

UNIVERZITA KARLOVA

Právnická fakulta

Michal Dolanský

Atomic swap: riziko pro AML regulaci?

Diplomová práce

Vedoucí diplomové práce: JUDr. Tomáš Sejkora, Ph.D.

Katedra: Katedra finančního práva a finanční vědy

Datum vypracování práce (uzavření rukopisu): 30. 11. 2021

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 135 954 znaků včetně mezer.

.....
Michal Dolanský

V Praze dne 30. 11. 2021

Obsah

Úvod	1
1. Atomové swapy – vymezení pojmů a základní charakteristika	3
1.1. Pojem atomový swap	3
1.2. Stručný popis pojmů a technologií potřebných k pochopení atomových swapů	4
1.2.1. Virtuální měna	4
1.2.2. Distribuované databáze	5
1.2.3. Blockchain	5
1.2.4. Veřejné a soukromé kryptografické klíče	6
1.2.5. Softwarové a hardwarové peněženky	6
1.2.6. Centralizované a decentralizované směnárny s virtuálními měnami	7
1.3. Evoluce atomových swapů	7
1.4. Jak atomové swapy fungují?	8
1.4.1. Atomové swapy využívající chytré smlouvy	8
1.4.2. Atomové swapy využívající tzv. adaptor signatures	9
1.4.3. On-chain a off-chain atomové swapy	10
1.4.4. Průběh atomových swapů krok za krokem	10
1.5. Výhody a nevýhody atomových swapů	11
1.6. Shrnutí	12
2. Současná regulace proti praní špinavých peněz a financování terorismu	13
2.1. AML regulace z pohledu FATF	13
2.2. Současná AML regulace v Evropské unii	14
2.2.1. Definice virtuální měny	15
2.2.2. Definice povinných osob	16
2.3. Česká AML regulace	17
2.4. Malý závěr	18
3. Rizika virtuálních měn a atomových swapů pro AML regulaci	19
3.1. Praní špinavých peněz	19
3.2. Nezákonné využití virtuálních měn	20
3.3. Je AML regulace virtuálních měn potřebná?	22
3.4. Rizika spojená s virtuálními měnami	23
3.4.1. Rizika spojená s virtuálními měnami v jednotlivých fázích praní špinavých peněz ...	24
3.4.2. Anonymita a sledovatelnost transakcí	25
3.4.3. Decentralizovaná povaha	28
3.4.4. Virtuální měny a financování terorismu	28
3.5. Rizika spojená s atomovými swapy	29

3.5.1. Off-chain atomové swapy	29
3.5.2. DEXs, DApps a DeFi.....	30
3.5.3. Analýza podílu P2P transakcí na trhu s virtuálními měnami a nezákonných aktivitách	31
3.5.4. Co z této analýzy vyplývá?	34
3.6. Shrnutí	35
4. Dopad připravovaných změn AML regulace v Evropské unii na virtuální měny.....	36
4.1. Nařízení o informacích doprovázejících převody peněžních prostředků	38
4.2. AML nařízení	39
4.3. Jsou připravované změny EU AML regulace dostatečné?	41
5. Způsoby řešení rizik s atomovými swapy	42
5.1. Zákaz virtuálních měn – Čína.....	42
5.2. Propojení peněženek s virtuálními měnami s bankovními účty – Jižní Korea.....	43
5.3. Přístup FATF	44
5.3.1. Regulace DEX, DApps a DeFi	45
5.3.2. Red flags	46
5.3.3. Risk based approach a opatření ke zmírnění rizik s atomovými swapy	47
5.3.4. Travel rule	49
5.3.5. Pravidla pro transakce na nebo z nesprávcovských peněženek	50
5.3.6. Míra implementace FATF pravidel	51
5.4. Návrh nové regulace nesprávcovských peněženek – USA.....	51
5.5. Regulace nesprávcovských peněženek – Švýcarsko	52
5.6. Blacklisting.....	52
5.7. Technologické řešení	54
Závěr.....	56
Seznam použitých zkratk.....	58
Seznam použitých zdrojů	60
Atomic swap: riziko pro AML regulaci?, Abstrakt, Klíčová slova	67
Atomic swap: a risk for AML regulation?, Abstract, Keywords	68

Úvod

Od zrodu Bitcoinu v roce 2008 si získalo oblibu velké množství dalších virtuálních měn. Je nepochybné, že se tento vzkvétající ekosystém vyvinul v obrovský finanční trh. Virtuální měny se ve velkém množství obchodují jak s fiat měnami, tak mezi sebou.

Regulátoři a finanční instituce po celém světě pozorují, jak virtuální měny a související platební systémy nabírají na síle, a uznávají, že pravděpodobně představují budoucnost pro platební systémy. Zároveň ale poskytují stále mocnější nástroj pro zločince, teroristy a osoby snažící se vyhnout mezinárodním sankcím. Tím vytvářejí nové jedinečné výzvy z hlediska regulace proti praní špinavých peněz a financování terorismu.

Vzhledem k neustále rostoucímu blockchainovému ekosystému se z interoperability, tedy schopnosti různých blockchainů vzájemně spolupracovat, stala jedna z nejdůležitějších vlastností. Atomové swapy, inteligentní protokoly pro směnu virtuálních měn, umožňují peer-to-peer transakce mezi různými virtuálními měnami, čímž propojují jinak izolované blockchainya a výrazně zvyšují jejich interoperabilitu.

Cílem této práce je zhodnocení rizik, které atomové swapy představují pro AML regulaci, a způsobů, kterými je tato rizika možné řešit.

V první části této práce jsou nejprve stručně popsány pojmy a technologie potřebné k pochopení atomových swapů. Mimo jiné jsou zde popsány distribuované databáze, kryptografické klíče, peněženky a směnárny s virtuálními měnami. Následuje popis evoluce atomových swapů a toho, jak atomové swapy fungují a jaké jsou jejich výhody a nevýhody.

Druhá část analyzuje současnou regulaci proti praní špinavých peněz a financování terorismu z pohledu FATF, Evropské unie a České republiky ve vztahu k virtuálním měnám a atomovým swapům. Zejména se zaměřuje na definici virtuálních měn a povinných osob.

Po pochopení fungování atomových swapů a analýze AML regulace ve vztahu k nim je možné zhodnotit, zda pro ni atomové swapy představují riziko. Tomu se věnuje třetí část této práce. Nejdřív obecně představuje problematiku praní špinavých peněz a využívání virtuálních měn pro nezákonné účely. Nakonec zkoumá rizika, která představují virtuální měny sami o sobě a která představují atomové swapy a technologie, které díky nim nabírají na popularitě. Takovou technologií je například DeFi, neboli softwarový program fungující na blockchainu a poskytující finanční služby s virtuálními aktivy.

Čtvrtá část zkoumá projednávané změny AML regulace v Evropské unii. Zejména jaké dopady budou změny mít na regulaci virtuálních měn a zda adresují rizika spojená s atomovými swapy.

Pátá část uvádí několik regulatorních přístupů k AML regulaci virtuálních měn a zkoumá, zda a jakým způsobem jednotlivé přístupy řeší rizika související s atomovými swapy. Zabývá se zákazem virtuálních měn v Číně, povinností propojit peněženky s virtuálními měnami s bankovními účty v Jižní Koreji, přístupem FATF, regulací peněženek s virtuálními měnami ve Spojených státech amerických a Švýcarsku, metodou zvanou blacklisting, a nakonec technologickými řešeními.

1. Atomové swapy – vymezení pojmů a základní charakteristika

Podle dostupných českých zdrojů se termín atomic swaps překládá jako atomické výměny¹ nebo atomové swapy². V této práci budu dále pro jednotnost používat výraz atomový swap.

První část práce zjednodušeně popisuje (i) pojem atomový swap, (ii) pojmy a technologie s atomovými swapy související, (iii) kde se atomový swap poprvé objevil a jaký byl jeho vývoj v průběhu času, (iv) jak atomové swapy fungují a (v) jaké jsou výhody a nevýhody atomových swapů.

Cílem této práce není přinést podrobné technické vysvětlení atomových swapů a jejich fungování. Jejich popis v této části je proto velmi stručný a omezuje se pouze na základní vysvětlení atomových swapů pro účely zhodnocení rizik spojených s atomovými swapy pro AML regulaci.

1.1. Pojem atomový swap

Atomové swapy známé také jako „atomic cross-chain swaps“ nebo „atomic cross-chain trades“, jsou peer-to-peer inteligentní transakce, které umožňují bezpečnou výměnu dvou různých virtuálních měn bez zapojení jakékoli třetí strany.³

Termín „atomický“ nebo „atomový“ byl převzat z terminologie databázových systémů, kde je atomická transakce omezena na množinu binárních výstupů. Je zaručeno, že transakce nastane buď úplně, nebo vůbec. Atomové swapy eliminují potřebu zprostředkovatele bez rizika, že jedna strana obchod nesplní. Atomové swapy tedy umožňují peer-to-peer výměnu virtuálních měn přímo mezi dvěma uživateli, přičemž oba mají plnou kontrolu nad svými virtuálními měnami, dokud k transakci skutečně nedojde.⁴

Pro lepší pochopení si lze atomový swap ukázat na praktickém příkladu. V tomto příkladu má Anna jeden Bitcoin a přeje si ho vyměnit za deset Litecoinů. Za normálních okolností by Anna musela tuto výměnu uskutečnit prostřednictvím zprostředkovatele, například burzy nebo směnárny virtuálních měn, a zaplatit zprostředkovateli poplatky za uskutečnění výměny. Předpokládejme,

¹ Internetové stránky kurzy.cz [online]. [cit. 2021-11-27].

Dostupné z: <https://www.kurzy.cz/tema/6193233.html>

² Internetové stránky ranking-chwilowek.net [online]. [cit. 2021-11-27].

Dostupné z: <https://cs ranking-chwilowek.net/atomovy-swap-co-to-je-a-jak-to-funguje-57>

³ MIRAZ, Mahdi H. a DONALD, David C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Annals of Emerging Technologies in Computing (AETiC)* [online]. 2019, roč. 3, č. 1 [cit. 2021-11-27]. ISSN 2516-029X. s. 44.

Dostupné z:

https://www.researchgate.net/publication/330041815_Atomic_Crosschain_Swaps_Development_Trajectory_and_Potential_of_Non-monetary_Digital-Token_Swap_Facilities

⁴ Ibid. s. 44.

že v tu stejnou chvíli Petr vlastní deset Litecoinů a chce je vyměnit za jeden Bitcoin. V takovém případě by mohli Anna a Petr prostřednictvím atomového swapu jednoduše vyměnit své mince mezi sebou bez nutnosti zprostředkování výměny zprostředkovatelem.⁵ Podrobnější popis fungování atomových swapů je v kapitole 1.4.

1.2. Stručný popis pojmů a technologií potřebných k pochopení atomových swapů

Před bližším popisem vývoje a fungování atomových swapů je užitečné vyjasnit několik pojmů, se kterými jsou atomové swapy neoddělitelně spojeny. Tato kapitola proto popisuje několik základních pojmů, technologií, služeb a aktorů, které jsou pro pochopení atomových swapů nezbytné.

1.2.1. Virtuální měna

Virtuální měny mohou být buď konvertibilní nebo nekonvertibilní. Konvertibilní virtuální měny mají nějakým způsobem danou ekvivalentní hodnotu k fiat meně. Nekonvertibilní virtuální měny se používají pouze v nějaké oblasti, např. v počítačové hře nebo v zákaznickém programu odměn. Správa virtuálních měn je buď centralizovaná nebo decentralizovaná. Centralizovaná správa je řízená jediným správcem a decentralizovaná je řízená softwarem využívajícím distributed ledger technologii.⁶

Pomocí těchto dichotomií můžeme kategorizovat jednotlivé virtuální měny. Bitcoin, který byl spuštěn roku 2009 je nejstarší a nejznámější virtuální měnou. Je to konvertibilní, decentralizovaná virtuální měna používající kryptografické principy k zajištění integrace transakcí navzdory neexistenci důvěryhodných zprostředkovatelů jako jsou například banky. Od spuštění bitcoinu bylo vytvořeno mnoho variant virtuálních měn s různými funkcemi. Mezi nejznámější patří například Litecoin, Ether nebo Ripple.⁷

⁵ POLICY DEPARTMENT FOR ECONOMIC, SCIENTIFIC ANF QUALITY OF LIFE POLICIES. Cryptocurrencies and blockchain *Legal context and implications for financial crime, money laundering and tax evasion* [online]. 9. 6. 2018 [cit. 2021-11-27]. s. 39.

Dostupné z:

<https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>

⁶ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches* [online]. 2018 [cit. 2021-11-27]. s. 26.

Dostupné z:

https://www.allenoverly.com/global/-/media/sharepoint/publications/publications/en-gb/documents/aml18_allenoverly.pdf?la=en-gb&hash=6D8F26DB73634846A427983AD2F217A7

⁷ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 27.

1.2.2. Distribuované databáze

Distribuovaný ledger (DL) je databáze replikovaných, sdílených a synchronizovaných digitálních dat, která je geograficky rozložena na více webech v síti. Spíše než centrálního správce, kterého mají například tradiční databáze bank, disponují systémem synchronizovaných databází, které poskytují informace o transakcích a jsou viditelné pro kohokoli v síti.⁸

1.2.3. Blockchain

Virtuální měny jako Bitcoin fungují na základě globálního záznamu transakcí známého jako blockchain. Blockchain je zjednodušeně forma DL, která ke svému rozšíření potřebuje vyřešení nového a náhodně vybraného kryptografického klíče. Takový klíč je vyřešen procesem známým jako „hashování“, kterého je dosaženo průběžným výpočetním hádáním všech počítačů v síti, dokud jeden z počítačů v síti neidentifikuje správný klíč. Tím se do existujícího řetězce přidá v chronologickém pořadí nový blok ověřených transakcí opatřený časovým razítkem. Tak jsou dokumentovány veškeré transakce provedené v historii daného blockchainu. Namísto uložení v centrálním systému je blockchain uložen v každém počítačovém uzlu v síti. Tento distribuovaný a zašifrovaný záznam poskytuje jistotu v tomto vzájemně anonymním prostředí.⁹

Blockchain je popisován jako anonymní, ale ne soukromý. Anonymita je vyvozována z toho, že strany provádějící transakci jsou identifikovány pouze pomocí blockchainových adres sloužících jako účty, na kterých může být hodnota přijímána i z nich odesílána. Blockchainovou adresu lze v zásadě vytvořit bez poskytnutí osobních identifikačních údajů.¹⁰

Na druhou stranu blockchain ale není soukromý, protože všechny transakce v DL jsou součástí veřejného záznamu a každá mince je spojena s jedinečnou historií transakcí. Uživatelé, kteří usilují o větší soukromí, mají k dispozici mnoho technologických nástrojů k zastření vztahu mezi jednotlivými adresami blockchainu a identitou stran transakce. Jako protiopatření jsou vyvíjeny čím dál složitější analytické metody, které jsou schopny identifikovat související transakce a přiřadit konkrétní adresy ke konkrétním uživatelům. I dobře peněžně a technologicky vybavení aktéři jsou ovšem limitováni v jejich schopnosti dešifrovat transakční aktivity uskutečňované na blockchainu. To virtuální měny činí velice atraktivní pro osoby zabývající se

⁸ NOCAROVÁ, Michaela. Jaký je rozdíl mezi technologií Blockchain a Distributed Ledger Technology? In: *kryptomagazin* [online]. 4. června 2020. [cit. 2021-11-27].

Dostupné z: <https://kryptomagazin.cz/jaky-je-rozdil-mezi-technologii-blockchain-a-distributed-ledger-technology/>

⁹ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 27.

¹⁰ Ibid. s. 27.

praním špinavých peněz a další subjekty snažící se vyměnit hodnotu mimo dohled formálního finančního sektoru.¹¹

1.2.4. Veřejné a soukromé kryptografické klíče

Systém virtuálních měn funguje odlišně od tradičních finančních systémů. Je často popisovaný jako otevřený, tedy umožňující zakládání účtů nezávisle na jakékoli finanční instituci a bez požadavků na ověření totožnosti. Namísto vedení účtů jako záznamů v centrálních databázích jsou účty virtuálních měn představovány kryptografickým klíčem. Veřejný klíč se používá jako identifikátor účtu (označovaný jako „adresa“) a pomocí soukromého klíče se autorizují platby. Kdokoliv může vytvořit novou dvojici klíčů a používat je k přijímání mincí. Tím pádem může systém fungovat zcela bez centrální autority. Vytváření klíčů je rychlé a levné. Proto mnoho virtuálních měn podporuje jednorázové používání adres.¹²

To znamená, že uživatel může vytvořit nový pár klíčů pokaždé, když obdrží virtuální měnu. Tím se zvyšuje soukromí uživatelů, protože jsou jejich transakce rozděleny mezi mnoho různých účtů. Bez dalších znalostí proto nelze snadno identifikovat adresy patřící stejnému uživateli.¹³

1.2.5. Softwarové a hardwarové peněženky

Virtuální měny nejsou vlastníky drženy v peněženkách v kapse vlastníků. Ve skutečnosti nikdy neopustí síť virtuální měny. Uživatel k nim má přístup prostřednictvím svých kryptografických klíčů. Tyto klíče jsou uloženy v peněženkách virtuálních měn.¹⁴

Softwarová peněženka je softwarová aplikace, která generuje a uchovává soukromé klíče a vytváří a podepisuje transakce s virtuálními měnami.¹⁵ Softwarové peněženky se dělí na „správcovské“ (custodial wallets) a „nesprávcovské“ (non-custodial, self-hosted nebo unhosted wallets) peněženky. Ve správcovských peněženkách je virtuální měna držena třetí stranou ve

¹¹ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 27.

¹² MÖSER, Malte a NARAYANAN, Arvind. *Effective Cryptocurrency Regulation Through Blacklisting* [online], 2019 [cit. 2021-11-27]. s. 3.

Dostupné z:

<https://maltemoeser.de/paper/blacklisting-regulation.pdf>

¹³ Ibid. s. 3.

¹⁴ POCHER, Nadia. Self-hosted wallets: the elephant in the crypto room? In: *kuleuven* [online]. 11. března 2021. [cit. 2021-11-27].

Dostupné z: <https://www.law.kuleuven.be/citip/blog/self-hosted-wallets/>

¹⁵ Internetové stránky btc-slovník.cz [online]. [cit. 2021-11-27].

Dostupné z: <https://btc-slovník.cz/>

prospěch vlastníka. V nesprávcovských peněženkách si vlastník virtuálních měn sám drží své soukromé klíče.¹⁶

Hardwarové peněženky jsou vždy nesprávcovské a obvykle vypadají jako USB paměťové zařízení s obrazovkou a analogovými tlačítky. Pro provedení transakce musí být připojeny k počítači nebo mobilnímu zařízení. Během transakce jsou technicky připojeny k internetu, podepisování transakce soukromými klíči ale probíhá offline v samotné hardwarové peněžence a až poté je transakce odeslána online do blockchainu k potvrzení.¹⁷

1.2.6. Centralizované a decentralizované směnárny s virtuálními měnami

Směnárny s virtuálními měnami za poplatek zprostředkovávají výměnu virtuálních měn mezi sebou, za fiat měny nebo za jiná aktiva.¹⁸ Díky rozšíření atomových swapů se rozšířily decentralizované směnárny s virtuálními měnami (**DEXs**). V rámci decentralizovaných směnáren se obchodníci podílejí na obchodech, které jsou regulovány inteligentními smlouvami obsahujícími protokol atomových swapů. Na rozdíl od centralizovaných směnáren (**CEXs**) jsou DEXs nesprávcovské a obchodníci do nich nemusí vkládat své virtuální měny.¹⁹

1.3. Evoluce atomových swapů

Od prvního představení blockchainu prostřednictvím Bitcoinu v roce 2008 trvalo téměř čtyři roky, než se podařilo vytvořit funkční nezprostředkovanou výměnu mezi různými blockchainy. V červenci roku 2012 Sergio Demian Lerner představil vedoucí návrh peer-to-peer swapu nazvaného "P2PTradeX", známého také jako „wallet-to-wallet trade“. Tento typ transakce ovšem nechával jednu stranu zranitelnou a závislou na chování protistrany.²⁰

¹⁶ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 27.

¹⁷ Internetové stránky platonlife.com [online]. [cit. 2021-11-27].

Dostupné z: <https://platonlife.com/cs/blog/platon-wallet-what-is-a-custodian-wallet/>

¹⁸ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 28.

¹⁹ HAN, Runchao, LIN, Haoyu a YU, Jiangshan. *On the optionality and fairness of Atomic Swaps* [online]. 2019 [cit. 2021-11-27]. s. 1.

Dostupné z:

https://www.researchgate.net/publication/334958051_On_the_optionality_and_fairness_of_Atomic_Swaps

²⁰ MIRAZ, Mahdi H. a DONALD, David C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Annals of Emerging Technologies in Computing (AETiC)*. op. cit. s. 4.

V květnu roku 2013 představil Tier Nolan koncept „Atomic Swaps“²¹, který je považován za první úplný návod pro atomickou transakci probíhající automaticky v binárním jádru příslušných blockchainů buď zcela nebo vůbec a nepodléhající změně v důsledku nepřijetí.²²

Od představení konceptu trvalo téměř další čtyři roky, než se první atomový swap uskutečnil. První známá realizace atomového swapu proběhla 20. září 2017 mezi Decredem a Litecoinem. Od té doby se na trhu objevily další koncepty jako například BarterDEX²³, které dále rozšiřují a pozměňují původní koncept z roku 2013.²⁴

1.4. Jak atomové swapy fungují?

V praxi není výměna pomocí atomového swapu tak jednoduchá, jak by se mohlo zdát z příkladu uvedeného v kapitole 1.1. V praxi taková výměna vyžaduje velké množství znalostí. Například musí být vytvořeno spojení mezi oběma blockchainy jednotlivých virtuálních měn, což vyžaduje implementaci IT protokolu známého jako Lightning Protocol. Kromě toho musí oba blockchainy sdílet stejnou kryptografickou funkci, aby byl atomový swap možný.²⁵

Tato kapitola proto popisuje (i) jak fungují atomové swapy využívající chytré smlouvy, (ii) jak fungují atomové swapy založené na scriptless scripts, (iii) rozdíl mezi on-chain a off-chain atomovými swapy a (iv) průběh atomových swapů krok za krokem.

