním životě.

Bakalářskou práci jsem rozdělil do dvou základních částí a to na teoretickou a praktickou část. V teoretické části je uvedeno základní vysvětlení kryptoměn a jejich systém. Dále se v teoretické části věnuji tématu Bitcoinu, jeho historii, jak tyto digitální peníze fungují a taktéž jejich využití. Dále zde uvádím rozdělení peněženek a jejich systém dělení. Taktéž jsou zde popsány altcoiny, jejich princip a využití. V další teoretické části bakalářské práce se zabírám tématem kybernetické kriminality, kde popisuji aktuální legislativu, o kterou se opírají orgány činné v trestním řízení. Dále se snažím vysvětlit téma kyberprostoru, jak se rozděluje a jak vše funguje. Obsahem tohoto tématu je i softwarový systém TOR, kde se snažím popsat jeho funkci a využití. Dalším tématem jsou temná tržiště sítě Darknet. Zde popisuji některá temná tržiště, která jsou v současné době již odpojená, ale jejich příběhy nám mohou poskytnout velmi zajímavé informace, které lze užít i v dalších budoucích případech. Součástí

tohoto tématu jsou i temná tržiště v době pandemické, kde je popsáno, jaký vliv měla pandemická opatření na tento fenomén. Posledním tématem je kapitola zaměřená na boj proti drogové kriminalitě v České republice. Toto téma se zaměřuje na pandemické roky a vývoj drogové kriminality v této době. Dílčími podkapitolami jsou specifikovaná drogová témata ze statistik Národní protidrogové centrály.

Praktická část mé bakalářské práce byla zpracována na základně řízených rozhovorů s policisty, kteří se tématu drog, popřípadě přímo drog v kyberprostoru, věnují. Zjišťoval jsem jejich názor na připravenost policie jako takové se s tímto fenoménem plně konfrontovat. Jejich názor na edukaci policistů, zda a jak pandemie ovlivnila internetový drogový trh. Výsledky, které byly zpracované do myšlenkových map, jsou mnohdy velice rozdílné, jednak je to dáno znalostmi tohoto tématu, jednak pozicí, na které policista pracuje. V rámci problematiky jsem vyhotovil i SWOT analýzu.

Závěr mé bakalářské práce obsahuje výsledky mého výzkumu a můj názor na problematiku, který jsem získal během psaní této bakalářské práce a který dávám do kontextu s názorem, který jsem měl předtím. Díky bakalářské práci jsem tento názor malinko pozměnil, zašel jsem více do hloubky a poznal jsem nová témata i oblasti, kterým bych se rád v budoucnu profesně věnoval.

1 Cíl a metodika bakalářské práce

V bakalářské práci budou řešeny kryptoměny, zejména nejrozšířenější Bitcoin, a jejich uplatnění v nákupu omamných a psychotropních látek prostřednictvím takzvaného „Dark Webu.“ V teoretické části bude vysvětlena charakteristika kryptoměn, jejich fungování na tzv. blockchainu, jejich princip, možnosti nákupu a vymezení základních pojmů. Zabývat se bude zejména Bitcoinem, jako nejčastější kryptoměnou, který v sobě kombinuje anonymitu hotovosti, pohodlnost elektronických peněz a neinflační povahu zlata. Kryptoměny v současné době aspirují na to, být plnohodnotnou formou peněz. Dále bude vysvětlen tzv. Dark Web, který představuje tajemné a nelegální místo v hloubi internetu, na němž lze zakoupit omamné a psychotropní látky a případně provádět jinou nelegální činnost. V bakalářské práci budou tyto informace vysvětleny metodou sběru informací z odborné literatury, které budou rozšířené o poznatky ze specializovaných pracovišť Policie České republiky.

Prioritní cíle bakalářské práce jsou stanoveny dva. Prvním je zjistit, jaký je aktuální trend a vývoj nákupu omamných a psychotropních látek na tzv. Dark Webu pomocí výzkumné metody sběr a analýza statistických dat. Druhým cílem je poté zjistit připravenost Policie České republiky se s tímto fenoménem plně konfrontovat. Hlavní výzkumnou metodou zde bude metoda řízeného rozhovoru s policisty ze specializovaných oddělení PČR, kteří se touto problematikou aktivně zabývají.

Jako sekundární cíl si bakalářská práce klade definovat fenomén kryptoměn, jejich anonymitu jako platebního prostředku a jejich další směřování v blízké budoucnosti, definování kyberprostoru a hlavně jeho, většině běžných uživatelů skrytý, Dark Web a tržiště, kde se provádí nelegální činnost.

2 Kryptoměny a jejich legální využití

Kryptoměna je virtuální měna, neboli digitální peníze, která na rozdíl od současných fiat měn, jakými jsou například americký dolar, euro anebo naše česká koruna, je peer-to-peer decentralizovaná a opírá se o asymetrickou kryptografii. Nejstarší a vůbec tou neznámější a nejdražší kryptoměnou na světě je „Bitcoin“¹.

2.1 Peer-to-peer

Na začátek je důležité si vysvětlit několik pojmů, abychom porozuměli fenoménu kryptoměn. Prvním takovýmto pojmem je takzvané P2P, neboli peer-to-peer (česky klient-klient). Tento pojem ve zkratce označuje typ počítačových sítí, ve kterých jsou si všechny jejich uzly rovnocenné a jednotliví klienti této sítě mezi sebou navzájem přímo komunikují a to bez jakéhokoliv prostředníka v podobě centrálního uzlu (centrálního serveru). Pokud systém peer-to-peer srovnáme s klasickým a to asymetrickým modelem, kde je jasně definovaný klient-server, tak v systému peer-to-peer s rostoucím počtem uživatelů exponenciálně roste taktéž přenosová kapacita sítě. Bohužel nevýhodou symetrie peer-to-peer je počáteční obtížnost navázání komunikace mezi uzly z důvodu absence centrálního uzlu, čili serveru².

2.2 Kryptografie

Dalším pojmem, který je potřeba vysvětlit je tzv. kryptografie (z anglického Cryptography). Kryptografii lze definovat jako matematickou disciplínu, která se zabývá šifrováním, tedy převádí zprávy do jejich utajené formy a naopak. Tyto převody lze použít pouze tehdy, kdy máme znalost šifrovacího klíče, za pomoci kterého můžeme tyto zašifrované zprávy čitelně a bezpečně přečíst. V tomto spektru můžeme též hovořit i o kryptografii asymetrické. O asymetrickou kryptografii se jedná pouze tehdy, pokud klíč použitý k dešifrování zprávy není stejný jako klíč, který byl použit k jejímu zašifrování. Například Bitcoin využívá poznatků matematické disciplíny kryptografie

¹ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

² STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

k bezpečnému fungování jeho sítě a to tím, že používá tzv. hashovací funkce a digitální podpis³.

2.3 Digitální otisk - Hash

Pojem hash a hashovací funkce. Pod pojmem hash si můžeme představit digitální otisk textu, který je výsledkem hashovací funkce. Tento digitální otisk má podobu unikátního seskupení alfanumerických znaků. Použití tohoto digitálního otisku textu uplatníme v rámci internetové bezpečnosti při zadávání hesel anebo elektronických podpisů. S tímto systémem hashování se setkala velká řada z nás, která si založila a používá například svou emailovou schránku. Anebo cokoliv jiného, kde při registrování své unikátní adresy vytvořila své jedinečné heslo. Toto heslo po jeho vytvoření projde tzv. hashovacím procesem a do cílové databáze se pouze uloží jako digitální otisk, který má podobu alfanumerických znaků. Pokaždé, když se uživatel přihlašuje například do svého emailu a zadává svůj login a heslo, tak hodnota hesla se algoritmicky porovná s hodnotou šifrovaného otisku a tímto ověřením se umožní vstup například do emailové schránky. Pokud by došlo k tomu, že by nějaký hacker prolomil databázi, kde jsou tyto hesla uloženy v podobě hashe, tak tyto zahashovaná hesla nepřečte z důvodu, že ať použité heslo je jakkoliv dlouhé, anebo složené z několika různých znaků, tak hash hesla bude vždy stejně dlouhý a hacker z takto zahashovaného hesla nemůže rozpoznat jeho délku. Z důvodu internetové bezpečnosti je důležité podotknout, že často používaná a slabá hesla lze odhalit pomocí slovních hashů a proto je důležité dbát na silných heslech, které nám mohou poskytnout oprávněný pocit internetové bezpečnosti. Dalším aspektem je po určité době měnit svá hesla anebo je nepoužívat duplicitně. Pokud změním v takovémto hesle i jeho jediný znak, tak i hash se kompletně změní a zároveň je nemožné z něj zrekonstruovat heslo původní⁴.

2.4 Blok a systém PoW / PoS

Dalším pojmem je tzv. blok, koncept PoW / PoS a řetězec bloků tzv. „Blockchain.“ Samotný blok je nejvýznamnější datová struktura, laicky řečeno „stavební kámen“ protokolu. Blok kóduje soubor objektů transakcí, které svým zahrnutím do jeho struktury potvrzuje. Pokud tento proces vztáhneme například na Bitcoin, tak vždy jedna z těchto transakcí v bloku bitcoinového protokolu je takzvanou generující transakcí,

³ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

⁴ Digitální pevnost. *Hash* [online]. 2018 [cit. 2022-02-13]. Dostupné z: <https://www.digitalnipevnost.cz/wiki/hash>

kteřá svým prostřednictvím vytvářív nové Bitcoinu. Další součástí bloku je i tzv. validní blok. Validní blok musí obsahovat určitou kryptografickou vlastnost, ale její splnění je velmi náročné na výpočetní výkon. Tato náročnost na výpočetní výkon je proměnná v čase a tato její vlastnost umožňuje tzv. zpětnovazebnou regulaci, díky které lze dosáhnout stability průměrné rychlosti generování bloků nových a tímto dosáhnout deterministické inflace měny. Tento koncept validního bloku v bitcoinovém protokolu se označuje jako „proof-of-work“ (PoW), ale můžeme se například i setkat s odlišným konceptem a to s „proof-of-stake“ (PoS), který funguje bez potřeby těžařů⁵. Tento koncept funguje na tzv. validátorech, neboli razičích (z angl. forger, minter), kteří uzamknou určité množství svých mincí do depozitu a tímto uzamčením získají právo ověřovat transakce vedené v jejich síti a tohoto procesu se mohou účastnit všichni tito validátoři bez výjimky. Každý validátor, který vytvořív nový blok je vybrán pseudonáhodně a to tak, že čím více má tento validátor uzamčených mincí, tak má větší šanci tento blok vytvořív. Ochranou této sítě je, že pokud validátor validuje nesprávné transakce, tak o své mince, které má takto uzamčené v depozitu, přijde. Odměnou validátorů za toto ověřování je transakční poplatek. Je důležité podotknout, že i tento systém odměn funguje v systému proof-of-work u Bitcoinu, ale tento není primárním zdrojem příjmu těžařů. Oba tyto systémy lze různě modifikovat anebo kombinovat do tzv. hybridních strategií, které lze uplatňovat po celém období funkčnosti kryptoměny. Oproti těžařům systému POW se raziči ze systému POS zaslужív o větší ochranu měny z důvodu, že ji osobně vlastní a propůjčují a tímto mohou mít i zásadní vliv na kvalitu generovaných bloků a taktěž se díky tomu razantně snižuje míra motivace kyberútoků na síť. Každý z těchto algoritmů má své výhody i nevýhody a nabízí nám různé škály uplatnění, pro které v současné době nemáme dostatečné znalosti. Díky absenci těchto znalostí, podle kterých bychom posoudili skutečné možnosti systému PoW a PoS, které by nám mohly teoreticky nabídnout, nemůžeme s jistotou říci, který je lepší^{6,7}.

2.5 Blockchain

Řetězec bloků, neboli blockchain. Jak sám název napovídá, tak jde o druh distribuované decentralizované databáze, která uchovává exponenciálně se rozšiřující

⁵ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

⁶ *Proof of Work a Proof of Stake* [online]. 13. 1. 2020 [cit. 2022-02-14]. Dostupné z: <https://m.alza.cz/proof-of-work-a-proof-of-stake>

⁷ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

řetězec záznamů dat. Tato data jsou mezi sebou provázána za pomoci kryptograficky zabezpečených P2P řetězů. Takto uložená data jsou v blockchainu uložena de facto navždy, jsou veřejně přístupná a nelze je falzifikovat, čímž jsou díky těmto náročným podmínkám unikátní⁸. V článku Blockchain, na Portálu Finex.cz je uvedena jednoduchá a dobře pochopitelná definice blockchainu, která uvádí, že: „*zjednodušeně řečeno, blockchain je jakousi online knihou účetních záznamů a velmi specifický druh databáze. Na rozdíl od běžných databází není centralizovaná, ale decentralizovaná, což znamená, že nemá žádného centrálního správce a nachází se na velkém množství počítačů po celém světě*“⁹.

3 Bitcoin

Bitcoin, jak je uvedeno v kapitole předešlé, je tou vůbec nejstarší, nejznámější a v současné době tou vůbec nejdražší kryptoměnou na světě. Bitcoin spatřil světlo světa v roce 2009, kdy byl vytvořen anonymním vývojářem, který se skrývá pod pseudonymem Satoshi Nakamoto. První průvodní zmínka o Bitcoinu byla publikovaná v článku od Nakamota již v říjnu roku 2008. Sám Nakamoto na internetovém fóru tvrdil, že na Bitcoinu pracoval již od roku 2007. Jakmile se Bitcoin rozšířil do podvědomí IT fanoušků, Nakamoto předal celou svou internetovou doménu www.bitcoin.org jednomu z fanoušků jeho projektu a to Gavinu Andresenovi, který se později stal hlavním vývojářem. Krátce po předání svého projektu se Nakamoto odmlčel. Do současné doby se jistě neví, zdali se pod tímto tajemným a zvučným pseudonymem skrýval geniální vývojář anebo šlo o celou skupinu odborníků zaměřených na IT, kryptografii a ekonomii. Teorií je velmi mnoho a zatím každá byla spolehlivě vyvrácena. Jediné co bylo zatím potvrzeno, je fakt, že Satoshi Nakamoto by měl mít ve vlastnictví zhruba jeden milión Bitcoinů, které vytěžil a převedl v letech 2009 - 2010 na své bitcoinové peněženky, které jsou od té doby bez pohybu. Dnes není zcela jisté, zda má on sám, či někdo jiný privátní přístupové klíče, které by k těmto peněženkám umožnily přístup anebo jsou Bitcoinu na nich navždy uzamknuté a ztracené^{10,11}.

⁸ CHOVANCULIAK, Róbert. *Pokrok bez povolení: Jak sdílená ekonomika, crowdfunding a kryptoměny změnily svět*. 1. vyd. Praha: Grada, 2020. 272 s. ISBN 978-80-271-1755-0.

⁹ Portál Finex.cz. *Blockchain: Co je blockchain a jak blockchain u kryptoměn funguje?* [online]. Aktualizováno 15. 2. 2022 [cit. 2022-02-16]. Dostupné z: <https://finex.cz/blockchain/>

¹⁰ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptoměny budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

3.1 Co je to Bitcoin a jak funguje

Bitcoin je decentralizovaná peer-to-peer síť v internetu, která spravuje historii platebních transakcí napříč mezi svými uzly. Základní jednotkou transakce v této síti je takzvaný Bitcoin, zkratka BTC. Jeho maximální počet jednotek je předem definovaný a omezený na celkové množství 21 milionů Bitcoinů a to je v řeči čísel přesně 20 999 999,9769 BTC. Všechny bitcoiny budou vytěženy k roku 2140 a už v roce 2033 bude vytěžena jejich naprostá většina. Nové bitcoiny vznikají procesem takzvané těžby, která je výsledkem procesu proof-of-work. Při těžbě se kromě vytěžení Bitcoinů potvrzují taktéž vlastní transakce na této síti a to tím, že dochází k převodům jednotek mezi adresami uživatelů bitcoinové sítě. První bitcoiny vytěžil sám Satoshi Nakamoto 3. ledna 2009 v 18:15:05 hodin a tímto činem započal tzv. „první kopnutí“, čímž získal odměnu 50 Bitcoinů a celému procesu dal pomyslnou zelenou. Od této doby se prvním vytěženému bitcoinovému bloku, který nese hashovaný název 00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f, mezi bitcoinovou komunitou říká příznačně dle knihy zrození „genesis blok.“ Fungování bitcoinové sítě je založeno na konsenzu, neboli společné shody pravidel, kdy informace od ostatních uzlů této sítě jsou akceptovány a splňují všechna již předem dohodnutá pravidla, která jsou všemi uzly předem očekávána. Kontrolu provádí každý takovýto uzel zcela samostatně. Proto jsou tyto operace zcela decentralizované a tudíž nejsou pod žádnou kontrolou centrální autority, která by na sebe přejímala supervizorní roli a dále s tímto nějakým způsobem manipulovala. Všechny transakce, které byly v této síti uskutečněny, jsou zapsány, uloženy a spravovány do tzv. „účetní knihy“ neboli blockchainu. Veškerá data, která jsou v blockchainu zapsána a uložena jsou plně k dispozici všem uzlům této sítě¹².

3.2 Bitcoin, jako měna budoucnosti?

Po vytěžení prvních Bitcoinů by se nám na první pohled mohlo zdát, že si je Satoshi Nakamoto někam na nějakou platformu uloží. Akorát toto neměl Satoshi Nakamoto vůbec v úmyslu. Jeho záměr byl zcela ryzí a jeho cíle mnohem větší. Dle Nakamota se měl Bitcoin jednou stát měnou budoucnosti. Z tohoto důvodu je potřeba, aby se do těžby připojili i další uživatelé, kteří by vytvářeli další bitcoiny, podíleli se na chodu

¹¹ CHOVANCULIAK, Róbert. *Pokrok bez povolení: Jak sdílená ekonomika, crowdfunding a kryptoměny změnily svět*. 1. vyd. Praha: Grada, 2020. 272 s. ISBN 978-80-271-1755-0.

¹² STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptoměny budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

a bezpečnosti sítě, kterou by tímto budovali a vytěžené Bitcoinů si mezi sebou posílali a nakonec s nimi platili za zakoupené zboží, služby anebo aby v nich mohli být přímo placeni za odvedenou práci. První transakci, během které byly odeslány Bitcoinů provedl Satoshi Nakamoto v lednu roku 2009. V této transakci poslal první Bitcoinů jím vytěžené vývojáři Halu Finneymu. Tato transakce je zaznamenána ve 170. bloku a společně s genesis blokem jsou to nejznámější bloky bitcoinové sítě. Shrnutí a potvrzení, Bitcoin se začal nápadně podobat zlatu a také i jeho těžba, čímž začal pomalu získávat vlastnosti dobrých peněz, které by z něho udělaly peníze samotné. Aby se s Bitcoinem dalo nakládat jako s platebním prostředkem, tak pro tyto účely bylo zapotřebí vytvořit tzv. adresu, na kterou by se dal posílat tam a zpět. I když se stal Hal Finney prvním příjemcem Bitcoinů na světě, tak tento Satoshiho počín nemůžeme pokládat za něco výjimečného. Nejdůležitější je okamžik, kdy bude někdo ochotný za zboží, či služby nabídnout Bitcoin jako platební prostředek. První vůbec takto provedená transakce, kdy byl Bitcoin použit jako platební prostředek za zboží se uskutečnila až po téměř roku a půl od první transakce mezi Nakamotem a Finneym. Každopádně si mezitím uživatelé a vlastníci Bitcoinů mezi sebou Bitcoin posílali, těžili ho a ukládali na své adresy. Taktéž v této době vznikly první ceny Bitcoinu vyjádřené v dolarech a taktéž první BTC burza Bitcoin Market. Prvním zlomem a milníkem byla nabídka, uveřejněná na fóru www.bitcointalk.org dne 21. května 2010. Konkrétně zde bylo uvedeno „*Zaplatím 10 000 Bitcoinů za pár pizz (..) za dvě velké, aby mi něco zbylo na další den. Rád si nechám kus pizzy na pozdější d'obání (..) Pokud máte zájem, dejte vědět, nějak se domluvíme. Díky, Laszlo*¹³.“ Za touto nabídkou stál Floridský programátor Laszlo Hanyecz, kdy po uběhnutí pouhých čtyř dnů odeslal jednomu „dobrovolníkovi“ z Anglie 10 000 bitcoinů a za tuto transakci mu přišly dvě pizzy objednané u Papa John's za částku 25 dolarů. Když si tuto částku přepočítáme a přeneseme se do května roku 2010, tak tehdy se dalo 10 tisíc Bitcoinů na burze prodat za dvojnásobek ceny dvou pizz. Po obdržení pizzy od Papa John's Hanyecz vše nafotil, aby měl důkaz o této transakci BTC za zboží a že vše proběhlo úspěšně. Je zajímavé, že tento příběh obletěl svět celkem dvakrát. Poprvé po této úspěšně provedené transakci a následně v druhé polovině roku 2013. Tehdy cena jednoho bitcoinu přesáhla 1 000,- USD. Při této ceně by v roce 2013 dvě pizzy od Papa John's stály kolem deseti milionů dolarů. Pokud se pomyslně přeneseme do února roku 2022, tak by jedna pizza vyšla na

¹³ Laszlo Hanyecz, příspěvek na fóru bitcointalk.org ze dne 21. 5. 2010. In: STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. Str. 43. ISBN 978-80-271-1043-8.

astronomických 201028000,00,- USD. Pokud se na tuto „nejdražší pizzu všech dob“ podíváme dnešní optikou, tak si můžeme oprávněně myslet, že Hanyecz udělal velkou chybu a dnes by mohl být milionářem. Je nutno podotknout, že v době této transakce o Bitcoinu moc lidí nevědělo a pouze jen hrstka IT nadšenců na internetových fórech typu bitcointalk.org se zde sdílela své zkušenosti a nabyté znalosti. Laszlo Hanyecz tímto dal možnost posunout Bitcoin směrem ke všeobecně přijímanému platebnímu prostředku a tímto se mu to nakonec povedlo. Zpráva o této transakci se šířila internetem a médií rychlostí světla. S jistotou můžeme říci, že tento okamžik byl zásadní z hlediska seznámení s Bitcoinem velké části inovátorů, autorů konkurenčních kryptoměn ale i mnohých startupů, které do dnešních dní Bitcoin obklopují. Je jisté, že za dnešním využití Bitcoinu, ale i jeho současnou cenou stojí jeho propagátor Laszlo Hanyecz. Bez této „nejdražší pizzy na světě“ by možná Bitcoin již dnes neexistoval. A jak se říká, s růstem hladu ve společnosti roste i chuť a to cena žádaného produktu a ještě podpořen skvělou reklamou „nejdražší pizzy na světě.“ Tato poptávka se nám odrazila i v datech, kdy po uplynutí čtyřech měsíců od této transakce se cena jedné Bitcoinové mince zdesetinásobila. O Bitcoin se začaly zajímat i významnější média, jako například slashdot.com, atd. Zajímavostí je, že byla dokonce objevena chyba v bitcoinové síti, která umožnila uměle vytvořit 184 miliard Bitcoinů. Tato chyba byla rychle napravena a vše se vrátilo do zajetých kolejí. Tato chyba je nepochybně nevídanou událostí pro něco, co se teprve tvoří, ale i takovýto útok nám ukazuje, jak oblíbeným a populárním se Bitcoin stal a k čemu směřuje. Jeden člen fóra kvůli Laszlo Hanyeczovi založil server ounce.me, který je zaměřen na sledování vývoje ceny tehdy zakoupených pizz. Tímto se Laszlova pizza stala vedle zlata, stříbra, amerického dolaru a nebo ropy indexem ceny. Strukal a Skalický k tomu ve své knize uvádějí, že: „*Dolarový svět má svůj BigMac index, tak svět kryptoměn má svůj Bitcoin index*“¹⁴. Díky těmto prvním krůčkům si dnes každý může za Bitcoin, či jiné altcoiny zakoupit pizzu na damejidlo.cz, nebo elektroniku na alza.cz. Tato transakce nebyla jednou zlomovou událostí roku 2010. V této době byla též založena jedna z tehdy největších a nechvalně známých burz obchodující s Bitcoinem Mt.Gox, nebo byla provedena první veřejně známá půjčka Bitcoinů, dále došlo k první transakci mezi mobilními telefony a představitelé vlád států začali poprvé veřejnost varovat před decentralizovanou

¹⁴ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. Str. 44. ISBN 978-80-271-1043-8.

digitální měnou, která se dá dle jejich výstupů snadno a efektivně využít k financování teroristických aktivit po celém světě¹⁵.

V dnešní době, kdy již celkem funguje LightningNetwork, už člověk nemusí posílat své Bitcoinů zdlouhavě a čekat na pizzu čtyři dny. Prostřednictvím Onchain platby je možné platit obdobně, jako když na internetu platíte bankovním převodem. Není to sice na lusknutí prstu a rychlost platby je závislá na zatížení sítě, ale je to rozhodně způsob, jak Bitcoin dostat do své peněženky. Namísto vyplnění čísla bankovního účtu příjemce napíšete jeho Bitcoinovou adresu, kterou vám poskytl, a částku mu ze své peněženky příkazem pošlete. Funguje to sice přes prostředníka, podobně jako u PayPal. Výhodou je okamžité potvrzení transakce, nízký poplatek za provedenou platbu a velmi vysoká úroveň soukromí. Lightning Network je napřímo provázaný s Onchain platebním systémem. Tato jejich vzájemná provázanost prakticky funguje tak, že se vytvoří tzv. platební kanál, na kterém je provedena běžná Onchain transakce s běžným poplatkem a je zařazená do bloku. Poté je již možné používat síť zcela bez Onchain plateb do doby, než z ní chcete vystoupit. Síla Lightning Network se ve skutečnosti projeví svými vlastnostmi, jakmile se bude používat přímo v reálném světě a v masové míře. Je důležité podotknout, že přímý efekt této sítě v našich podmínkách prakticky neexistuje. Z pohledu síťového efektu je Lightning Network jakýmsi altcoinem, jelikož je do jisté míry nezávislá. Adresa pro platební transakci vypadá jinak, než při Onchain platbě. Bitcoinů se posílají trochu jiným způsobem a zároveň i přijímají. Tuto vlastnost Lightning Network lze sledovat v BTCPaysserveru při příjmu, kde je uvedená nabídka dvěma způsoby platby a to „Bitcoin“ a „Bitcoin Lightning“. Pokud si vyberete možnost druhou, tak peníze za transakci vám přijdou do tzv. Lightning peněženky. V současnosti je již jisté, že klasické Bitcoinové peněženky a peněženky Lightning budou postupně sloučeny v jednu, jako je tomu v případě u Phoenix Wallet¹⁶.

3.3 Bitcoinová adresa

Adresa je určena k identifikaci příjemce platby. Tuto adresu můžeme přirovnat například k číslu bankovního účtu. Bitcoinová adresa v sobě snoubí zakódované číslo do řetězce alfanumerických znaků, jehož délka je něco mezi 27-34 znaky a taktéž se u něj rozlišují velká a malá písmena. Pro představu bych uvedl příklad takovéto adresy:

¹⁵ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

¹⁶ BEDNÁR, Juraj. *Kryptomeny: platobná sieť internetu*. Elektronická kniha. 2020. 204 s. ISBN 999-00-030-7093-7.

1KZ7MCXC5UJKiNYtvG8c9qEc9WdCz87LBf. Zápis jinou formou může vypadat takto: bc1q6rggkagqa8arkyvwy5zzqyjd2945xyjfy130ul. Je nutno podotknout, že bitcoinovou adresu lze vygenerovat též bez spolupráce sítě v režimu offline, protože bitcoinová adresa je pouze hashem veřejného klíče. Z důvodu, že vygenerování bitcoinové adresy není nikterak energeticky náročné a tudíž se jedná o celku levnou operaci, lze vytvořit novou adresu pro každou i nesouvisející transakci. Díky tomuto lze znemožnit jakékoliv stopování. Veškeré adresy a klíče k nim patřící spravuje uživateli jeho bitcoinová peněženka, neboli Wallet¹⁷.

3.4 Bitcoinové peněženky

Jak je uvedeno výše, tak bitcoinová peněženka, neboli Wallet, je software, který spravuje soukromé klíče patřící k bitcoinovým adresám uživatele. Bitcoinová peněženka nám ukazuje výpočty zůstatků na adresách uživatele, kde je například uvedeno, kolik coinů uživatel vlastní a též je mu ukázána i jejich aktuální hodnota ve fiat měně, kterou si zvolil. Tomuto se říká „portfolio value“ neboli česky řečeno „hodnota portfolia.“ Dále bitcoinová peněženka umožňuje uživateli odesílání a přijímání plateb, zobrazuje historii všech uskutečněných transakcí na adrese anebo umožňuje vést evidenci známých adres, které byly pro platby již použity anebo si je uživatel přidal do záložky „oblíbené.“ Aktuálně se používají softwarové a hardwarové peněženky¹⁸.

3.4.1 Softwarová peněženka

Softwarovou peněženku může mít uživatel nainstalovanou ve svém PC, či ve svém mobilním telefonu. Výhodou takovéto peněženky je to, že jich můžete mít ve svém zařízení mít několik a máte k nim de facto neomezený a rychlý přístup. V současné době se používají například softwarové peněženky od tržiště binance TRUST, nebo MetaMask, či EXODUS a další. Nevýhodou takovéto peněženky oproti hardwarové je to, že je lze jednodušeji napadnout a zcizit Vám vaše kryptoměny. Výhodou softwarové peněženky je možnost stakování vybraných a podporovaných kryptoměn. Pojem stakování, čili systém PoS jsme si vysvětlili v kapitole předešlé¹⁹.

¹⁷ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

¹⁸ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

¹⁹ Binance Academy. *Co je kryptoměnová peněženka?* [online]. 18. 6. 2019, aktualizace 11. 11. 2021 [cit. 2022-02-18]. Dostupné z: https://academy.binance.com/cs/articles/crypto-wallet-types-explained?utm_source=BinanceAcademy&utm_medium=Academy&utm_campaign=StaySAFU

3.4.2 Hardwarová peněženka

Hardwarová peněženka je pravým opakem softwarové. Hardwarová peněženka je obdoba flash disku, který je chráněn zahashovaným přístupovým kódem, který si každý uživatel zvolí sám a následně je chráněná z důvodu její obnovy (ztráty, či zapomenutí přístupového kódu) tzv. seed kódem. Tento kód je souborem náhodně a unikátně vybraných anglických slov, které umožní uživateli přístup do jeho adresy z jakéhokoliv takového zařízení. Velmi důležité je, aby každý uživatel HW peněženky měl svůj unikátní seed bezpečně a trvanlivě uložený z důvodu, že ho může kdykoliv potřebovat. Mezi nejznámějšími hardwarovými peněženkami ve světě kryptoměn jsou český TREZOR anebo konkurenční LEDGER. Hardwarové peněženky spravují jak bitcoinové adresy, tak i adresy jiných kryptoměn jako například Ethereum, Solana, Cardano, Polkadot, atp. Nevýhodou hardwarové peněženky oproti softwarové je její pořizovací cena, neumožnění okamžitého přístupu (připojení k PC, zadání hesla, spuštění nativní aplikace), či přímo její fyzické vlastnictví. Naprostou výhodou je její ukázkové a de facto neprolomitelné zabezpečení²⁰. Jedny z prvních bitcoinových peněženek umožnily jejímu uživateli těžit nové bloky a díky této funkci se jednalo o plnohodnotného klienta sítě. Peněženka obecně může být kromě její konvenční aplikace (viz SW peněženka) i v online formě, jako např. Blockchain.info nebo BitGo²¹.

3.5 Bitcoin a WikiLeaks

Bitcoin umožnil v roce 2011 serveru WikiLeaks přijímat finanční dary pro jeho provoz navzdory tomu, že Pentagon označil stránky, které patří spoluzakladateli a šéfovi serveru Julianovi Assange za hrozbu pro národní bezpečnost Spojených států a byly jimi zablokované veškeré finanční toky. Server WikiLeaks byl zablokovaný Pentagonem z důvodu, že zveřejnil například tajné dokumenty o mučení, kterého se dopustila armáda USA v Iráku, anebo dokumenty o špionážní síti složené ze zastupitelských úřadů USA. Julian Assange, po této uvedené blokadě jeho finančních aktivit, zveřejnil na adrese webu WikiLeaks krátkou adresu své bitcoinové peněženky a tímto krokem mohl přijímat namísto dolarů příspěvky od svých podporovatelů v Bitcoinech. Tímto krokem Julian Assange udělal této kryptoměně velkou reklamu a taktéž obešel zablokování veškerých finančních toků Pentagonem. Je nutno

²⁰ Binance Academy. *Co je kryptoměnová peněženka?* [online]. 18. 6. 2019, aktualizace 11. 11. 2021 [cit. 2022-02-18]. Dostupné z: https://academy.binance.com/cs/articles/crypto-wallet-types-explained?utm_source=BinanceAcademy&utm_medium=Academy&utm_campaign=StaySAFU

²¹ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

podotknout, že v současné době uvalený ban na WikiLeaks už pominul platnosti a lze již přispívat na provoz stránek i jinými metodami, nežli pouze Bitcoinem. Tato situace poukázala na to, že díky Bitcoinu mohou stránky WikiLeaks a jím podobné přijímat finanční prostředky a normálně fungovat, ať se to světovým vládám líbí či nikoliv. Koneckonců Bitcoin začal měnit pole diplomacie, mezinárodní vztahy a politiku²².

4 Altcoiny, jejich princip a využití

Bitcoin není pouze jedinou kryptoměnou. Existují i tisíce dalších kryptoměn. Altcoin je zkratkou pro označení kryptoměn jako „alternative coin“. První alternativní kryptoměnou, která kdy spatřila světlo světa kryptoměn byla měna nazvaná jejími tvůrci jako „Namecoin“. Myšlenka vytvoření jiných kryptoměn a vytvoření alternativy v kdysi hegemonním světě Bitcoinu byla prostá. Spouště uživatelům vadil obtížný a pomalý proces těžby nových mincí Bitcoinu a rychlost provedených plateb napříč uzly. Uživatelé chtěli proto něco nového a rychlého. A z těchto oprávněných důvodů vznikla myšlenka alternativních kryptoměn, které by tyto neduhy odstranily a přinesly něco nového a revolučního. Altcoiny nazýváme všechny ostatní kryptoměny, kromě Bitcoinu. Mezi ně si například můžeme uvést Ethereum, Litecoin, Dash, Solana, Cardano, Monero, Dogecoin, a mnoho jiných. Každý z těchto altcoinů funguje na určitém principu a nabízí jiné možnosti využití. Některé z nich například zlepšují rychlost validace a provedení plateb – Solana, či jiné nabízí bezkonkurenční anonymitu – Monero, anebo jejich blockchain nabízí svou architekturu k dalším projektům – Ethereum a s ním související fenomén poslední doby NFT. Většina altcoinů je zalistovaná na velkých globálních kryptoburzách a tudíž zde s nimi můžete volně obchodovat. Existují ale i takové altcoiny, které chtějí těžit z krátkodobé popularity a nemají reálné využití. Pro představu si můžeme uvést takový TrumpCoin a nebo PutinCoin. Staly se i případy, kdy některé altcoiny využily popularitu někoho jiného, přiživily se na obrovské vlně oblíbenosti a bez jakéhokoliv praktického využití či dlouhodobé strategie vývojářů po dosažení cíle takto vzrostlé hodnoty ukončily své servery a jejich vývojáři zmizeli s penězi do neznáma. Tyto altcoiny nazýváme z angl. scamcoins, nebo shitcoins. Jako příklad si můžeme uvést Squid Coin, jehož prostřednictvím se jeho vývojáři přiživili na globálně oblíbeném seriálu od Netflixu Squid Game, neboli česky Hra na Oliheň, se kterou ale neměli vůbec nic společného.

²² STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

Tvůrci, kteří zůstali v anonymitě, využili celosvětového boomu seriálu a vytvořili pro něj projekt a digitální mince. Mince byli zalistované na největších kryptoburzách na světě. Už jen po prvním týdnu tato virtuální měna vzrostla o neuvěřitelných 230 tisíc procent. Pro představu to znamená, že 26. října 2021 byla hodnota jedné mince kolem 3 000 USD. Mince jste mohli nakupovat a prodávat. Byl v tom ale jeden háček. Tvůrci vytvořili jakousi karanténní dobu, kdy jste mince sice mohli zakoupit, ale nemohli jste s nimi obchodovat a prodávat je. Tato možnost se měla uživatelům otevřít až po tom, co se měly spustit servery jejich nové on-line hry nazvané Squid Game. Dalším takovýmto háčkem byla i výše vstupního poplatku do hry, který byl tvůrci stanoven na 456 mincí. Pro zajímavost si můžeme uvést, že v době největšího růstu měla tato výše vstupního poplatku hodnotu více než jednoho milionu dolarů. Před uplynutím této doby v souvislosti s velkou oblíbeností seriálu stoupala i cena mincí do závratných výšin. Pak ale bublina praskla, jejich on-line hra nikdy nebyla dokončena a vývojáři projektu zmizeli i s penězi obdržnými za jejich mince neznámo kam. V současnosti jsou všechny jejich prezentace projektů včetně jejich účtů na sociálních sítích uzavřeny a hodnota jejich mince nemá ani půl centu^{23,24,25}.

První altcoiny začaly vznikat v roce 2011. Masovou popularitu si altcoiny získaly v rozmezí let 2013 a 2014. Tehdy byla většina altcoinů obchodovatelná proti BTC. Oproti Bitcoinu byla u některých altcoinů obří volatilita a spousta lidí začala provozovat trading a organizovat akce typu pump & dump. To ve zkratce znamená uměle cenu obchodované mince vynést do závratných výšin a posléze ji nechat prudce padnout až na její samotné dno. Kdo předem obdržel informace o těchto akcích, tak si mohl přijít na nemalé peníze. Většina altcoinů je postavena na volně dostupném software repozitáři Bitcoinu a tyto ho dále upravují a vylepšují. Existují ale i takové altcoiny, které jsou postaveny na protokolu CryptoNote. Tento protokol například umožňuje anonymizaci kryptoměny na něm postavené. Příkladem může být kryptoměna Monero, Zcash nebo Dash. Pro další dělení altcoinů si můžeme uvést, že se může jednat o univerzální platformu pro odvozené projekty. Takovýmto případem může být Barcelona Fan Tokens (\$BAR), který pro své fanoušky vytvořil světoznámý fotbalový

²³ ŠTASTNÝ, Josef. [Pro začátečníky] Co je to altcoin [online]. 29. 8. 2020 [cit. 2022-04-01]. Dostupné z: <https://kryptomagazin.cz/pro-zacatecniky-co-je-to-altcoin/>

²⁴ VÁVRA, Jan. *Squid Game na vlastní kůži. Kryptoměna inspirovaná seriálem tvrdě ztrestala spekulanty* [online]. 2. 11. 2021 [cit. 2022-04-01]. Dostupné z: <https://www.e15.cz/kryptomeny/squid-game-na-vlastni-kuzi-kryptomena-inspirovana-serialem-tvrde-ztrestala-spekulanty-1384919>

²⁵ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

klub FC Barcelona. Každé altcoiny se liší svou stavbou a využitelností. Mezi tyto rozdíly oproti Bitcoinu například řadíme fungibilitu, neboli zaměnitelnost mincí. Další rozdíl může být v takzvaném „smart property“, kdy se jedná o barevné mince, nebo digitální tokeny, které představují určitý typ fyzického nebo i digitálního vlastnictví. Taktéž je důležitý rozdíl u monetární strategie altcoinů oproti Bitcoinu. Spousta z nich je deterministická (ve zkratce se jedná o strategii jednoznačnou a předem dopředu známou) a konečně inflační, jako je tomu u Bitcoinu. To znamená, že Bitcoinů se vytěží pouze 21 milionů mincí a další už nebude možné vytěžit. Taktéž jsou i známé případy, kdy je altcoin nekonečně inflační a tempo uvolňování nových mincí je předem známo. Tento případ se týká konkrétně kryptoměny Monero. Dále se altcoiny liší v prvotní distribuci mincí. Jsou takové, které vycházejí ze systému POW od nulové počáteční zásoby, kdy těžba postupně uvolňuje do oběhu další mince, až nakonec dojde k úplnému vytěžení. U některých altcoinů nemusí existovat samotná těžba a je vydané pouze určité množství mincí do oběhu. Tento případ se týká konkrétně kryptoměny Ripple. Dále existují takové altcoiny, které fungují v systému POW, ale před jejich uveřejněním a zalistováním do burz měl výhradně právo těžit pouze tým vývojářů. Tento systém se nazývá „premine“, neboli přetěžba. Taktéž si můžeme uvést další systém, u kterého je projekt financován tím, že každý vytěžený blok jeho blockchainu odvede autorům projektu předem definovanou část nových mincí. Příkladem může být Zcash. Další odlišnost altcoinů oproti Bitcoinu je například ve strategii konsensu zápisu do blockchainu, aj.²⁶.

4.1 Altcoiny a jejich neomezené možnosti

Pokud hledáme snadný a levný převod peněz, tak alternativní kryptoměna Ripple (XRP) v sobě snoubí tyto přednosti. Něco podobného nám může nabídnout kryptoměna Stellar Lumens, kterou mají na svém kontě stejní vývojáři. Existují i takové kryptoměny, které zcela nahrazují měny klasické, či drahé kovy anebo i jiná aktiva? Pro tyto důvody byla vytvořena digitální měna nazvaná USDT (Tether), která umí převést klasickou měnu USD do jejich virtuální podoby a přičemž zachová jeho aktuální hodnotu. To prakticky znamená, že jedna mince USDT má hodnotu jednoho USD. Jiným takovýmto příkladem může být společnost Digix a její platforma Digix DAO. Společnost se zabývá obchodem s drahými kovy a to zejména se zlatem. Přes její platformu Digix DAO si můžete zlato u ní přímo zakoupit a záleží pouze a jen na Vás, zda si zlato v jeho fyzické

²⁶ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

podobě necháte zaslat domů, či si místo něj zakoupíte digitální minci nazvanou DGX, jejíž hodnota jedné její mince koreluje s hodnotou jednoho gramu zlata. Taktéž existují i kryptoměny, jejichž digitální mince jsou určeny jak pouze pro video-herní průmysl, nebo pro sázení a hraní hazardních her v online prostředí, tak i pro prostředí sociálních sítí²⁷.