1.4.1. Atomové swapy využívající chytré smlouvy

Atomové swapy můžeme považovat za funkci, která zajišťuje, že všechny předem stanovené podmínky budou splněny před uskutečněním transakce.²⁶ Původní verze atomových

²¹ NOLAN, Tier. Alt chains and atomic transfers. In: *Bitcoin Forum* [online]. 2. května 2013 [cit. 2021-11-27] Dostupné z: <https://bitcointalk.org/index.php?topic=193281.0>

²² MIRAZ, Mahdi H. a DONALD, David C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Annals of Emerging Technologies in Computing (AETiC)*. op. cit. s. 4.

²³ JL777. BarterDEX – A Practical Native DEX. In: *github* [online]. 5. listopadu 2016. [cit. 2021-11-27].

Dostupné z: <https://github.com/SuperNETorg/komodo/wiki/BarterDEX-%E2%80%93-A-Practical-Native-DEX>

²⁴ MIRAZ, Mahdi H. a DONALD, David C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Annals of Emerging Technologies in Computing (AETiC)*. op. cit. s. 4.

²⁵ POLICY DEPARTMENT FOR ECONOMIC, SCIENTIFIC AND QUALITY OF LIFE POLICIES. Cryptocurrencies and blockchain *Legal context and implications for financial crime, money laundering and tax evasion*. op. cit. s. 41.

²⁶ Why Atomic Swaps Are Revolutionizing Decentralized Crypto Trading. In: *learn.bybit* [online]. 12. října 2021. [cit. 2021-11-27].

Dostupné z: <https://learn.bybit.com/blockchain/what-are-atomic-swaps/>

swapů využívá chytré smlouvy nazývané HTLCs (Hash Time-Lock Contracts).²⁷ Tyto chytré smlouvy umožňují kombinaci kryptografické hashovací funkce a časové prodlevy.²⁸

Chytré smlouvy vyžadují úspěšné vygenerování hashe, který může být ověřen mezi zúčastněnými stranami nebo sítí. V atomovém swapu poháněném HTLCs musí obě strany pomocí kryptografické hashovací funkce potvrdit přijetí prostředků v určitém časovém období. Pokud tak obě strany nebo některá z nich neučiní, celý obchod se zruší a nic se nevymění. Atomový swap tak eliminuje rizika stran transakce a zajišťuje, že je celý proces automatický.²⁹

Dvě strany se tedy například mohou dohodnout na stanovení hodinového časového omezení pro atomový swap. Pokud některá ze stran nesplní všechny podmínky obchodu do jedné hodiny, smlouva pošle virtuální měnu zpět původnímu vlastníkovi.³⁰

HTLCs na podkladové blockchainya kladou určité požadavky. Zaprvé oba blockchainya musí umožňovat vytvoření hash locks (hashovacích zámků) a zadruhé musí podporovat timelocks (časové zámky).³¹ Hashovací zámek zajišťuje, že je transakce dokončena ve chvíli, kdy obě strany předloží kryptografické důkazy ze svých stran transakce. Časový zámek je bezpečnostní mechanismus, který stanoví konečný termín pro danou transakci. Tím zaručuje, že dané virtuální měny budou účastníkům transakce vráceny v případě, že transakce nebude z jednoho nebo více důvodů ve stanovené lhůtě dokončena.³²

1.4.2. Atomové swapy využívající tzv. adaptor signatures

Postupem času a díky vývoji v technologii získává na popularitě nový způsob atomových swapů používajících tzv. adaptor signatures (označované též jako Scriptless Scripts). Atomové swapy používající adaptor signatures mají oproti atomovým swapům užívajícím HTLCs několik výhod. Těmi jsou zaprvé nižší cena za jednotlivé atomové swapy a zadruhé fakt, že při transakcích nemusí být použit stejný hash na každém řetězci a transakce proto spolu nemohou být propojeny.³³

²⁷ HOENISCH, Philipp a PINO, Lucas Soriano del. *Atomic Swaps between Bitcoin and Monero* [online]. 2021 [cit. 2021-11-27]. s. 2.

Dostupné z: https://www.researchgate.net/publication/348928221_Atomic_Swaps_between_Bitcoin_and_Monero

²⁸ MIRAZ, Mahdi H. a DONALD, David C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Annals of Emerging Technologies in Computing (AETiC)*. op. cit. s. 7.

²⁹ MIRAZ, Mahdi H. a DONALD, David C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Annals of Emerging Technologies in Computing (AETiC)*. op. cit. s. 7.

³⁰ Why Atomic Swaps Are Revolutionizing Decentralized Crypto Trading. In: *learn.bybit*. op. cit.

³¹ HOENISCH, Philipp; PINO, Lucas, *Atomic Swaps between Bitcoin and Monero*. op.cit. s. 2.

³² Why Atomic Swaps Are Revolutionizing Decentralized Crypto Trading. In: *learn.bybit*. op. cit.

³³ HOENISCH, Philipp; PINO, Lucas, *Atomic Swaps between Bitcoin and Monero*. op.cit. s. 2.

1.4.3. On-chain a off-chain atomové swapy

V závislosti na tom, kde jsou transakce prováděny, mohou být atomové swapy rozděleny na on-chain a off-chain atomové swapy.³⁴ U on-chain atomových swapů dochází k transakci přímo v blockchainech jednotlivých virtuálních měn.³⁵ Na rozdíl od on-chain atomových swapů probíhají off-chain atomové swapy na samostatné vrstvě blockchainu. Příkladem takové samostatné vrstvy je například Lightning Network blockchainu Bitcoinu. Díky použití Lightning Networku jsou off-chain atomové swapy okamžité.³⁶

1.4.4. Průběh atomových swapů krok za krokem

V této podkapitole je rozebrán atomový swap od začátku do konce, krok za krokem:

- Krok č. 1: První strana vygeneruje adresu a uloží na ní virtuální měnu, kterou chce vyměnit. Později je vygenerován a zahashován přístupový kód známý jako preimage (předobraz), který následně tuto transakci uzavře.
- Krok č. 2: První strana pošle vygenerovaný předobraz druhé straně, aby si ověřila, že virtuální měna byla na adrese uložena.
- Krok č. 3: Druhá strana uloží svou virtuální měnu na novou adresu se stejným hashem vygenerovaným v kroku č. 1.
- Krok č. 4: Jakmile druhá strana uloží virtuální měnu na novou adresu, první strana jí může odemknout pomocí tajného kódu použitého při uložení její virtuální měny v kroku č. 1.
- Krok č. 5: Odemčením adresy první stranou v kroku č. 4, a tedy získáním virtuální měny uložené druhou stranou, získá druhá strana tajný kód k odemčení adresy vytvořené první stranou v kroku č. 1. Druhá strana dokončí proces atomového swapu odblokováním vkladu provedeného první stranou.³⁷

V příkladu uvedeném v kapitole 1.1., ve kterém Anna chce vyměnit svůj 1 Bitcoin za 10 Litecoinů Petra, by atomový swap probíhal následovně. Anna by nejdřív uložila Bitcoin na bezpečnou HTLC adresu. Při vytváření kontraktu Anna vygeneruje přístupový klíč a s Petrem bude sdílet kryptografický hash. Petr ale zatím nemá přístup k uloženému Bitcoinu, protože zná pouze hash, nikoliv přístupový klíč.³⁸

³⁴ HOENISCH, Philipp; PINO, Lucas, *Atomic Swaps between Bitcoin and Monero*. op.cit. s. 5.

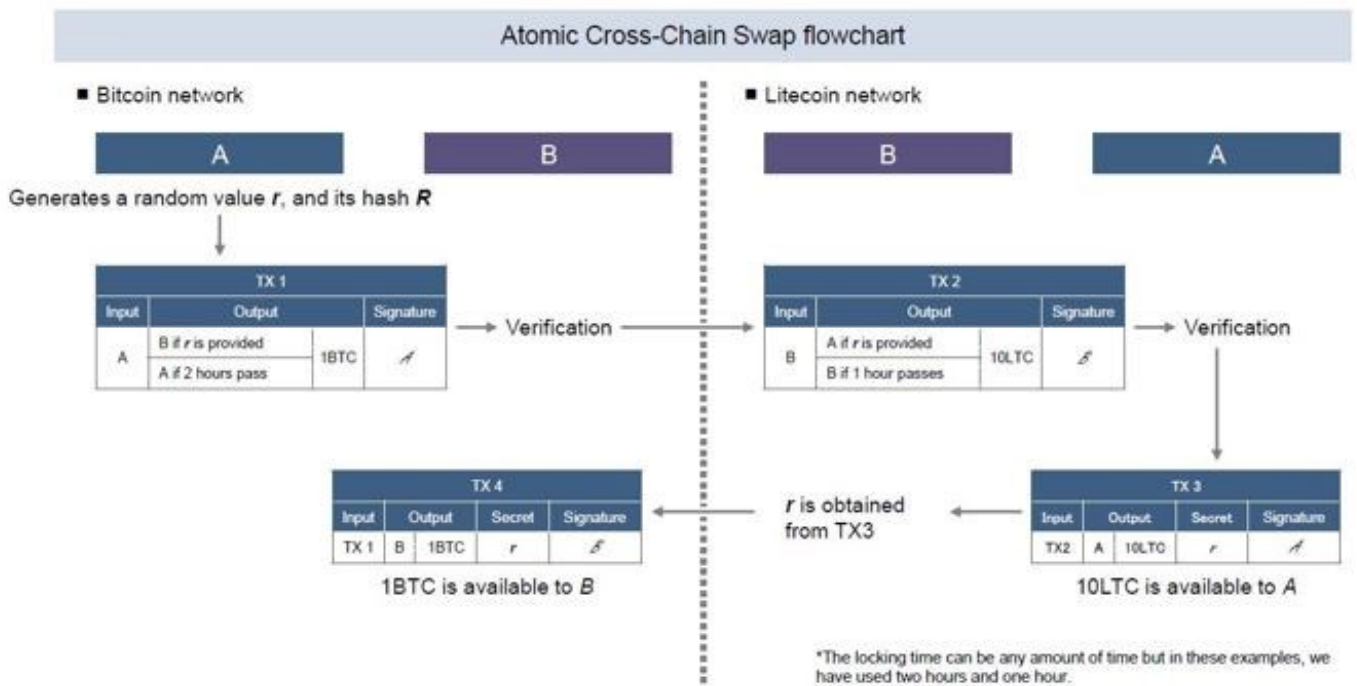
³⁵ Ibid. s. 6.

³⁶ Ibid. s. 5.

³⁷ Why Atomic Swaps Are Revolutionizing Decentralized Crypto Trading. In: *learn.bybit*. op. cit.

³⁸ HAN, Runchao, LIN, Haoyu a YU, Jiangshan. *On the optionality and fairness of Atomic Swaps*. op. cit. s. 2.

Petr poté vytvoří další bezpečnou HTLC adresu pomocí hashe poskytnutého Annou a uloží na ní své Litecoiny. K tomu, aby Anna mohla vybrat Petrem uložené Litecoiny, potřebuje stejný přístupový klíč, který byl vygenerovaný při uložení jejího Bitcoinu na jí vytvořenou adresu. Tím, že Anna vybere Petrem uložené Litecoiny, Petr získá přístupový klíč k Bitcoinu uloženém Annou a může je tím pádem vybrat.³⁹ Průběh transakce je popsán na obrázku č. 1.



Obrázek č. 1: Grafické znázornění ilustračního příkladu off-chain atomového swapu z kapitoly 1.1.⁴⁰

Transakce probíhají postupně nebo, pokud nejsou splněny podmínky (například není splněný časový limit stanovený stranami), neproběhne žádná transakce a vše se vrátí do původního stavu.

1.5. Výhody a nevýhody atomových swapů

Atomové swapy přináší celou řadu výhod. Zaprvé hrají důležitou roli u decentralizovaných směnárů s virtuálními měnami. Do atomových swapů DEXs operovali pouze na jednom blockchainu, díky atomovým swapům mohou DEXs zprostředkovávat i transakce mezi několika

³⁹ HAN, Runchao, LIN, Haoyu a YU, Jiangshan. *On the optionality and fairness of Atomic Swaps*. op. cit. s. 2.

⁴⁰ FINANCIAL SERVICES AGENCY. *Research on privacy and traceability of emerging blockchain based financial transactions* [online]. 20. března 2019. [cit. 2021-11-27]. s. 62-63.

Dostupné z: https://www.fsa.go.jp/en/policy/bgin/ResearchPaper_MRI.pdf

blockchainy. Dále jsou díky atomovým swapům menší poplatky za transakce a je zkrácena doba transakcí.⁴¹

Další výhodou atomových swapů je fakt, že uživatelé mají své virtuální měny po celou dobu transakce na svých peněženkách a neposílají je žádné další entitě. Tím je vyloučena možnost krádeže nebo podvodu na úrovni CEXs. Ty jsou kvůli akumulaci velkého množství virtuálních měn cílem mnohých hackerských útoků.⁴²

Nevýhodou atomových swapů je, že umožňují pouze transakce mezi virtuálními měnami mezi sebou, ale neumožňují transakce mezi fiat měnami a virtuálními měnami. Nevýhoda z AML hlediska je, že transakce učiněné pomocí off-chain atomového swapu jsou špatně sledovatelné.⁴³

1.6. Shrnutí

Zjednodušeně řečeno atomové swapy představují model peer-to-peer transakcí s virtuálními měnami. Tento model transakcí umožňuje vlastníkům virtuálních měn dohodnout se na ceně a výměně virtuálních měn, aniž by k tomu potřebovali zprostředkování důvěryhodnou třetí stranou. Pokud během transakce dojde k nějaké chybě nebo pokud se v průběhu transakce některá ze stran rozhodne v transakci nepokračovat, vše se vrátí do původního stavu a každá ze stran obdrží své virtuální mince zpět.⁴⁴

⁴¹ Why Atomic Swaps Are Revolutionizing Decentralized Crypto Trading. In: *learn.bybit*. op. cit.

⁴² ERGUN, Huseyin, RAZBONYALI, Mesut, GUVENOGLU, Erdal a RAZBONYALI, Can. Distributed Atomic Swap on Cryptocurrencies. *Computer Engineering and Intelligent Systems* [online]. 2020, roč. 11, č. 4 [cit. 2021-11-27]. ISSN 2222-2863. s. 37.

Dostupné z: <https://www.researchgate.net/publication/344158341>

⁴³ Why Atomic Swaps Are Revolutionizing Decentralized Crypto Trading. In: *learn.bybit*. op. cit.

⁴⁴ ERGUN, Huseyin, RAZBONYALI, Mesut, GUVENOGLU, Erdal a RAZBONYALI, Can. Distributed Atomic Swap on Cryptocurrencies. *Computer Engineering and Intelligent Systems*. op. cit. s. 43

2. Současná regulace proti praní špinavých peněz a financování terorismu

Druhá část této práce zkoumá stávající AML regulaci FATF, Evropské unie a České republiky ve vztahu k virtuálním měnám a atomovým swapům. Pro odpověď na otázku, zda jsou atomové swapy rizikem pro AML regulaci, je důležité zejména jak AML regulace definuje virtuální měny a povinné osoby, které jsou podle dané regulace nositeli povinností.

Virtuálními měnami a riziky s nimi spojenými se zabývají velké mezinárodní organizace. To je dané vzhledem ke globální povaze virtuálních měn nerespektujících hranice jednotlivých právních řádů. Mezinárodní organizace, mimo jiné např. FATF, vydávají v souvislosti s virtuálními měnami a jejich AML regulací zprávy a doporučení, které státy i Evropská unie implementují do svých právních řádů.⁴⁵

2.1. AML regulace z pohledu FATF

Finanční akční výbor (FATF) je nezávislý mezivládní orgán, který vyvíjí a podporuje opatření na ochranu globálního finančního systému před praním špinavých peněz, financováním terorismu a financováním šíření zbraní hromadného ničení. Doporučení vydávaná FATF jsou uznávána jako celosvětový standard pro boj proti praní špinavých peněz a financování terorismu.⁴⁶

Virtuální aktivum je podle FATF digitální reprezentace hodnoty, se kterou lze digitálně obchodovat nebo kterou lze převádět a může být použita k platebním nebo investičním účelům. Virtuální aktiva v sobě nezahrnují digitální reprezentaci fiat měn, cenných papírů a jiných finančních aktiv uvedených jinde v dokumentu⁴⁷ FATF, který obsahuje definici virtuálního aktiva.⁴⁸

Poskytovatelem služeb s virtuálními aktivy se podle FATF rozumí jakákoli fyzická nebo právnická osoba, která jako podnikání provozuje jednu nebo více z následujících činností:

- směna mezi virtuálními aktivy a fiat měnami;
- směna mezi jednou nebo více formami virtuálních aktiv;

⁴⁵ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition* [online]. srpen 2018 [cit. 2021-11-27]. ISSN 2631-2999. s. 163.

Dostupné z:

https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

⁴⁶ Internetové stránky FATF [online]. [cit. 2021-11-27].

Dostupné z: <https://www.fatf-gafi.org/about/>

⁴⁷ FATF. *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* [online]. 16. února 2012, říjen 2021. [cit. 2021-11-27].

Dostupné z: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

⁴⁸ Ibid. s. 130.

- převod virtuálních aktiv;
- úschova a/nebo správa virtuálních aktiv nebo nástrojů umožňujících kontrolu nad virtuálními aktivy; a
- účast na finančních službách a poskytování finančních služeb souvisejících s nabídkou a/nebo prodejem virtuálního aktiva.⁴⁹

Peer-to-peer transakce FATF definuje jako transakce virtuálních aktiv prováděné bez využití nebo zapojení poskytovatele služeb s virtuálními aktivy nebo jiného povinného subjektu. Například se jedná o transakce mezi dvěma nesprávcovskými peněženkami jejichž uživatelé jednají svým vlastním jménem. Takové transakce nejsou podle úpravy FATF výslovně předmětem AML/CFT pravidel. To je dáno tím, že FATF obecně ukládá povinnosti spíše zprostředkovatelům než samotným fyzickým osobám (s výjimkou například cílených finančních sankcí).⁵⁰

FATF zastává extenzivní výklad definici virtuálních aktiv a poskytovatelů služeb s virtuálními aktivy. Dále zastává názor, že do většiny platform, které se prohlašují za P2P platformy, je alespoň v nějaké fázi vývoje nebo uvedení produktu na trh zapojena entita, která spadá pod definici poskytovatele služeb s virtuálními aktivy. Proto by se jurisdikce platform, které se prohlašují za P2P platformy měly zaměřit na jejich činnost, a ne na jejich označení nebo podnikatelský model.⁵¹

Můžeme pozorovat určitou harmonizaci v souladu s pohledem FATF, že by se na virtuální měny měly vztahovat stejná pravidla jako na fiat měny. Většina evropských zemí vydala pravidla nebo pokyny, které podrobily výměnu virtuálních měn za fiat měny AML regulaci a s ní spojenými povinnostmi.⁵²

2.2. Současná AML regulace v Evropské unii

Na evropské úrovni se virtuálními aktivy poprvé zabývala Evropská centrální banka (ECB) ve své zprávě o virtuálních měnách z roku 2012⁵³. V ní mimo jiné uvedla, že míra anonymity

⁴⁹ FATF. *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. op. cit. s. 130.

⁵⁰ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers* [online]. 28. října 2021. [cit. 2021-11-27]. s. 18.

Dostupné z:

<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>

⁵¹ Ibid. s. 35.

⁵² POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe. Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 167.

⁵³ ECB. *Virtual Currency Schemes* [online]. říjen 2012. [cit. 2021-11-27].

Dostupné z: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

poskytovaná virtuálními měnami může představovat rizika v oblasti praní špinavých peněz a financování terorismu. Regulace virtuálních měn by proto podle ECB tato rizika mohla zmírnit nebo přinejmenším snížit motivaci teroristů, zločinců a osob zabývajících se praním špinavých peněz, využívat virtuální měny k nezákonným účelům.⁵⁴

V roce 2014 Evropský orgán pro bankovníctví (**EBA**) vydala formální stanovisko k virtuálním měnám.⁵⁵ V něm uvedla, že virtuální měny kvůli potenciálním rizikům spojeným s praním špinavých peněz a financování terorismu představují vysoké riziko pro finanční integritu Evropské unie.⁵⁶ V roce 2015 Evropská unie přijala IV AML směrnici, která implementovala doporučení⁵⁷ FATF. Téma virtuálních měn a jejich poskytovatelů ale přišlo v projednávacím procesu IV AML směrnice příliš pozdě. Proto v ní virtuální měny ani jejich poskytovatelé nebyly vůbec zahrnuty.⁵⁸

Evropská komise si uvědomovala rizika vyplývající z toho, že poskytovatelé služeb s virtuálními aktivy a poskytovatelé virtuálních peněženek nemají v Evropské unii povinnost identifikovat podezřelou činnost.⁵⁹ V roce 2016 proto Evropská komise navrhla změnu IV AML směrnice, která se mimo jiné zaměřovala na řešení rizik spojených s virtuálními měnami. V AML směrnice byla v Evropské unii přijata v roce 2018 a rozšířila oblast působnosti IV AML směrnice o poskytovatele služeb s virtuálními aktivy a poskytovatele virtuálních peněženek.⁶⁰

2.2.1. Definice virtuální měny

Dodnes neexistuje jednotná celosvětová definice pojmu „kryptoměna“ nebo „virtuální měna“. V roce 2012 ECB definovala virtuální měny jako "*druh neregulovaných digitálních peněz,*

⁵⁴ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe. Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition. op. cit. s. 167.*

⁵⁵ EBA. *EBA Opinion on 'virtual currencies'* [online]. 4. července 2014. [cit. 2021-11-27].

Dostupné z:

<https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1>

⁵⁶ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe. Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition. op. cit. s. 167.*

⁵⁷ FATF. *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.* Op. cit.

⁵⁸ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe. Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition. op. cit. s. 167.*

⁵⁹ Směrnice Evropského parlamentu a rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU. Odstavec 9 preambule.