4.1.1 Monero - plně anonymní digitální měna

Vznik Monera (XMR) datujeme k 18. dubnu roku 2014, kdy bylo známo pod jeho tehdejšími názvem BitMonero. Tento název byl po krátkém čase zkrácen pouze na Monero. Vychází z kryptoměny Bytecoin ale s tím rozdílem, že je na rozdíl od něho nekonečně inflační. Jeho inflační index je nastaven klesající k nule ve dvou fázích. Na konci roku 2021 bylo uvolněno 18,4 milionů mincí a od té doby druhá fáze vykazuje postupně klesající křivku inflace s podílem menším než 1 % za kalendářní rok. Monero se dělí na menší a větší jednotky pro které má své označení. Největší z nich se nazývá meganero a naopak nejmenší je piconero. Fee, neboli tzv. poplatek za transakci je menší v závislosti na počtu transakcí za časovou jednotku. Fixní není ani velikost bloku, která je v tomto případě adaptivní. To znamená, že z posledního sta bloků se vypočítá medián velikosti a výsledkem tohoto mohou být další následující bloky větší. Hlavní devizou Monera je jeho anonymizační schopnost, kterou jí poskytuje protokol CryptoNote. Anonymizace tkví v tom, že odesílatele ani příjemce platby není možné vidět. Pouze lze zjistit výši částky v uvedené transakci. Technika pro ověřování transakcí se nazývá „Confidential Transactions.“ S touto myšlenkou přišel vývojář Greg Maxwell. Podepisování transakcí funguje jiným způsobem, než je to u Bitcoinu. Z důvodu mixování vstupů. Vývojáři Monera přišli se způsobem, jak se dají používané ring signatures zkombinovat s Confidential Transactions. Schéma, které touto kombinací vzniklo, nazýváme ringCT, neboli „Ring Confidential Transactions.“ RingCT byl do Monera implementován začátkem roku 2017. Díky tomuto schématu není možné vysledovat od koho, komu a kolik bylo za transakci zapláceno²⁸.

²⁷ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

²⁸ STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

5 Kyberkriminalita

Internet je mocný nástroj, který může ve špatných rukách napáchat velké škody napříč celou společností. Kyberprostor můžeme definovat jako jakési virtuální prostředí, které nemá jasně definovaný konec ani začátek, nezná hranice států a nelze s jistotou určit, jak je toto internetové prostředí velké. Dynamicky se rozvíjející informační technologie s sebou ruku v ruce přináší společensky škodlivé jevy, z nichž některé mohou naplnit skutkovou podstatu trestného činu. Toto jednání je potíráno Policií České republiky dle platných zákonů jak v běžném světě, tak i v prostředí kyberprostoru a v informačních a komunikačních technologiích. Tato oblast může být předmětem útoku anebo se může stát významným prostředkem k páchání trestné činnosti. Policie České republiky sleduje a eviduje veškeré známé trestné činy, které jsou spáchané v kyberprostoru. Zajímavostí je, že tento fenomén vzrůstá exponenciálně na pomyslné přímce této problematiky. V roce 2011 bylo Policií České republiky evidováno na 1502 známých trestných činů, spáchaných v kyberprostoru. V roce 2019 bylo známých trestných činů evidováno již 8417. To je takřka osminásobek vzrůstu veškerých známých trestných činů, které se staly v kyberprostoru. Bohužel latentní trestné činy, které se odehrály v kyberprostoru nelze měřit a tudíž k nim nelze vytvořit evidenci, která by je monitorovala a mohla by poskytnout tvrdá data²⁹.

5.1 Legislativa

Kybernetická kriminalita je velmi různorodá a je obsažena napříč společenským spektrem. Tuto problematiku ustanovuje a řeší trestní zákoník, který byl přijatý Parlamentem České republiky a vyhlášený ve sbírce zákonů pod číslem 40/2009 Sb. Dnem 1. ledna 2010 byl tímto novým trestním zákoníkem nahrazen dřívější československý trestní zákon. Trestní zákoník definuje trestní předpisy a je jakousi „kuchařkou“ trestního práva hmotného. Drtivá část trestných činů spáchaných v kyberprostoru je obsažena v hlavě V. „Trestné činy proti majetku“ zákona č. 40/2009 Sb., trestního zákoníku (dále jen TrZ). K trestným činům obsažených v hlavě V. TrZ lze uvést například trestný čin dle ust. § 209 TrZ „Podvod“, anebo jeho další deriváty, které jsou popsány v ust. dle § 210, § 211, § 212 TrZ. Dále lze uvést trestný čin dle ust. § 213 TrZ „Provozování nepoctivých her a sázek“, anebo trestný čin dle ust. § 216 TrZ „Legalizace výnosů z trestné činnosti.“ Taktéž je důležité si uvést trestné činy, při nichž je prostřednictvím počítače páchána trestná činnost v kyberprostoru. Vyjmenujeme si

²⁹ POLICIE ČESKÉ REPUBLIKY. *Kyberkriminalita* [online]. Nedatováno [cit. 2022-04-01]. Dostupné z: <https://www.policie.cz/clanek/kyberkriminalita.aspx>

pouze několik z nich. Prvním takovýmto segmentem trestných činů jsou trestné činy, které jsou obsaženy v hlavě III. TrZ „Trestné činy proti lidské důstojnosti v sexuální oblasti.“ Jakousi alfa a omega je v této hlavě trestního zákoníku uveden trestný čin dle ust. § 191 TrZ „Šíření pornografie“, nebo také trestný čin dle ust. § 192 TrZ „Výroba a jiné nakládání s dětskou pornografií“, anebo trestný čin dle ust. § 193b TrZ „Navazování nedovolených kontaktů s dítětem.“ Další trestné činy, které stojí za zmínku, jsou trestné činy hospodářské, které jsou uvedené v hlavě VI. TrZ. Mezi tyto trestné činy řadíme například trestný čin dle ust. § 255 TrZ „Zneužití informace v obchodním styku“, který je uveden v díle 3. „Trestné činy proti závazným pravidlům tržní ekonomiky a oběhu zboží ve styku s cizinou“, anebo trestný čin dle ust. § 270 TrZ „Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi“, který je uveden v díle 4. „Trestné činy proti průmyslovým právům a proti autorskému právu.“ Dalšími trestnými činy jsou trestné činy proti pořádku ve věcech veřejných, které jsou uvedené v hlavě X. TrZ. V díle 5., který nám uvádí trestné činy narušující soužití lidí, si můžeme uvést dva aktuální a populární trestné činy, ke kterým hojně dochází na sociálních sítích. Za prvé se jedná o trestný čin dle ust. § 356 TrZ „Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod“ a za druhé o trestný čin dle ust. § 357 TrZ „Šíření poplašné zprávy.“ Například si můžeme uvést trestné činy dle hlavy II. TrZ. Zde se jedná o trestné činy proti svobodě a právům na ochranu osobnosti soukromí a listovního tajemství. Zde si můžeme uvést trestný čin dle ust. § 175 TrZ „Vydírání“ a trestný čin dle ust. § 184 TrZ „Pomluvy“³⁰.

Pro tuto bakalářskou práci jsou ale stěžejní a jakousi „alfou a omegou“ trestné činy obecně nebezpečné, které jsou obsaženy v hlavě VII. TrZ a to konkrétně v díle 1., kde se jedná o „Trestné činy obecně ohrožující.“ Konkrétně je zde nutno uvést jeden z nejčastějších trestných činů a to trestný čin dle ust. § 283 TrZ „Nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a s jedy“ anebo též trestný čin dle ust. § 287 TrZ „Šíření toxikomanie.“ Ruku v ruce s těmito výše uvedenými trestnými činy jsou i trestné činy dle ust. § 284 TrZ „Přechovávání omamné a psychotropní látky a jedu“ a dle ust. § 286 TrZ „Výroba a držení předmětu k nedovolené výrobě omamné a psychotropní látky a jedu.“ Též si můžeme i uvést trestný čin dle ust. § 285 TrZ „Nedovolené pěstování rostlin obsahujících omamnou nebo psychotropní látku.“ Toto ustanovení lze užít, pokud někdo pěstuje například

³⁰ ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: Sbírká zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

Marihuanu anebo jiné psychedelika jako například halucinogenní houby, které obsahují psilocybin^{31,32}.

5.2 Temná síť internetu

„Dark Web představuje tajemné nelegální místo v hloubi internetu, na němž si můžete nakoupit drogy, sledovat dětskou pornografii či zaplatit nájemného vraha³³.“ Pod touto větou se skrývá to, co se většinou píše o Dark Webu. Jenže Dark Web není pouze černobílým světem, ve kterém se za temnou oponou skrývá velké zlo a zlí lidé. V této kapitole si přiblížíme, co je to Dark Web, jakým způsobem funguje, jaký je jeho potenciál a co se na něm dá najít³⁴.

5.2.1 Surface web

Slovo web je zkrácenina tzv. World Wide Web, respektive předpony všech stránek, které jsou nám na internetu známy – www. Web se dá rozdělit na to, co se pomyslně nachází na jeho povrchu a na to, co se nachází pod jeho pomyslným povrchem, tj. v jeho hloubi. Webové stránky nacházející se na tzv. povrchu nám umožňují pracovat například s vyhledávači od Google, nebo Seznam. Pokud něco hledáte, tak Vám postačí, abyste do výše uvedeného vyhledávače napsali frázi, nebo to co konkrétně hledáte a tento vyhledávač Vám na Vaši otázku vygeneruje odpovědi a případné odkazy, kde lze na Vaši otázku odpovědět, či Vás přeměrovat k nějakému podobnému tématu. Takto funguje tzv. surface web neboli pomyslný povrch webu. Vše ostatní, co nemůžeme najít pomocí robotických vyhledávačů na surface webu se skrývá hluboko pod jeho povrchem, čili na tzv. Deep webu³⁵.

5.2.2 Deep web

K tomuto se vybízí otázka, zdali je veškerý obsah, který se nachází na Deep webu nelegální. Opak je pravdou. Spousta dat, informací a věcí, které se zde nachází

³¹ MACHÁLKOVÁ, Zuzana. *Nejoblíbenějšími psychedeliky Čechů jsou LSD a houby, ukázal výzkum. Experti ale varují před riziky* [online]. 22. 8. 2021 [cit. 2022-04-12]. Dostupné z: https://www.irozhlas.cz/zivotni-styl/psychedelika-ldd-houby-narodni-psychedelicky-vyzkum-nudz_2108221936_btk

³² ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: Sbirka zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

³³ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. Str. 9. ISBN 978-80-271-2934-8.

³⁴ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

³⁵ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

jsou legální. Vedle nelegálního obsahu, který tu samozřejmě najdeme, se zde nachází například všechny Vaše emaily, které jste kdy odeslali a přijali, nebo veškerá soukromá konverzace a neveřejné statusy ze sociálních sítí typu Facebook, Instagram, VKontakte, atd. Vlastně by se dalo říci, že velkou část Deep webu tvoří data, ke kterým mají přístup jen jejich vlastníci a to přes přístupové údaje, jako je uživatelské jméno a heslo. Díky nepřehlednému počtu informací je Deep web mnohem rozsáhlejší než surface web. Zajímavostí je, že celkových 96 procent veškerého obsahu, který je na internetu, se bravurně skrývá jakýmkoliv vyhledávačům. Tudíž surface web tvoří pouze 4 procenta z celkového množství dat, která jsou k dispozici na internetu. V kontextu s Deep webem je jeho součástí i jedna malá část, která ale patří k jeho nejzajímavějším^{36,37}.

5.2.3 Darknet

Darknet je jakousi podmnožinou Deep webu. Jedná se o tzv. temnou síť internetu. Tato síť je plně decentralizovaná. Pro jeho lepší pochopení si můžeme představit, že jde o jakýsi tajný spolek, který existuje v běžném světě. Kdysi se členové tajných spolků scházeli na tajných schůzkách, o kterých běžný smrtelník nevěděl. Abyste se mohli dostat na takovouto schůzku, museli jste znát alespoň některého ze stálých členů tajného spolku a na jeho doporučení jste se mohli schůzky zúčastnit. Tito členové tajných spolků se scházeli nejen na zcela tajných místech, ale i na místech veřejnosti přístupných. Pouze jejich členové měli přesné informace o tom, kde a kdy se schůzka bude konat. Pokud tento formát převedeme do kyberprostoru, tak Darknet funguje jako jakýsi tajný spolek. Využívá stejné technologie, jako zbytek Clear Webu a to například webové stránky, emaily anebo sdílení souborů mezi jeho uživateli. Tyto technologie jsou přístupné komukoliv a kdykoliv. Dotyčný musí pouze vlastnit speciální software a musí vědět co, a koho chce na této temné síti vyhledat³⁸.

5.2.4 Dark Web

Dark Web je nám blíže, než bychom si mohli představit. Spousta z nás si může myslet, že Dark Web se nachází kdesi v temných hlubinách internetu. Jenže opak je

³⁶ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

³⁷ KAVALLIEROS, Dimitrios et. al. *Understanding the Dark Web*. In: BABAK, Akhgar et. al. *Dark Web Investigations*. Cham (CHE): Springer Nature Switzerland AG, 2021. ISBN 978-3-030-55343-2.

³⁸ REDAKCE CHIP. *DARKNET - Temná strana internetu* [online]. 8. 2. 2012 [cit. 2022-04-12]. Dostupné z: <https://www.chip.cz/novinky/trendy/darknet-temna-strana-internetu/>

pravdou. Dark Web je všem uživatelům globální sítě internet bez výjimek dostupný na několik kliknutí. Stačí k tomu mít stažený speciální prohlížeč, který na první pohled z uživatelského hlediska nerozeznáte od svého standardního prohlížeče, kterým brouzdáte na surface webu. Pokud máte stažený tento speciální prohlížeč, pak stačí kliknout na webovou adresu obdobně, jako při otevírání klasických webových stránek na internetu. Jen tato webová stránka oproti té klasické vypadá malinko jinak a zpravidla končí .onion. Poté se vám otevře úplně jiný svět, než na který jste zvyklí. Zde totiž můžete snadno narazit na různá zvěrstva, která nemají v civilizované společnosti místo. Dark Web je až po jeho pomyslný strop plný drogami všeho druhu, tisíci hodinami dětské pornografie a nepřeborného množství odcizených kreditních karet. Je možné si na Dark Webu objednat a zaplatit nájemného vraha k vykonání vraždy? Je důležité říci, že reálně to není možné. Existují různé nabídky těchto služeb, ale v každém případě se jednalo o podvod s cílem z objednavatele získat co nejvíce peněz. Taktéž není reálně na Dark Webu zakoupit palné zbraně. Jsou případy, kdy k tomuto článku bylo založeno i speciální tržiště s prozaickým názvem „The Armory,“ které tyto služby uživatelům nabízelo. Jenže i zde docházelo k velkému množství podvodů a po jejich odhalení tržiště uzavřelo své brány. Lze si na Dark Webu najmout ďábelského hackera, který by byl schopný mávnutím kyberproutku zlikvidovat například nějakého vlivného politika? Takovýchto nabídek je na Dark Webu hodně a všechny Vás budou ujišťovat, že je to možné. I v těchto případech se bude jednat o podvod, kdy výsledek Vašeho objednaného útoku nikdy nevidíte a taktéž nikdy nevidíte své peníze, které jste do toho vložili. Je nutné říci, že Dark Web neumí efektivně vytvořit a provozovat trh s nájemnými vraždami ale vzato umí bravurně a velice efektivně vytvořit a provozovat trh s drogami všeho druhu pro všechny bez rozdílu. Stačí mít peníze anebo Bitcoin, trochu znalostí a nenaletět podvodníkovi. Dark Web není jen zlým místem, jak jsme si popsali výše. Dark Web například velmi dobře slouží novinářům ze zemí, které jsou sevřeny pevnou totalitní rukou režimu a silnou cenzurou. Tito novináři pomocí Dark Webu anonymně publikují své články, své myšlenky a názory, které by za normálních okolností nebylo možné v těchto zemích publikovat. Dark Web slouží ke sdílení neomezeného a jakkoliv necenzurovaného množství informací. Taktéž velmi dobře slouží k ochraně soukromí. Dark Web má své ilegální ale i legální použití a je zde pro všechny bez výjimky. Záleží jen a pouze na nás, jak tento prostředek použijeme a pro co ho budeme využívat. Dark Web skýtá nekonečné možnosti o kterých ještě ani nevíme a taktéž nevíme, co vše nám může tato platforma nabídnout. Pokud to chceme zjistit, musíme mít v počítači stažený speciální

software. Nejznámějším je prohlížeč TOR, ale též není jediným. Těchto speciálních prohlížečů existuje velká řada, ale v této bakalářské práci se budeme zabývat pouze prohlížečem TOR³⁹.

5.2.5 Prohlížeč TOR

V květnu roku 2016 prohlásil na konferenci s názvem „Uvnitř Dark Webu“ v New Yorku Paul Syverson, že on vymyslel a vytvořil Dark Web. Je pravdou, že Syverson nelhal a stál za první webovou stránkou, která kdy spatřila světlo světa na Dark Webu. Takového Dark Webu, jak ho v této podobě známe dnes. Syverson působil v polovině devadesátých let dvacátého století v námořnictvu USA, kde vedl výzkum a tým lidí. Jeho tým přišel s myšlenkou a poté i s celým softwarem, který by jeho uživatelům poskytoval anonymní prohlížení webových stránek na internetu. Tomuto softwaru dali jméno The Onion Router, čili ve zkratce TOR. Proč Syverson a jeho tým zvolil takovýto název pro jejich software? Onion, je přeloženo z anglického jazyka cibule. A vývojářům TOR cibuli nápadně připomínal. Jejich software byl schopen přesně jako cibule zakrýt aktivitu do velkého množství vrstev. Cibuli není až tak snadné plně rozkrýt. Každý z nás, kdo surfuje na internetu prostřednictvím standardního prohlížeče, po sobě zanechává elektronickou stopu, kterou si mnohdy ani neuvědomuje. Tato aktivita se dá snadno zjistit a díky tomu lze i snadno určit, kde se konkrétní uživatel zrovna nachází. Z těchto důvodů vytvořil Syverson se svým týmem pro námořnictvo USA prostředek, jehož prostřednictvím by mohly vládní úřady mezi sebou anonymně komunikovat a takto nezanechávat za sebou žádné stopy. Jenže vláda USA se později rozhodla, že zdrojový kód TORu má být volně a zdarma a poskytla ho veřejnosti. Pokud by ke zveřejnění nedošlo, tak projekt TORu byl v době svého vytvoření v IT komunitě již známý, hojně diskutovaný, a někdo jiný by dříve nebo později jistě vytvořil jeho kopii. Síť TOR funguje na principu dobrovolníků, kteří poskytují své servery. Přes tyto servery, které se nazývají uzly, je možné se připojit do sítě. Přihlášením do sítě se Vám zobrazí seznam k těmto uzlům. Poté dojde k odfiltrování dat, která mohou sloužit k vystopování uživatele. Data, která zůstanou, se dále rozdělí na menší části a posléze opět zašifrují. Ty následně skáčou od jednoho uzlu k druhému, až naleznou ten poslední, přes který se připojí k požadovanému webu^{40,41}.

³⁹ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

⁴⁰ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

5.3 Temná tržiště

Koupit drogy online je mnohem jednodušší, než chodit po temných uličkách a shánět toho správného dealera. Na temném tržišti, nebo také z anglického jazyka „Dark Market,“ najdete spousty prodejců nabízející různé druhy zboží – drogy, opiáty, dětskou pornografii, kradené kreditní karty, padělané peníze či dokumenty. A v případě drog, kde si chtějí dealeři své zákazníky udržet, není riziko vadného zboží až tak velké, jak bychom jej mohli čekat. Na rozdíl od nabídek zbraní, nájemných vražd a hackerských útoků, které byly ve většině podvodné. Prodejcům může zákazník napsat hodnocení, případně se o svou zkušenost podělit na diskusním fóru. Vždy platí, že by se všichni měli držet daných pravidel temného tržiště. Na některých je zákaz prodeje dětské pornografie, nebo zbraní, jinde ale najdete spoustu drog roztrženyých do kategorií, dozvíte se i předpokládanou dobu doručení, či možnosti platby (Bitcoin, Monero atd.) Ta nejlepší temná tržiště trochu připomínají eBay, ale pro ilegální zboží. A jsou taktéž důvodem, proč většina lidí dnes Bitcoin považuje pouze za něco špatného. V době spuštění prvního tržiště (rok 2011) byl Bitcoin měnou, která neměla reálné využití. Nemohli jste si za něj koupit potraviny, elektroniku, ani auto. V té době vznikající temná tržiště řešila, jak udělat jejich obchody plně anonymní. Poslat peníze z vlastního bankovního účtu nepřipadalo v úvahu. Stejně tak dobírka. A tak objevili Bitcoin. Měnu, která fungovala plně v rámci internetu, byla přepočítatelná na fiat měnu a zdála se být anonymní. Ideální prostředek k nákupu ilegálního zboží. Nebo ne?⁴²

5.3.1 Silk Road

Autora prvního velkého tržiště na Darknetu, vystupujícího pod přezdívkou Dread Pirate Robert, usvědčil jeho vlastní deník. V roce 2010 si do něj totiž zapsal: „*začínám pracovat na projektu, který mi ležel v hlavě už déle než rok. Původně jsem ho nazýval Underground Brokers, ale nakonec padla volba na jméno Silk Road. Myšlenkou je vytvoření webové stránky, kde mohou lidé anonymně nakupovat cokoliv, bez zanechání jakékoliv stopy.*“⁴³ Vytvořit takovéto místo se mu doopravdy povedlo. Silk Road (česky hedvábná stezka) byl spuštěn někdy v první polovině roku 2011. Jeho začátky byly velmi skromné. Trvalo mu skoro dva měsíce, než dosáhlo počtu tisíc uživatelů a aktivních nabídek bylo jen pár desítek. Za jeho vzestupem stál raketový růst Bitcoinu.

⁴¹ CHOVANCULIAK, Róbert. *Pokrok bez povolení: Jak sdílená ekonomika, crowdfunding a kryptoměny změnilly svět*. 1. vyd. Praha: Grada, 2020. 272 s. ISBN 978-80-271-1755-0.

⁴² STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

⁴³ Zápis v deníku Rose Ulbrichta z roku 2010. In: STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. Str. 26. ISBN 978-80-271-2934-8.

Je pravděpodobné, že i následující růst této kryptoměny byl ovlivněn vzájemnou interakcí s tímto tržištěm. Silk Road byl opravdu prvním tržištěm na Dark Webu, kde se dalo reálné zboží směnit za Bitcoin. Od té doby se mezi lidmi traduje tvrzení, že Bitcoin je nástrojem zločinu. Ačkoliv tomu tak dnes již není, v této době měl Bitcoin opravdu nakročeno k tomu, aby byl pouze nástrojem zločinců⁴⁴.

Silk Road obsahoval oproti jiným (pozdějším) několik zajímavostí. Například něco, co se dá nazvat chytrou karanténou. Každý, kdo chtěl něco prodávat, musel složit jistinu ve výši několika stovek dolarů. Tato jistina mu byla vrácena ve chvíli, kdy prokázal, že své zboží odesílá a nemá negativní hodnocení. Tato strategie měla za cíl odradit podvodníky, kterých je Darknet plný. Zároveň zde fungoval systém úschovy peněz (který se mimochodem používá i na dnešních Dark Marketech), kdy mezi kupujícím a prodejcem byl prostředník, který prodejci uvolnil peníze až poté, co kupující potvrdil, že mu zboží dorazilo. Nikdo nechce přijít o své peníze. Na Silk Road šlo koupit skoro vše. Nemohli jste zde ale zakoupit ukradené kreditní karty, jedy, výbušniny anebo dětskou pornografii. Důvodem byl takzvaný etický kodex, kde bylo uvedeno, že můžete prodat cokoli, co přímo neohrožuje nebo neublíží ostatním lidem. Vystala ale otázka, zda prodávat zbraně. Ty přece slouží i k sebeobraně. Experiment se speciálním tržištěm nazvaným „The Armory,“ tedy zbrojnice, nebyl úspěšný. Dodnes se neví, zda byl některý obchod realizovaný. Za prvé o zbraně nebyl moc velký zájem, za druhé se to zde hemžilo podvodníky. Pokud prodáváte drogy, chcete, aby zákazníci nakupovali opakovaně. Případný podvod by byl velice rychle odhalen a prodejci by se ani nevyplatil. U zbraní to ale neplatí, tam stačí „prodat“ jednu zbraň za tisíce dolarů a obchodník může zmizet bez odeslání „zboží.“ Dread Pirate Roberts se v úvodním sdělení návštěvníkům snažil předat i pár základních rad jak nebýt okraden, nebo jak se správně na tržišti chovat. Osobně mě zaujal odstavec, ve kterém apeluje na zdravý rozum návštěvníka. Ve volném překladu do češtiny se tam píše: *„se svobodou přichází zodpovědnost, ... zde budete mít jednoduchý přístup k věcem, které vás mohou dostat do problémů se zákonem a které jsou vyloženě nebezpečné pro vaše*

⁴⁴ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

*zdraví. A jen proto, že můžete, ještě neznamena, že byste je měli zkoušet.*⁴⁵ Nabízí se tedy otázka, proč zakládal stránku, která toto vše umožňuje a zjednodušuje^{46,47}?

Jedno české přísloví říká, že boží mlýny melou pomalu, ale jistě. Totéž platilo i u Dread Pirate Robertse. Dne 3. října 2013 byl Ross Ulbrich, který se za touto přezdívkou skrýval, zadržen v knihovně v San Franciscu, kde byl připojen na místní veřejnou Wi-Fi síť a ze svého osobního počítače byl připojen ke svému temnému impériu. Agenti FBI ho sledovali a v okamžik jeho nepozornosti jej zadrželi. Po zajištění jeho notebooku zjistili, že Ross Ulbrich byl aktivně přihlášen v administrátorském módu účtu Dread Pirate Roberts na Silk Road, dále byl přihlášen do své bitcoinové peněženky a taktéž do veškerých komunikačních účtů. Agenti FBI taktéž zjistili, že měl Ulbrich ve svém počítači nezaheslovaný deník, v kterém byla kompromitující data o jeho osobě. Dodnes je spouště lidí divné, že by Ulbrich nestihl zavřít svůj počítač, nebo nestačil znehodnotit svá data. Ještě divnější je, že jeho počítač byl krátce po zabavení zničen, údajně omylem, jedním z policistů. Ještě ředším si ale jiný policista stihl zkopírovat data z jeho počítače na svůj přenosný harddisk. Zvláštní náhody. I přes to byl Ross Ulbrich odsouzen na dvě doživotí bez možnosti propuštění. Silk Road ještě nějakou dobu fungoval, spravoval jej Ulbrichtovo kamarád Gary Davis pod názvem Silk Road 2.0. I ten byl ale v brzké době zadržen a Silk Road přestalo existovat natrvalo⁴⁸.

5.3.2 AlphaBay

AlphaBay je považováno za jedno z nejlepších tržišť, které kdy vznikly. Mimo možnosti prodat a koupit zde ilegální zboží, převážně drogy, zde bylo i diskusní fórum. V jednu chvíli měla AlphaBay zaregistrováno přibližně 400000 uživatelů. Americká FBI se dlouho marně snažila přijít na to, kdo stránku provozuje, aby ji mohla „shodit.“ A jejího tvůrce poslat za mříže. Provedli dokonce několik nákupů a registrací. Při jedné registraci si povšimli, že pokud chtějí odpovědět na uvítací email, automaticky se vyplní email, který po dalším pátrání spojili s uživatelem sítě LinkedIn. Tento profil patřil Alexandru Cazesovi. Ten se narodil 19. října 1991 v malém městečku u kanadského

⁴⁵ Úvodní slovo Dread Pirate Roberts na Silk Road. Volně přeloženo. In: ORMSBY, Eileen. *Silk Road*. 1. vyd. Sydney: Pan Macmillian Australia, 2014. 352 p. ISBN 978-1742614090. (EN).

⁴⁶ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

⁴⁷ ORMSBY, Eileen. *Silk Road*. 1. vyd. Sydney: Pan Macmillian Australia, 2014. 352 p. ISBN 978-1742614090. (EN).

⁴⁸ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

Montrealu. Alex pocházel z chudších poměrů a z tohoto důvodu se ve svých sedmnácti letech rozhodl sám vydělávat a začal podnikat. V roce 2009 založil v Montrealu firmu EBX Technologies, která byla zaměřená na servis počítačů a prodej softwarových produktů. Alexova firma postupem času rostla, ale nikdo z jeho okolí nevěděl proč. Rodičům Alexe postačilo vysvětlení, že jejich syn začal dobře investovat do kryptoměn. Zajímavostí je, že v době kdy Alexovi bylo 22 let, tak cena jedné mince Bitcoinu během jednoho kalendářního roku vzrostla stonásobně. Ve skutečnosti Alexova firma EBX Technologies byla pouze zástěrkou pro praní špinavých peněz. Můžeme se ptát, jakým způsobem se mohl Alex Cazes dostat k takovému bohatství. V roce 2014 využil díry na trhu, která se nacházela v obchodu s nelegálním zbožím. Vytvořil na Darknetu tržiště s názvem AlphaBay, které mělo, dle něj, být tím nejdivočejším místem na internetu, kde se dá prodat a koupit de facto cokoli. Zakázán zde byl prodej dětské pornografie a nabídky nájemných vražd. Tržiště fungovalo téměř tři roky a to do roku 2017 a Cazes vystupující pod přezdívkou alpha02 vládnul celému internetovému podsvětí a užíval si legendárního bohatství drogových kmostrů bez toho, aby si umazal ruce. Díky Darknetu se tento byznys de facto otočil o 180 %. AlphaBay vyrostla do takových obřích rozměrů, že to sám Cazes psychicky neunesl. Žil výstředním životem, koupil si, co chtěl a koho chtěl. Včetně občanství několika dalších zemí, např. Thajska, kde se svou thajskou manželkou poklidně žil. A to do doby, než do brány jeho domu narazil automobil. Alex vyběhl ven, dokonce i s telefonem v ruce, aby řidičům vynadal. Bohužel pro něj to byla dobře připravená lest a on byl okamžitě zadržen policisty. Telefon mu byl odebrán a při následné domovní prohlídce byl nalezen počítač, který byl údajně bez hesla a otevřený a Cazes byl na něm přihlášený jako alpha02 ke svému administrátorskému účtu k AlphaBay. Tuto přezdívkou použil i mnohem dříve na veřejné chatovací stránce, kde dokonce původně uvedl i své jméno. Někteří lidé pochybují o tom, že by mohl být ten, kdo vybudoval AlphaBay tak neopatrný, a že by naservíroval policii důkazy o své vině takzvaně na stříbrném podnose. I přes to se má za prokázané, že za AlphaBay stojí právě Alexander Cazes. V červenci roku 2017 v době před uzavřením tržiště bylo v nabídce aktivních 396 000 nabídek nelegálního zboží, kdy ve většině případů se jednalo o drogy. Temné tržiště AlphaBay se stalo průkopníkem směny Bitcoinu za nelegální zboží a taktéž jejím největším odbytištěm. Spousta uživatelů si ale mylně myslela, že Bitcoin jsou zcela anonymní. Mnohé z nich to posléze usvědčilo a dostalo za mříže. Cazes se dostal k obrovskému bohatství. Vtip tkvěl v tom, že Cazes si z každého uskutečněného obchodu na jeho tržišti vzal poplatek za zprostředkování ve výši 2 - 4 % a tento poplatek byl v Bitcoinech. Dle zveřejněných

dokumentů orgánů činných v trestním řízení bylo uvedeno, že tržištěm AlphaBay mezi květnem 2015 až únorem 2017 proběhlo celkem čtyři miliony transakcí v hodnotě kolem 840 000 BTC. V době zatčení Cazes se šlo o částku kolem deseti miliard Kč. Z této částky se tak dá snadno zjistit, že Cazes si vydělal na poplatcích za provedené transakce zhruba 300 mil Kč. Tržiště AlphaBay bylo největším tržištěm, jaké kdy na Darknetu existovalo. Samozřejmě po uzavření AlphaBay nelegální obchod na Dark Webu nevyvymizel. Byla založena spousta jiných tržišť, jako například Sheep Marketplace, Hydra Market a další. Tyto nástupci kdysi slavného AlphaBay se vydali trochu jinou cestou, ale ve svém nitru zůstali tím, co ve skutečnosti nabízí. Místem, kde se dá koupit cokoli^{49,50}.

5.3.3 Hansa Market

Příběh AlphaBay hraje svou roli ještě v jednom příběhu temných tržišť. V takovém, který je dokonce čistě evropský. A inspirovali se jím i autoři populární série „Jak prodávat drogy online (rychle),“ z dílny Netflix. Řeč je o tržišti s názvem Hansa. Nebylo ani tak velké, ani tak proslulé. Tedy dokud americká FBI nezadržela Alexe Cazes a neuzavřela AlphaBay. Hansa poté zaznamenala stonásobný nárůst registrací. Lidé prostě potřebovali někde nakupovat a prodávat své zboží, převážně drogy. Nikdo z těchto lidí ale netušil zásadní věc. Administrátory tržiště Hansa zadržela německá policie asi tak týden předtím, než byl zadržen Alex Cazes. A zatímco AlphaBay byla ihned uzavřena, Hansa i nadále fungovala. Říkáte si, jak je to možné? Někdo to přeci provozovat musel, někdo musel opravovat chyby, spravovat zákaznickou podporu, komunikovat s moderátory chatovacích místností a jinak udržovat servery. Ano, někdo to provozovat musel. Nizozemská policie. Na případu Hansa totiž spolupracovaly úřady více zemí, hlavně Německo, Nizozemsko a americká FBI a DEA. Policie jej provozovala dalších 27 dní, dokud jej taktéž nevyřadili z provozu. Pomocí dalších malých podvůdků dostali za mříže drogové dealery a další prodejce ilegálního zboží. Ukázali tak, že ani na Darknetu se nedá jednoduše schovat⁵¹.

⁴⁹ STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

⁵⁰ RHYSIDER, Jack. *Operation Bayonet. Dark Net Diaries* [online]. 15. 10. 2018 [cit. 2022-03-03]. Dostupné z: <https://darknetdiaries.com/episode/24/>

⁵¹ RHYSIDER, Jack. *Operation Bayonet. Dark Net Diaries* [online]. 15. 10. 2018 [cit. 2022-03-03]. Dostupné z: <https://darknetdiaries.com/episode/24/>

5.3.4 Sheep Marketplace

Sheep Marketplace, česky ovčí trh, byl spuštěn v březnu roku 2013. Toto tržiště vzniklo v dobách největší slávy temného tržiště Silk Road. Po uzavření tržiště Silk Road vládními orgány hledali jeho uživatele náhradu a mnozí z nich ji našli právě v tomto tržišti. Tržiště svou architekturou a prostředím velmi připomínalo tržiště Silk Road a podobně i fungovalo. Sheep Marketplace měl ale jedno specifikum a to, že pokud jste chtěli obchodovat, museli jste si na svou peněženku, která byla součástí uživatelského účtu nahrát Bitcoin. Tyto Bitcoin de facto spravoval administrátor serveru a po uzavření obchodu mezi uživateli patřičné mince uvolnil. Bylo zjištěno, že v jeden moment měl administrátor tržiště k dispozici 96 tisíc Bitcoinů. V tehdejších cenách se jednalo o celkem dvě miliardy korun. Vše fungovalo bez problémů až do jednoho dne, když si zakladatel a správce tržiště usmyslel, že všechny uživatele okrade. V době této loupeže šlo celkem o jedno procento celosvětové zásoby Bitcoinu a jeho stopy, které za sebou nezakryl, vedly do České republiky. Velká část odcizených peněz ale byla majetkem drogových dealerů. Bezpečnostní složky z počátku přeshlapovaly takřka na místě, ale po uplynutí krátké doby zjistily, že všechny stopy vedou k osobě jistého Tomáše Jiříkovského. Je nutné podotknout, že orgánům činným v trestním řízení pomohl i fakt, že pana Jiříkovského hledala i spousta podvedených uživatelů jeho tržiště. Tak jako Alex Cazes udělal i Tomáš Jiříkovský spoustu chyb. Jednou z chyb, které se Jiříkovský dopustil, je ta, že si neuvědomil fakt, že Bitcoin je pouze pseudo-anonymní digitální měnou. Tudíž ho lze snadno sledovat. Zanedlouho se objevila bitcoinová adresa, která figurovala v transakcích za 467 000 BTC. Kupříkladu uživatel vystupující pod přezdívkou „sheepreloaded2“ na sociální síti Reddit stopoval 49 bitcoinových adres, které vlastnil Sheep Marketplace a nacházely se na nich peníze jeho uživatelů. Výsledkem bylo nalezení dalších adres a bitcoinových praček, které mají za úkol mixovat Bitcoin pocházející z ilegální činnosti a tím je opět zlegalizovat. Je to obdoba praní špinavých peněz, ale v digitálním světě kryptoměn. Jenže v těchto bitcoinových pračkách bylo najednou tolik mincí od jednoho uživatele, že se míchaly mezi sebou a tudíž je i po jejich vyprání šlo lehce identifikovat a sledovat. Jiříkovský se snažil vyprat své ukradené Bitcoin a tímto spálil miliony dolarů jen proto, aby je vypral. Bohužel pro něj pral vlastní Bitcoin mezi sebou. Další chybou bylo to, že Jiříkovský vlastnil na surface webu hosting Šnekweb, kde běžela jeho fanouškovská stránka sheepmarketplace.com. Tato stránka byla podobně naprogramována jako jeho nechvalně známá obdoba. Jeho fanouškovský web a i temné tržiště byly naprogramovány v PHP frameworku Nette a komentáře CSS byly v českém jazyce.

Další chybou bylo to, že se s tímto veřejně chlubil mezi vývojáři. Osudným mu bylo i to, že nedlouho po uzavření Sheep Marketplace přišlo na bankovní účet jeho manželky zhruba 900 tisíc korun z jedné kryptoměnové burzy. Poslat si na bankovní účet peníze z burzy není nijak zvláštní a není ani trestné. Banka se chtěla pouze ujistit, že peníze nepocházejí z nějakého ilegálního obchodu, či z trestné činnosti. A díky této kontrole zjistila, že podobným způsobem na tento bankovní účet přišlo už 8,7 miliónů korun. Tyto peníze Jiříkovský investoval do nemovitosti kdesi na Hodonínsku, kterou napsal na svého dědu. Dne 9. října 2017 byl Tomáš Jiříkovský odsouzen k trestu odnětí svobody v trvání devíti let nepodmíněně. K tomuto trestu přispěl i fakt, že Jiříkovský nelegálně držel několik zbraní. Zajímavostí celého příběhu je i to, že Jiříkovský nevydělal spoustu peněz na poplatcích uživatelů jeho tržiště. Bylo zjištěno, že poplatky mu vynesly něco kolem milionu korun. Původně se odhadovalo, že v době kdy Jiříkovský tržiště uzavřel, mohlo být v úschově až 96 tisíc BTC. Část z toho (5 400 BTC) mu jeho vlastní chybou ukradli dva Američané těsně před tím, než tržiště uzavřel. Přesný počet Bitcoinů které si Jiříkovský svým podvodem přisvojil ale, není známý. Soud nakonec operoval s variantou, že to bylo něco kolem jednoho tisíce Bitcoinů. To ale úplně nesedí. Kdyby ukradl pouze jeden tisíc Bitcoinů, jednalo by se v tehdejších cenách o asi 16 mil Kč. Jemu a jeho manželce ale byl zabaven majetek za 25 mil Kč, ačkoliv neměli žádné příjmy. Kde by se mohl nacházet zbytek všech Bitcoinů, které byly na Sheep Marketplace a kolik jich vůbec Jiříkovský ukradl, se asi nikdy nedozvíme. Jeho Sheep Marketplace je ale typickým příkladem tzv. exit scamu. Ironií je, že podvedl a okradl drogové dealery, kteří si sice nepůjdou stěžovat na policii, ani jej nebudou žalovat, na druhou stranu ale nezapomínají a Jiříkovský tak může být rád, že je alespoň prozatím „uklizený“ z jejich dosahu^{52,53}.

5.3.5 Hydra Market

Zmínku o Hydře jsem původně neplánoval uvádět, jelikož se jednalo o fungující tržiště. V době psaní mé bakalářské práce se ale na internetu objevila zpráva o tom, že Hydra byla odpojena a její administrátoři uvězněni. Jednalo se opět o společnou práci německých a amerických policistů. Hydra fungovala hlavně pro rusky mluvící trh a to od roku 2015 a probíhalo na ní dle odhadů až 80 % obchodů na Darknetu. Neprodávaly

⁵² STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

⁵³ NEVYHOŠTĚNÝ, Martin. *Internetová loupež za 800 milionů: Stopa vede k českému programátorovi* [online]. 2. 12. 2013 [cit. 2022-20-03]. Dostupné z: https://www.lidovky.cz/byznys/velka-internetova-loupez-za-800-milionu-stopa-vede-k-ceskemu-programatorovi.A131202_110252_firmy-trhy_mev

se na ní pouze drogy, ale i kreditní karty, falešné peníze a sloužila i k praní špinavých Bitcoinů. Nabízela i mnoho druhů falešných průkazů, od řidičáků po cestovní pasy, vše na přání kupujícího. Registrováno na ní bylo cca 17 milionů zákazníků a 19 tisíc prodejců. Měla i funkci k zatajování digitálních transakcí, samozřejmě za poplatek⁵⁴.