⁶⁰ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe. Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition. op. cit. s. 167.*

kteře jsou vydávány a obvykle kontrolovány jejich tvůrci a používány a přijímány mezi členy určité virtuální komunity".⁶¹

EBA potom v roce 2014 definoval virtuální měny jako „digitální vyjádření hodnoty, které není vydáváno centrální bankou nebo orgánem veřejné moci, ani není nutně spojeno s fiatovou měnou, ale je přijímáno fyzickými nebo právníckými osobami jako platební prostředek a může být převáděno, uchovááno nebo elektronicky obchodováno“.⁶²

S cílem zajistit společný regulační přístup se Evropská unie rozhodla prostřednictvím V AML směrnice přijmout definici virtuální měny odvozenou ze zprávy vydané FATF.⁶³ Virtuální měny V AML směrnice definuje jako: „digitální reprezentaci hodnoty, která není vydána či garantována centrální bankou ani orgánem veřejné moci, není nutně spojena se zákonně stanovenou měnou a nemá právní status měny či peněz, je však fyzickými nebo právníckými osobami přijímána jako prostředek směny a může být elektronicky převáděna, uchováána a obchodována.“⁶⁴ Vzhledem k obsáhlosti této definice spadá do působnosti V AML směrnice většina forem virtuálních měn.⁶⁵

2.2.2. Definice povinných osob

Okruh povinných osob byl V AML směrnicí rozšířen o (i) poskytovatele směnářských služeb mezi virtuálními měnami a měnami s nuceným oběhem a (ii) poskytovatele virtuálních peněženek.⁶⁶ Na poskytovatele směnářských služeb mezi virtuálními měnami mezi sebou se ovšem V AML směrnice nevztahuje.⁶⁷

Některé transakce mezi virtuálními měnami ovšem mohou spadat do působnosti V AML směrnice, pokud jsou uskutečněny poskytovateli virtuálních peněženek. Těmi jsou podle V AML směrnice subjekty poskytující služby, jejichž cílem je ochraňovat jménem klientů soukromé šifrovací klíče za účelem držení, uchováání a převodu virtuálních měn.⁶⁸

⁶¹ ECB. *Virtual Currency Schemes*. op. cit. s. 13.

⁶² EBA. *EBA Opinion on 'virtual currencies'*. op. cit. s. 11.

⁶³ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 164.

⁶⁴ Čl. 1 odst. 2 písm. d) V AML směrnice.

⁶⁵ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 164.

⁶⁶ Čl. 1 odst. 1 písm. c) V AML směrnice.

⁶⁷ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 168.

⁶⁸ Čl. 1 odst. 2 písm. d) V AML směrnice.

Definice zahrnuje pouze poskytovatele správcovských peněženek. Těmi jsou poskytovatelé, kteří mají prostřednictvím soukromého kryptografického klíče kontrolu nad peněženkami zákazníků a v nich uloženými aktivy. Poskytovatelé softwarových nesprávcovských peněženek a hardwarových peněženek, kteří poskytují tyto služby s virtuálními měnami bez kontroly nad soukromými kryptografickými klíči uživatelů, do působnosti V AML směrnice nespádají.⁶⁹

2.3. Česká AML regulace

Český zákonodárce předběhl evropskou regulaci a definici virtuálních aktiv zahrnul do AML zákona již zákonem č. 183/2017⁷⁰ s účinností od 1. ledna 2017. Tato definice byla obsažena v § 2 odst. 1 písm. l) AML zákona a stanovila, že virtuální měny jsou „*elektronicky uchovávané jednotky bez ohledu na to, zda mají nebo nemají emitenta, a které nejsou peněžním prostředkem podle zákona o platebním styku, ale jsou přijímány jako platby za zboží nebo služby i jinou osobou odlišnou od jejího emitenta*“.⁷¹

Tato definice ale později neodpovídala definici uvedené v V AML směrnici. Proto byla změněna novelou AML zákona⁷² s účinností od 1. ledna 2021 implementující V AML směrnici. Nyní je definice virtuálního aktiva obsažena v § 4 odst. 9 AML zákona a zní následovně:

„Virtuálním aktivem se pro účely tohoto zákona rozumí elektronicky uchovatelná nebo převoditelná jednotka, která je

a) způsobilá plnit platební, směnnou nebo investiční funkci, bez ohledu na to, zda má nebo nemá emitenta, pokud se nejedná o

- 1. cenný papír, investiční nástroj, nebo peněžní prostředek podle zákona o platebním styku,*
- 2. jednotku podle § 3 odst. 3 písm. c) bodů 4 až 7 zákona o platebním styku, nebo*
- 3. jednotku, kterou je prováděna platba podle § 3 odst. 3 písm. e) zákona o platebním styku, nebo*

⁶⁹ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 168.

⁷⁰ Zákon č. 183/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích.

⁷¹ MARTINÍK, Pavel. *Aktuální otázky AML regulace* [online]. 16. prosince 2019. [cit. 2021-11-27].

Dostupné z: <https://advokatnidenik.cz/2019/12/16/aktualni-otazky-aml-regulace/>

⁷² § 2 odst. 1 písm. l) AML zákona

*b) jednotkou podle písmene a) bodu 2 a kterou lze v konečném důsledku zaplatit pouze za úzce vymezený okruh zboží nebo služeb, který zahrnuje elektronicky uchovatelnou nebo převoditelnou jednotku podle písmene a).*⁷³

Povinnou osobou pro účely AML zákona i po novele AML zákona zůstává „osoba poskytující služby spojené s virtuálním aktivem“.⁷⁴ AML zákon specifikuje osobu poskytující služby s virtuálním aktivem v § 4 odst. 8 kde stanovuje tuto definici: „osoba, která jako předmět své podnikatelské činnosti kupuje, prodává, uchovává, pro jiného spravuje, převádí nebo zprostředkovává nákup nebo prodej virtuálního aktiva, poskytuje finanční služby týkající se nabídky nebo prodeje virtuálního aktiva, případně poskytuje jiné obdobné služby spojené s virtuálním aktivem.“⁷⁵

Oproti původní verzi přibylo v definici osob poskytujících služby s virtuálním aktivem převádění virtuálních aktiv a taktéž poskytování finančních služeb týkajících se nabídky nebo prodeje virtuálních aktiv. Převáděním virtuálních aktiv lze mimo jiné chápat i směnu virtuálních aktiv mezi sebou. Definice obsažená v AML zákoně je tedy širší než definice v V AML směrnici.

2.4. Malý závěr

Představují za současné úpravy atomové swapy riziko pro AML regulaci? Atomové swapy jsou modelem peer-to-peer transakcí dvou virtuálních měn. Z toho důvodu by mohly sloužit jako prostředek k legalizaci výnosů z trestné činnosti nebo financování terorismu. Jedním ze způsobů zamezení tohoto rizika je AML regulace.

Evropská AML regulace na směnu dvou virtuálních měn téměř (s výjimkou směny virtuálních měn uskutečňovanou poskytovateli správcovských peněženek) nedopadá, jelikož mezi povinné osoby neřadí poskytovatele směnářenských služeb mezi virtuálními měnami mezi sebou. Povinnými osobami jsou pouze poskytovatelé směnářenských služeb mezi virtuálními měnami a fiat měnami. AML regulace v českém právním řádu je oproti evropské úpravě rozsáhlejší a mezi povinné osoby řadí i osoby zprostředkující směnu virtuálních aktiv mezi sebou.

Do působnosti AML regulace FATF, EU ani České republiky ovšem nespádají peer-to-peer transakce dvou virtuálních měn. To znamená, že jsou atomové swapy potenciálním rizikem pro AML regulaci. Jestli atomové swapy představují reálná, a ne pouze potenciální, rizika, je rozebráno v následující části této práce.

⁷³ § 4 odst. 9 AML zákona

⁷⁴ § 2 odst. 1 písm. l) AML zákona

⁷⁵ § 4 odst. 8 AML zákona

3. Rizika virtuálních měn a atomových swapů pro AML regulaci

Tato část má za cíl objasnit jaká rizika virtuální měny a atomové swapy představují pro praní špinavých peněz a financování terorismu. Proto vysvětluje (i) jak probíhá proces praní špinavých a jeho jednotlivé fáze, (ii) jaká je míra využívání virtuálních měn k nezákonným účelům, (iii) jestli je AML regulace virtuálních měn potřebná, (iv) jaká rizika jsou spojená s virtuálními měnami, a (v) nakonec jakou roli v tom všem hrají atomové swapy a jaká rizika představují.

3.1. Praní špinavých peněz

Praní špinavých peněz je definováno jako metoda, kterou zločinci využívají k zamaskování zdroje nelegálně získaných peněz. Tato metoda zahrnuje proces získávání nelegálních peněz, který způsobuje mnoho neblahých dopadů na ekonomiku tím, že zvyšuje kriminalitu a korupci a negativně ovlivňuje a oslabuje finanční instituce.⁷⁶

Úřad Spojených národů pro drogy a trestnou činnost (UNODC) uvedl, že každý rok činí objem vypraných peněz 2-5 % celosvětového HDP nebo 800 miliard až 2 biliony amerických dolarů. Praní špinavých peněz podporuje další trestné činy včetně obchodu s drogami, pašování, obchodu se zbraněmi a financování terorismu.⁷⁷

Z největších případů praní špinavých peněz lze zmínit dvě situace z případových studií FATF. První je případ, ve kterém Altaf Khanani vypral miliardy dolarů, z nichž financoval nelegální obchody s drogami, zbraněmi a mnoho teroristických skupin. Podobně byly v jiném případě vyprány peníze na podporu trestního řízení v Nigérii, kde tato osoba získala finanční prostředky a rozdělila je na více účtů pomocí 12 podvodných bankovních převodů během šesti týdnů.⁷⁸

Praní špinavých peněz se dělí do tří fází: (a) umístění, (b) vrstvení a (c) integrace. Tyto fáze mohou probíhat současně nebo postupně. Tři fáze praní špinavých peněz mají za cíl zahrnutí nezákonně získaných prostředků do ekonomického cyklu jako by se jednalo o zákonně získané prostředky.⁷⁹

⁷⁶ SHARMA, Avin M. *Cryptocurrency and financial risks* [online]. prosinec 2020. [cit. 2021-11-27]. s. 36.

Dostupné z: <https://digitalcommons.liberty.edu/doctoral/2791/>

⁷⁷ Ibid. s. 36.

⁷⁸ Ibid. s. 25.

⁷⁹ Ibid. s. 37.

Fáze č. 1 – Umístění

V první fázi jde o umístění nelegálně získaných prostředků zpět do legálního finančního systému. Toho lze docílit převedením finančních prostředků do vhodné formy a jejich vložením do finančního toku, aby nevzniklo podezření donucovacích orgánů.⁸⁰

Fáze umístění je však nutná pouze v případě, že získané peněžní prostředky budou vloženy do finančního systému. Použití nelegálně získaných peněz například k nákupu zbraní či dávání úplatků krok umístění nevyžaduje. Peníze v takových případech vůbec nemusí procházet bankami ani žádnými finančními institucemi.⁸¹

Fáze č. 2 – Vrstvení

Druhá fáze má za cíl, aby byly nelegálně získané prostředky nevystopovatelné. Tato fáze se nazývá vrstvení, protože se v ní vytváří vrstvy finančních transakcí. Tyto vrstvy komplikují sledovatelnost peněz, aby byl skryt zdroj finančních prostředků. Jakmile je ukončena fáze umístění, druhá fáze odděluje nelegální peníze tím, že zakrývá jejich stopu a ztěžuje tím regulátorům vysledování zdroje peněz.⁸²

Fáze č. 3 - Integrace

Poslední fáze nazývaná integrace pomáhá přesunout nelegálně získané peníze zpět do normální ekonomiky, aby mohly být využité například k podnikání či investování. Mezi integrační metody patří například obchodování s nemovitostmi, podvodné půjčky či předkládání falešných faktur.⁸³

3.2. Nezákonné využití virtuálních měn

Virtuální měny jsou mimo jiné ideálním platebním prostředkem pro nákup nelegálního zboží a služeb od narkotik, orgánů, dětské pornografie a dalšího sortiment nabízeného na dark netu až po obchodování s lidmi. Jedním z nepozoruhodnějších internetových trhů s takovými druhy zboží byl tzv. Silk Road na němž všechny transakce probíhaly prostřednictvím Bitcoinu.⁸⁴ Mimo to jsou virtuální měny využívány k daňovým únikům, vyhýbání se sankcím nebo investičním podvodům.⁸⁵

⁸⁰ SHARMA, Avin M. *Cryptocurrency and financial risks*. op. cit. s. 37.

⁸¹ Ibid. s. 37.

⁸² Ibid. s. 38.

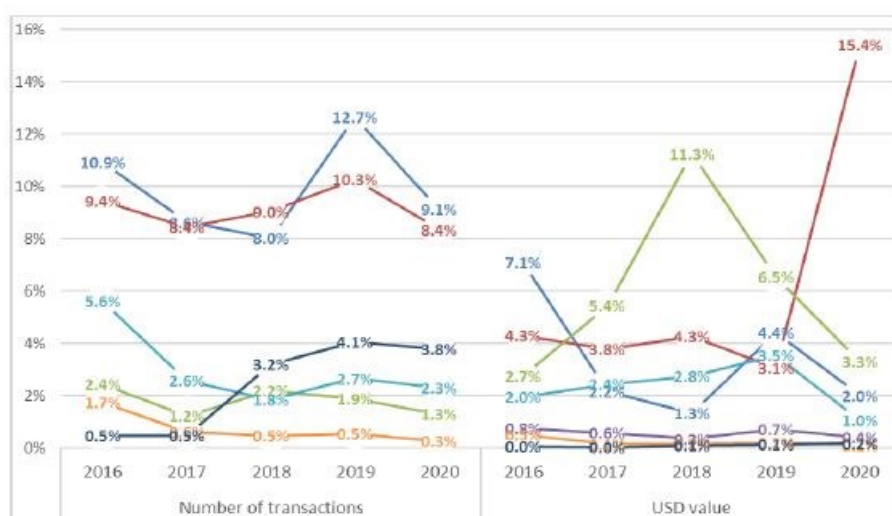
⁸³ Ibid. s. 38.

⁸⁴ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 31.

⁸⁵ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 22.

Společnost Chainalysis, která pomocí analýzy dat sleduje transakce s virtuálními měnami, uvádí, že kriminální subjekty v roce 2019 převedly na směnárny Bitcoinu v hodnotě 2,8 miliard dolarů. To byl víc jak dvojnásobný nárůst oproti 1 miliardě dolarů v roce 2018.⁸⁶

Do druhého přezkumu FATF norem poskytlo šest analytických společností údaje o transakcích Bitcoinu, které označily za nezákonné. Grafy č. 1 ukazují podíl identifikovaných nezákonných transakcí v procentuálním poměru k počtu všech transakcí a k hodnotě všech transakcí v USD v letech 2016-2020 pro Bitcoin.⁸⁷



Grafy č. 1: Procentuální podíl nezákonných transakcí v poměru ke všem provedeným transakcím s Bitcoinem v letech 2016-2020.⁸⁸

Údaje poskytnuté jednotlivými společnostmi se od sebe velmi liší a nevykazují jasný trend zvyšování nebo snižování počtu nezákonných transakcí. Všechny společnosti identifikovaly určitý podíl nezákonné činnosti v oblasti bitcoinů v letech 2016-2020. K tomu je nutné podotknout, že se jedná pouze o údaje, které společnosti byly schopné identifikovat jako nezákonné na základě seznamů známých nebo podezřelých nezákonných adres. Pokud je tento soubor podezřelých adres neúplný, podíl transakcí považovaných za nezákonné bude spíše podhodnocený. Poskytnuté údaje se také týkají především nezákonné činnosti, které mají počátek ve virtuálních aktivech (např. platby výkupného, darknetové trhy, podvody a investiční podvody a hackerské útoky). Tyto údaje obecně nezahrnují ML/TF aktivity, při nichž jsou virtuální aktiva využívána k praní výnosů

⁸⁶ ORCUTT, Mike. Criminals laundered \$2.8 billion in 2019 using crypto exchanges, finds a new analysis. In: *technologyreview* [online]. 16. ledna 2020. [cit. 2021-11-27].

Dostupné z:

<https://www.technologyreview.com/2020/01/16/130843/cryptocurrency-money-laundering-exchanges/>

⁸⁷ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op.cit. s. 26.

⁸⁸ Ibid. s. 27.

z trestné činnosti, které mají původ ve fiat měně (např. využívání virtuálních aktiv k praní výnosů z prodeje nelegálních drog v hotovosti).⁸⁹

Podle druhého přezkumu FATF norem z července 2021 je ovšem hodnota virtuálních aktiv zapojených do dosud zjištěných případů praní peněz a financování terorismu ve srovnání s případy využívajícími tradičnější finanční služby a produkty stále relativně nízká.⁹⁰

3.3. Je AML regulace virtuálních měn potřebná?

Vzhledem k rychlému vývoji virtuálních měn si regulační orgány a finanční instituce po celém světě uvědomují, že virtuální měny a jejich podkladové protokoly pravděpodobně představují budoucnost platebních systémů. Zároveň ale podle nich slouží zločincům a osobám financujícím terorismus jako nástroj k přesunu a uchování nezákonných finančních prostředků mimo dosah donucovacích orgánů. V důsledku toho vytvářejí nová rizika a výzvy v oblasti AML regulace.⁹¹

Nepanuje ovšem shoda, zda či v jaké míře by měly být virtuální měny regulovány. Tato otázka není hlavním předmětem této práce. Proto jsou zde jen velmi stručně popsány hlavní argumenty pro a proti regulaci virtuálních měn.

Argumenty proti přílišné regulaci jsou mimo jiné to, že regulace virtuálních měn nemusí být prospěšná, protože technologie spojená s virtuálními měnami mohou vést k finanční globalizaci, což by mělo za následek ekonomický nárůst. Dále že by mělo být virtuálním měnám dovoleno být experimentem, který může být inovací přispívající k technologickému pokroku zemí. V neposlední řadě hraje roli obava, že by přílišná regulace mohla zpomalit další vývoj virtuálních měn.⁹²

Nicméně, argumenty pro regulaci jsou, že nedostatečná regulace v oblasti virtuálních měn vede k podvodům, oslabení ekonomiky a nárůstu nelegálních plateb, což ve výsledku vede k poškozování finančního systému jako celku.⁹³ Nedostatek regulace navíc znamená, že programátoři mohou kdykoli změnit pravidla fungování virtuálních měn podle jejich přání. Zároveň regulace virtuálních měn může podnikatelům a startupům pomoci zavést a usnadnit

⁸⁹ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op.cit. s. 29.

⁹⁰ Ibid. s. 22.

⁹¹ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 163.

⁹² SHARMA, Avin M. *Cryptocurrency and financial risks*. op. cit. s. 59.

⁹³ Ibid. s.58.

rychlejší fungování odkudkoli na světě, chránit investory před problémy s likviditou a zároveň podpořit inovace a pokračovat v usnadňování financování podnikatelů.⁹⁴

3.4. Rizika spojená s virtuálními měnami

Přesun virtuálních měn není technicky obtížnější v situaci, kdy se jejich hodnota pohybuje v milionech dolarů než v situaci, kdy se pohybuje ve stovkách milionů dolarů.⁹⁵ I proto podle některých autorů virtuální měny vytvořily útočiště pro praní špinavých peněz usnadňující páchaní trestné činnosti. Pro finanční instituce je navíc stále obtížnější spojovat transakce s trestnou činností.⁹⁶

EBA analyzuje vývoj ML/FT rizik představovaných virtuálními měnami. EBA je podle článku 6 odst. 5 IV AML směrnice povinna každé dva roky předložit stanovisko o rizicích v oblasti praní peněz a financování terorismu, která mají dopad na finanční sektor Evropské unie.⁹⁷

Ve stanovisku z roku 2019 většina příslušných orgánů vyhodnotila virtuální měny jako nástroj představující významné ML/FT riziko. Příslušné orgány poukázaly na rizika související s rostoucí poptávkou zákazníků, často neregulovanou povahou souvisejících produktů a služeb a s tím souvisejícím nedostatkem v identifikaci klientů.⁹⁸

V březnu 2021 EBA vydala třetí stanovisko⁹⁹ o rizicích v oblasti praní peněz a financování terorismu. Jak je patrné z grafu č. 2, hodně příslušných orgánů v dotazníkú od EBA uvedlo, že se rizika spojená s virtuálními měnami od roku 2019 zvýšila. Klíčovým faktorem zvyšujícím rizika je růst trhu virtuálních aktiv, především co se týče objemu prováděných transakcí a počtu klientů firem, které využívají virtuální měny nebo jsou poskytovateli služeb s virtuálními aktivy. Nejvýznamnějším rizikovým faktorem, který příslušné orgány identifikovaly, je omezená transparentnost transakcí a totožnosti koncových zákazníků. To může v důsledku usnadnit nezákonné činnosti, jako jsou investiční podvody, obchodování s nelegálním zbožím nebo službami a financování terorismu.¹⁰⁰

⁹⁴ SHARMA, Avin M. *Cryptocurrency and financial risks*. op. cit. s. 59.

⁹⁵ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, *Cryptocurrency compliance and risks: A European KYC/ AML perspective*, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 163.

⁹⁶ SHARMA, Avin M. *Cryptocurrency and financial risks*. op. cit. s. 24.

⁹⁷ EBA. *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector* [online]. 3. března 2021. [cit. 2021-11-27]. s. 1.

Dostupné z:

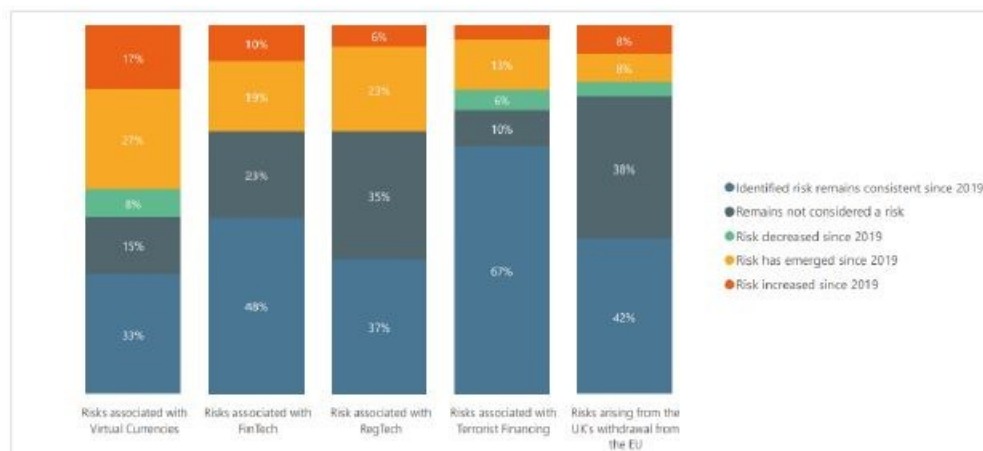
<https://www.eba.europa.eu/eba-highlights-key-money-laundering-and-terrorist-financing-risks-across-eu>

⁹⁸ Ibid. s. 28.