5.3.6 Temná tržiště v době pandemické

Začátek roku 2020 se stal začátkem globální pandemie nového a velmi nakažlivého virového onemocnění COVID-19, které má na svědomí mnoho obětí. Celá společnost se změnila ze dne na den společně i se svými prioritami a potřebami. Prodejci zdravotnických potřeb zaznamenali obrovský zájem o jejich produkty a to vedlo k nezřízenému zdražování a nedostatku. Problém byl v centralizaci výroby soustředěných převážně v zemích Asie a tento fakt vedl ke značným logistickým problémům. V tomto období počínajících restrikcí a omezeních se temná tržiště na Dark Webu začala přeorientoávat na nově vzniklou celosvětovou poptávku. Vše začalo v době, kdy v Itálii začal strmě stoupat počet nakažených onemocněním COVID-19 a Italská vláda uvalila na své občany karanténu. Smyslem této karantény byl přísný zákaz pohybovat se volně mimo domov a scházet se s jinými lidmi. Mnoho lidí zůstalo ve svých domovech bez jakéhokoliv kontaktu se svým okolím. Prodejci na temných tržištích se velmi rychle na novou situaci adaptovali a začali nabízet různé ochranné pomůcky (roušky, masky, latexové rukavice), nebo zázračné léky proti onemocnění COVID-19 (Chloroquine), anebo antidepresiva (Xanax). Prodejci začali lákat na výhodné slevy a akce. Zboží označené „COVID-19“ a „CORONA“ se na temných tržištích stalo de facto světovou značkou. Cena zboží byla plně navázaná i na množství zboží daného prodejce. Když se jim začali tenčit zásoby, tak i cena začala stoupat do hodnot velmi převyšujících cenu zboží před vládními opatřeními. Prodejci navýšení cen často odůvodňovali tím, že k navýšení ceny zboží došlo z důvodu speciálních hygienických opatření, aby byl produkt plně bezzávadný. I tento fakt prodejci využili jako marketingový tah a začali se mezi sebou předhánět, kdo měl lepší hygienická opatření a jak byl produkt před odesláním ošetřen. Též strmě stoupal i zájem o OPL, kdy mnohdy byla cena navýšena i o 70 %. Prodejci na temných tržištích sice vydělávali nemalé peníze, ale velký problém měli s distribucí zboží zákazníkům. Nebylo

⁵⁴ THE U. S. DEPARTMENT OF JUSTICE. *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace: Russian Resident Indicted on Conspiracy Charges Related to Operating Hydra Market* [online]. 5. 4. 2022 [cit. 2022-04-06]. Dostupné z: <https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace>

výjimkou, že zákazník čekal na svou zásilku klidně i dva měsíce. Proto nastoupili jejich subdodavatelé operující na diskusních fórech a blocích, kteří vytvořili jakousi interaktivní celosvětovou mapu zvanou „Corona Timeline“. V této „mapě“ bylo v reálném čase patrné, jaká země má jaké opatření a jaké jsou podmínky pro vstup a výstup do ní a jaká je vytíženost. Tyto informace velmi pomohly jak prodejcům, tak i subdodavatelům k pašování produktů, ale i zákazníkům, kteří obdrželi informace o tom, kdy mohou dostat své zboží. Z důvodu vysoké poptávky netrvalo dlouho a prodejci začali mít problémy se svými skladovými zásobami a jeho doplněním. Spousta OPL byla nedostupná z důvodu nedostatku chemikálií určených k jejich výrobě a taktéž měla delší dodací lhůtu. Odpovědí na tyto problémy bylo zdražení prekurzorů a samotných finálních produktů OPL a navýšení rozmanitosti produktů v rámci ochranných potřeb, léků a testů na onemocnění COVID-19. Většinou se jednalo o zboží odcizené z nemocničních skladů a zásilek určených pro zdravotnická zařízení, které byly určeny pro boj s onemocněním COVID-19. Tomuto segmentu napomohlo i to, že vlády tyto zboží zcela zakázaly k volnému prodeji a temná tržiště díky tomuto doslova zažívala žně. Perličkou je, že nejčastěji prodáváný lék s obsahem látky chloroquin se na eshopech Clear Webu před těmito opatřeními prodával za částku kolem 180,- Kč za jedno balení. Po uvedení restrikcí v platnost se cena jednoho balení zvedla na částku kolem 1360,- Kč. Na tento lék bylo poté uvaleno i obchodní embargo z důvodu, že se tento lék primárně využívá k léčbě malárie a v afrických zemích ho byl velký nedostatek. Proto byl prodej přeměrován na temná tržiště. Během pandemické situace došlo na temných tržištích k regulacím. Před lety došlo k regulaci nabídky dětské pornografie, tak posléze došlo i k omezení nabídky fentanylu a hlavně léčiv určených pro boj s onemocněním COVID-19, které se nazývají „Covid Cure.“ Obchodníci s těmito léčivy se postupně přeorientovali pouze k prodeji ochranných pomůcek a testovacích sad. Zajímavé je, že prodej OPL, které mají z dlouhodobého hlediska prokazatelně devastující účinek na lidský organismus, správcům temných tržišť nevadí. Technicky vzato se jedná o tzv. psychologickou hru a hraní si na kladě se v rámci společenských norem. Taktéž je lepší, když bezpečnostní složky vyšetřují pouze určité prodejce za jejich prohřešky, než by se zaměřili na celé tržiště a rozkryly jeho ilegální byznys. Zakoupit kromě nám známých OPL lze i zakoupit tzv. nové psychoaktivní substance (dále jen „NPS“), které mají podobné psychotropní vlastnosti a lze je zakoupit nejen na temných tržištích Darknetu. NPS jsou oproti OPL daleko levnější, ba i v některých zemích jsou legální. Mají pouze jednu nevýhodu a to, že při nesprávném dávkování (dokonce i po první aplikaci) mohou mít až smrtelné účinky pro konzumenta.

Doba se vyvíjí a společnost se vrací pomalu do normálu. To stejné platí i pro temná tržiště. Pandemie COVID-19 a celkové problémy s dodávkou OPL byla pro mnoho prodejců likvidační. Celá tato situace spíše globální trh s OPL stimulovala, než aby mu uškodila a poukázala i na to, že prodejci a temná tržiště obecně dokázala velmi pružně reagovat na nově vzniklou poptávku⁵⁵.

5.4 Odhalování a vyšetřování kybernetické kriminality

5.4.1 Pachatel kybernetické kriminality a jeho motiv

V této problematice je důležité si nejprve uvést několik pojmů, které jsou taxativně obsaženy v zákoně č. 40/2009 Sb., trestní zákoník, které nám pomohou pochopit tento fenomén. Definice pachatele trestného činu je uvedena v § 22 odst. 1 zákona č. 40/2009 Sb., trestního zákoníku, kde je konkrétně uvedeno že „*pachatelem trestného činu je, kdo svým jednáním naplnil znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná*“⁵⁶. Dále lze v této souvislosti uvést i § 22 odst. 2 zákona č. 40/2009 Sb., trestního zákoníku, který hovoří o tom, že „*pachatelem trestného činu je i ten, kdo k provedení činu užil jiné osoby, která není trestně odpovědná pro nedostatek věku, ...*“⁵⁷ V této problematice je nutné si zmínit i § 24 odst. 1 zákona č. 40/2009 Sb., trestního zákoníku, kde se hovoří o organizátorovi, návodci a pomocníku trestného činu. Taktéž je nutné si v této souvislosti uvést § 25 téhož zákona, který upravuje věk pachatele trestného činu a § 26 téhož zákona, který upravuje pojem nepřičetnosti. Z těchto zákonných norem lze usoudit, že způsoby a motivace páčání trestné činnosti budou rozdílné s přihlédnutím k věku pachatele, jeho osobnostní vyspělosti, ale i možné příležitosti k provedení trestného činu, či okolností důležitých k jeho spáchání, které reflektují zejména technické znalosti a získané dispozice pachatele. Kriminalita se v průběhu jejího vývoje prakticky nezměnila. Můžeme konstatovat, že vražda zůstane vraždou, i když k tomuto pachatel užije namísto neolitického sekeromlatu například současnou pistoli. Záměr a výsledek zůstává neměnný. Jen způsob provedení je specifický pro danou dobu spáchání trestné činnosti. Moderní technologie posledních let přinesly do našich životů i mnoho nových druhů trestné činnosti. Internet, servery a počítače obsahují databáze, které jsou plné nejrůznějších informací. Pokud pachatel

⁵⁵ OMASTA, Adam. Adaptace virtuálních tržišť s návykovými látkami na vládní opatření COVID-19. *Drugs & forensics bulletin*. 2020, roč. XXVI, čís. 3. ISSN 1211-8834.

⁵⁶ ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. §22, odst. 1. In: Sbíрка zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

⁵⁷ ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. §24, odst. 2 In: Sbíрка zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

trestné činnosti má jejich znalost, anebo možnost s nimi nějakým způsobem manipulovat, tak tyto získané poznatky mu mohou poskytnout nemalou výhodu, kterou může využít ve svůj prospěch^{58,59}.

Pachatel kybernetické kriminality k páčání trestné činnosti užívá svého intelektu a to velmi chytrým způsobem. Motiv pachatele je velmi důležitý k jeho natipování orgánem činným v trestním řízení tak, aby se vymežil okruh podezřelých. Například toto lze provést u poškozené firmy, či organizace, kde by byl možný okruh tipovaných osob v řadách zaměstnanců, ať těch současných, či již bývalých. Pokud orgán činný v trestním řízení zjistí odpověď na exemplární otázku, „kdo má ze spáchaného trestného činu prospěch?“ která vede k jejímu pachateli, tak následuje otázka dokazování. Dokazování motivu trestného činu v kybernetické kriminalitě, dále jeho trestní klasifikace a stupeň společenské škodlivosti má velmi značný význam při řešení a následně určení výše trestu. Existují i některé případy, kdy trestný čin tohoto charakteru nebylo bezpečně možné vyjádřit v penězích. Typické motivy kybernetické kriminality v kriminalistické praxi jsou zejména uvedeny nejen samostatně, ale i v různých kombinacích. Typickým příkladem si lze uvést zjištěný motiv v kombinaci s touhou dokázat si svou intelektuální převahu, či touha po získání moci v kombinaci s politickým vlivem. Kombinací je nespočet a ten je závazný na motiv pachatele. Motiv zjištěnosti je v tomto fenoménu zcela dominantním a to například z důvodu, že touto formou kriminality lze generovat ohromné zisky během krátkého časového úseku oproti klasické kriminalitě. Pachatele zcela jistě a velmi motivuje touha po bezpracném zisku a osobního obohacení. Sledovat ale můžeme i různé kombinace. Lze si uvést pachatele, který primárně touží po pocitu převahy nad PČR, veřejností, či zaměstnavatelem, ale který sekundárně touží po neodhalitelnosti, či chce pouze dokázat svou intelektuální dominanci. Též si lze uvést možný motiv pachatele, který je jeho krycím motivem pro zcela jiný aspekt trestné činnosti. Tento příklad se může týkat daňových úniků, či zpronevěry. Pokud se podíváme do historie, tak můžeme ve velkých případech počítačových podvodů spatřit společný psychologický motiv jejich pachatelů. Zejména se jedná o pocit nedocení zaměstnavatelem anebo společností. Tento motiv je často

⁵⁸ ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: Sbirka zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

⁵⁹ SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozš. a aktual. vyd. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

doprovázený pocitem nenáklonnosti druhého pohlaví k osobě pachatele. Nezřídka bývá psychologický profil pachatele doprovázen neurózou na bázi sociální fobie^{60,61}.

Tyto pachatele si lze dále rozdělit do šesti kategorií. Zprv si lze uvést zaměstnance poškozené organizace, či firmy, anebo zaměstnanci jejich dodavatelů a subdodavatelů. Ve druhé kategorii si lze uvést pachatele, kteří jsou takzvanými hackery. Tito pachatelé mají ve většině případů anarchistické rysy, kdy tomuto odpovídají i jejich trestné činy. Mezi jejich aktivity si lze uvést DoS/DDoS útoky malého i velkého rozsahu, průniky do vládních počítačových sítí a jejich vyřazení, odhalování utajovaných informací, anebo spamming pomocí trojských koní a botů, či phishing. Taktéž si ještě můžeme uvést porušování autorských práv, které je ve společnosti označované pod pojmem počítačové pirátství. Třetí kategorií jsou organizované skupiny pachatelů, kteří využívají svých IT know-how. Pod touto kybernetickou kriminalitou si lze představit praní špinavých peněz, výrobu a distribuci padělků různého softwaru a platebních prostředků, zejména se jedná o platební karty, či výrobu a distribuci pornografie. Čtvrtou skupinou jsou profesionálové, kteří se živí hackerskou činností, která je uvedena u druhé skupiny a částečně i u třetí skupiny pachatelů. Tito profesionální hackeři ve většině případů stojí za útoky, které směřují na různé části infrastruktury jimi napadeného státu. Pátá kategorie je vyčleněná pro pachatele kyberterorismu. Pod tímto fenoménem si lze představit promyšlený, politicky motivovaný a koordinovaný útok organizovaných skupin, nebo jednotlivců, který je přímo zaměřen na informační sítě, počítačové programy a data. Poslední šestou kategorií jsou pachatelé, kteří svým věkem nedovršili osmnácti let. Zejména se jedná o osoby mladistvé. Mladiství mnohdy nepřemýšlejí o svém protiprávním jednání a příliš si nedělají starost o jeho následcích. Tyto osoby ve většině případů ani netuší, že konají nějakou protiprávní věc. Pokud je orgán Policie odhalí, tak se snaží hájit hloupě. Pachatelé si většinou myslí, že nedojde k odhalení jejich jednání. Pakliže dojde k jejich odhalení, tak nekladou orgánu policie přímý odpor. Tito pachatelé se převážně hají tvrzeními, že nevěděli o tom, že jednali protiprávně, protože ostatní to dělají také. Nebo že k této věci došlo omylem, či se stali obětí svého distributora^{62,63}.

⁶⁰ SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozš. a aktual. vyd. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

⁶¹ POŽÁR, Josef. *Informační bezpečnost*. 1. vyd. Plzeň: Aleš Čeněk, 2005. 311 s. ISBN 80-86898-38-5.

⁶² KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metody vyšetřování*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2021. 417 s. ISBN 978-80-7380-859-4.

5.4.2 Kriminální stopy

Během vyšetřování trestných činů a přestupků v rámci kybernetické kriminality se lze setkat s celou řadou kriminálních stop. Každý případ je specifický a od tohoto se odvíjí i celkové množství zjištěných a zajištěných stop, jejich různorodost i rozmístění. V kybernetické kriminalitě se lze setkat se stopami materiálními nebo paměťovými. Uvedeme si pouze pro příklad několik z nich, kdy tyto příklady pochopitelně nejsou taxativní. Setkat se můžeme se stopami daktyloskopickými, které se mohou nacházet na počítačovém hardwaru, či s mechanoskopickými, které můžeme nalézt například na přerušených vodičích. V rámci této problematiky můžeme vzít v úvahu, že se můžeme setkat i s kriminálními stopami fonoskopickými, kdy pachatel trestné činnosti svůj počítač užil jako hlasový záznamník. Tyto kriminální stopy, které jsme si vyjmenovali výše, ale nejsou pro kybernetickou kriminalitu zcela typické. U digitálních stop se nachází jedna zvláštnost a to, že každé zařízení, které operuje s daty, tak za touto činností zanechává záznamy. Tudíž digitální stopa je jakýmsi záznamem nehmotné informace, která je zakódovaná do jejího digitálního formátu. Tyto digitální stopy se vyskytují jak na veškerých záznamových zařízeních, které operují s daty, tak i kdekoli v kyberprostoru. Bohužel pro OČTŘ tyto digitální stopy mají několik negativních vlastností, které svou charakteristickou znesnadňují vyšetřování. Za zmínku si můžeme uvést několik vlastností digitálních stop a to nehmotnost digitálních stop, její latentnost a nízkou životnost, dále manipulovatelnost s časem v počítačových systémech, způsob uchování záznamů, komplexnost prostředí a například velký geografický rozsah prostoru, kde se tyto digitální stopy vyskytují⁶⁴.

5.4.3 Počítačové stopy a jejich kategorie

Charakteristické kriminální stopy pro tuto problematiku jsou takzvané počítačové stopy. Jedná se o stopy, které jsou datovou informací, nebo změnou takovéto informace, nacházející se na materiálním nosiči. Tato data, nebo změny dat, mají důkazní, ale i kriminálně-taktickou hodnotu. Musí být ale prostřednictvím aktuálních metod, prostředků, postupů a operací zjistitelné a využitelné, jinak tuto hodnotu ztrácí. V kybernetické kriminalitě rozdělujeme kriminální počítačové stopy zejména na tři kategorie. První kategorie jsou stopy, které se vyskytují na

⁶³ SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozš. a aktual. vyd. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

⁶⁴ KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metody vyšetřování*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2021. 417 s. ISBN 978-80-7380-859-4.

výpočetní technice, kdy do tohoto lze zařadit též neoprávněné zásahy. Druhou kategorií jsou stopy, které se nacházejí na záznamových zařízeních. Taktéž sem patří i data, která jsou uložena na těchto zařízeních. Dle trestního zákona se jedná o nosiče informací. Jako příklad si můžeme zmínit pevné disky a to externí, tak i pevné v PC, dále datové nosiče a to CD, DVD, Blue-ray disky, či paměťové karty SD, anebo Memory Stick. Třetí kategorií jsou stopy na kancelářské a organizační technice, která uživateli umožňuje zaznamenání a následné uchování dat. Sem si můžeme pro příklad uvést chytré mobilní telefony, záznamníky, faxy, diktafony, zabezpečovací kamerové systémy, ale i skenery a tiskárny. V posledních dvou příkladech se můžeme setkat s tím, že tyto přístroje ve svých pamětech mohou obsahovat data, která mohou poskytnout orgánu činného v trestním řízení důležitý poznatek pro vyšetřování. K tomuto si můžeme ještě uvést, že některé barevné tiskárny umí implementovat do vytištěného dokumentu informace, které následně mohou tiskárnu bezpečně identifikovat⁶⁵. Jeremy Martin ve své knize upozorňuje na důležitost počítačových stop, nacházející se zejména v tzv. živé paměti počítače. Ta totiž mohou být v případě vypnutí počítače nenávratně ztracena. Jedná se zejména o přístupy k účtům, nebo probíhající internetová komunikace. I proto policisté v kapitole o Silk Road i AlphaBay vymýšleli způsoby, jak zadržet pachatele bez toho aniž by dostali možnost zavřít svůj počítač. I počítač, který byl „vymazaný,“ může přinést cenná data, zejména ta, která se již zapsala na pevný disk. Ty se totiž reálně vymažou až přepisem, což může trvat až rok. Důležitou počítačovou stopou mohou být i tzv. META data, což jsou data, která známe zejména z fotografií z mobilních telefonů, a obsahují např. GPS lokace, identifikace zařízení které fotografii pořídilo nebo informace o tom, že fotka byla jakkoliv upravena⁶⁶.

5.4.4 Účetní stopy

Účetní stopy jsou další typickou skupinou kriminalistických stop problematiky kybernetické kriminality. Tyto stopy se mohou nacházet, tak jako stopy počítačové v údajích prvotních dokladů, uzávěrkách anebo v různých účetních výkazech. Data se mohou objevovat jak v listinné formě, tak i ve formě digitální. Živná půda kybernetické

⁶⁵ KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metody vyšetřování*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2021. 417 s. ISBN 978-80-7380-859-4.

⁶⁶ MARTIN, Jeremy. *The Beginner's Guide to the Internet Underground*. 2. vyd. Elektronická kniha. Information Warfare Center LLC, 2014. 42 s. Bez ISBN. Dostupné z: https://books.google.cz/books?id=3b4iAQAAQBAJ&dq=the+beginners+guide+to+the+internet+underground+2nd+ed&hl=cs&source=gbs_navlinks_sground%20nd%20ed&f=false

kriminality umožnila vzniknout celé řadě písemností, která by mohla být v této souvislosti použita k páchání trestné činnosti⁶⁷.

5.4.5 Paměťové stopy

Pod pojmem paměťová stopa si můžeme představit informaci, kterou získala určitá osoba svými smysly a která je následně schopna tyto informace aplikovat do výpovědi. Je nutno podotknout, že tyto stopy lze užít jak pro svůj důkazní charakter, tak i pro svoji vlastnost informativního charakteru, který může OČTŘ posloužit svou hodnotou při dalším vyšetřování. Pro příklad si můžeme uvést, že paměťovou stopou mohou být informace, které se týkají způsobu přípravy trestného činu, nebo informace vedoucí k popisu, zjištění a následnému ztotožnění pachatele, způsobu chování a jednání pachatele před spácháním trestného činu, v průběhu páchání trestné činnosti a v době po jeho spáchání, či informace týkající se páchání a utajování kybernetické kriminality. Pro důkazní sílu, životnost těchto stop, určení v jakém pořadí a rozsahu budou vyhledávány, zajišťovány a následně zkoumány platí obecná kriminalisticko-technická doporučení, která tento postup upravují. Obecným pravidlem u počítačových stop platí to, že je nutné dbát na možnost její okamžité likvidace pachatelem, či možného zahlazení stop pachatelem anebo jeho spolupachateli⁶⁸.

5.4.6 Odhalování kybernetické kriminality

V této podkapitole si přiblížíme několik pojmů. Zejména si zde uvedeme a popíšeme postup OČTŘ před zahájením trestního stíhání, Dále se budeme zabývat samotným vyšetřováním a dokazováním. Nejprve bych chtěl zmínit významný prvek vyšetřovacích situací týkajících se kybernetické kriminality a to, že vyšetřování samotné mnohdy může kolidovat se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tento zákon například definuje a ukládá povinnost mlčenlivosti a taktéž upravuje utajované informace⁶⁹.

⁶⁷ KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metody vyšetřování*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2021. 417 s. ISBN 978-80-7380-859-4.

⁶⁸ KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metody vyšetřování*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2021. 417 s. ISBN 978-80-7380-859-4.