⁹⁹ Ibid.

¹⁰⁰ Ibid. s. 28.

Figure 1: Evolutions of risks compared to the risks identified in the Joint Opinion 2019



Graf č. 2: Vývoj ML/FT rizik podle EBA od roku 2019.¹⁰¹

3.4.1. Rizika spojená s virtuálními měnami v jednotlivých fázích praní špinavých peněz

Virtuální měny představují rizika pro praní špinavých peněz zejména kvůli dvěma aspektům, na kterých je postaveno celé jejich fungování. Těmito aspekty jsou anonymita a decentralizace.¹⁰² Tato podkapitola přibližuje, jak se tyto aspekty projevují v jednotlivých fázích praní špinavých peněz.

Fáze č. 1 – Umístění

Možnost rychlého otevření anonymních účtů poskytuje zločincům prostředek ke konverzi a konsolidaci nelegální hotovosti s malým rizikem.¹⁰³

Fáze č. 2 – Vrstvení

Např. neregistrované ICOs¹⁰⁴ poskytují dobré příležitosti pro rozsáhlé vrstvení. Pokud osoby, které perou špinavé peníze, kontrolují ICOs, mohou použít metodu navyšování kapitálu, aby převedli své nelegálně získané výnosy zpět do fiat měny.¹⁰⁵

¹⁰¹ EBA. *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector.* op. cit. s. 28.

¹⁰² RODRIGUES, Gustavo, LAHIS, Kurtz. *Cryptocurrencies and anti-money laundering regulation in the G20* [online]. 27. září 2019. [cit. 2021-11-27]. s. 12.

Dostupné z: <https://irisbh.com.br/en/publicacoes/19906/>

¹⁰³ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches.* op. cit. s. 32.

¹⁰⁴ ICO je způsob získávání finančních zdrojů, při kterém dochází ke směně tokenů za virtuální měny, resp. za fiat měny. Tokeny pak pro svoje držitele inkorporují určitá práva. Viz. COLLOMB, Alexis, DE FILIPPI, Primavera a SOK, Klara. *From IPOs to ICOs: The Impact of Blockchain Technology on Financial Regulation.* [online]. 26. května 2018. [cit. 2021-11-27]. s. 1.

Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3185347

¹⁰⁵ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches.* op. cit. s. 32.

Fáze č. 3 - Integrace

Virtuální měny jsou ideálním prostředkem k přesunu nezákonných výnosů přes hranice. Při přeshraničních převodech jsou virtuální měny použity například jako „splátky“ za skutečné nebo fiktivní zboží.¹⁰⁶

Rostoucí množství zboží, které je možné zakoupit za virtuální měny rozšiřuje možnosti integrace. Například v Itálii bylo notářům doporučeno, aby podávali hlášení o podezřelých transakcích pokaždé, když asistují stranám při nákupu nemovitosti prostřednictvím virtuálních měn, protože anonymita virtuálních měn může znemožnit identifikaci stran transakce.¹⁰⁷

3.4.2. Anonymita a sledovatelnost transakcí

Jako nejčastější riziko spojené s virtuálními měnami se uvádí anonymita účastníků transakcí a plateb. Zároveň představuje největší důvod pro regulaci virtuálních měn, jelikož nedostatek dostatečného monitorování podezřelých transakcí z virtuálních měn činí ideální prostředek pro praní špinavých peněz a pro financování terorismu.¹⁰⁸

Většina virtuálních měn jako je Bitcoin nebo Ether jsou už podle jejich designu anonymní nebo pseudoanonymní. To znamená, že identita uživatele není spojena s určitou peněženkou nebo transakcí. Identita uživatelů na DL, na kterém daná virtuální měna funguje, není veřejně viditelná. Na DL jsou ovšem veřejně přístupné informace o datu provedení transakcí, adresách protistrany transakce a hodnotě, o kterou se v transakci jednalo. Orgány dohledu jsou proto teoreticky schopny sledovat transakce až do bodu, kde by účtem nebo adresou mohla být spojena identita konkrétní osoby.¹⁰⁹

Některé virtuální měny, jako je například Dash, Monero nebo Zcash, jsou navrženy tak, aby byly zcela anonymní. To znamená, že na jejich DL nejsou veřejně přístupné informace o transakcích a peněženkách uživatelů. Tím je zajištěna naprostá anonymita a zabraňují identifikaci skutečného vlastníka virtuálních měn.¹¹⁰

Anonymní nebo pseudoanonymní design virtuálních měn představuje zřejmé riziko z hlediska AML regulace. Veřejná povaha DL ovšem působí jako zmírňující faktor, protože nabízí úplný přehled proběhlých transakcí, a tak představuje nezměnitelný elektronický záznam

¹⁰⁶ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 32.

¹⁰⁷ Ibid. s. 32.

¹⁰⁸ SHARMA, Avin M. *Cryptocurrency and financial risks*. op. cit. s. 58.

¹⁰⁹ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, *Cryptocurrency compliance and risks: A European KYC/ AML perspective*, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 166.

¹¹⁰ Ibid. s. 166.

transakcí. Sledovatelnost jednotlivých transakcí ovšem může být omezena použitím nástrojů k anonymizaci, které obfuskují řetězec transakcí.¹¹¹

Například mixovací služby (nebo anglicky tzv. „tumblers“) jsou jedním z nejvýznamnějších nástrojů pro praní špinavých peněz pomocí virtuálních měn. Zaměřují se převážně na hlavní virtuální měny jako je Bitcoin, Litecoin nebo Ethereum.¹¹² Mixovací služby agregují transakce od mnoha uživatelů a umožňují zakrytí původu jednotlivých transakcí. Stopa jednotlivých transakcí takto může být zastřena. Skutečnost, že k mixovací aktivitě došlo, bude ale na DL zjistitelná.¹¹³

Realita je komplexnější, než se může na první pohled zdát. Většinu¹¹⁴ virtuálních měn lze za splnění určitých podmínek s poměrně vysokou pravděpodobností úspěchu dohledat až k jejich vlastníkovi. Podobně jako peněženka, kterou lidé nosí v kapse, neobsahuje virtuální peněženka žádný identifikační prvek. Obsahuje pouze soukromé nebo veřejné klíče pro různé měny a přístupové kódy k nim. Jakmile jsou tedy virtuální mince ve virtuální peněžence, jsou mince v podstatě anonymní jako mince v peněžence v naší kapse.¹¹⁵

Jak bylo řečeno, všechny transakce jsou s výjimkami zaznamenávány na DL. To znamená, že je relativně snadné získat cestu každé mince a zpětně se dopátrat k její původní emisi. Pokud se například Bitcoin nachází v peněžence X, údaje o transakci zaznamenané v bloku blockchainu poskytnou údaje o odesílající straně - peněžence Y. Sledování vlákn ke zdroji nebo vzniku mince se potom stává otázkou výpočetního výkonu.¹¹⁶

Pokud bychom se zaměřili pouze na údaje z blockchainu, potom obchody s virtuálními měnami stále zůstávají zahalené tajemstvím. Stopa, kterou za sebou virtuální měna zanechává, ovšem většinou v nějakém bodě svého cyklu protne poskytovatele služeb s virtuálními aktivy. To se stane, pokud vlastník virtuální měny chce svou virtuální měnu směnít za jinou virtuální měnu nebo za fiat měnu. Takovou transakci většinou uskuteční prostřednictvím poskytovatele služeb

¹¹¹ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 166.

¹¹² DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic* [online]. 10. srpna 2020. [cit. 2021-11-27]. s. 11.

Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3681297

¹¹³ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 166.

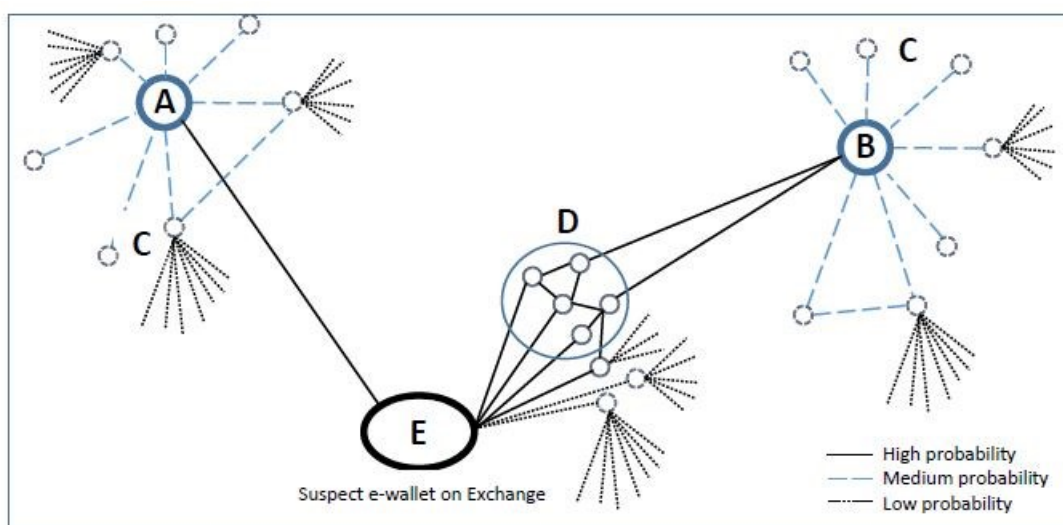
¹¹⁴ S výjimkou virtuálních měn Dash, Monero a Zcash, díky jejich unikátním transakčním protokolům.

¹¹⁵ DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic*. op. cit. s. 8.

¹¹⁶ Ibid. s. 8.

s virtuálními aktivy. Ty, minimálně v Evropské unii a České republice, spadají do působnosti AML regulace a vztahují se na ně KYC pravidla.¹¹⁷

Obrázek č. 2 ukazuje zjednodušenou verzi, jak lze sledovat transakce s virtuálními měnami, pokud jsou zprostředkovány poskytovatelem služeb s virtuálními aktivy. Pokud směnárna (E) spadá do působnosti AML regulace a řídí se AML pravidly, potom jsou identifikováni všichni obchodníci a potenciální podezřelé osoby, které jejím prostřednictvím provádějí transakce mezi virtuálními měnami navzájem nebo mezi virtuálními měnami a fiat měnami. Virtuální peněženka (A) je zařazena mezi uzly, na kterých je s vysokou pravděpodobností prováděno praní špinavých peněz. Vlastnictví tohoto uzlu je spojeno s podezřelou osobou. Virtuální peněženky (C) jsou zařazeny mezi uzly s nižším rizikem, ale zůstávají pod dohledem, pokud by se jejich cesty protnuly nebo sblížily. Systém může zároveň odhalit, pokud by se obchodník snažil oddělit prostředky z virtuální peněženky (jak je znázorněno ve shluku pod písmenem D) a poté je přeskupit ve virtuální peněženku (B), která se tím stane součástí vyšetřování. Plné čáry na obrázku č. 2 představují vysokou pravděpodobnost zapojení do nelegálních aktivit, zatímco čárkované čáry mají nižší hodnocení z hlediska rizika, ale díky procesům popsaným výše mohou získat na významu.¹¹⁸



Obrázek č. 2: Grafické znázornění procesu sledování transakcí s virtuálními měnami prostřednictvím poskytovatelů služeb.¹¹⁹

V roce 2014 byla vytvořena studie, která ukázala, že transakce s Bitcoinem lze efektivně mapovat s vysokou mírou pravděpodobnosti, dokonce vyšší než 90%. Od té doby se oblast

¹¹⁷ DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic*. op. cit. s. 8.

¹¹⁸ Ibid. s. 9.

¹¹⁹ Ibid. s. 9.

sledování kryptoměn přesunula z akademické sféry do komerčního světa. Softwary jako CypherTrace, Orbit nebo Elliptic AML, nyní umožňují deanonymizovat digitální transakce a vyhodnotit pravděpodobnost, že zdroj prostředků je nelegální. Existuje tedy kompletní záznam o cestě virtuální měny. Vlastníka virtuální měny ovšem není možné dopadnout, pokud všechny uzly nepodléhají AML regulaci a neaplikují se na ně KYC pravidla.¹²⁰

Stručně by se dalo říct, že brána ze světa virtuálních měn do fiat měn je z hlediska AML regulace poměrně dobře střežena. Každý subjekt by podle tohoto pohledu měl v určitém okamžiku projít portálem pro převod z virtuálních měn na fiat měny a tím riskovat svou identifikaci. Peněženky s virtuálními měnami by tímto způsobem mělo být možné přiřadit k jejich skutečnému vlastníkovi.¹²¹

3.4.3. Decentralizovaná povaha

Většina virtuálních měn je decentralizovaná. To znamená, že je distribuována na tzv. peer-to-peer bázi, ve které neexistuje potřeba ověření řádné autority, která by systém centrálně spravovala. Jak uvádí FATF, autority se tím pádem při vyšetřování nebo zabavení majetku nemohou zaměřit na jedno centrální místo nebo na jednoho správce. Záznamy o uživatelích a transakcích mohou být často u různých subjektů v různých jurisdikcích. To autoritám a regulátorům zásadně ztěžuje přístup k takovým entitám.¹²²

Decentralizovaná struktura virtuálních měn navíc umožňuje zakládání více účtů na různých místech, které nespravuje jediná entita a které existují pouze na internetu nebo ve virtuálních peněženkách.¹²³ Decentralizace posledně znamená nezávislost transakcí s virtuálními měnami ve vztahu k centralizovaným institucím. To ztěžuje uplatnění velké části AML režimu, protože jeho rámec je výhradně zaměřen na regulaci a dohled nad subjekty, které centralizují většinu tradičních transakcí, jako jsou banky a finanční instituce.¹²⁴

3.4.4. Virtuální měny a financování terorismu

Anonymita a snadnost vytváření virtuálních měn činí účty s virtuálními měnami ideální pro přijímání plateb osobami, u kterých by jinak bylo podezření z financování terorismu nebo

¹²⁰ DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic*. op. cit. s. 9.

¹²¹ Ibid. s. 11.

¹²² POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, *Cryptocurrency compliance and risks: A European KYC/ AML perspective*, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 167.

¹²³ SHARMA, Avin M. *Cryptocurrency and financial risks*. op. cit. s. 58.

¹²⁴ RODRIGUES, Gustavo, LAHIS, Kurtz. *Cryptocurrencies and anti-money laundering regulation in the G20*. op.cit. s. 13.

porušování mezinárodních sankcí. Virtuální měny zatím nejsou v oblasti financování terorismu příliš rozšířené. Teroristické skupiny s nimi ale experimentují už od roku 2014. Bitcoin byl pro teroristické skupiny získáván mimo jiné i prostřednictvím kampaní na sociálních sítích. Mimo to státy, na které jsou uvaleny mezinárodní sankce, začínají vytvářet svoje vlastní státem sponzorované virtuální měny. Venezuela takovou virtuální měnu vytvořila v roce 2018.¹²⁵

3.5. Rizika spojená s atomovými swapy

Zjednodušeně řečeno byly peer-to-peer transakce jako jsou atomové swapy vytvořeny s cílem umožnit vlastníkům virtuálních měn obejít institucionální zprostředkovatele transakcí, kteří v globálním AML režimu fungují jako základní strážci proti praní špinavých peněz a financování terorismu. Potenciál vzájemné anonymity stran transakce poskytovaný u peer-to-peer transakcí tudíž maří KYC a CIP procedury, na nichž je AML regulace založena.¹²⁶

Atomové swapy proto hrají v souvislosti s ML/FT riziky velkou roli. Jak je uvedeno v této kapitole, jejich roli můžeme pozorovat především v souvislosti s (i) cross-chain atomovými swapy, (ii) rozvojem DEXs a DeFi a (iii) s rozvojem využívání P2P transakcí k nezákonným aktivitám.

3.5.1. Off-chain atomové swapy

Atomové swapy výrazně zvyšují rizika spojená se špatnou sledovatelností transakcí s virtuálními měnami. Tato rizika nejsou tak významná, pokud se jedná o transakce na jednom DL nebo na jednom protokolu řídícím danou virtuální měnu. Situace se však stává mnohem složitější, pokud se jedná o off-chain atomové swapy, které umožňují provedení transakcí mezi jednotlivými DL.¹²⁷

Při off-chain atomových swapech probíhají transakce v soukromém kanálu a započtený výsledek transakce je vysílán do sítě těžařů. Kromě zúčastněných stran transakce tak nikdo ve skutečnosti nezná podrobnosti transakce.¹²⁸ To mimo jiné snižuje sledovatelnost takových transakcí tím, že může vyžadovat přístup k informacím, které se nenacházejí na blockchainu, ale které se nacházejí pouze u stran transakce.¹²⁹

¹²⁵ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 32.

¹²⁶ Ibid. s. 26.

¹²⁷ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 167.

¹²⁸ MIRAZ, Mahdi H. a DONALD, David C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Annals of Emerging Technologies in Computing (AETiC)*. op. cit. s. 48.

¹²⁹ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 167.

3.5.2. DEXs, DApps a DeFi

DEXs jsou definovány jako DL protokoly a aplikace, které uživatelům umožňují provádět transakce s virtuálními měnami, aniž by museli důvěřovat centralizovanému subjektu, který by zprostředkoval transakci nebo spravoval jejich virtuální měny. DEXs fungují online, anonymně, využívají on-chain chytré smlouvy a k dokončení transakce od uživatelů nevyžadují ani jejich emailovou adresu.¹³⁰ Takto nastavená struktura transakcí minimalizuje riziko útoků hackerů na servery s cílem krádeže virtuálních měn uživatelů.¹³¹

Do modelu CEXs naproti tomu uživatelé vkládají své prostředky a CEX jim vydává prostředek, se kterým lze na platformě volně obchodovat. Když uživatel požádá o výběr své virtuální měny, jsou tyto prostředky převedeny zpět na virtuální měnu, kterou představují, a odeslány jejich vlastníkovvi.¹³²

Po celou dobu transakce DEXs umožňují uživatelům kontrolovat své soukromé klíče. Zároveň jsou distribuované, takže nehrozí potenciální selhání jednoho bodu (e.g. výpadkem jednoho serveru, jako se to v minulosti stalo CEXs). Nezahrnují žádné třetí strany, není zde žádné riziko od protistrany a nemohou být uzavřeny vládami států. V podstatě se vlastníci virtuálních měn stávají svou vlastní bankou.¹³³

Absence centrálních serverů nabádá některé decentralizované směnárny k tomu, aby fungovaly bez ohledu na právní požadavky a pravidla spojená s jednotlivými jurisdikcemi, ve kterých poskytují služby. Jedna decentralizovaná směnárna dokonce v únoru 2018 zveřejnila příspěvek na blogu, ve kterém zdůrazňovala kritickou výhodu své služby, a to že funguje „bez KYC“.¹³⁴ Touha uživatelů vyhnout se KYC požadavkům centralizovaných směnáren virtuálních měn a provádět transakce ve větším soukromí hraje velký faktor ve velkém růstu v oblibě DEXs.¹³⁵

¹³⁰ DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic*. Op. cit. s. 17.

¹³¹ FANUSIE, Yaya J. Financial Authorities Confront Two Cryptocurrency Ecosystems. In: *Global Governance to Combat Illicit Financial Flows* [online]. 11. října 2018. [cit. 2021-11-27]. s. 58.

Dostupné z:

https://backend-live.cfr.org/sites/default/files/report_pdf/Discussion_Paper_Collection_Kahler_et_al_IFFs_OR.pdf#page=59

¹³² What Is a Decentralized Exchange (DEX)? In: *CryptoCompare* [online]. 12. března 2019

Dostupné z: <https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/>

¹³³ DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic*. op. cit. s. 17.

¹³⁴ FANUSIE, Yaya J. Financial Authorities Confront Two Cryptocurrency Ecosystems. In: *Global Governance to Combat Illicit Financial Flows*. op. cit. s. 58.

¹³⁵ LIN, Lindsay X., *Deconstructing decentralized exchanges* [online]. 5. ledna 2019. [cit. 2021-11-27]. s. 2.

Dostupné z: <https://stanford-jblp.pubpub.org/pub/deconstructing-dex/release/1>

Pojem „decentralizovaná nebo distribuovaná aplikace“ (**DApps**) označuje softwarový program fungující na blockchainu nebo podobné technologii. Někdy takové aplikace usnadňují nebo podporují jiné protokoly, aplikace nebo virtuální měny a jejich převod. DApps nabízející finanční služby shodně se službami nabízenými regulovanými poskytovateli služeb s virtuálními aktivy jsou označovány jako decentralizované finance (**DeFi**).¹³⁶

Podle FATF je jedním z hlavních problémů definice poskytovatelů služeb s virtuální aktivy její aplikace na decentralizované struktury jako jsou DEXs, DApps a DeFi, přičemž zejména DeFi v poslední době velmi roste popularita. Navzdory nárůstu v oblíbenosti těchto struktur ovšem FATF hodnotí, že stále zůstávají pouze malým prvkem celkového trhu s virtuálními měnami. Mohou ale představovat výzvu pro AML regulaci. Zejména proto, že může být obtížné určit entitu s odpovědností za dodržování AML/CFT povinností.¹³⁷ Pohled FATF k této otázce je uveden v podkapitole 5.3.1. této práce.

3.5.3. Analýza podílu P2P transakcí na trhu s virtuálními měnami a nezákonných aktivitách

Podle FATF mohou peer-to-peer transakce představovat specifické riziko praní špinavých peněz a financování terorismu, protože mohou být potenciálně využity k obcházení kontrolních AML/CFT mechanismů. Pokud transakce virtuálních měn probíhají na P2P bázi, nejsou do nich zapojeny žádné povinné subjekty, které by vyžadovaly dodržování preventivních nebo zmírňujících AML opatření. Toho mohou nelegální subjekty využít k zastření výnosů z trestné činnosti.¹³⁸

Cílem druhého přezkumu FATF norem z července 2021 proto bylo mimo jiné pochopit, v jaké míře jsou transakce prováděny s poskytovateli služeb a v jaké míře jsou transakce prováděny na P2P bázi. Dalším cílem bylo pochopit rizika spojená s P2P transakcemi.¹³⁹

Masové přijetí takzvaných stablecoinů nebo jiných virtuálních měn by v budoucnu mohlo potenciálně snížit využívání poskytovatelů služeb pro transakce nebo pro úschovu virtuálních měn. Pokud by ale data ukazovaly, že většina transakcí probíhá prostřednictvím poskytovatelů služeb, potom by měl být kladen ještě větší důraz na zajištění AML regulace těchto subjektů.¹⁴⁰

¹³⁶ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 26-27.