⁶⁹ KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metody vyšetřování*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2021. 417 s. ISBN 978-80-7380-859-4.

Postup OČTŘ před zahájením trestního řízení se nazývá prověřování. Zákon č. 141/1961 Sb., trestní řád, upravuje v rámci § 159 skončení prověřování, kdy je uvedeno v odst. 1), že: „*policejní orgán je povinen prověřit skutečnosti nasvědčující k tomu, že byl spáchán trestný čin.*“⁷⁰ V rámci prověřování policejní orgán zajišťuje potřebné podklady a stopy, které vedou k objasnění skutečností, že byl spáchán trestný čin a získané poznatky by vedly k ustanovení pachatele spáchaného trestného činu. Během prověřování může nastat i situace, že vzhledem ke zjištěným okolnostem ke skutku nedošlo vůbec, anebo se nejedná o trestný čin, ale o přestupkové jednání. V rámci prověřování může být policejním orgánem zjištěno, že skutek, který je prověřován, splňuje znaky a skutkovou podstatu trestného činu a že jej například spáchala konkrétní osoba. Pro policejní orgán v rámci úkonů prověřování kybernetické kriminality jsou velmi důležité odborná vyjádření a znalecké posudky, ale taktéž i ohledání věci a též i ohledání místa činu. V rámci hospodářské kriminality na úseky kybernetické kriminality je možné v rámci prověřování též provádět odposlechy a záznamy telekomunikačního provozu, ale i sledování osob a věcí. Při tomto sledování lze pořizovat zvukové, obrazové záznamy za použití příslušných technických prostředků, jakými mohou být různé kamery, mobilní telefony, záznamníky, aj. Během těchto výše uvedených činností policejní orgán provádí sběr informací, které se vztahují k trestnému činu, místu jeho spáchání a k osobám podezřelým ze spáchání trestného činu. Policejní orgán vyhodnocuje získané upotřebitelné informace buďto sám anebo využije k tomuto odborníky, kteří OČTŘ poskytnou svá odborná vyjádření, či své znalecké posudky. V závažných případech a v skutkově složitých věcech může policejní orgán a státní zástupce využít dle § 157 odst. 3) zk. č. 141/1961 Sb., trestního řádu, odborné pomoci konzultanta, který je vázán mlčenlivostí. Odborný konzultant má znalosti ze speciálního oboru, který je zapotřebí ke správné orientaci v problému a k následnému dokazování. Pokud odborný konzultant v rámci své činnosti poukáže, že je potřeba objasnit nějakou důležitou skutečnost pro potřeby trestního řízení, tak OČTŘ si vyžádá odborné vyjádření a pokud je spatřována jistá složitost posuzované otázky, tak je opatřením přibrán znalec. Samotná činnost odborného konzultanta a také výsledek jeho činnosti nemůže sloužit v trestním řízení jako důkaz. Smyslem konzultanta je OČTŘ poskytnout pomoc v závažných a složitých skutkových věcech. Odborný konzultant by měl být

⁷⁰ ČESKO. Zákon č. 141/1961 Sb., zákon o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: Sbirka zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/1961-141>

náležitě orientován v problematice a taktéž by se měl orientovat ve skutkových okolnostech a měl by následné dokazování zaměřit tím správným směrem⁷¹.

Úsek od zahájení trestního stíhání po podání obžaloby, či jiným mimosoudních způsobů vyřízení se nazývá vyšetřování. Pokud jsou během prověřování dle § 158 zákona. č. 141/1961 Sb., trestního řádu, zjištěny odůvodněné skutečnosti, které nasvědčují tomu, že byl spáchán trestný čin a taktéž je řádně a dostatečně odůvodněn závěr, že jej spáchala určitá osoba, tak policejní orgán rozhodne o zahájení trestního stíhání této osoby, kdy tato osoba se stává obviněným. Dle trestního řádu je oprávněn policejní orgán opatřovat a provádět důkazy před samotným zahájením trestního stíhání v rámci prověřování. Zejména si můžeme uvést dle § 105 zk. č. 141/1961 Sb., trestního řádu, odborná vyjádření a znalecké posudky. Toto oprávnění je zejména důležité v rámci kybernetické kriminality z důvodu problému časového odstupu od okamžiku spáchání trestného činu, kdy toto je pro OČTŘ nežádoucím jevem. Tyto posudky mohou mít ve stádiu prověřování charakter neodkladného úkonu. Je nutno podotknout, že i když platí princip rovnosti stran v trestním řízení, tak bývá obvyklé, že shromáždění důkazů bývá provázeno delším časovým odstupem. Většinou bývají důkazy shromážděné až ve fázi prostudování spisu dle § 166 zk. č. 141/1961 Sb., trestního řádu. Z těchto důvodů lze od počátku užít postup dle § 65 odst. 1) zk. č. 141/1961 Sb., trestního řádu. V tomto ustanovení je upraven postup, kdy se může obvinění poškozený, osoba zúčastněná a taktéž i jejich obhájci, či zmocněnci nahlížet do spisu. Výjimku pak tvoří protokol o hlasování a osobních údajích svědka, do kterého výše jmenovaní nahlížet nemohou. Taktéž si nemohou pořídit na vlastní náklady kopie spisů a jejich částí, či si pořizovat obrazové záznamy a zápisky, či jakékoliv jiné poznámky. Státní zástupce a policejní orgán mohou v přípravném řízení využít dle § 65 odst. 2) zákona č. 141/1961 Sb., trestního řádu oprávnění odmítnout poskytnout spisový materiál k nahlédnutí ze závažných důvodů a tímto jim toto oprávnění odepřít^{72,73}.

Dokazování je nejdůležitější činností OČTŘ vedle rozhodování. Samotné dokazování má svůj význam v tom, že OČTŘ si mohou a též i musí zajistit skutkový podklad pro své následné rozhodnutí, či pro jiný postup ve věci. V rámci posuzování

⁷¹ SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozš. a aktual. vyd. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

⁷² SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozš. a aktual. vyd. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

⁷³ ČESKO. Zákon č. 141/1961 Sb., zákon o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: Sbíрка zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/1961-141>

v trestním řízení bývají mnohdy přítomné takové události vnějšího světa, které mohou mít charakter významné skutečnosti nebo skutku, kdy tyto se staly v minulosti a OČTŘ, který o nich musí rozhodovat, nebyl tomuto přítomen a nemohl tyto skutečnosti přímo pozorovat. OČTŘ se s těmito posuzovanými skutečnostmi může seznámit pouze nepřímo a to způsobem, že průběh skutečností rekonstruuje pomocí zjištěných důkazů. Dalším významem dokazování je i to, že všem stranám v trestním řízení umožňuje aktivní účast a též jim umožňuje i uplatnění jejich práv. Dokazování má za úkol zjistit skutkovou podstatu věci. Tento postup je upraven v § 2 odst. 5) zk. č. 141/1961 Sb., trestního řádu. OČTŘ si dokazováním zjišťuje a opatřuje hodnověrné informace významné pro potřeby trestního řízení, díky nimž pomocí logického postupu ve věci odvozuje úsudek o předmětu dokazování. Důvodem je, aby bylo jejich rozhodování rádě podložené, odůvodněné a následně i přezkoumatelné^{74,75}.

6 Drogová kriminalita v České republice

Návykovými látkami se rozumí dle § 2 odst. 1) písm. a) zákona č. 167/1998 Sb., o návykových látkách a o změně některých dalších zákonů, omamné a psychotropní látky přírodního či syntetického charakteru, které jsou svým účinky na člověka psychoaktivní. Tyto látky jsou současně uvedeny v příloze č. 1 až 7 nařízení vlády o seznamu látek. Výjimku tvoří látky extraktu rostliny konopí a její tinktury, kdy ze skupiny tetrahydrokanabinolů obsahují maximálně 1 % těchto látek. Jedná se zejména o masti, šampony a jiné drogistické potřeby⁷⁶.

6.1 Drogy na internetu i mimo něj

Problematika drog je velmi široké téma, ale vzhledem k tomu, že panuje konsensus o tom, že na Dark Webu se nachází v největší míře právě drogy a pornografie, chtěl bych tomuto tématu alespoň pár řádků věnovat. Darknet totiž nabídl všem lidem, kteří alespoň trochu umí s počítačem, zajímavý nástroj k experimentování. Už to není o tom, že mladí lidé si musí nejprve najít dodavatele, ideálně ještě přes nějakého kamaráda a vybrat si z okleštěné nabídky drog, kterou tento dealer nabízí. Stačí jim pár kliknutí k tomu, aby se dostali na jakýkoli Dark Market a vybrali si z široké nabídky. S tím

⁷⁴ SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozš. a aktual. vyd. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

⁷⁵ ČESKO. Zákon č. 141/1961 Sb., zákon o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: Sběrka zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/1961-141>

⁷⁶ ČESKO. Zákon č. 167/1998 Sb., zákon o návykových látkách a o změně některých dalších zákonů. In: Sběrka zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/1998-167>

souvisí i zvýšený výskyt tzv. designových drog. Jedná se o látky, které se zatím nevyskytly na seznamech zakázaných látek, ale způsobují pocity a stavy podobné těm, které na těchto seznamech jsou. Bohužel jejich užívání je často doprovázeno nežádoucími účinky, jako tomu bylo např. v případě nové drogy „Krokodýl.“ Dalším problémem bývá snížená možnost detekce běžnými způsoby, které Policie ČR používá, např. známý orientační tester na drogy DrugWipe. Stejným problémem se zabývají i pracovníci laboratoří, kteří se zaměřují na toxikologická vyšetření. Zejména u akutních otrav drogami totiž není zprvu jasné, co za látku si postižený vzal. A přístupnost drog a látek z celého světa tomu zrovna dvakrát nepomáhá. Proto je dobré znát alespoň základní příznaky takovýchto otrav^{77,78}.

6.2 Základní dělení drog

Základní dělení drog najdeme v zákoně č. 167/1998 Sb., zákon o návykových látkách. Ten rozděluje návykové látky do dvou skupin a to na omamné látky a psychotropní látky, které dále dělí. Hromady tak můžeme mluvit o omamných a psychotropních látkách (dále OPL). Nejužívanější rozdělení je na látky stimulující centrální nervový systém (dále CNS), tlumící CNS a ovlivňující vnímání. Další používané rozdělení je dle rychlosti vzniku závislosti na měkké, lehké (např. marihuana) a tvrdé, těžké (kam patří např. heroin, nebo crack)^{79,80}.

6.2.1 Látky stimulující centrální nervový systém

Kapitola je nazvaná látky, protože se sem neřadí pouze drogy, tak jak je známe z definic, ale jedná se i o legální látky, které jsou společensky akceptované, například nikotin, nebo kofein. Pokud bychom se měli bavit o drogách jako takových, zařadili bychom sem určitě kokain, amfetamin a metamfetamin. Hlavním příznakem je neklid, nekontrolovatelné pohyby, obecně roztěkanost, ale mohou se vyskytnout i křeče a stavy bezvědomí. Často je přítomno špendlíčkovité stažení zornic⁸¹.

⁷⁷ BALÍKOVÁ, Marie. *Forezní a klinická toxikologie: laboratorní toxikologická vyšetření*. 2. dopl. vyd. Praha: Galén, 2017. 127 s. ISBN 978-80-7492-304-3.

⁷⁸ HESS, Ladislav a Radim UZEL. *Sex, drogy a násilí*. 1. vyd. Praha: Mladá fronta, 2018. 314 s. ISBN 978-80-204-4941-2.

⁷⁹ KVAPILOVÁ, Helena a Michal DOGOŠI. *Soudní lékařství pro právníky a policisty*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2007. 243 s. ISBN 978-80-7380-059-8.

⁸⁰ BALÍKOVÁ, Marie. *Forezní a klinická toxikologie: laboratorní toxikologická vyšetření*. 2. dopl. vyd. Praha: Galén, 2017. 127 s. ISBN 978-80-7492-304-3.

⁸¹ BALÍKOVÁ, Marie. *Forezní a klinická toxikologie: laboratorní toxikologická vyšetření*. 2. dopl. vyd. Praha: Galén, 2017. 127 s. ISBN 978-80-7492-304-3.

Pravděpodobně nejrozšířenější drogou z této skupiny je metamfetamin, známý pod názvem pervitin. Jedná se o látku ze skupiny takzvaných budivých aminů, která se nejčastěji užívá nitrožilně. Metamfetamin zpočátku člověka povzbudí, uživatel má tak často pocit, že nemusí vůbec spát, lépe mu to myslí, lépe se mu navazují vztahy a obecně je výkonnější. Některým může vyhovovat i pocit, že nemusí vůbec jíst. Většina uživatelů pervitinu mívá pocity neporazitelnosti a obrovské síly a přílivu energie. No, na dojezdu už je to horší. Jedná se o stav úplného vyčerpání organismu, kdy je uživatel v útlumu. Může se dostavit tzv. zásek, nebo opakování stereotypních pohybů. Rizikem je i velké přetížení organismu, spojené s bolestmi na hrudi a rizikem selhání srdce. Uživatel také často bývá paranoidní, má pocit, že ho všichni sledují, všichni jsou policisté, kteří po něm jdou, cítí se ohrožen. Stav může dojít až do tzv. toxické psychózy, při které má uživatel halucinace a bludy, ačkoliv není pod vlivem látky. Uživatelé taktéž bývají velmi hubení⁸².

6.2.2 Látky tlumící centrální nervový systém

Látky zařazené do této kapitoly, jsou často běžnými léky, např. na epilepsii, psychiatrické poruchy, deprese, navození spánku nebo opiáty. Z běžně dostupných sem patří i alkohol, z drog bychom sem potom mohli zařadit heroin. Všechny tyto léky jsou často zneužívány a prodávány na Darknetu, dokonce jejich prodej v tomto směru postupně roste a s příchodem pandemie COVID-19 se ještě rapidně zvýšil. Látky způsobují otupělost, v případě předávkování může dojít až k útlumu dechového centra a následně smrti⁸³.

Na Dark Webu se ve velké míře obchoduje s léky, které jsou na předpis. Jedná se zejména o skupinu léčiv zvanou benzodiazepiny, což jsou léky, které se využívají k uklidnění zejména od stresu, nebo k navození spánku. Hlavními projevy je tak únava, ospalost, neschopnost plné koncentrace, zpomalení reflexů a myšlení. Nejznámějším léčivem je diazepam, u nás prodáváný pod názvem Apaurin, nebo Diazepam. Dále léky Rivotril, nebo Rohypnol, který se dnes již v České Republice nesmí prodávat. V devadesátých letech byl totiž zneužíváný uspávacími k trestné činnosti. Na Darknetu se diazepam nejčastěji prodává pod názvem Valium, což ukazuje na

⁸² KALINA, Kamil a kol. *Klinická adiktologie*. 1. vyd. Praha: Grada, 2015. 696 s. ISBN 978-80-247-9791-5.

⁸³ BALÍKOVÁ, Marie. *Forezní a klinická toxikologie: laboratorní toxikologická vyšetření*. 2. dopl. vyd. Praha: Galén, 2017. 127 s. ISBN 978-80-7492-304-3.

zahraniční produkci. Dalším rozšířeným lékem na Dark Marketech je Xanax, který sice není typický benzodiazepin, ale jedná se o léky na úzkosti a nespavost. Jeho účinnou látkou je alprazolam a v České Republice ho mnohem častěji najdeme pod názvem Neurol^{84,85}.

6.2.3 Látky ovlivňující vnímání

Látky, které obecně můžeme nazvat halucinogeny, asi není potřeba blíže představovat a to i vzhledem ke statistikám Policie ČR z roku 2019. Dle nich totiž v ČR má každý třetí obyvatel zkušenost s užitím drogy, kdy nejčastěji se jednalo o kanabinoidy, extázi a halucinogenní houbičky⁸⁶. Všechny tyto látky mají v této kategorii své místo a mohou se jen předhánět v účincích na lidský organismus. Halucinace, sluchové i zrakové, dezorientace v prostoru, místě i čase, bludy. U člověka, který takovouto drogu užil, můžeme pozorovat zrychlené dýchání, zvýšenou tělesnou teplotu, zrychlený puls a rozšířené zornice⁸⁷.

MDMA, neboli extáze, je považována za taneční drogu, která se užívá zejména na akcích s reprodukovanou elektronickou hudbou. Projevuje se zpočátku neklidem a mírnou zmateností, v další fázi ale přichází pohoda, ustupuje stres a zlepšuje se nálada. Uživatelé mají touhu dotýkat se ostatních, jsou velmi empatictí a zlepšuje se i jejich komunikativnost. Většinou nejsou přítomny halucinace. Jenže pocity navozené extází jednou skončí. Na druhý den se objevuje stav podobný kocovině, taktéž se dostaví zhoršení nálady, případně nevolnost a pocity na zvracení. Mohou se dostavit i projevy podobné chřipce – únava, bolesti kloubů a svalů, potřeba spánku. Užití extáze může u uživatele podpořit rozvoj psychických onemocnění, např. deprese⁸⁸.

⁸⁴ HIRT, Miroslav. *Dopravní nehody v soudním lékařství a soudním inženýrství*. Praha: Grada, 2012. 160 s. ISBN 978-80-247-4308-0.

⁸⁵ BALÍKOVÁ, Marie. *Forezní a klinická toxikologie: laboratorní toxikologická vyšetření*. 2. dopl. vyd. Praha: Galén, 2017. 127 s. ISBN 978-80-7492-304-3.

⁸⁶ EVROPSKÉ MONITOROVACÍ CENTRUM PRO DROGY A DROGOVOU ZÁVISLOST. *Evropská zpráva o drogách 2019: trendy a vývoj* [online]. Lucemburk: úřad pro publikace Evropské unie, 2019. ISBN 978-92-9497-400-6. Dostupné z:

https://www.emcdda.europa.eu/system/files/publications/11364/20191724_TDAT19001CSN_PDF.pdf

⁸⁷ BALÍKOVÁ, Marie. *Forezní a klinická toxikologie: laboratorní toxikologická vyšetření*. 2. dopl. vyd. Praha: Galén, 2017. 127 s. ISBN 978-80-7492-304-3.

⁸⁸ KALINA, Kamil a kol. *Klinická adiktologie*. 1. vyd. Praha: Grada, 2015. 696 s. ISBN 978-80-247-9791-5.

6.3 Boj proti drogové kriminalitě v České republice

Tato kapitola, která vychází zejména z Výroční zprávy Národní protidrogové centrály (dále jen NPC) pro rok 2020 se zaměřuje jak na běžný prodej drog „na ulici“, tak zejména na prodej drog v online prostředí. Je nutné si uvědomit, že tento rok je poznamenaný pandemií nemoci COVID-19 a protipandemickými opatřeními, které zasáhly i drogový trh a částečně zapříčinily jeho přesun do kyberprostoru. Výroční zpráva NPC pro rok 2020 uvádí, že došlo k výraznému úbytku příležitostí spojených s výrobou a distribucí OPL. Zejména se jednalo o dovoz prekurzorů ze zahraničí (u nás nejčastěji prekurzory metamfetaminu dovážené z Polska) z důvodů uzavření státních hranic. Zajímavostí je nárůst požárů a výbuchů při tzv. domácí výrobě drog v začátku pandemie COVID-19. Pandemická omezení ovlivnila i užívání OPL koncovými zákazníky. Zejména se snížil počet příležitostných uživatelů „lehčích“ drog z důvodu uzavření tanečních klubů a barů. Stejně tak se snížila míra pouličního prodeje. I přes zpočátku zaznamenaný pokles se drogová scéna rychle vzpamatovala a našla si cesty a možnosti jak pokračovat v prodeji. NPC zaznamenala vzrůstající trend fenoménu temných tržišť a s ním souvisejícím prodejem OPL. Pro distribuci byly využity poštovní a zásilkové služby. S touto spojitostí byl zaznamenán vzrůstající trend kryptoměn, které byly využity jakožto platební prostředek za OPL na temných tržištích. V koncovém důsledku měla pandemie COVID-19 na výrobu a distribuci drog jen malý vliv a nebyly zaznamenány větší výpadky v zásobování. Byl však zpozorován nárůst zneužívání psychoaktivních léčiv a přípravků a jejich následné distribuce na drogových trzích. Odpovědí na tento problém je zvyšování tlaku na regulaci psychoaktivních látek a jejich následnému zapsání na seznamy zakázaných látek⁸⁹.