¹³⁷ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 33.

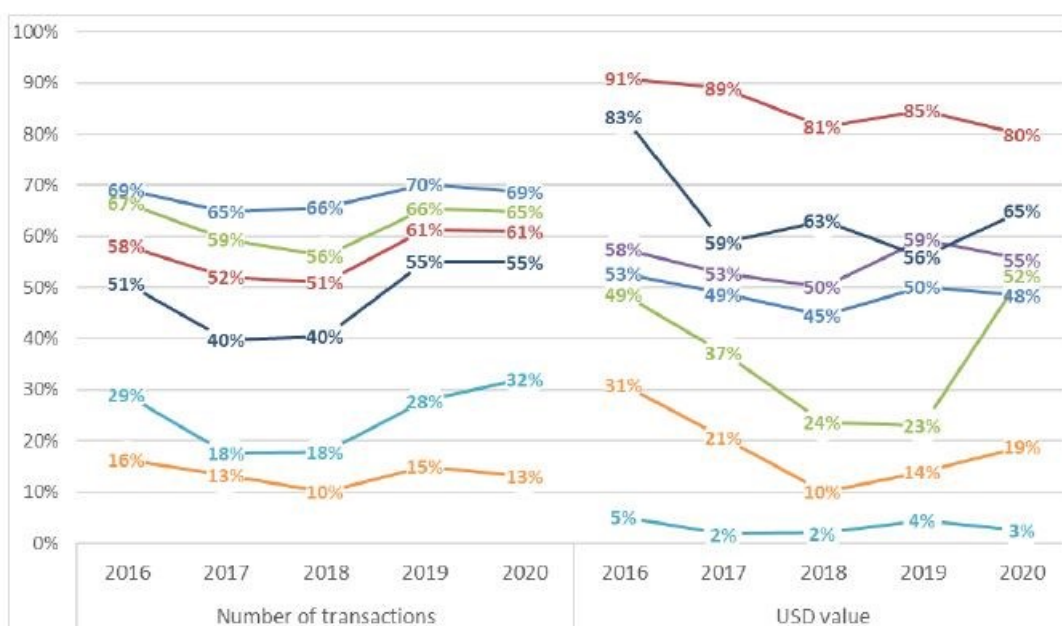
¹³⁸ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 18.

¹³⁹ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 23, 34.

¹⁴⁰ *Ibid.* s. 24.

Za účelem pochopení trhu s virtuálními měnami a podílu P2P transakcí vybral FATF sedm společností analyzujících trhy s virtuálními měnami a pověřila je úkolem vypracovat soubor tržních metrik o tom, v jakém rozsahu (i) jsou virtuální měny využívány na P2P bázi, (ii) jsou převáděny pomocí poskytovatelů služeb či jejich prostřednictvím a (iii) dochází k využívání P2P transakcí k nezákonným účelům. Každá společnost používá jinou metodologii a nástroje. Proto se výsledky velmi liší, jak je vidět na grafech uvedených níže. Společnosti vypracovaly metriky pro virtuální měny bitcoin, ether a tether. V grafech níže jsou znázorněny pouze data týkající se bitcoinu, protože má u společností největší pokrytí.¹⁴¹

Grafy č. 3 znázorňuje podíl P2P transakcí z hlediska počtu transakcí a hodnoty v USD v letech 2016-2020. Je obtížné z grafu vyvodit jasné závěry vzhledem k míře rozdílnosti údajů poskytnutých jednotlivými společnostmi. Navzdory rozdílům mezi údaji poskytnutými jednotlivými společnostmi jsou údaje v jednom ohledu konzistentní. Údaje neukazují jasný a konzistentní posun směrem k P2P transakcím nebo odklon od transakcí s užitím poskytovatelů služeb. Co se týče počtu transakcí zůstává podíl transakcí s užitím poskytovatelů služeb a bez nich v letech 2016-2020 do značné míry stabilní.¹⁴²



Grafy č. 3: Procentuální znázornění množství bitcoinových P2P transakce provedených v letech 2016-2020.¹⁴³

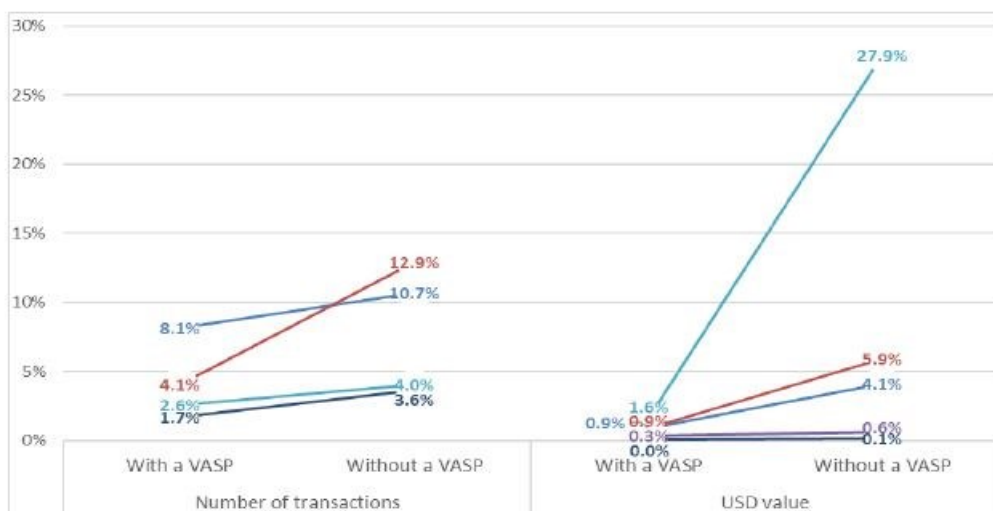
Čtyři společnosti na základě seznamu adres, o nichž je známo, že jsou spojeny s nelegální aktivitou, poskytly data o počtu nelegálních P2P transakcí s Bitcoinem. Všechny společnosti

¹⁴¹ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 24.

¹⁴² Ibid. s. 25.

¹⁴³ Ibid. s. 26.

zjistily, že celkově je prováděno víc nezákonných transakcí na P2P bázi než prostřednictvím poskytovatelů služeb. Stejně tak podle nich byl pomocí P2P transakcí převedený větší objem v přepočtu na americké dolary. Tyto data jsou znázorněny na grafech č.4.



Grafy č. 4: Procentuální znázornění podílu nelegálních bitcoinových P2P transakcí oproti transakcím prostřednictvím poskytovatelů služeb v letech 2016-2020.¹⁴⁴

Míra rozdílů mezi údaji jednotlivých společností je velmi vysoká, a proto z nich je obtížné vyvodit jednoznačné závěry. Přesto FATF určité závěry vyvozuje. Údaje ukazují, že značná část transakcí se uskutečňuje na P2P bázi. U Bitcoinu není vidět žádný trend k jejich většímu či menšímu využívání. Podle FATF ale existují ukazatele potenciálního trendu směrem k většímu počtu P2P transakcí u virtuálních měn ether a tether. To by mohlo být způsobeno nárůstem DeFi projektů v posledních letech.¹⁴⁵

Z dat dále vyplývá, že existují značné rozdíly mezi tím, jak se používá bitcoin, ether a tether. To ukazuje, že P2P využívání se může lišit u jednotlivých virtuálních měn na základě jejich odlišných charakteristik. Budoucí virtuální měny proto mohou mít z pohledu P2P využití různé profily.¹⁴⁶

Stejně tak se zdá, že více nelegálních transakcí se uskutečňuje na P2P bázi než prostřednictvím poskytovatelů služeb, a to zejména v případě bitcoinu. To znamená, že v P2P sektoru existují větší ML/FT rizika. Podle některých společností ale potom, co jsou vyměněny prostřednictvím P2P transakcí, skončí mnoho nelegálních prostředků u poskytovatelů služeb. To

¹⁴⁴ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 28.

¹⁴⁵ Ibid. s. 28.

¹⁴⁶ Ibid. s. 28.

by mohlo být způsobeno současnou obtížností při používání virtuálních měn bez poskytovatelů služeb.¹⁴⁷

Snaha FATF udělat přehled o P2P transakcích dále ukázala, jak je takový výzkum náročný. Každá společnost má vlastní metody analýzy dat a spojování reálných subjektů s virtuálními peněženkami vyžaduje od společností značný čas, zdroje, odborné znalosti a investice. Jedná se o přetrvávající výzvu, protože se snadno vytváří stále více peněženek, vznikají nové služby, uvolňují se nové virtuální měny a služby fungují na stále větším počtu blockchainů. Zároveň subjekty, včetně regulovaných poskytovatelů služeb, často mění své adresy, což dále komplikuje proces analýzy dat z blockchainu.¹⁴⁸

3.5.4. Co z této analýzy vyplývá?

Výsledky analýzy tržních metrik v předchozí podkapitole ukazují, že potenciálně významné množství určitých virtuálních měn je převáděno na P2P bázi. Ve srovnání s transakcemi prostřednictvím poskytovatelů služeb se zdá být podíl nezákonných transakcí u P2P transakcí vyšší.¹⁴⁹

Značné rozdíly v údajích poskytnutých jednotlivými společnostmi však znamenají, že velikost P2P sektoru a s ním spojená MI/CFT rizika zůstávají nejasná. Vzhledem k neexistenci jasných důkazů ohledně rizik spojených s P2P transakcemi a vzhledem k existenci přesvědčivých důkazů o rizicích představovaných poskytovateli služeb, kteří dostatečně neaplikují AML pravidla nebo nejsou subjekty AML regulace, by podle FATF měl být za současného stavu kladen důraz na kontrolu zprostředkovatelů, jako jsou poskytovatelé služeb s virtuálními aktivy.¹⁵⁰

To ovšem neznamená, že by FATF v případě změny situace v budoucnosti svůj přístup nezměnila. FATF si je vědoma toho, že se může počet P2P transakcí rapidně zvýšit. Takový trend by sebou mohl přinést vážnější rizika, protože by FATF opatření ke zmírnění AML rizik prostřednictvím regulace poskytovatelů služeb nebyla účinná. Pokud by došlo k nárůstu P2P transakcí do takové míry, že by transakce probíhaly téměř výhradně na P2P bázi a zločinci by mohli existovat výhradně v ekosystému virtuálních měn, aniž by kdy přišli do styku s regulovanými poskytovateli služeb, mohly by stávající pravidla vyžadovat výraznou revizi, aby taková rizika dokázala dostatečně zmírnit.¹⁵¹

¹⁴⁷ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 29.

¹⁴⁸ Ibid. s. 29-30.

¹⁴⁹ Ibid. s. 34.

¹⁵⁰ Ibid. s. 34.

¹⁵¹ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 34-35.

Zároveň je nutné podotknout, že se trendy v P2P oblasti mohou projevit až za několik let. Proto by měly jurisdikce a soukromý sektor předem zvážit, jak identifikovat a zmírnit rizika, která P2P sektor představuje.¹⁵² K tomu blíže kapitola 5.3. této práce.

3.6. Shrnutí

Bez dohledu nad vytvářením nových účtů chybí u virtuálních měn bod, přes který by bylo možné vymáhat dodržování AML pravidel. Identitu uživatelů lze získat a ověřit ve chvíli, kdy překročí pomyslnou hranici mezi světem virtuálních měn a tradičním finančním systémem. Tuto hranici uživatelé překračují prostřednictvím regulovaných poskytovatelů služeb s virtuálními aktivy. Ani skrz interakci uživatele s regulovaným poskytovatelem služeb ale poskytovatel služeb nezíská kompletní přehled o transakcích jednotlivce. Uživatel může k transakcím používat velké množství adres a o většině z nich poskytovatel služeb nemusí vůbec vědět.¹⁵³

Díky P2P transakcím uživatelé mohou obejít poskytovatele služeb s virtuálními aktivy. Tím představují riziko pro AML regulaci, protože umožňují obejít důležitý bod, skrz který lze identifikovat vlastníky jednotlivých peněženek a mincí. Off-chain atomové swapy navíc ztěžují sledovatelnost transakcí a jednotlivých mincí, protože probíhají na neveřejném DL.

Druhý přezkum FATF norem za účelem zhodnocení rizik spojených s P2P transakcemi poskytl přehled o tom (i) v jakém množství jsou virtuální měny využívány na P2P bázi a (ii) v jaké míře jsou P2P transakce zneužívány k nezákonným účelům. Podle této zprávy je potenciálně významné množství virtuálních měn převáděno na P2P bázi a podíl identifikovaných nezákonných P2P transakcí je větší než u transakcí s využitím poskytovatelů služeb s virtuálními aktivy. Vysoká míra rozdílů mezi získanými údaji ovšem neumožňuje přesně určit velikost P2P sektoru a s ním spojených ML/FT rizik.¹⁵⁴

Vzhledem k tomu, že v současné době není možné určit velikost P2P sektoru a s ním spojená rizika, by podle FATF měl být regulátory kladen důraz spíše na regulaci poskytovatelů služeb s virtuálními aktivy a na důsledné vymáhání těchto pravidel. Zároveň je možné, že se díky rozsáhlejší regulaci poskytovatelů služeb s virtuálními aktivy zvýší využívání P2P sektoru a bude potřeba současný přístup přehodnotit.

¹⁵² Ibid. s. 35.

¹⁵³ MÖSER, Malte a NARAYANAN, Arvind. *Effective Cryptocurrency Regulation Through Blacklisting*. op. cit. s. 3.

¹⁵⁴ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 20.

4. Dopad připravovaných změn AML regulace v Evropské unii na virtuální měny

Stávající AML regulace v Evropské unii od přijetí V AML směrnice definuje virtuální měny a mezi povinné osoby zahrnuje poskytovatele směnářských služeb mezi virtuálními měnami a měnami s nuceným oběhem a poskytovatele virtuálních peněženek. V rámci V AML směrnice ovšem existuje řada slepých míst, které by mohly zločinci využít k praní špinavých peněz nebo k financování terorismu.¹⁵⁵

Toho si byla Evropská unie vědoma již při přijímání V AML směrnice. To je patrné zejména z 9. odstavce preambule V AML směrnice. Ten uvádí, že: „*zahrnutí poskytovatelů směnářských služeb mezi virtuálními měnami a měnami s nuceným oběhem a poskytovatelů virtuálních peněženek nevyřeší zcela otázku anonymity spojenou s transakcemi s virtuální měnou, jelikož velká část prostředí virtuálních měn je i nadále anonymní, neboť uživatelé mohou provádět transakce i bez těchto poskytovatelů. Za účelem boje proti rizikům spojeným s anonymitou by měly být vnitrostátní finanční zpravodajské jednotky oprávněny získávat informace umožňující jim propojit adresy virtuálních měn s totožností majitele virtuální měny. Dále je třeba blíže posoudit možnost, aby se uživatelé sami dobrovolně přihlásili určeným orgánům.*“¹⁵⁶

Evropská komise 20. července 2021 představila nový balíček legislativních návrhů v oblasti AML a CFT regulace včetně návrhu na vytvoření nového samostatného orgánu pro boj s praním špinavých peněz (AMLA). Cílem tohoto balíčku je zlepšit odhalování podezřelých transakcí a činností a odstranit mezery využívané k praní špinavých peněz nebo financování teroristických aktivit prostřednictvím finančního systému.¹⁵⁷

Balíček legislativních návrhů sestává z:

1. návrhu nařízení o zřízení nového orgánu pro boj proti praní peněz,¹⁵⁸

¹⁵⁵ DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic*. op. cit. s. 3.

¹⁵⁶ Odstavec 9 preambule V AML směrnice.

¹⁵⁷ HAVLÍČEK, Ondřej a ŠARAPATKA, Matěj. *Novinky z oblasti české a evropské regulace finančních institucí za měsíc červenec 2021* [online]. 11. srpna 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.epravo.cz/top/aktualne/novinky-z-oblasti-ceske-a-evropske-regulace-financnich-instituci-za-mesic-cervenec-2021-113417.html>

¹⁵⁸ Návrh nařízení Evropského parlamentu a Rady, kterým se zřizuje Orgán pro boj proti praní peněz a financování terorismu a mění nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

2. návrhu nařízení o předcházení využívání finančního systému k praní peněz nebo financování terorismu (**AML nařízení**);¹⁵⁹

3. návrhu šesté směrnice o praní špinavých peněz (**VI AML směrnice**);¹⁶⁰ a

4. návrhu nařízení o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv – revize nařízení 2015/847 o informacích doprovázejících převody finančních prostředků (**nařízení o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv**).¹⁶¹

Podle Evropské komise tento balíček opatření výrazně posílí stávající rámec Evropské unie tím, že zohlední nové a vznikající výzvy spojené s technologickými inovacemi, mimo jiné s virtuálními měnami.¹⁶²

Ve srovnání s předchozím právním rámcem jsou v rámci balíčku všechna pravidla vztahující se na soukromý sektor převedena na AML nařízení. Organizace institucionálního systému boje proti praní peněz a financování terorismu na vnitrostátní úrovni je ponechána na VI AML směrnici. Přípravované změny počítají se zrušením V AML směrnice.¹⁶³

V současné době jsou do působnosti AML pravidel zahrnuty pouze některé kategorie poskytovatelů služeb s virtuálními měnami. Navrhovaná reforma rozšíří tato pravidla na celý kryptografický sektor a uloží všem poskytovatelům služeb povinnost provádět due diligence svých zákazníků. Tyto změny podle Evropské komise zajistí plnou sledovatelnost převodů virtuálních měn, jako je Bitcoin, a umožní prevenci a odhalování jejich možného použití k praní špinavých peněz nebo financování terorismu.¹⁶⁴

Eurokomisařka pro finanční služby Mairead McGuinnessová ve svém tweetu ze dne 20. července 2021 shrnula navrhovaná pravidla Evropské komise a napsala: „*Naše pravidla se nyní*

¹⁵⁹ Návrh nařízení Evropského parlamentu a Rady o předcházení využívání finančního systému k praní peněz nebo financování terorismu.

¹⁶⁰ Návrh směrnice Evropského parlamentu a rady o mechanismech, které mají členské státy zavést za účelem předcházení využívání finančního systému k praní peněz nebo financování terorismu, a o zrušení směrnice (EU) 2015/849.

¹⁶¹ Návrh nařízení Evropského parlamentu a Rady o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv.

¹⁶² EVROPSKÁ KOMISE. *Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules* [online]. 20. července 2021. [cit. 2021-11-27].

Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

¹⁶³ RECOVÁ, Alžběta. *Evropský legislativní balíček AML a relevantní ustanovení pro advokáty* [online]. 29. září 2021. [cit. 2021-11-27].

Dostupné z:

<https://advokatnidenik.cz/2021/09/29/evropsky-legislativni-balicek-v-oblasti-aml-a-relevantni-ustanoveni-pro-advokaty/>

¹⁶⁴ Ibid.

*budou vztahovat na celé odvětví virtuálních měn. Zakážeme anonymní peněženky virtuálních měn a zajistíme, aby převody virtuálních měn byly dohledatelné.*¹⁶⁵

Místo zákazu anonymních peněženek virtuálních měn přinese nová regulace přísnější pravidla pro poskytovatele služeb s virtuálními měnami, jako jsou směnárny virtuálních měn nebo poskytovatelé správcovských virtuálních peněženek. Nová pravidla totiž zakazují poskytování anonymních služeb, jako je úschova virtuálních měn nebo směnářenské účty poskytované třetí stranou, ale nezakazují poskytování softwarů pro vlastní úschovu virtuálních měn. Zákaz anonymních peněženek je zároveň téměř nemyslitelný, jelikož téměř každá peněženka virtuálních měn je ve výchozím nastavení anonymní a softwarové peněženky jako např. MyCrypto, Exodus a Electrum jsou dostupné ke stažení po celém světě.¹⁶⁶

Legislativní balíček nyní projedná Evropský parlament a Rada Evropské unie. Budoucí orgán pro boj proti praní peněz by měl začít fungovat v roce 2024 a svou činnost přímého dohledu zahájí o něco později jakmile bude VI AML směrnice transponována a začne platit nový regulační rámec.¹⁶⁷

4.1. Nařízení o informacích doprovázejících převody peněžních prostředků

Nařízení 2015/847¹⁶⁸ bylo přijato s cílem zajistit jednotné uplatňování požadavků FATF na poskytovatele služeb bankovních převodů, a zejména povinnosti poskytovatelů platebních služeb doprovázet převody peněžních prostředků informacemi o plátcích a zboží v celé EU. Nařízení 2015/847 se vztahuje pouze na převod finančních prostředků, které jsou definovány jako bankovky, mince a elektronické peníze.¹⁶⁹

Podle Evropské komise revize nařízení 2015/847 umožní sledovat převody s virtuálními měnami a omezí velké hotovostní platby. Jejím cílem je rozšířit oblast působnosti nařízení 2015/847 tak, aby zahrnovala převody s virtuálními měnami prováděné poskytovateli služeb

¹⁶⁵ McGUINNESS, Mairead. Cryptocurrency. In: *Twitter* [online]. 20. července 2021. [cit. 2021-11-27].

Dostupné z: <https://twitter.com/McGuinnessEU/status/1417494016741023753>

¹⁶⁶ MORRIS, David Z. *No, the European Union Is Not 'Banning Anonymous Crypto Wallets'* [online]. 21. července 2021. [cit. 2021-11-27].

Dostupné z:

https://finance.yahoo.com/news/no-european-union-not-banning-171752952.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2x1LmNvbS8&guce_referrer_sig=AQAAAE0jTjBW0fLHKyu39PYJaBfOo4bTZc2HuQfH5HFfISvXWelCPogj2Q5SI9sBXUJXUq9of8KtSOmSlvenJhJmIfO8j_1X8hPOoa6RfKHQyHOfXUvLRMzK1cq3ZDLK8Y5T35jHalbAmmZTZ_cvLidqrXjaA44oEo6yfyc_wK_YXTaAR

¹⁶⁷ EVROPSKÁ KOMISE. *Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules*. Op. cit.

¹⁶⁸ Nařízení Evropského parlamentu a Rady (EU) 2015/847 ze dne 20. května 2015 o informacích doprovázejících převody peněžních prostředků a o zrušení nařízení (ES) č. 1781/2006.

¹⁶⁹ RECOVÁ, Alžběta. *Evropský legislativní balíček AML a relevantní ustanovení pro advokáty*. op. cit.

s virtuálními aktivy. Tím bude do evropského práva promítnuto doporučení 15 FATF o nových technologiích z června 2019.¹⁷⁰

Zprostředkovatel převodu virtuálních měn bude povinen připojit k transakci, jejíž celková hodnota převyší 1 000 EUR, informace obsahující jméno nebo název převodce i příjemce, číslo účtu převodce i příjemce, a také adresu a identifikační číslo nebo datum a místo narození převodce. Před provedením transakce bude poskytovatel služby povinen ověřit si správnost těchto doprovodných informací ze spolehlivého nezávislého zdroje.¹⁷¹

Pokud převod virtuálních měn neprobíhá mezi účty, ale např. mezi peněženkami, bude zprostředkovatel převodu povinen uložit v síti informace, které umožní identifikovat konkrétní transakci a adresy jejích účastníků. Pro jednotlivé transakce do max. hodnoty 1 000 EUR se uplatní zjednodušený postup.¹⁷²

Vzhledem k tomu, že virtuální měny mají stejný, ne-li větší, potenciál působit jako nástroje pro praní špinavých peněz, jednalo se o velmi potřebnou změnu, která umožní národním finančním zpravodajským jednotkám i nově vytvořenému orgánu pro boj s praním špinavých peněz zajistit lepší sledovatelnost peněžních toků, čímž dále rozšíří jejich nástroje použitelné v boji proti praní špinavých peněz.¹⁷³

4.2. AML nařízení

Cílem navrhovaného AML nařízení je vytvořit nový soubor pravidel EU pro boj proti praní peněz, který by měl obsahovat povinnosti soukromých subjektů současnosti vyplývající z V AML směrnice. Důvodem pro tuto změnu je nejednotnost AML regulace v Evropské unii v důsledku rozdílného způsobu, jakým jednotlivé členské státy implementovali V AML směrnici do svých právních řádů.¹⁷⁴

¹⁷⁰ FEBBI, Stefano. *EU publishes package of legislative proposals aimed at strengthening AML/CFT rules* [online]. srpen 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.twobirds.com/en/news/articles/2021/global/eu-publishes-package-of-legislative-proposals-aimed-at-strengthening-aml-cft-rules>

¹⁷¹ ERBSOVÁ, Hana. *Kryptoměny: EU připravuje přísnější AML regulaci* [online]. 31. srpna 2021. [cit. 2021-11-27].

Dostupné z: <https://www.amlolutions.cz/aktuality/kryptomeny-eu-pripravuje-prisnejsi-aml-regulaci>

¹⁷² Ibid.

¹⁷³ PAPHITIS, Sotiris. *The EU's AML Package: an examination* [online]. 12. října 2021. [cit. 2021-11-27].

Dostupné z: <https://europeanlawblog.eu/2021/10/12/7922/>

¹⁷⁴ Ibid.

Soubor pravidel bude mimo jiné obsahovat ustanovení, která budou aktualizovat normy Evropské unie týkající se praní špinavých peněz prostřednictvím virtuálních měn. Toho chce dosáhnout novým vymezením regulovaných aktiv a poskytovatelů služeb s nimi spojených.¹⁷⁵

Pokud jde o definici virtuálních aktiv a poskytovatelů služeb s virtuálními aktivy, AML nařízení i VI AML směrnice upouští od vlastního vymezení těchto pojmů a odkazují se na další připravovanou normu, a to na nařízení o trzích s kryptoaktivy¹⁷⁶ (MiCa).¹⁷⁷

MiCa obsahuje podstatně podrobnější a širší definici virtuálních aktiv a poskytovatelů služeb s virtuálními aktivy než stávající AML předpisy. Pro poskytovatele určitých služeb spojených s virtuálními měnami zavádí i povinnost získat povolení k této činnosti a povinnou registraci. K nabývání a pozbývání významných podílů v poskytovatelích těchto služeb by se měl vyjadřovat stát. V neposlední řadě pak MiCa omezuje nabízení virtuálních aktiv veřejnosti, přičemž od vydavatelů vyžaduje splnění poměrně přísných podmínek, včetně příslušného povolení v některých případech.¹⁷⁸

Dále by MiCa mělo vytvořit novou kategorii poskytovatelů služeb s virtuálními aktivy, která je definována jako *"jakákoli osoba, jejíž povolání nebo podnikání spočívá v poskytování jedné nebo více služeb v oblasti kryptoaktiv třetím stranám na profesionálním základě"*.¹⁷⁹ Definice zahrnuje služby, jako je obchodování, směnárenská činnost, úschova virtuálních měn, a dokonce i poskytování poradenství.¹⁸⁰ Tato definice zahrnuje i směnárny virtuálních aktiv mezi sebou. To je z hlediska evropské AML regulace dobrým krokem, protože podle 5 AML směrnice byly regulovány pouze směnárny virtuálních měn s fiat měnami.¹⁸¹

Pokud jde o praní špinavých peněz, mezi cíle MiCa patří zajistit, aby (i) osoby v oblasti virtuálních aktiv měli dostatečné odborné znalosti v oblasti boje proti praní špinavých peněz a boje proti financování terorismu, (ii) byly zavedeny spolehlivé a účinné mechanismy vnitřní kontroly a hodnocení rizik, systémy a postupy, které zajišťují integritu a důvěrnost informací a (iii) poskytovatelé služeb s virtuálními aktivy vedli záznamy o všech transakcích, příkazech a službách souvisejících s virtuálními aktivy.¹⁸²

¹⁷⁵ PAPHITIS, Sotiris. *The EU's AML Package: an examination*. op. cit.

¹⁷⁶ Návrh nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937.

¹⁷⁷ ERBSOVÁ, Hana. *Kryptoměny: EU připravuje přísnější AML regulaci*. op. cit.

¹⁷⁸ Ibid.

¹⁷⁹ Článek 3 odst. 1 č. 8 MiCa

¹⁸⁰ *Ensuring cryptocurrency exchange KYC compliance* [online]. 11. února 2021. [cit. 2021-11-27].

Dostupné z: <https://medium.com/the-regtech-hub/ensuring-cryptocurrency-exchange-kyc-compliance-9899056a554>

¹⁸¹ PAPHITIS, Sotiris. *The EU's AML Package: an examination*. op. cit.

¹⁸² *Ensuring cryptocurrency exchange KYC compliance*. op. cit.

4.3. Jsou připravované změny EU AML regulace dostatečné?

Navrhovaný balíček nových AML opatření má za cíl odstranit nedostatky stávající AML regulace. Zavedení jednotného souboru pravidel a vytvoření celoevropského orgánu pro jejich prosazování by mohlo odstranit stávající nesrovnalosti mezi přístupy členských států. To s sebou nese vyhlídku na zlepšení boje proti praní špinavých peněz, čímž by se Evropská unie stala lepším trhem pro podnikání. Jedním ze slibných rysů této reformy je její moderní přístup. Zabývá se riziky, která představují nově vznikající technologie, jako jsou například virtuální měny a technologie s nimi spojené. Díky tomu se Evropská unie vyrovná se současnými standardy stanovenými FATF.¹⁸³

Je však třeba si uvědomit, že balíček opatření proti praní peněz zůstává návrhem, který má před sebou ještě dlouhou cestu k plné implementaci. Je možné, že do té doby budou některé aspekty reformy, například její přístup k virtuálním měnám, zastaralé vzhledem k jejich rychle se vyvíjející povaze.¹⁸⁴

To je patrné i z hlediska atomových swapů. Atomové swapy jsou v podstatě čistou formou směny virtuálních měn, který může fungovat bez jakéhokoliv prostředníka. Jsou mimo oblast působnosti současné V AML směrnice a z důvodu absence zprostředkovatele je a bude obtížné je do působnosti AML regulace v budoucnosti zahrnout.¹⁸⁵

Ani nově navrhovaný balíček AML opatření tento problém neřeší, jelikož, jak byl uvedeno výše, zpřísněná pravidla dopadnou pouze na poskytovatele služeb s virtuálními měnami. To ale neovlivní AML rizika spojený s atomovými swapy, které fungují na peer-to-peer principu a mohou být využity bez jakéhokoliv zprostředkování poskytovateli takových služeb.

¹⁸³ PAPHITIS, Sotiris. *The EU's AML Package: an examination*. op. cit.

¹⁸⁴ Ibid.

¹⁸⁵ POLICY DEPARTMENT FOR ECONOMIC, SCIENTIFIC ANF QUALITY OF LIFE POLICIES. *Cryptocurrencies and blockchain Legal context and implications for financial crime, money laundering and tax evasion*. op. cit. s. 77.

5. Způsoby řešení rizik s atomovými swapy

Jak vyplývá z předchozích částí této práce, AML regulace se obecně zaměřuje zejména na regulaci poskytovatelů služeb s virtuálními aktivy, tedy na pomyslnou bránu mezi virtuálními měnami a fiat měnami. Je ovšem nejasné, zda takový přístup, přijatý např. v V AML směrnici nebo v navrhovaném balíčku nových evropských AML opatření, obstojí při rostoucím počtu DEXs, atomových swapů a další P2P aplikací.¹⁸⁶

Tato část se proto zaměřuje na to, jakými způsoby jednotlivé AML přístupy řeší rizika spojená s virtuálními aktivy a jestli mají potenciál vyřešit rizika spojená s atomovými swapy. Zkoumá (i) zákaz virtuálních měn v Číně, (ii) povinnost propojení peněženek s virtuálními měnami s bankovními účty v Jižní Koreji, (iii) přístup FATF v několika oblastech, (iv) návrh nové regulace nesprávcovských peněženek ve Spojených státech, (v) současnou regulaci nesprávcovských peněženek ve Švýcarsku, (vi) doplňový prostředek AML regulace tzv. blacklisting a na konec (vii) možné technologické řešení zmírnění rizik spojených s atomovými swapy.

5.1. Zákaz virtuálních měn – Čína

Čína zaujala jeden z nejpřísnějších přístupů k virtuálním měnám ze všech velkých světových ekonomik. Plošný zákaz všech virtuálních měn je vyústěním vývoje trvajícím od roku 2013, kdy centrální banka Číny zdůrazňovala rizika praní špinavých peněz spojená s Bitcoinem a dalšími virtuálními měnami a vyzvala banky k dohledu nad virtuálními měnami. V roce 2017 následně vydala oznámení, ve kterém řekla, že virtuální měny nemají právní status ani vlastnosti, které by je stavěly na stejnou úroveň jako fiat měny, a tím pádem by neměly být jako fiat měny používány.¹⁸⁷

Oznámení z roku 2017 zakázalo vydávání ICOs. Zároveň bylo organizacím a jednotlivcům, kteří prostřednictvím ICOs vybrali peníze před vydáním oznámení, přikázáno, aby poskytli náhrady nebo učinili jiná opatření, aby přiměřeně chránili práva a zájmy investorů a řádně řešili rizika, která mohla vzniknout. Zároveň oznámení nařídilo směnárnám virtuálních měn, aby přestaly nabízet služby spojené s virtuálními měnami.¹⁸⁸

¹⁸⁶ POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS. *Virtual currencies and terrorist financing: assessing the risks and evaluating responses* [online]. květen 2018. [cit. 2021-11-27]. s. 42. Dostupné z: [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)

¹⁸⁷ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 31.

¹⁸⁸ Ibid. s. 31.

Čínští uživatelé nicméně po zákazech z roku 2017 začali využívat služeb zahraničních, zejména japonských, směnáren. Proto k nim začala vláda od února 2018 blokovat přístup skrze Velký čínský firewall. Ten vedle přístupu k zahraničním směnárnám znemožňuje i přístup k nákupům tokenů vydávaných v rámci ICOs.¹⁸⁹

Nicméně, ačkoliv to orgány Čínské lidové republiky nedoporučovali, individuální nákupy nebo peer-to-peer obchodování s virtuálními měnami nebylo z pohledu Čínské lidové republiky zakázáno.¹⁹⁰

To se změnilo v září 2021. Čínská centrální banka uvedla, že obchodní aktivity spojené s virtuální měnou jsou nezákonné finanční aktivity, a varovala, že vážně ohrožují bezpečnost majetku lidí. Toto prohlášení jasně uvádí, že kdo se podílí na nezákonných finančních aktivitách se dopouští trestného činu a bude trestně stíhán. Stejně tak se nezákonné činnosti dopouštějí zahraniční webové stránky poskytující takové služby čínským občanům.¹⁹¹

V praxi stále existuje možnost pro čínské investory, jak přísné zákazy obejít a obchodovat s virtuálními měnami skrz zahraniční poskytovatele služeb s virtuálními aktivy. DEXs s anonymitou, kterou uživatelům poskytují DEXs, z nich činí pro čínské investory ideální prostředek. Minimálně ale nebudou čínští investoři moci převést takto získané prostředky na čínské bankovní účty.¹⁹²

Je důležité poznamenat, že FATF nedoporučuje zákaz virtuálních měn. Naopak je FATF názoru, že by takový zákaz mohl činnosti s virtuálními měnami zahnat do podsvětí, což by vedlo k tomu, že by se tyto činnosti staly naprosto nepřehledné a nekontrolovatelné.¹⁹³

5.2. Propojení peněženek s virtuálními měnami s bankovními účty – Jižní Korea

V Jižní Koreji začal regulovat virtuální měny korejský orgán dohledu FSC prostřednictvím své pravomoci k regulaci bank. V lednu roku 2018 oznámil opatření, která vyžadují, aby

¹⁸⁹ Ministerstvo financí České republiky. *Veřejná konzultace Blockchain, virtuální měny a aktiva (využití technologie blockchain k evidenci cenných papírů)* [online]. 30. listopadu 2018. [cit. 2021-11-27]. s. 17.

Dostupné z:

<https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613>

¹⁹⁰ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 31.

¹⁹¹ BBC. *China declares all crypto-currency transactions illegal* [online]. 24. září 2021. [cit. 2021-11-27].

Dostupné z: <https://www.bbc.com/news/technology-58678907>

¹⁹² OLCOTT, Eleanor. *Chinese cryptocurrency traders look for ways around ban* [online]. 20. října 2021. [cit. 2021-11-27].

Dostupné z: <https://www.ft.com/content/e7d3b78c-a479-4d4a-9f99-b6f0f90b0935>

¹⁹³ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe. *Cryptocurrency compliance and risks: A European KYC/ AML perspective*, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 170.

obchodování s virtuálními měnami probíhalo pouze prostřednictvím účtů, které budou spojené s neanonymními bankovními účty.¹⁹⁴

Zavedeno bylo zejména pravidlo zakazující držení virtuálních měn na anonymních účtech. Každou virtuální peněženku je tedy nutno spárovat s účtem v některém z bank. Zakázáno bylo rovněž, aby prostředky na těchto peněženkách drželi cizinci, děti a mladiství.¹⁹⁵

V praxi to znamená, že si každý musí otevřít účet na své skutečné jméno u stejné banky, u které má účet poskytovatel služeb s virtuálními aktivy, aby mohl provést vklad nebo vybrat prostředky ze své virtuální peněženky. Banka i poskytovatel služeb musí ověřit totožnost uživatele v souladu s AML předpisy a s pravidly o hlášení transakcí.¹⁹⁶

Rovněž byly zveřejněny závazné pokyny pro banky spravující bankovní účty propojené s virtuálními měnami, které mají zajistit, aby byly dodržovány pravidla boje proti praní špinavých peněz. Tyto pokyny rovněž nařizují bankám, aby odmítly zřízení účtu poskytovatelům služeb s virtuálními aktivy, pokud neposkytnou identifikační údaje svých uživatelů.¹⁹⁷ Tyto pravidla vedly k tomu, že je trh v Jižní Koreji ovládaný čtveřicí hlavních poskytovatelů služeb s virtuálními aktivy.¹⁹⁸

Nicméně, nesprávcovské peněženky a transakce na P2P bázi nejsou touto regulací postiženy. Důvodem je pravděpodobně to, že neumožňují směnu virtuálních měn s fiat měnou. Vládu tudíž zřejmě virtuální měny nezajímají do té doby, než jsou převáděny na korejské wony.¹⁹⁹

5.3. Přístup FATF

FATF hraje v oblasti AML regulace nezaměnitelnou roli. Tato kapitola proto rozebírá přístup a doporučení v oblastech:

- regulace DEX, DApps a DeFi;

¹⁹⁴ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 31.

¹⁹⁵ Ministerstvo financí České republiky. *Veřejná konzultace Blockchain, virtuální měny a aktiva (využití technologie blockchain k evidenci cenných papírů)*. op. cit. s. 17.

¹⁹⁶ *Cryptocurrency Regulations in South Korea* [online]. 4. července 2018. [cit. 2021-11-27].

Dostupné z:

<https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-south-korea/>

¹⁹⁷ HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*. op. cit. s. 31.

¹⁹⁸ IM, Felix. *S. Korea's Crypto Rules Might Only Help the 'Big 4' Exchanges* [online]. 1. dubna 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.coindesk.com/policy/2021/04/01/s-koreas-crypto-rules-might-only-help-the-big-4-exchanges/>

¹⁹⁹ Ibid.

- indikátorů značících potenciální praní špinavých peněz či financování terorismu prostřednictvím virtuálních měn a jakou roli hrají P2P transakce;
- risk based approach a opatření ke zmírnění rizik spojených s atomovými swapy;
- travel rule a jeho aplikace na transakce s virtuálními měnami; a
- pravidel pro transakce na nebo z nesprávcovských peněženek.

5.3.1. Regulace DEX, DApps a DeFi

Jak bylo uvedeno v podkapitole 3.5.2., regulace decentralizovaných struktur je jednou z nových výzev AML regulace. Tyto aplikace nebo platformy většinou běží na DL, často ale mají centrální entitu s určitou mírou zapojení nebo kontroly. To se může projevat např. při vytvoření a spuštění virtuální měny, vývoji DApp funkcí a uživatelského rozhraní pro účty s administrativním klíčem nebo vybírání poplatků. Často může být DApp naprogramovaná tak, že vyžaduje, aby uživatel za interakci s DApp zaplatil poplatek, který by jinak běžně platil poskytovateli služeb. Tento poplatek plyne vlastníkovi, provozovateli, vývojáři nebo celé komunitě.²⁰⁰

Aplikace DeFi (tedy softwarový program) není podle standarů FATF považován za poskytovatele služeb s virtuálními měnami, protože se standardy nevztahují na základní software nebo technologii. Nicméně, tvůrci, vlastníci, provozovatelé a některé další osoby, které mají kontrolu nebo dostatečný vliv nad DeFi, mohou spadat pod FATF definici poskytovatelů služeb, pokud poskytují nebo aktivně usnadňují služby jinak poskytované regulovanými poskytovateli služeb. To platí i v případě, kdy se na službě podílejí další osoby nebo kdy jsou části procesu zautomatizovány. Vlastníky či provozovatele lze rozlišit podle jejich vztahu k prováděným činnostem. Může se jednat o vliv nad prostředky nebo jinými aspekty protokolu služby nebo se může jednat o existenci obchodního vztahu mezi takovými osobami a uživateli, a to i v případě, že je obchodní vztah vykonáván prostřednictvím chytré smlouvy nebo hlasovacích protokolů. V potaz mohou být brány i jiné parametry. Například jestli osobě plyne ze služby zisk nebo zda má možnost nastavovat nebo měnit její parametry.²⁰¹

Marketingové termíny nebo vlastní identifikace jako DeFi nejsou rozhodné v tom, zda je konkrétní vlastník nebo provozovatel poskytovatelem služeb podle definice FATF. Je zcela běžné, že se DeFi struktura označuje za decentralizovanou, i když ve skutečnosti zahrnuje osobu

²⁰⁰ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 27.

²⁰¹ *Ibid.* s. 27.

s kontrolou nebo dostatečným vlivem. Jurisdikce by v takových případech měly uplatňovat definici poskytovatelů služeb bez ohledu na vlastní označení. Zároveň by se měly řídit zásadou, že záměrem FATF je do definice zahrnout fyzické nebo právnické osoby, které provádějí dané finanční služby jako podnikání.²⁰²

Pokud nelze identifikovat právnickou nebo fyzickou osobu, která by měla kontrolu nebo dostatečný vliv na uspořádání DeFi, nemusí existovat ústřední vlastník nebo provozovatel, který by splňoval definici poskytovatele služeb s virtuálními aktivy. V takových situacích by měly země sledovat vznik rizik představované DeFi službami, a to i prostřednictvím zapojení zástupců z DeFi komunity. Pokud země ví o DeFi službách, které takto operují, měly by zvážit případná zmírňující opatření. Například mohou země zvážit možnost požadovat zapojení entity spadající pod FATF definici poskytovatele služeb s virtuálními aktivy do DeFi služeb operujících bez takové osoby. Země také mohou zvážit jiná zmírňující opatření v souvislosti s P2P transakcemi, která jsou vedena v podkapitole 5.3.3. této práce.²⁰³

5.3.2. Red flags

V dokumentu²⁰⁴ ze září 2020 zveřejnila FATF řadu indikátorů spojených s virtuálními měnami, které mohou značit potenciální užívání virtuálních měn k praní špinavých peněz či financování terorismu.²⁰⁵ Nicméně pouhá přítomnost těchto ukazatelů v nějaké činnosti automaticky neznamená, že se jedná o nezákonnou činnost či transakci. Například použití hardwarové peněženky může být legitimní způsob zabezpečení virtuálních měn proti krádeži. Přítomnost těchto ukazatelů je tedy potřeba posuzovat v kontextu dalších vlastností a charakteristik zákazníka, daného vztahu nebo logického obchodního vysvětlení.²⁰⁶

Zde jsou indikátory značící potenciální ML/CFT hrozby v souvislosti s P2P transakcemi:

1. osoby působí jako neregistrovaní/nelicencovaní poskytovatelé služeb s virtuálními aktivy na webových stránkách P2P směnárén. Tento indikátor je důležitý zejména, pokud existují obavy, že osoby zpracovávají obrovské množství převodů

²⁰² FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 27.

²⁰³ Ibid. s. 28.

²⁰⁴ FATF. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing red flags report* [online]. 14. září 2020. [cit. 2021-11-27].

Dostupné z:

<https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html>

²⁰⁵ FATF. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing red flags report*. op. cit. s. 3.