6.3.1 Obchod s metamfetaminem

V České republice je dlouhodobě pozorován fenomén vysokého počtu varen zabývajících se výrobou metamfetaminu. Tento fenomén je sice nejvyšší v Evropě, ale nikoliv objemem výroby. Ve valné většině odhalených případů se jedná o malé domácí varny, které mají maximální výrobní kapacitu kolem desítek gramů látky na jeden výrobní cyklus. Jejich produkce je primárně určená pro domácí trh a nikoliv pro zahraniční. Zahraničním trhům se věnují průmyslové varny, které mají produkci v řádu desítek kilogramů. Tyto varny v tuzemských podmínkách představují kolem 7 % všech odhalených varen. NPC zpozorovala aktuální trend přesunu průmyslových varen do

⁸⁹ NÁRODNÍ PROTIDROGOVÁ CENTRÁLA. *Výroční zpráva 2020* [online]. 25. 6. 2021 [cit. 2022-04-10]. Dostupné z: <https://www.policie.cz/clanek/vyrocní-zprava-npc-za-rok-2020.aspx>

Polska a Holandska. Průmyslové varny na území České republiky zejména provozují vietnamské kriminální skupiny, které též organizují přesun výroby do dalších zemí Evropy. NPC zaznamenala dovoz prekurzorů a pomocných látek potřebných pro výrobu metamfetaminu do České republiky z Polska. Polsko pro výrobce této drogy představuje hlavního dodavatele pseudoefedrinu a taktéž červeného fosforu. Nejčastěji je zaznamenán dovoz farmaka Cirrus. Též je pozorována vzrůstající tendence dovozu léčiv ze Španělska, Turecka, Rumunska anebo z Bosny a Hercegoviny, který je primárně organizován cizinci s dlouhodobým povolením k pobytu v České republice. Pandemická omezení přinesla krátký útlum a výpadek v tomto segmentu, ale brzy se situace stabilizovala. Snížená dostupnost též měla vliv i na konečnou cenu drogy a taktéž i na její vývoz z České republiky. Německá policie za rok 2020 zaznamenala kolem šedesáti případů, kdy cizinci anebo občané Německé spolkové republiky pašovali metamfetamin z České republiky, což je méně, než v předchozích letech. Tento klesající trend je způsobem přesunem průmyslových výroben vietnamských kriminálních uskupení z České republiky do Nizozemí, kde je evidentní i vysoká míra dostupnosti metamfetaminu zapříčiněná drogovými kartely pocházejícími z Mexika. Tyto kartely dovážejí z Mexika velké množství kvalitního metamfetaminu v lodních kontejnerech do přístavů v Nizozemí a odtud jej dále v rámci kooperace s vietnamskými zločineckými skupinami exportují do dalších zemí Evropy, Českou republiku nevyjímaje. V rámci Evropy je taktéž sledován a zachycován metamfetamin pocházející ze střední Asie a to zejména z Afghánistánu a Íránu⁹⁰.

6.3.2 Obchod s konopnými látkami

Obchod s konopnými látkami zaujímá společně s metamfetaminem v tuzemsku nejvyšší podíl. Výroba konopí v roce 2020 zahrnovala jak malé pěstírny, tak i ty velké, které pěstují stovky rostlin. Dominantou tohoto trendu jsou převážně malé pěstírny a to převážně vnitřní, ale i venkovní, které rostliny pěstují v klimaticky vhodných regionech země. Obchod s konopnými produkty je organizovaně řízen obchodníky, kteří je z jedné části distribuují na tuzemský trh a z druhé části je distribuují dalším odběratelům do dalších zemí Evropské unie. Zejména se jedná o sousední státy České republiky, severské státy, či Maďarsko. V rámci vládních opatření a pandemických omezení vzrostl obchod s marihuanou v prostředí Darknetu a jeho temných tržištích. Díky tomuto se snížila míra záchytu při příhraničním obchodu. Polská policie ve své zprávě

⁹⁰ NÁRODNÍ PROTIDROGOVÁ CENTRÁLA. *Výroční zpráva 2020* [online]. 25. 6. 2021 [cit. 2022-04-10]. Dostupné z: <https://www.policie.cz/clanek/vyrocní-zprava-npc-za-rok-2020.aspx>

uvádí, že Česká republika je dominantním producentem a vývozcem marihuany do Polska. Velké pěstírny a velkoprodukce konopných produktů jsou doménou kriminálních skupin pocházejících z balkánských zemí. Jejich členové se prokazují falešnými cestovními doklady, pronajímají si nemovitosti, které posléze využívají jakožto pěstírny. Organizátoři se k trestné činnosti na území České republiky napřímo nezapojují a zisky z prodeje konopí legalizují v zemích jejich původu. Jejich produkce je primárně určena k exportu. Obchod se syntetickými kanabinoidy, které slouží jako náhražka marihuany je na klesající tendenci. Tento trend je patrný jak v České republice, tak i v celé Evropě⁹¹.

6.3.3 Obchod s MDMA

V době pandemických opatření je zpozorováno uzavření některých distribučních míst a obecně snížení poptávky po extázi. Obchod s touto látkou se primárně přesunul do internetového prostředí a to do prostředí Darknetu a jeho ilegálních temných tržišť. Dále je zaznamenán zvýšený nárůst obchodů s MDMA a to v podobě tablet, ale i v práškové podobě, která je určená k dalšímu zpracování. V kyberprostoru jsou zaznamenány obchody s malým množstvím v řádu tablet, ale i ve velkém množství v řádu kilogramů. Zdrojovou zemí je zejména Nizozemí a Belgie. Distribuce je řešena prostřednictvím přepravních společností formou zásilek. Taktéž je zaznamenán nový trend mladých zákazníků, kteří si drogu obstarávají na temných tržištích. S tímto fenoménem je i spjat výskyt nových prodejců z řad mladé generace. Tito prodejci hojně využívají anonymitu, kterou Darknet nabízí a tento obchod využívají jako jakýsi snadný přivýdělek. Rok 2020 přinesl i nárůst obchodu s MDMA v podobě krystalických látek, které jsou konzumenty aplikovány tzv. šňupáním, anebo jsou rozpouštěny v tekutinách a posléze vypity. Nový trend, který byl bezpečnostními složkami zaznamenán již v loňském roce, bylo zapojení vietnamských organizovaných zločineckých skupin, které obchodují s MDMA a následně je přes Českou republiku vyvázejí do Vietnamu. Tato droga zažila ve Vietnamu velký nárůst oblíbenosti⁹².

⁹¹ NÁRODNÍ PROTIDROGOVÁ CENTRÁLA. *Výroční zpráva 2020* [online]. 25. 6. 2021 [cit. 2022-04-10]. Dostupné z: <https://www.policie.cz/clanek/vyrocní-zprava-npc-za-rok-2020.aspx>

⁹² NÁRODNÍ PROTIDROGOVÁ CENTRÁLA. *Výroční zpráva 2020* [online]. 25. 6. 2021 [cit. 2022-04-10]. Dostupné z: <https://www.policie.cz/clanek/vyrocní-zprava-npc-za-rok-2020.aspx>

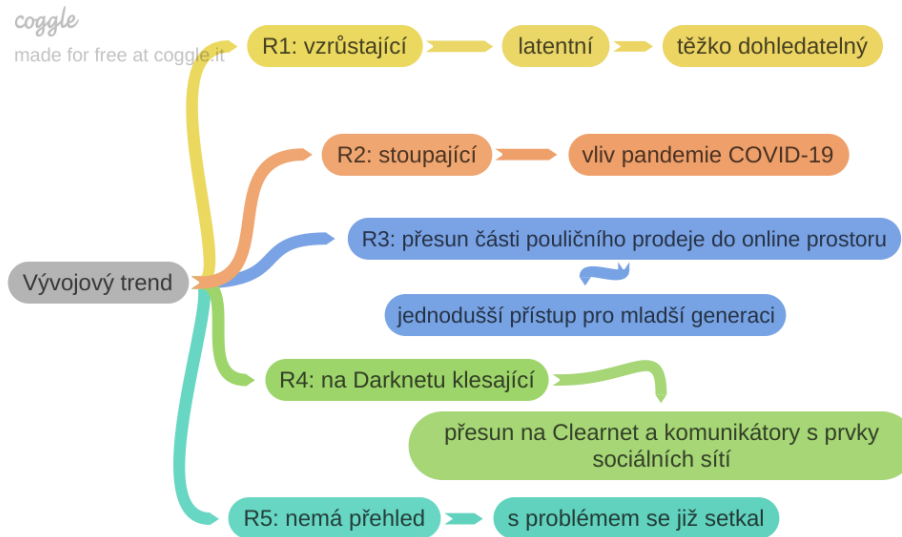
7 Vyhodnocení výzkumu

Praktickou část bakalářské práce jsem zpracoval formou řízených rozhovorů, kterých se nakonec účastnilo pět policistů, kteří se s problematikou buď pravidelně setkávají ve své práci, tedy že ji přímo řeší, případně se s problematikou více či méně setkali. Rozhovorů jsem měl původně domluveno více, ale někteří policisté následně odmítli účastnit se rozhovoru z vlastního přesvědčení, či pracovního vytížení. Někteří mi otázky vyplnili a odeslali emailem, s některými jsem se osobně sešel a měl jsem tak možnost s nimi strávit cenný čas. Výsledky jsem posléze zpracoval pomocí programu coggle.it do myšlenkových map.

Policisté byli všichni muži s délkou praxe od devíti do třiceti sedmi let u Policie České republiky. Dva pracují u SKPV na problematice TOXI (protidrogová policie), další tři u NPC v různých krajských městech s různou délkou specializace. Z důvodu zachování anonymity jsem policisty označil jako respondenty s čísly 1 – 5 a proházet jsem jejich pořadí.

7.1 Víte, jaký je aktuální vývojový trend nákupu OPL v internetovém prostředí?

Tabulka 1 Vývojový trend nákupu OPL v internetovém prostředí

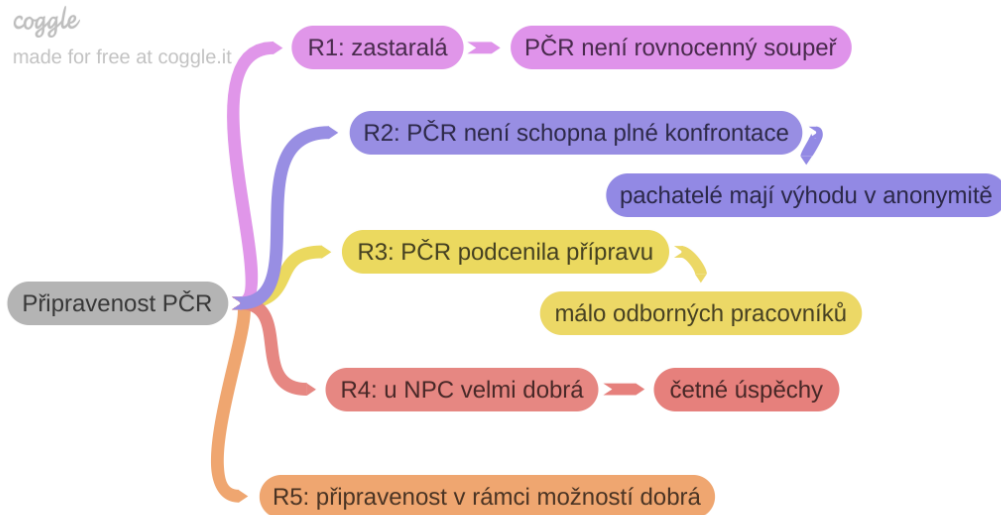


Zdroj: vlastní

Většina respondentů si myslí, že trend nákupu OPL na internetu je na vzestupu. Respondent s číslem 4 ale upřesňuje, že co se týče Darknetu, je trend spíše klesající a prodej drog se přesouvá na Clear Web a do specializovaných skupin v komunikátorech, jako je například Telegram, kde má možnost získat mnohem více zákazníků. Pandemii COVID-19 ve svých odpovědích zmiňují respondenti s čísly 2 a 4. R2 k tomu uvádí, že se dle něj přesunulo do kyberprostoru větší množství kriminality, která je podle R1 tímto mnohem latentnější a pro policisty hůře dohledatelná. R4 ale zmiňuje, že jistý úpadek Dark Webu policie zaznamenává od chvíle, kdy se na tuto problematiku začali více zaměřovat, což bylo někdy kolem let 2017 - 2018. Tento respondent také uvádí, že pandemie COVID-19 znamenala jisté oživení temných tržišť k prodeji drog, na úroveň před lety 2017 se ale již tržiště nedostala. I přes to respondent 3 míní, že se jistá obliba prodeje drog na internetu stále drží a to zejména mezi mladší generací, která nemá problém s internetovými nákupy, ani s platbou ve virtuálních měnách. Mezi těmito zákazníky jsou oblíbeny hlavně taneční a designové drogy, prodejci pervitinu a marihuany stále preferují pouliční prodej. Pátý respondent odpovídá, že o aktuálním vývoji přesný přehled nemá, ale ví, že Darknet je problémem. S touto problematikou se taktéž ve své práci setkal.

7.2 Jaká je dle Vás připravenost orgánu PČR se s tímto fenoménem plně konfrontovat?

Tabulka 2 Připravenost PČR



Zdroj: vlastní

Většina z těch, kteří se s problematikou běžně ve své práci nesetkávají, odpovídají, že je dle nich připravenost Policie České republiky v tomto směru zastaralá a není připravena na plnou konfrontaci. Toto tvrzení rozporují policisté, kteří se problematikou zabývají mnohem častěji. Je možné, že jen jejich výsledky nejsou tolik vidět, jako například zprávy o dalších a dalších podvedených v rámci kybernetických podvodů typu „voják na misi“ nebo „výhodná investice do kryptoměn“ a „Váš účet byl napaden.“ Policie naopak zaznamenala řadu úspěchů při potírání české drogové scény, která se z části přesunula do kyberprostoru. Dokonce i se zajištěním přibližně 100 BTC, pocházející z trestné činnosti. V přepočtu na české koruny se jedná o něco málo přes 90 mil Kč dle aktuálního kurzu. Respondent 2 ale míní, že: „v IT prostředí je pachatel TČ prakticky nedohádatelný a má vůči OČTŘ (pozn., orgány činné v trestním řízení) patrnou výhodu.“ Třetí respondent označil připravenost Policie ČR jako nástup do rozjetého vlaku. Podle pátého respondenta je ale připravenost na dobré úrovni, přestože je velice těžké s takovýmto fenoménem držet neustále ten správný krok.

7.3 Na jaké úrovni je dle Vás současná situace v rámci edukace policistů v oblasti kyberkriminality?

Tabulka 3 Úroveň edukace policistů v oblasti kyberkriminality

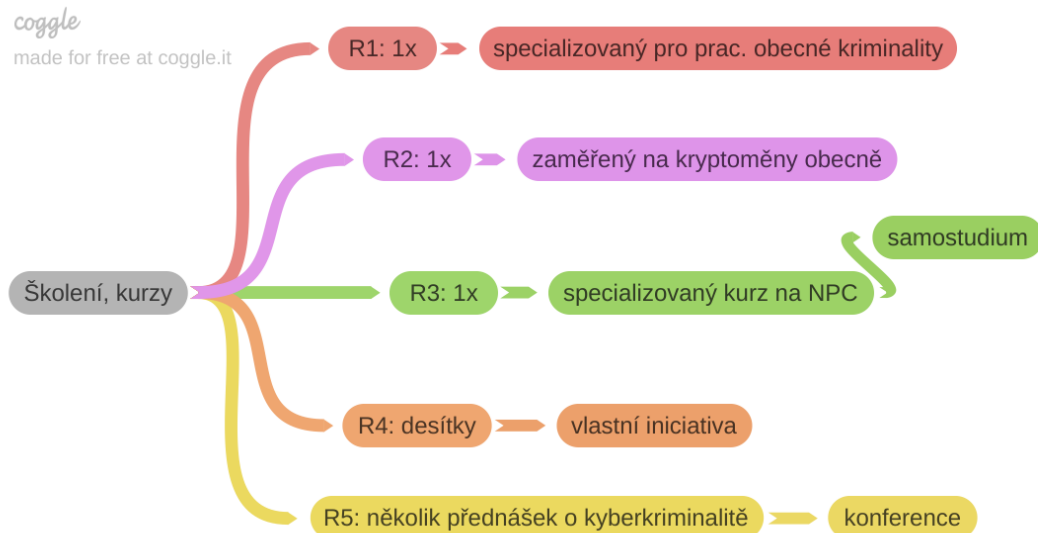


Zdroj: vlastní

V této otázce se respondenti shodují na obecně nižší úrovni edukace policistů v oblasti kybernetické kriminality. Respondent s číslem 4 ale jedním hlasem dodává, že zaznamenal v poslední době zlepšení. Pátý respondent si už teď myslí, že úroveň edukace je pro běžné, uniformované policisty dostačující. Respondenti s čísly 1, 2 a 3 vnímají úroveň edukace pořád nízkou, shodují se ale na tom, že na velmi vysoké úrovni jsou policisté, kteří se na tuto problematiku přímo specializují. Prakticky všichni oslovení respondenti vnímají problém s edukací i v nedostatku lektorů. Jedná se totiž o problematiku, kde musí lektor stavět na kvalitních teoretických základech, přidat k nim zkušenosti z praxe a v ideálním případě i trošku lektorského umu, aby byl dobrým a kvalitním školitelem, jak uvádí respondent s číslem čtyři. Uvádí k tomu i zajímavý přírámek: „stejně tak jako nemůže někdo přijít a říct, jo viděl jsem spoustu akčních filmů s výbuchy a absolvoval jsem desetidenní kurz o petardách a teď budu učit pyrotechniky, jak se to dělá.“ Respondent 2 označuje kromě problému s lektory i nedostatek finančních prostředků. Respondent číslo 5 jedním hlasem taktéž dodává, že boj s kybernetickou kriminalitou by se měl nechat na specialistech a neměly by se do něj přehnaně pouštět obyčejní policisté.

7.4 Jakými školeními či kurzy jste si v rámci této problematiky prošel, případně víte i o nějakých dalších?

Tabulka 4 Školení a kurzy v oblasti kryptoměn

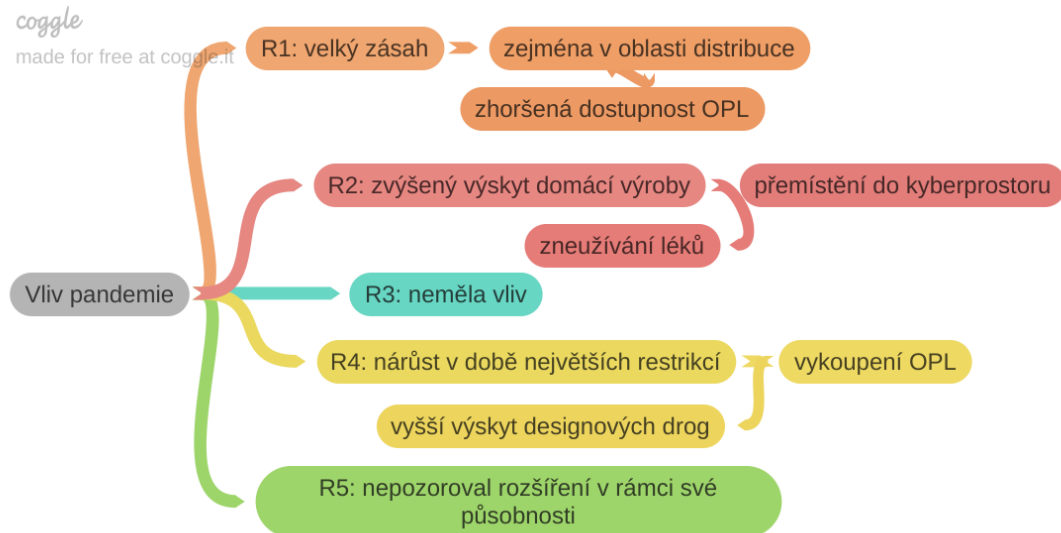


Zdroj: vlastní

V této otázce jsem zjišťoval, zda mají policisté přehled o možných kurzech s touto problematikou. Jak jsem se již dozvěděl z předchozí otázky, je problém s lektory, čili i specializovaných kurzů je velice málo. Mnozí policisté se tak vzdělávají v rámci samostudia, civilních kurzů nebo na konferencích, zaměřených na tuto tematiku. Místy vycházejí i odborné články v časopisech určených pro policisty, například v *Drugs & Forensics Bulletin*, který vydává NPC.

7.5 Pokud můžete srovnat vývoj nákupu OPL před pandemií COVID-19 a situaci v následujících pandemických letech, došlo v této problematice k nějakému vývoji a rozšíření?