²⁰⁶ Ibid. s. 11.

virtuálních měn jménem svých zákazníků a účtují svým zákazníkům vyšší poplatky než transakční služby nabízené jinými směnárny;

2. abnormální objem transakcí s virtuálními měnami získanými z peněženek spojených s P2P platformou bez logického obchodního vysvětlení; a
3. virtuální měny převedené na nebo z peněženek, jejichž aktivita byla v minulosti spojena s mixovacími službami nebo P2P platformami.²⁰⁷

5.3.3. Risk based approach a opatření ke zmírnění rizik s atomovými swapy

Podle FATF je pro boj proti praní špinavých peněz a financování terorismu klíčový přístup založený na monitorování nově vznikajících rizik (**RBA**). Monitorování vznikajících rizik, včetně rizik souvisejících s novými technologiemi, by mělo sloužit jako podklad pro proces hodnocení těchto rizik a mělo by být vodítkem pro přidělování příslušných zdrojů na zmírnění těchto rizik.²⁰⁸

Předchozí verze dokumentu²⁰⁹ z roku 2015 vycházející z předchozích zpráv FATF, entitám zapojený do obchodu s virtuálními měnami poskytovala pokyny pro aplikaci doporučení FATF ve vztahu k virtuálním měnám. FATF zastával názor, že subjekty poskytující služby v oblasti směny virtuálních měn na fiat měny by měly podléhat odpovídající AML/CFT regulaci.²¹⁰

V říjnu 2021 byly pokyny z roku 2015 aktualizovány. Revidované pokyny se zaměřily na šest klíčových oblastí, v nichž bylo potřeba většího vedení ze strany FATF. Jednou z těchto klíčových oblastí bylo poskytnutí pokynů k rizikům a nástrojům, které mají země k dispozici k řešení rizik praní peněz a financování terorismu ve vztahu k peer-to-peer transakcím.²¹¹

Výsledky druhého přezkumu FATF norem zdůrazňují potřebu, aby země porozuměly rizikům praní peněz a financování terorismu spojeným s P2P transakcemi a tomu, jak jsou P2P transakce využívány v jejich zemích. Ačkoli FATF zatím nezaznamenal výrazný posun k většímu využívání P2P transakcí, přetrvává potenciální riziko, že se více transakcí s virtuálními měnami přesune do P2P prostoru. Potenciální větší přesun do P2P prostoru by mohl být motivován

²⁰⁷ FATF. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing red flags report*. op. cit. s. 9.

²⁰⁸ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 7.

²⁰⁹ Ibid.

²¹⁰ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, *Cryptocurrency compliance and risks: A European KYC/ AML perspective*, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 170.

²¹¹ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 9.

vyhnutím se regulaci či dohledu, protože stále více jurisdikcí implementuje standardy FATF a reguluje a dohlíží na poskytovatele služeb s virtuálními aktivy.²¹²

Pokud by se počet P2P transakcí zvýšil do té míry, že by prostřednictvím P2P transakcí docházelo ve značné míře k nezákonné činnosti, mohlo by to potenciálně snížit účinnost standardů FATF. Rizika související s P2P transakcemi by proto měla být průběžně a výhledově monitorována. V rámci toho by se země měli snažit pochopit, které typy P2P transakcí představují vyšší nebo nižší riziko. Mezi relevantní faktory potenciálně ovlivňující rozsah využití virtuální měny v P2P transakcích patří dostupnost virtuální měny a její transparentnost, bezpečnost a související transakční poplatky.²¹³

Pokud země zjistí, že P2P transakce představují vyšší AML/CFT rizika, která vyžadují další zmírňující opatření, mohou k jejich snížení na základě vyhodnocení rizik zvážit implementaci zmírňujících opatření.²¹⁴

Mezi opatření, která by státy měly zvážit k pochopení rizik P2P transakcí podle FATF patří:

1. komunikace s osobami ze soukromého sektoru, včetně poskytovatelů služeb v oblasti virtuálních měn a zástupců z P2P sektoru (např. pro konzultaci nových AML/CFT požadavků na P2P transakce);
2. školení pracovníků orgánů dohledu, finančních zpravodajských jednotek a pracovníků donucovacích orgánů; a
3. podpora vývoje metodik a nástrojů ke shromažďování, vyhodnocování a řešení rizik spojených s P2P transakcemi. Podpora vývoje metodik k identifikaci podezřelého chování a určení, zda jsou peněženky správcovské nebo nesprávcovské, a zapojení programátorů a vývojářů v této oblasti.²¹⁵

V závislosti na tom, jak jednotlivé státy vyhodnotí rizika spojená s P2P transakcemi nebo pouze určitými typy P2P transakcí, by země měly zvážit zavedení vhodných opatření ke zmírnění těchto rizik. Mezi taková zmírňovací opatření mimo jiné patří:

1. zavedení kontrol, které usnadní transparentnost P2P aktivit a/nebo aktivit překračujících hranice mezi povinnými a nepovinnými subjekty (tyto kontroly by

²¹² FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 18.

²¹³ Ibid. s. 19.

²¹⁴ Ibid. s. 19.

²¹⁵ Ibid. s. 39.

mohly zahrnovat ekvivalenty k hlášením o měnových transakcích nebo pravidlo pro vedení záznamů týkajících se takových převodů);

2. průběžný dohled nad poskytovateli služeb s virtuálními aktivy a subjekty působícími v oblasti virtuálních měn se zvláštním zaměřením na transakce s nesprávcovskými peněženkami (např. dohled který potvrdí, zda poskytovatel služeb v oblasti virtuálních měn dodržuje platné předpisy týkající se těchto transakcí);
3. uložení povinnosti poskytovatelům služeb s virtuálními aktivy zprostředkovávat transakce pouze na a z adres, které jsou podle jejich vlastního zhodnocení rizik považovány za přijatelné;
4. uložení povinnosti poskytovatelům služeb s virtuálními aktivy zprostředkovávat transakce pouze od a pro další poskytovatele služeb s virtuálními aktivy a případně další povinné osoby podle AML regulace;
5. uložení dodatečných AML požadavků na poskytovatele služeb s virtuálními aktivy, kteří umožňují transakce z a do subjektů, které nejsou povinnými osobami (např. zvýšené požadavky na vedení záznamů o transakcích, zvýšené požadavky na due diligence uživatelů);
6. pokyny zdůrazňující důležitost toho, aby poskytovatelé služeb s virtuálními aktivy uplatňovali RBA při jednání se zákazníky, kteří se účastní P2P transakcí nebo je usnadňují;
7. vydávání veřejných pokynů a doporučení a provádění informačních kampaní s cílem zvýšit povědomí o rizicích, která P2P transakce představují.²¹⁶

5.3.4. Travel rule

Doporučení č. 16²¹⁷ stanoví požadavky na elektronické převody prostředků. Jedná se o tzv. „travel rule“ a je to klíčové opatření v oblasti AML/CFT, které má zajistit, aby původci a příjemci finančních transakcí byli identifikovatelní a nebyli anonymní.²¹⁸

²¹⁶ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 39-40.

²¹⁷ FATF. *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. op. cit. s. 16.

²¹⁸ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 17.

Travel rule zahrnuje povinnost získávat, uchovávat a předkládat požadované informace o příkazci a příjemci v transakcích s virtuálními měnami za účelem identifikace a hlášení podezřelých transakcí, přijímání opatření ke zmrazení a zákazu transakcí s určenými osobami a subjekty. Tyto požadavky se vztahují jak na poskytovatele služeb s virtuálními aktivy, tak na další povinné osoby, jako jsou finanční instituce, které přijímají nebo odesílají virtuální měny jménem klienta.²¹⁹ Na dodržování těchto požadavků ze strany poskytovatelů služeb s virtuálními měnami je kladen největší důraz.²²⁰ Zároveň ale mohou být zavedeny určité limity na objem transakce pro uplatnění těchto požadavků, aby byly vyloučeny transakce s nižším rizikem.²²¹

Jak vyplývá z druhého přezkumu FATF norem, většina jurisdikcí a většina poskytovatelů služeb s virtuálními aktivy nedodržuje požadavky vyplývající z doporučení č. 16. Tato skutečnost je jedním z největších překážek boje proti praní špinavých peněz a financování terorismu a snižuje to účinnost a dopad FATF standardů. Mimo to stále není k dispozici dostatek ucelených technologických řešení pro globální implementaci travel rule a zdá se, že pokrok se od posledního dvanáctiměsíčního přezkumu zpomalil.²²²

5.3.5. Pravidla pro transakce na nebo z nesprávcovských peněženek

Nesprávcovské (unhosted, self-hosted) peněženky nejsou poskytovány nebo spravovány finanční institucí nebo poskytovatelem služeb s virtuálními aktivy. Místo toho jsou umístěny na počítači uživatele nebo na hardwarovém zařízení. Vlastník virtuální měny kontroluje soukromé klíče spojené s adresami a může je mít uložené nebo je používat bez jakéhokoliv zásahu třetí strany.²²³

Poskytovatelé služeb by si měly být vědomi rizika, které představují převody na nesprávcovské peněženky a s tím související P2P transakce. Poskytovatelé služeb by kvůli snížení těchto rizik měli shromažďovat informace o transakcích na a z nesprávcovských peněženek. Tyto informace by potom měli monitorovat a vyhodnocovat, aby mohli určit, do jaké míry je daná transakce riziková a jaké opatření by vůči transakci nebo jednotlivému zákazníkovi měli uplatnit. Stejně by měli poskytovatelé služeb postupovat při zvažování rizik představovaných poskytovateli

²¹⁹ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 82.

²²⁰ FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 17.

²²¹ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 170.

²²² FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. op. cit. s. 18-19.

²²³ PAESANO, Federico. *Will new FinCEN rules drive cryptocurrency users underground?* [online]. 7. ledna 2021. [cit. 2021-11-27].

Dostupné z: <https://baselgovernance.org/blog/will-new-fincen-rules-drive-cryptocurrency-users-underground>

služeb, kteří ještě nemají licenci nebo nejsou registrovaní a není nad nimi vykonáván dohled, protože sídlí v jurisdikci, která ještě neimplementovala FATF standardy pro virtuální měny a poskytovatele služeb s nimi spojenými.²²⁴

Poskytovatelé služeb mohou v souladu s jejich analýzou rizik zavést další omezení, kontroly nebo zákazy transakcí s nesprávcovskými peněženkami. Mezi potenciální opatření navrhované FATF patří:²²⁵

1. rozšíření kontrolního rámce o specifická rizika, která představují transakce s nesprávcovskými peněženkami (např. zohledněním konkrétních uživatelů, vzorců chování, místních a regionálních rizik, a informací od regulátorů a donucovacích orgánů); a
2. prozkoumání možnosti zprostředkování transakcí pouze s jinými poskytovateli služeb a jinými povinnými osobami nebo s nesprávcovskými peněženkami, které poskytovatel služeb vyhodnotil jako spolehlivé.²²⁶

5.3.6. Míra implementace FATF pravidel

V posledním roce došlo k širšímu přijetí AML pravidel pro poskytovatele služeb s virtuálními aktivy. Ve srovnání s travel rule je celková míra implementace vyšší. Stále ovšem podle FATF není dostatečná k tomu, aby umožnila globální AML režim pro poskytovatele služeb s virtuálními aktivy. Pouze 35 z 58 jurisdikcí aplikujících FATF pravidla pro poskytovatele služeb s virtuálními aktivy má funkční AML režim. Nedostatečná regulace nebo její nedostatečné vynucování umožňuje jurisdikční arbitráž. To znevýhodňuje poskytovatele služeb s virtuálními aktivy, kteří plní své AML povinnosti, a zároveň poskytuje zločincům možnosti k nezákonným aktivitám.²²⁷

5.4. Návrh nové regulace nesprávcovských peněženek – USA

Úřad ministerstva financí Spojených států FinCEN (Sít' pro postihování finanční kriminality), který se zabývá bojem proti financování terorismu a praní špinavých peněz, vydal v prosinci 2020 návrh na regulaci nesprávcovských peněženek.²²⁸

²²⁴ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 86.

²²⁵ Ibid. s. 86.

²²⁶ Ibid. s. 87.

²²⁷ FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. op. cit. s. 36-37.

²²⁸ *FinCEN's Self-Hosted Wallet KYC Regulation Proposal* [online]. 8. ledna 2021. [cit. 2021-11-27]. Dostupné z: <https://www.coinfirm.com/blog/kyc-self-hosted-wallet-regulation-fincen/>

Uživatelé, kteří budou chtít převést virtuální měnu z centralizovaných směnárů do nesprávcovské peněženky, budou muset směnárně poskytnout osobní údaje o vlastníkovi dané peněženky, pokud bude odeslaná hodnota vyšší než 10 000 USD za jeden den. Směnárny budou navíc povinné předkládat a uchovávat záznamy zahrnující transakce s celkovou hodnotou vyšší než 10 000 amerických dolarů v daném období a záznamy o transakcích nad 3 000 amerických dolarů.²²⁹

5.5. Regulace nesprávcovských peněženek – Švýcarsko

Švýcarsko od 1. ledna 2020 vyžaduje, aby poskytovatelé služeb s virtuálními aktivy při transakcích v hodnotě nad 1000 CHF prokazovali identitu vlastníků peněženek. Ve své regulaci jde Švýcarsko nad rámec FATF úpravy a zakazuje převody neregulovaným poskytovatelům peněženek.²³⁰

Pokud poskytovatel služeb není schopen získat informace požadované pro provedení transakce, jsou tyto transakce povoleny pouze z a do externích peněženek klientů tohoto poskytovatele. Převod z nebo do peněženky patřící třetí straně je možný pouze tehdy, pokud dohlížená instituce, stejně jako v případě vztahu s klientem, nejprve ověřila totožnost třetí strany, zjistila totožnost skutečného vlastníka a prokázala vlastnictví peněženky třetí stranou pomocí vhodných technických prostředků.²³¹

5.6. Blacklisting

Vytvoření „černé listiny“ nelegálních finančních prostředků (takzvaný blacklisting) je doplňkovým prostředkem AML regulace, který vyžaduje, aby poskytovatelé služeb před přijetím prostředků zkontrolovali, jestli se nenachází na černé listině s nelegálními finančními prostředky.²³²

Na rozdíl od fiat měn a bankovního systému u virtuálních měn není efektivní blacklisting adres s virtuální měnou. Na rozdíl od bankovního systému, kde je účet vázán na identitu osoby, mohou být adresy s virtuálními měnami vytvořeny anonymně, v neomezeném množství a bez centrálního dohledu. To způsobuje, že je blacklisting adres virtuálních měn do značné míry neúčinný. Zločinci mohou vytvářet nové adresy, které nelze snadno propojit s existujícími

²²⁹ Ibid.

²³⁰ *Crypto Travel Rule in Switzerland by Swiss Financial Regulator (FINMA)* [online]. 1. října 2021. [cit. 2021-11-27].

Dostupné z:

<https://notabene.id/world/switzerland#:~:text=It%20went%20into%20effect%20on,proactive%20regulators%20on%20crypto%20assets.>

²³¹ Ibid.

²³² MÖSER, Malte a NARAYANAN, Arvind. *Effective Cryptocurrency Regulation Through Blacklisting*. op. cit. s. 1.

adresami uvedenými na černých listinách. Zároveň lze blacklisting adres snadno obejít převodem finančních prostředků na jinou adresu prostřednictvím nově vytvořených adres.²³³ Místo zařazování adres na černou listinu musí být pro efektivní regulaci zařazovány na černou listinu výstupy jednotlivých transakcí. Výstupy transakcí si lze představit jako jednotlivé mince. Tímto způsobem lze sledovat jednotlivé finanční prostředky pocházející z nezákonné činnosti.²³⁴

Blacklisting v kontextu virtuálních měn znamená vytvoření černých listin obsahujících konkrétní mince, o kterých je známo, že pocházejí z nezákonných zdrojů. To umožní sledovat nelegálně získané mince a jejich použití v nové transakci. Kdykoliv budou nezákonně získané mince použity v transakci, dostanou všechny mince použité ve stejné transakci status nezákonně získané mince, čímž je zajištěno, že mince nebude možné vyprat jejich přesunováním prostřednictvím řetězce transakcí na neznámou adresu. Výhodou tohoto přístupu je, že není nutné znát identitu uživatelů účastnících se transakcí.²³⁵

Kdokoliv by mohl zkontrolovat, zda jsou mince v konkrétní transakci na černé listině či nikoliv. Pouze regulovaní poskytovatelé služeb by byli ze zákona povinni odmítnout nebo zabavit nelegální mince. Každý uživatel by ale měl motivaci kontrolovat, zda jsou mince na černé listině, protože by mince na černé listině nemohl sám utratit.²³⁶ Motivace protistrany transakce ke kontrole mincí kvůli riziku budoucího zařazení na černou listinu platí jak u transakcí provedených prostřednictvím zprostředkovatelů, tak i pro atomové swapy, jejichž použitím si uživatelé mohou vyměnit své mince s jiným uživatelem bez zapojení těchto zprostředkovatelů.²³⁷

Implementace blacklistingu virtuálních měn vyžaduje další infrastrukturu a ztěžuje odesílání a přijímání virtuálních měn, protože by uživatelé museli před přijetím mincí zkontrolovat, zda se mince nenachází na černé listině. Pro efektivní využití blacklistingu by byla nutná určitá míra mezinárodní koordinace, aby bylo zabráněno zločincům přesměrování finančních prostředků přes země, které by černé listiny nepodporovali. Regulátoři by mohli projevovat neochotu zveřejňovat informace o nezákonné činnosti. Stejně tak by samotní uživatelé mohli mít s takovým přístupem problém, protože zavádí centralizovanou kontrolu, které se virtuální měny snaží od počátku vyhnout.²³⁸

²³³ Ibid. s. 1.

²³⁴ Ibid. s. 1.

²³⁵ MÖSER, Malte a NARAYANAN, Arvind. *Effective Cryptocurrency Regulation Through Blacklisting*. op. cit. s. 4.

²³⁶ Ibid. s. 4.

²³⁷ Ibid. s. 17.

²³⁸ Ibid. s. 4.

5.7. Technologické řešení

Boj proti nezákonným činnostem spojeným s virtuálními měnami bude nejspíš vyžadovat technologické inovace. To je dáno mimo jiné skutečností, že existuje více typů virtuálních měn, fungujících na jiných principech. Tím pádem například nástroje dobře fungující při sledování bitcoinových transakcí nefungují při sledování transakcí s Monerem. Zároveň je rozdíl, zda se v jednotlivých případech jedná o centralizované nebo decentralizované poskytovatele služeb s virtuálními aktivy. Donucovací orgány mohou po centralizovaných poskytovatelích služeb požadovat informace o jejich zákaznících podezřelých z nezákonných transakcí. Mnoho decentralizovaných poskytovatelů služeb ovšem nevede žádné záznamy o totožnosti uživatelů a neuchovává přehled provedených transakcí.²³⁹

Donucovací orgány by proto měli spolupracovat s odborníky na blockchainovou technologii. Společně totiž sdílejí stejný cíl, minimalizovat nezákonné financování v systému virtuálních měn. Odborníci na AML regulaci a odborníci na virtuální měny by měli společně prozkoumat možné využití platform virtuálních měn k podpoře ML/FT cílů, a to buď větším zhodnocením čistších mincí nebo zapojením uživatelů do ověřování hlášení o nezákonných transakcích a uživatelích.²⁴⁰

Vlastnosti DL technologií a protokolů by mohly být potenciálně využity ke zmírnění ML/FT rizik spojených s virtuálními měnami. Na specializovaném DL přístupném pouze poskytovatelům služeb s virtuálními měnami a donucovacím orgánům by mohly být registrovány a ověřovány informace o jednotlivých transakcích a skutečných majitelích virtuálních měn. Toto řešení sebou ovšem nese značné technické a právní problémy, zejména z hlediska požadavků ochrany osobních údajů. Kromě toho by přístup k těmto informacím a jejich využívání donucovacími orgány muselo být přísně regulováno, aby bylo zabráněno jakémukoliv zásahu do nich. To znamená, že by takový soukromý DL musel splňovat podmínky nastavené mezinárodními pravidly. Taková pravidla by musela být přijata všemi jurisdikcemi, pod které by spadaly všechny entity zapojené do takové sítě. K přijetí takových pravidel, a potenciálnímu využití DL technologie pro AML/CFT účely, dnes existuje řada překážek. Zejména nedostatek jasných mezinárodních pokynů v tomto směru.²⁴¹

²³⁹ FANUSIE, Yaya J. Financial Authorities Confront Two Cryptocurrency Ecosystems. In: *Global Governance to Combat Illicit Financial Flows*. op. cit. s. 29.

²⁴⁰ Ibid. s. 29.

²⁴¹ POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition*. op. cit. s. 172.

Podle FATF mohou být k dispozici i jiná technologická řešení. Mimo jiné by mohl být vyvinutý systém k identifikaci a verifikaci zákazníků, sledování transakcí a dalších due dilligence požadavků. Podle FATF by ke snížení AML/CFT rizik mohly sloužit aplikační programové rozhraní (APIs), které poskytují informace o identifikaci klienta nebo umožňují nastavit podmínky, které musí být splněny, než se jednotlivé transakce uskuteční.²⁴²

Mimo to jsou vyvíjeny nové produkty snižující možnosti zločinců prát špinavé peníze. Například společnost Chainalysis pomáhá sledovat původ finančních prostředků z anonymních peněženek i za situace, kdy byly využity mixovací služby nebo bylo provedeno velké množství transakcí.²⁴³

²⁴² Ibid. s. 172.

²⁴³ DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic*. op. cit. s. 3.

Závěr

Atomové swapy představují model peer-to-peer transakcí s virtuálními měnami. To znamená, že umožňují směnu virtuálních měn bez zprostředkování třetí stranou. Zároveň uživatelům poskytují jistotu, že jim budou jejich mince navraceny, pokud druhá strana transakce nesplní předem sjednané podmínky nebo se v průběhu transakce rozhodne, že o směnu nemá zájem.

Atomové swapy uživatelům využívajícím nesprávcovské peněženky umožňují při transakcích obejít poskytovatele služeb s virtuálními měnami, kteří jsou povinnými osobami z pohledu současné AML regulace. Off-chain atomové swapy navíc znesnadňují sledovatelnost jednotlivých mincí, protože probíhají na soukromém kanálu, a kromě zúčastněných stran nikdo nezná podrobnosti transakce. Z toho důvodu mohou být zneužity jako nástroj k praní špinavých peněz nebo financování terorismu a tím pádem jsou potenciálním rizikem pro AML regulaci.