Tabulka 5 Vliv pandemie COVID-19 na nákup OPL



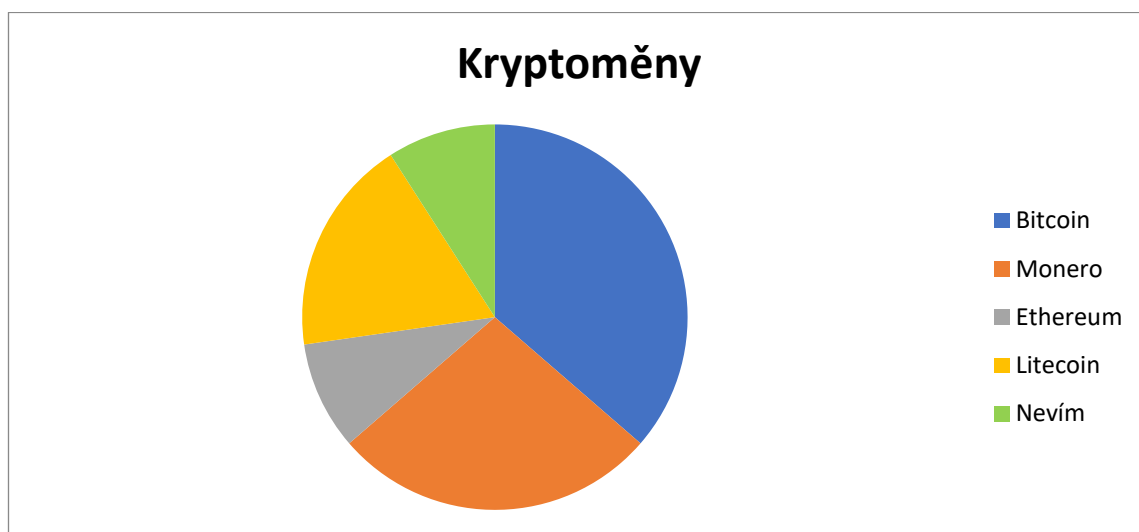
Zdroj: vlastní

Pandemii COVID-19 zmiňovali někteří respondenti již v první otázce. První respondent zaznamenal, že: „*pandemie rozhodně zasáhla do prostředí TOXI, zejména v oblasti distribuce.*“ Podle něj drogoví dealéři provádějí svou ilegální činnost latentněji. S tím ale souvisí i zhoršená dostupnost OPL pro běžné zákazníky. Respondent 2 zaznamenal zejména přesun drogové problematiky z ulice do domácího prostředí. S tím souvisí i nárůst domácích výroben drog, které byly v některých případech odhaleny náhodou, kdy pachatelé neodbornou manipulací způsobili požár nebo výbuch. Tento respondent míní, že se prodej drog z části přesunul do kyberprostoru a taktéž došlo k rozšíření problematiky ve společnosti, zejména byl zaznamenán výskyt častějšího zneužívání léků a OPL z důvodu depresí, nebo zhoršení psychického stavu. Naopak respondent s číslem tři nezaznamenal ve své působnosti žádný zásadní vliv na proměnu s OPL směrem do virtuálního prostředí. Čtvrtý respondent se k této problematice vyjádřil již v první otázce, kde uvedl, že v rámci virtuálního trhu s OPL je od roku 2018 zaznamenáván strmý pád, který byl jen nepatrně oživen právě při restrikcích spojených s pandemií COVID-19. Tato data potvrzují i nejnovější studie, například od European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). Taktéž k tomu tento respondent uvádí, že: „*docházelo ke*

kuriózním případům, kdy vinou depresí a home office stylu práce, byly OPL vykoupěny a lidé začali experimentovat s designovými drogami, které pořizovali v Clearnetu.“ Respondent s číslem pět nepozoroval ve svém okrese rapidní rozšíření za pandemie. Všeobecně ale určitý nárůst oblíbenosti Darknetu zaznamenal.

7.6 Jaké kryptoměny se dle Vás používají k nákupu OPL na Darknetu?

Tabulka 6 Kryptoměny používané na Darknetu



Zdroj: vlastní

Většina respondentů, kromě jednoho, který uvedl, že neví, jaké měny jsou používány k nákupu OPL na Darknetu, všichni ostatní uvedli, že se používá Bitcoin. Jako další měny uvedli Monero, které uvedli tři respondenti, Litecoin, které uvedli dva respondenti a Ethereum, které uvedl jeden respondent. To koresponduje s mými zjištěními z teoretické části bakalářské práce.

7.7 SWOT analýza

Pro interpretaci výsledků mého výzkumu jsem zpracoval SWOT analýzu, která vychází z části z rozhovorů s policisty ze specializovaných oddělení PČR a z části z vlastních zkušeností a poznatků.

Silné stránky					
1. Řešení na celonárodní úrovni	1	1	1	1	2
	2	3	4	5	
2. Spolupráce specializovaných oddělení PČR a Obvodních oddělení PČR		2	2	2	2
		3	4	5	
3. Existence preventivních programů a jejich podpora			3	3	2
			4	5	
4. Dobře nastavená a fungující mezinárodní spolupráce				4	0
				5	
5. Vysoká odbornost policistů, kteří se problematikou přímo zabývají					4

	počet	n+1	váha	hodnocení	hodnocení x váha
1.	2	3	0,20	5	1,00
2.	2	3	0,20	4	0,80
3.	2	3	0,20	3	0,60
4.	0	1	0,07	4	0,27
5.	4	5	0,33	5	1,67
	15	1,00			4,33

Slabé stránky					
1. Málo policistů, kteří se aktivně zabývají problematikou	1	1	1	1	1
	2	3	4	5	
2. Mezery ve vzdělávání běžných policistů z Obvodních oddělení PČR		2	2	2	2
		3	4	5	
3. Problém vystopování transakcí provedených v kryptoměnách			3	3	4
			4	5	
4. Problém se záchytem OPL				4	1
				5	
5. Zasílání malých těžko vystopovatelných zásilek					2

	počet	n	váha	hodnocení	hodnocení x váha
1.	1	1	0,10	-4	-0,40
2.	2	2	0,20	-5	-1,00
3.	4	4	0,40	-5	-2,00
4.	1	1	0,10	-5	-0,50
5.	2	2	0,20	-5	-1,00
	10	1,00			-4,90

Příležitosti					
1. Spolupráce s kryptoměnovými burzami	1	1	1	1	1
	2	3	4	5	
2. Edukace dětí a rodičů		2	2	2	1
		3	4	5	
3. Navýšení povědomí běžných policistů o problematice			3	3	4
			4	5	
4. Navýšení počtu policistů zabývajících se problematikou				4	3
				5	
5. Zlepšení komunikace v rámci PČR a ostatních OČTŘ					1

	počet	n	váha	hodnocení	hodnocení x váha
1.	1	1	0,10	4	0,40
2.	1	1	0,10	3	0,30
3.	4	4	0,40	5	2,00
4.	3	3	0,30	5	1,50
5.	1	1	0,10	4	0,40
	10	1,00			4,60

Hrozby					
1. Anonymita	1	1	1	1	3
	2	3	4	5	
2. Pandemie COVID-19 a s ní související přesun drogové kriminality do kyberprostoru		2	2	2	2
		3	4	5	
3. Jednodušší přístup nezletilých a mladistvých na Darknet			3	3	2
			4	5	
4. Rychlé předávání informací				4	1
				5	
5. Rychlý rozvoj drogové kriminality díky její medializaci					2

	počet	n	váha	hodnocení	hodnocení x váha
1.	3	3	0,30	-5	-1,50
2.	2	2	0,20	-5	-1,00
3.	2	2	0,20	-3	-0,60
4.	1	1	0,10	-2	-0,20
5.	2	2	0,20	-4	-0,80
	10	10			-4,10

Z výsledků SWOT analýzy plyne, že policejní orgán není v současné době schopen se s problematikou kyberkriminality v rámci kryptoměn a s ním souvisejícím nákupem OPL na Darknetu napřímo konfrontovat a efektivně s tímto fenoménem bojovat. Důvodem je nízká edukace běžných policistů, nízké početní stavy, a zároveň vynalézavost a vysoká úroveň znalostí na poli IT technologií pachatelů této trestné činnosti. Z těchto zjištěných skutečností bych doporučil, aby OČTŘ zvýšili obecné povědomí mezi běžnými policisty v rámci kryptoměn a pojmem Darknetu tak, aby se mohli aktivně zapojit a případně aby mohli v rámci získaných znalostí a zkušeností působit preventivně, ale i edukačně.

Závěr

Drogový byznys, který probíhá v temných hlubinách internetu, už zdaleka není tak nespolehlivý a složitě dosažitelný, jak by se mohlo zdát. Stačí vlastnit počítač, připojení k internetu, TOR, trochu Bitcoinu (nebo jiné kryptoměny) a koupíte skoro cokoliv, na co máte peníze. A pokud chcete drogy, někdy ani nemusíte na Darknet. Pro ilustraci si uveďme webovou stránku Shiny flakes, která nabízela různé drogy s doručením přes poštovní službu, minimálně do větší části Evropy. A která fungovala na Clear Webu, tedy na internetu, který všichni běžně používáme.

Cílem bakalářské práce bylo definovat pojem kyberprostor a jeho části, na které se rozděluje. Dále vysvětlit fenomén kryptoměn, jejich význam a použití, jak v legálním, tak i v ilegálním způsobu, a to zejména v nákupu omamných a psychotropních látek. Druhá část bakalářské práce byla zpracována formou řízených rozhovorů s příslušníky z řad Policie České republiky, kteří pracují na specializovaných odděleních a s drogovou kriminalitou se aktivně zabývají.

V teoretické části bakalářské práce popisují kryptoměny, jejich architekturu, funkci a široké možnosti uplatnění. Zejména zde pojednávám o nejvýznamnější digitální měně Bitcoin, ale i o dalších alternativních digitálních měnách, které jsou jeho úspěšnými následovníky a které do světa kryptoměn přináší obsáhlé spektrum inovací. Dále je v této části bakalářské práce popsán kyberprostor a jeho rozdělení. Toto dělení kyberprostoru čtenáři přibližuje to, co je „na povrchu“ a to, co se skrývá „pod povrchem.“ V této temné části kyberprostoru se ukrývá 96 % veškerých dat, které jsou na internetu. Je důležité říci, že ne vše co se skrývá „pod povrchem“ je nutně špatné, nebo ilegální. I přesto, nebo právě proto, může být tato temná část velmi přitažlivá. Nalézt můžeme různá temná tržiště, kde prodejci nabízejí své zboží a služby, které se nedají zařadit mezi legální. Setkat se zde lze s širokou nabídkou různých drog a farmak, zbraněmi všech typů, dále s odcizenými kreditními kartami, přístupy na webové stránky firem, dětskou pornografií, DoS/DDoS útoky hackerů na objednávku, či objednání vraždy u skupiny nájemných vrahů. V této části jsem některá, avšak významná temná tržiště Darknetu představil a popsal jejich příběh, který neskončil slovy: „a žili spolu šťastně až na věky,“ ale v naprosté většině případů jejich příběh skončil slovy: „This website has been seized“ a jejich správci byly za jejich trestné činy pravomocně odsouzeni. Dále jsem v teoretické části povrchně představil boj proti drogové kriminalitě v České republice z dostupných dat, které jsem získal z veřejných

informačních zdrojů. Samozřejmě má Policie České republiky mnohem více možností, jak bojovat proti této problematice, avšak z důvodu bezpečnosti je nechci v této práci uvádět. Věnoval jsem se také v krátkosti drogové problematice, kterou jsem zaměřil zejména na nákup drog na internetu.

Praktickou část své bakalářské práce jsem zpracoval formou řízených rozhovorů s policisty z oddělení zabývajícími se drogovou problematikou, přičemž někteří z nich přímo bojují proti drogové kriminalitě v internetovém prostředí. Záměrně zde neuvádím, kde přesně tito policisté pracují, ani další data, podle kterých by mohli být identifikováni. I přes počáteční obtíže se získáváním rozhovorů způsobených z části pandemií COVID-19, velkým množstvím případů i nechutí k rozhovorům, se mi podařilo zpracovat celkem pět rozhovorů. I přes tento malý vzorek respondentů jsou výsledky zajímavé a pro mě osobně i velice přínosné. Je zajímavostí, že v některých otázkách si respondenti dokonce rozporovali. Tento rozpor je pravděpodobně způsobený tím, že respondenti, kteří se s problematikou v kyberprostoru přímo nesetkávají, vycházejí převážně ze svých domněnek více, než z reálných faktů. Například v otázce o popularitě Darknetu většina uváděla, že je na vzestupu, kdežto jiní respondenti zaznamenali, že se on-line prodej drog přesouvá z Darknetu směrem do Clearwebu a na komunikační síť typu Telegram. I díky těmto rychlým změnám je pro Policii České republiky obtížné na tyto změny rychle reagovat a přizpůsobit se jim. Toto přizpůsobení tak proběhne jen na nejvyšších postech, kdežto obyčejní uniformovaní policisté nejsou schopni na tyto změny rychle a efektivně reagovat. V poslední době se ale povědomí běžných policistů zlepšuje.

Snažil jsem se také zjistit, jak do této problematiky zasáhla pandemie COVID-19. Je evidentní, že během pandemie se drogoví dealeri i jejich zákazníci potýkali s celou řadou problémů. Ty byly částečně vyřešeny přesunem z ulice do prostorů Darknetu a jeho temných tržišť. V současné době se ale vše vrací do situace, která tu panovala před pandemií. Naopak díky pandemii získali nové zákazníky zejména ti, kteří nabízeli různé léky a to například benzodiazepiny, či léky na deprese. I tento fenomén se ale postupně přesouvá spíše do prostor Clearnetu. Přesto bychom na Darknet neměli zapomínat, vnímat jej jako určitý typ hrozby a aktivně proti němu bojovat.

Seznam použitých zdrojů

Literární zdroje

BALÍKOVÁ, Marie. *Forezní a klinická toxikologie: laboratorní toxikologická vyšetření*. 2. dopl. vyd. Praha: Galén, 2017. 127 s. ISBN 978-80-7492-304-3.

BEDNÁR, Juraj. *Kryptomeny: platobná sieť internetu*. Elektronická kniha. 2020. 204 s. ISBN 999-00-030-7093-7.

HESS, Ladislav a Radim UZEL. *Sex, drogy a násilí*. 1. vyd. Praha: Mladá fronta, 2018. 314 s. ISBN 978-80-204-4941-2.

HIRT, Miroslav. *Dopravní nehody v soudním lékařství a soudním inženýrství*. Praha: Grada, 2012. 160 s. ISBN 978-80-247-4308-0.

CHOVANCULIAK, Róbert. *Pokrok bez povolení: Jak sdílená ekonomika, crowdfunding a kryptoměny změnilly svět*. 1. vyd. Praha: Grada, 2020. 272 s. ISBN 978-80-271-1755-0.

KALINA, Kamil a kol. *Klinická adiktologie*. 1. vyd. Praha: Grada, 2015. 696 s. ISBN 978-80-247-9791-5.

KAVALLIEROS, Dimitrios et. al. *Understanding the Dark Web*. In: BABAK, Akhgar et. al. *Dark Web Investigations*. Cham (CHE): Springer Nature Switzerland AG, 2021. ISBN 978-3-030-55343-2.

KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metody vyšetřování*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2021. 417 s. ISBN 978-80-7380-859-4.

KVAPILOVÁ, Helena a Michal DOGOŠI. *Soudní lékařství pro právníky a policisty*. 2. rozš. vyd. Plzeň: Aleš Čeněk, 2007. 243 s. ISBN 978-80-7380-059-8.

MARTIN, Jeremy. *The Beginner's Guide to the Internet Underground*. 2. vyd. Elektronická kniha. Information Warfare Center LLC, 2014. 42 s. Bez ISBN. Dostupné z:

https://books.google.cz/books?id=3b4iAQAAQBAJ&dq=the+beginners+guide+to+the+internet+underground+2nd+ed&hl=cs&source=gbs_navlinks_sground%202nd%20ed&f=false

OMASTA, Adam. Adaptace virtuálních tržišť s návykovými látkami na vládní opatření COVID-19. *Drugs & forensics bulletin*. 2020, roč. XXVI, čís. 3. ISSN 1211-8834.

ORMSBY, Eileen. *Silk Road*. 1. vyd. Sydney: Pan Macmillian Australia, 2014. 352 p. ISBN 978-1742614090. (EN).

POŽÁR, Josef. *Informační bezpečnost*. 1. vyd. Plzeň: Aleš Čeněk, 2005. 311 s. ISBN 80-86898-38-5.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozš. a aktual. vyd. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.

STROUKAL, Dominik; SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Historie, ekonomie a technologie kryptoměn. 3. vyd. Praha: Grada, 2021. 291 s. ISBN 978-80-271-1043-8.

Elektronické zdroje

Binance Academy. *Co je kryptoměnová peněženka?* [online]. 18. 6. 2019, aktualizace 11. 11. 2021 [cit. 2022-02-18]. Dostupné z: https://academy.binance.com/cs/articles/crypto-wallet-types-explained?utm_source=BinanceAcademy&utm_medium=Academy&utm_campaign=StaySAFU

Digitální pevnost. *Hash* [online]. 2018 [cit. 2022-02-13]. Dostupné z: <https://www.digitalnipevnost.cz/wiki/hash>

EVROPSKÉ MONITOROVACÍ CENTRUM PRO DROGY A DROGOVOU ZÁVISLOST. *Evropská zpráva o drogách 2019: trendy a vývoj* [online]. Lucemburk: úřad pro publikace Evropské unie, 2019. ISBN 978-92-9497-400-6. Dostupné z:

https://www.emcdda.europa.eu/system/files/publications/11364/20191724_TDAT19001_CSN_PDF.pdf

MACHÁLKOVÁ, Zuzana. *Nejoblíbenějšími psychedeliky Čechů jsou LSD a houby, ukázal výzkum. Experti ale varují před riziky* [online]. 22. 8. 2021 [cit. 2022-04-12]. Dostupné z: https://www.irozhlas.cz/zivotni-styl/psychedelika-ld-houby-narodni-psychedelicky-vyzkum-nudz_2108221936_btk

NÁRODNÍ PROTIDROGOVÁ CENTRÁLA. *Výroční zpráva 2020* [online]. 25. 6. 2021 [cit. 2022-04-10]. Dostupné z: <https://www.policie.cz/clanek/vyrocní-zprava-npc-za-rok-2020.aspx>

NEVYHOŠTĚNÝ, Martin. *Internetová loupež za 800 milionů: Stopa vede k českému programátorovi* [online]. 2. 12. 2013 [cit. 2022-20-03]. Dostupné z: https://www.lidovky.cz/byznys/velka-internetova-loupez-za-800-milionu-stop-a-vede-k-ceskemu-programatorovi.A131202_110252_firmy-trhy_mev

POLICIE ČESKÉ REPUBLIKY. *Kyberkriminalita* [online]. Nedatováno [cit. 2022-04-01]. Dostupné z: <https://www.policie.cz/clanek/kyberkriminalita.aspx>

Portál Finex.cz. *Blockchain: Co je blockchain a jak blockchain u kryptoměn funguje?* [online]. Aktualizováno 15. 2. 2022 [cit. 2022-02-16]. Dostupné z: <https://finex.cz/blockchain/>

Proof of Work a Proof of Stake [online]. 13. 1. 2020 [cit. 2022-02-14]. Dostupné z: <https://m.alza.cz/proof-of-work-a-proof-of-stake>

REDAKCE CHIP. *DARKNET - Temná strana internetu* [online]. 8. 2. 2012 [cit. 2022-04-12]. Dostupné z: <https://www.chip.cz/novinky/trendy/darknet-temna-strana-internetu/>

RHYSIDER, Jack. *Operation Bayonet. Dark Net Diaries* [online]. 15. 10. 2018 [cit. 2022-03-03]. Dostupné z: <https://darknetdiaries.com/episode/24/>

ŠŤASTNÝ, Josef. *[Pro začátečníky] Co je to altcoin* [online]. 29. 8. 2020 [cit. 2022-04-01]. Dostupné z: <https://kryptomagazin.cz/pro-zacatecniky-co-je-to-altcoin/>

THE U. S. DEPARTMENT OF JUSTICE. *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace: Russian Resident Indicted on Conspiracy Charges Related to Operating Hydra Market* [online]. 5. 4. 2022 [cit. 2022-04-06]. Dostupné z: <https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace>

VÁVRA, Jan. *Squid Game na vlastní kůži. Kryptoměna inspirovaná seriálem tvrdě ztrestala spekulanty* [online]. 2. 11. 2021 [cit. 2022-04-01]. Dostupné z: <https://www.e15.cz/kryptomeny/squid-game-na-vlastni-kuzi-kryptomena-inspirovana-serialem-tvrde-ztrestala-speklanty-1384919>

Legislativní dokumenty

ČESKO. Zákon č. 141/1961 Sb., zákon o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: Sbíрка zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/1961-141>

ČESKO. Zákon č. 167/1998 Sb., zákon o návykových látkách a o změně některých dalších zákonů. In: Sbíрка zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/1998-167>

ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: Sbíрка zákonů, Česká republika. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

Seznam zkratek

BTC - Bitcoin

CNS - centrální nervová soustava

DEA – Drug Enforcement Administration, v češtině Úřad pro potírání drog

FBI – Federal Bureau of Investigation, v češtině Federální úřad pro vyšetřování

HW - Hardware

IT – informační technologie

Kč – Koruna česká

MDMA – 3,4-methylenedioxy-N-metylamfetamin - extáze

NPC – Národní protidrogová centrála

OČTŘ – orgány činné v trestním řízení

OPL – omamné a psychotropní látky

P2P - peer-to-peer, v češtině klient-klient

PC – Personal Computer, v češtině osobní počítač

PČR – Policie České republiky

PoS - Proof of Stake

PoW - Proof of Work

SKPV PČR – Služba kriminální policie a vyšetřování Policie České republiky

SW – Software

TČ – trestný čin

TOR – the onion router, v češtině doslova cibulový směrovač, zkratka pro speciální software pro přístup na Darknet

TrZ – trestní zákoník

USD - United States Dollar, v češtině Americký Dolar

www – Word Wide Web, v češtině

XMR – Monero

Seznam tabulek a grafů

<i>Tabulka 1 Vývojový trend nákupu OPL v internetovém prostředí</i>	58
<i>Tabulka 2 Připravenost PČR</i>	59
<i>Tabulka 3 Úroveň edukace policistů v oblasti kyberkriminality</i>	60
<i>Tabulka 4 Školení a kurzy v oblasti kryptoměn</i>	61
<i>Tabulka 5 Vliv pandemie COVID-19 na nákup OPL</i>	62
<i>Tabulka 6 Kryptoměny používané na Darknetu</i>	63