Otázkou zůstává, jestli jsou rizika spojená s atomovými swapy tak velká a aktuální, aby vyžadovala revizi současné AML regulace. FATF s cílem zodpovědět tuto otázku nechal vypracovat soubor metrik o tom, v jakém rozsahu (i) jsou virtuální měny využívány na P2P bázi, (ii) jsou převáděny pomocí poskytovatelů služeb či jejich prostřednictvím a (iii) dochází k využívání P2P transakcí k nezákonným účelům.

Z údajů poskytnutých FATF lze vyvodit několik závěrů. Na P2P bázi je převáděno potenciálně velké množství virtuálních měn, ale není zde trend k jejich většímu využívání. U P2P transakcí je větší podíl nezákonných transakcí ve srovnání s transakcemi prostřednictvím poskytovatelů služeb s virtuálními aktivy. Díky rozdílům v poskytnutých údajích je ovšem velikost P2P sektoru a s ním spojených rizik nejasná. Proto by se podle FATF měly jednotlivé jurisdikce zaměřit spíše na regulaci poskytovatelů služeb s virtuálními aktivy a důsledné vynucování těchto pravidel.

Na druhou stranu i FATF připouští, že se situace může změnit. Trendy v P2P oblasti se mohou projevit až za několik let a počet P2P transakcí se může rapidně zvýšit. To může být mimo jiné způsobené velkým nárustem popularity DeFi nebo tím, že budou globálně přijímána a vynucována přísnější pravidla pro poskytovatele služeb s virtuálními aktivy. Nárustem P2P sektoru by se mohly zvýšit i rizika s ním spojená. Současný, ani Evropskou unií v současné době projednávaný, rámec AML regulace na zvýšení rizik těchto rizik není připravený.

Jakým způsobem lze tato rizika zmírnit? Ani tak přísné regulace jako mají v Číně nebo Jižní Koreji nemusí být efektivním řešením rizik spojených s P2P transakcemi virtuálních měn.

Naopak je možné, že zákaz virtuálních měn nebo povinnost propojení správcovských peněženek s bankovním účtem, povedou k nárstu P2P platformem a jejich menší přehlednosti a možnosti kontroly.

Existují ale efektivnější způsoby řešení těchto rizik. Podle FATF je zejména potřeba, aby země rizikům spojeným s P2P transakcemi rozuměly, monitorovaly je a v případě potřeby implementovaly adekvátní zmírňující opatření. Za tímto účelem by země měly spolupracovat s osobami z oboru virtuálních měn, a to jak s odborníky na problematiku virtuálních měn, tak s poskytovateli služeb s virtuálními aktivy. Zmírňující opatření by se měly soustředit zejména na regulaci transakcí s nesprávcovskými peněženkami a důsledné vymáhání aplikace travel rule. Švýcarsko je příkladem země s důslednou regulací nesprávcovských peněženek.

Ve vztahu k DeFi a decentralizovaným platformám je důležitý zejména extenzivní výklad definice poskytovatelů služeb s virtuálními aktivy z pohledu FATF. Podle něj lze za povinné osoby považovat i platformy, které sebe sami označují za decentralizované a nepovažují se za povinné osoby podle AML regulace.

Podpurným opatřením k AML regulaci může být tzv. blacklisting. Tedy vytvoření listiny finančních prostředků, které mají původ v nezákonné činnosti. Účastníci transakcí s virtuálními měnami by kontrolovali, zda mince, které mají být předmětem transakce, nejsou uvedené na této listině. V případě, že by mince na listině byly uvedené, by účastník transakce ve svém vlastním zájmu transakci neuskutečnil, protože by mince sám nemohl později utratit. Poskytovatelé služeb by měli povinnost transakce s takovými mincemi neuskutečnit.

Vedle regulatorního řešení se nabízí technologické řešení. Samotné vlastnosti DL technologií a protokolů by mohly být využity ke zmírnění rizik spojených s P2P platformami. To ještě víc zdůrazňuje potřebu spolupráce odborníků na AML regulaci s odborníky na virtuální měny a blockchain technologii.

Seznam použitých zkratek

AML	Anti Money Laundering
AML nařízení	Návrh nařízení Evropského parlamentu a Rady o předcházení využívání finančního systému k praní peněz nebo financování terorismu
AML zákon	Zákon č. 527/2020 Sb., kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a další související zákony, zákony související s přijetím zákona o evidenci skutečných majitelů a zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů
CEXs	Centralized exchanges
CFT	Combating the Financing of Terrorism
DApp	Decentralized applications
DeFi	Decentralized finance
DEXs	Decentralized exchanges
DL	Distributed ledger
druhý přezkum FATF norem	Second 12-Month Review of Revised FATF Standards on Virtual Assets and VASPs
EBA	Evropský orgán pro bankovníctví
ECB	Evropská centrální banka
EU	Evropská unie
FATF	Finanční akční výbor
FT	Terrorism Financing
HTLCs ICOs	Hash Time Locked Contracts Initial Coin Offerings
ML	Money Laundering

MiCa	Návrh nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937
nařízení 2015/847	Nařízení Evropského parlamentu a Rady (EU) 2015/847 ze dne 20. května 2015 o informacích doprovázejících převody peněžních prostředků a o zrušení nařízení (ES) č. 1781/2006
nařízení o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv	Návrh nařízení Evropského parlamentu a Rady o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv
P2P	peer-to-peer
RBA	Risk-based approach
IV AML směrnice	Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES
V AML směrnice	Směrnice Evropského parlamentu a rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU
VI AML směrnice	Návrh směrnice Evropského parlamentu a rady o mechanismech, které mají členské státy zavést za účelem předcházení využívání finančního systému k praní peněz nebo financování terorismu, a o zrušení směrnice (EU) 2015/849

Seznam použitých zdrojů

1. Seznam použitých internetových zdrojů

BBC. China declares all crypto-currency transactions illegal [online]. 24. září 2021. [cit. 2021-11-27]. Dostupné z: <https://www.bbc.com/news/technology-58678907>

COLLOMB, Alexis, DE FILIPPI, Primavera a SOK, Klara. *From IPOs to ICOs: The Impact of Blockchain Technology on Financial Regulation*. [online]. 26. května 2018. [cit. 2021-11-27]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3185347

Cryptocurrency Regulations in South Korea [online]. 4. července 2018. [cit. 2021-11-27]. Dostupné z: <https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-south-korea/>

Crypto Travel Rule in Switzerland by Swiss Financial Regulator (FINMA) [online]. 1. října 2021. [cit. 2021-11-27]. Dostupné z: <https://notabene.id/world/switzerland#:~:text=It%20went%20into%20effect%20on,proactive%20regulators%20on%20crypto%20assets.>

DUPUIS, Daniel a GLEASON, Kimberley. *Money laundering with cryptocurrency: open doors and the regulatory dialectic* [online]. 10. srpna 2020. [cit. 2021-11-27]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3681297

EBA. *EBA Opinion on 'virtual currencies'* [online]. 4. července 2014. [cit. 2021-11-27]. Dostupné z: <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1>

EBA. *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector* [online]. 3. března 2021. [cit. 2021-11-27]. Dostupné z: <https://www.eba.europa.eu/eba-highlights-key-money-laundering-and-terrorist-financing-risks-across-eu>

ECB. *Virtual Currency Schemes* [online]. říjen 2012. [cit. 2021-11-27]. Dostupné z: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

Ensuring cryptocurrency exchange KYC compliance [online]. 11. února 2021. [cit. 2021-11-27]. Dostupné z: <https://medium.com/the-regtech-hub/ensuring-cryptocurrency-exchange-kyc-compliance-9899056a554>

ERBSOVÁ, Hana. *Kryptoměny: EU připravuje přísnější AML regulaci* [online]. 31. srpna 2021. [cit. 2021-11-27]. Dostupné z: <https://www.amlolutions.cz/aktuality/kryptomeny-eu-pripravuje-prisnejsi-aml-regulaci>

ERGUN, Huseyin, RAZBONYALI, Mesut, GUVENOGLU, Erdal a RAZBONYALI, Can. Distributed Atomic Swap on Cryptocurrencies. *Computer Engineering and Intelligent Systems* [online]. 2020, roč. 11, č. 4 [cit. 2021-11-27]. ISSN 2222-2863.

Dostupné z: <https://www.researchgate.net/publication/344158341>

EVROPSKÁ KOMISE. *Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules* [online]. 20. července 2021. [cit. 2021-11-27].

Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

FANUSIE, Yaya J. Financial Authorities Confront Two Cryptocurrency Ecosystems. In: *Global Governance to Combat Illicit Financial Flows* [online]. 11. října 2018. [cit. 2021-11-27].

Dostupné z:

https://backend-live.cfr.org/sites/default/files/report_pdf/Discussion_Paper_Collection_Kahler_et_al_IFFs_OR.pdf#page=59

FATF. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs* [online]. 5. července 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>

FATF. *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* [online]. 16. února 2012, říjen 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

FATF. *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers* [online]. 28. října 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>

FATF. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing red flags report* [online]. 14. září 2020. [cit. 2021-11-27].

Dostupné z:

<https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html>

FEBBI, Stefano. *EU publishes package of legislative proposals aimed at strengthening AML/CFT rules* [online.] srpen 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.twobirds.com/en/news/articles/2021/global/eu-publishes-package-of-legislative-proposals-aimed-at-strengthening-aml-cft-rules>

FINANCIAL SERVICES AGENCY. *Research on privacy and traceability of emerging blockchain based financial transactions* [online]. 20. března 2019. [cit. 2021-11-27].

Dostupné z: https://www.fsa.go.jp/en/policy/bgin/ResearchPaper_MRI.pdf

FinCEN's Self-Hosted Wallet KYC Regulation Proposal [online]. 8. ledna 2021. [cit. 2021-11-27].
Dostupné z: <https://www.coinfirm.com/blog/kyc-self-hosted-wallet-regulation-fincen/>

HAN, Runchao, LIN, Haoyu a YU, Jiangshan. *On the optionality and fairness of Atomic Swaps* [online]. 2019 [cit. 2021-11-27].

Dostupné z:

https://www.researchgate.net/publication/334958051_On_the_optionality_and_fairness_of_Atomic_Swaps

HAVLÍČEK, Ondřej a ŠARAPATKA, Matěj. *Novinky z oblasti české a evropské regulace finančních institucí za měsíc červenec 2021* [online]. 11. srpna 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.epravo.cz/top/aktualne/novinky-z-oblasti-ceske-a-evropske-regulace-financnich-instituci-za-mesic-cervenec-2021-113417.html>

HOENISCH, Philipp a PINO, Lucas Soriano del. *Atomic Swaps between Bitcoin and Monero* [online]. 2021 [cit. 2021-11-27].

Dostupné z:

https://www.researchgate.net/publication/348928221_Atomic_Swaps_between_Bitcoin_and_Monero

HOLMAN, Daniel a STETTNER Barbara. *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches* [online]. 2018 [cit. 2021-11-27].

Dostupné z:

https://www.allenoverly.com/global/-/media/sharepoint/publications/publications/en-gb/documents/aml18_allenoverly.pdf?la=en-gb&hash=6D8F26DB73634846A427983AD2F217A7

IM, Felix. *S. Korea's Crypto Rules Might Only Help the 'Big 4' Exchanges* [online]. 1. dubna 2021. [cit. 2021-11-27].

Dostupné z:

<https://www.coindesk.com/policy/2021/04/01/s-koreas-crypto-rules-might-only-help-the-big-4-exchanges/>

Internetové stránky btc-slovník.cz [online]. [cit. 2021-11-27].

Dostupné z: <https://btc-slovník.cz/>

Internetové stránky FATF [online]. [cit. 2021-11-27].

Dostupné z: <https://www.fatf-gafi.org/about/>

Internetové stránky kryptomagazin.cz [online]. [cit. 2021-11-27].

Dostupné z:

<https://kryptomagazin.cz/jaky-je-rozdil-mezi-technologie-blockchain-a-distributed-ledger-technology/>

Internetové stránky kurzy.cz [online]. [cit. 2021-11-27].

Dostupné z: <https://www.kurzy.cz/tema/6193233.html>

Internetové stránky platonlife.com [online]. [cit. 2021-11-27].

Dostupné z: <https://platonlife.com/cs/blog/platon-wallet-what-is-a-custodian-wallet/>

Internetové stránky ranking-chwilowek.net [online]. [cit. 2021-11-27].

Dostupné z: <https://cs ranking-chwilowek.net/atomovy-swap-co-to-je-a-jak-to-funguje-57>

JL777. BarterDEX – A Practical Native DEX. In: *github* [online]. 5. listopadu 2016. [cit. 2021-11-27].

Dostupné z:

<https://github.com/SuperNETorg/komodo/wiki/BarterDEX-%E2%80%93-A-Practical-Native-DEX>

LIN. Lindsay X., *Deconstructing decentralized exchanges* [online]. 5. ledna 2019. [cit. 2021-11-27].

Dostupné z: <https://stanford-jblp.pubpub.org/pub/deconstructing-dex/release/1>

MARTINÍK, Pavel. *Aktuální otázky AML regulace* [online]. 16. prosince 2019. [cit. 2021-11-27].

Dostupné z: <https://advokatnidenik.cz/2019/12/16/aktualni-otazky-aml-regulace/>

McGUINNESS, Mairead. Cryptocurrency. In: *Twitter* [online]. 20. července 2021. [cit. 2021-11-27].

Dostupné z: <https://twitter.com/McGuinnessEU/status/1417494016741023753>

Ministerstvo financí České republiky. *Veřejná konzultace Blockchain, virtuální měny a aktiva (využití technologie blockchain k evidenci cenných papírů)* [online]. 30. listopadu 2018. [cit. 2021-11-27].

Dostupné z:

<https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613>

MIRAZ, Mahdi H. a DONALD, David C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Annals of Emerging Technologies in Computing (AETiC)* [online]. 2019, roč. 3, č. 1 [cit. 2021-11-27]. ISSN 2516-029X.

Dostupné z:

https://www.researchgate.net/publication/330041815_Atomic_Crosschain_Swaps_Development_Trajectory_and_Potential_of_Non-monetary_Digital-Token_Swap_Facilities

MORRIS, David Z. *No, the European Union Is Not ‘Banning Anonymous Crypto Wallets’* [online]. 21. července 2021. [cit. 2021-11-27].

Dostupné z:

https://finance.yahoo.com/news/no-european-union-not-banning-171752952.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guc e_referrer_sig=AQAAAE0jTjBW0fLHKyu39PYJaBfOo4bTZc2HuQfH5HFfISvXWElCPogj2Q5SI9sBXUJXUq9of8KtSOMSlvcnJhJmIfO8j_1X8hPOoa6RfKHQyHOfXUvLRMzK1cq3ZDLK8Y5T35jHalbAmmZTZ_cvLidqrXjaA44oEo6yfyc_wKYXTaAR

MÖSER, Malte a NARAYANAN, Arvind. *Effective Cryptocurrency Regulation Through Blacklisting* [online]. 2019 [cit. 2021-11-27].

Dostupné z:

<https://maltemoeser.de/paper/blacklisting-regulation.pdf>

NOCAROVÁ, Michaela. Jaký je rozdíl mezi technologií Blockchain a Distributed Ledger Technology? In: *kryptomagazin* [online]. 4. června 2020. [cit. 2021-11-27].
Dostupné z: <https://kryptomagazin.cz/jaky-je-rozdil-mezi-technologii-blockchain-a-distributed-ledger-technology/>

NOLAN, Tier. Alt chains and atomic transfers. In: *Bitcoin Forum* [online]. 2. května 2013 [cit. 2021-11-27]
Dostupné z: <https://bitcointalk.org/index.php?topic=193281.0>

OLCOTT, Eleanor. *Chinese cryptocurrency traders look for ways around ban* [online]. 20. října 2021. [cit. 2021-11-27].
Dostupné z: <https://www.ft.com/content/e7d3b78c-a479-4d4a-9f99-b6f0f90b0935>

ORCUTT, Mike. Criminals laundered \$2.8 billion in 2019 using crypto exchanges, finds a new analysis. In: *technology review* [online]. 16. ledna 2020. [cit. 2021-11-27].
Dostupné z: <https://www.technologyreview.com/2020/01/16/130843/cryptocurrency-money-laundering-exchanges/>

PAESANO, Federico. *Will new FinCEN rules drive cryptocurrency users underground?* [online]. 7. ledna 2021. [cit. 2021-11-27].
Dostupné z: <https://baselgovernance.org/blog/will-new-fincen-rules-drive-cryptocurrency-users-underground>

PAPHITIS, Sotiris. *The EU's AML Package: an examination* [online]. 12. října 2021. [cit. 2021-11-27].
Dostupné z: <https://europeanlawblog.eu/2021/10/12/7922/>

POCHER, Nadia. Self-hosted wallets: the elephant in the crypto room? In: *kuleuven* [online]. 11. března 2021. [cit. 2021-11-27].
Dostupné z: <https://www.law.kuleuven.be/citip/blog/self-hosted-wallets/>

POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS. *Virtual currencies and terrorist financing: assessing the risks and evaluating responses* [online]. květen 2018. [cit. 2021-11-27].
Dostupné z: [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)

POLICY DEPARTMENT FOR ECONOMIC, SCIENTIFIC ANF QUALITY OF LIFE POLICIES. *Cryptocurrencies and blockchain Legal context and implications for financial crime, money laundering and tax evasion* [online]. 9. 6. 2018 [cit. 2021-11-27].
Dostupné z: <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>

POSKRIAKOV, Fedor, CHIRIAEVA, Maria a CAVIN, Christophe, Cryptocurrency compliance and risks: A European KYC/ AML perspective, In: *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, First Edition* [online]. 2018 [cit. 2021-11-27]. ISSN 2631-2999.

Dostupné z:

https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

RECOVÁ, Alžběta. *Evropský legislativní balíček AML a relevantní ustanovení pro advokáty* [online]. 29. září 2021. [cit. 2021-11-27].

Dostupné z:

<https://advokatnidenik.cz/2021/09/29/evropsky-legislativni-balicek-v-oblasti-aml-a-relevantni-ustanoveni-pro-advokaty/>

RODRIGUES, Gustavo, LAHIS, Kurtz. *Cryptocurrencies and anti-money laundering regulation in the G20* [online]. 27. září 2019. [cit. 2021-11-27].

Dostupné z: <https://irisbh.com.br/en/publicacoes/19906/>

SHARMA, Avin M. *Cryptocurrency and financial risks* [online]. prosinec 2020. [cit. 2021-11-27].

Dostupné z: <https://digitalcommons.liberty.edu/doctoral/2791/>

What Is a Decentralized Exchange (DEX)? In: *CryptoCompare* [online]. 12. března 2019

Dostupné z:

<https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/>

Why Atomic Swaps Are Revolutionizing Decentralized Crypto Trading. In: *learn.bybit* [online]. 12. října 2021. [cit. 2021-11-27].

Dostupné z: <https://learn.bybit.com/blockchain/what-are-atomic-swaps/>

2. Seznam použitých právních předpisů

Nařízení Evropského parlamentu a Rady (EU) 2015/847 ze dne 20. května 2015 o informacích doprovázejících převody peněžních prostředků a o zrušení nařízení (ES) č. 1781/2006.

Návrh nařízení Evropského parlamentu a Rady o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv.

Návrh nařízení Evropského parlamentu a Rady o předcházení využívání finančního systému k praní peněz nebo financování terorismu.

Návrh nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937.

Návrh nařízení Evropského parlamentu a Rady, kterým se zřizuje Orgán pro boj proti praní peněz a financování terorismu a mění nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

Návrh směrnice Evropského parlamentu a rady o mechanismech, které mají členské státy zavést za účelem předcházení využívání finančního systému k praní peněz nebo financování terorismu, a o zrušení směrnice (EU) 2015/849.

Směrnice Evropského parlamentu a rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU.

Zákon č. 183/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích.

Zákon č. 527/2020 Sb., kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a další související zákony, zákony související s přijetím zákona o evidenci skutečných majitelů a zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů.

Atomic swap: riziko pro AML regulaci?

Abstrakt

Tato diplomová práce se zabývá atomovými swapy. Zejména jejich charakteristikou a vztahem k AML regulaci. Cílem této práce je zhodnocení rizik, které atomové swapy představují pro AML regulaci, a způsobů, kterými je tato rizika možné řešit.

V první části této práce jsou nejprve stručně popsány pojmy a technologie potřebné k pochopení atomových swapů. Mimo jiné jsou zde popsány distribuované databáze, kryptografické klíče, peněženky a směnárny s virtuálními měnami. Následuje popis evoluce atomových swapů a toho, jak atomové swapy fungují a jaké jsou jejich výhody a nevýhody.

Druhá část analyzuje současnou regulaci proti praní špinavých peněz a financování terorismu z pohledu FATF, Evropské unie a České republiky ve vztahu k virtuálním měnám a atomovým swapům. Zejména se zaměřuje na definici virtuálních měn a povinných osob.

Po pochopení fungování atomových swapů a analýze AML regulace ve vztahu k nim je možné zhodnotit, zda pro ni atomové swapy představují riziko. Tomu se věnuje třetí část této práce. Nejdřív obecně představuje problematiku praní špinavých peněz a využívání virtuálních měn pro nezákonné účely. Nakonec zkoumá rizika, která představují virtuální měny sami o sobě a která představují atomové swapy a technologie, které díky nim nabírají na popularitě. Takovou technologií je například DeFi, neboli softwarový program fungující na blockchainu a poskytující finanční služby s virtuálními aktivy.

Čtvrtá část zkoumá projednávané změny AML regulace v Evropské unii. Zejména jaké dopady budou změny mít na regulaci virtuálních měn a zda adresují rizika spojená s atomovými swapy.

Pátá část uvádí několik regulatorních přístupů k AML regulaci virtuálních měn a zkoumá, zda a jakým způsobem jednotlivé přístupy řeší rizika související s atomovými swapy. Zabývá se zákazem virtuálních měn v Číně, povinností propojit peněženky s virtuálními měnami s bankovními účty v Jižní Koreji, přístupem FATF, regulací peněženek s virtuálními měnami ve Spojených státech amerických a Švýcarsku, metodou zvanou blacklisting, a nakonec technologickými řešeními.

Klíčová slova: kryptoměny, P2P, AML

Atomic swap: a risk for AML regulation?

Abstract

This thesis deals with atomic swaps. Particularly it deals with their characteristics and relation to AML regulation. The aim of this thesis is to assess the risks that atomic swaps pose to AML regulation and the ways in which these risks can be addressed.

The first part of this thesis briefly describes the concepts and technologies needed to understand atomic swaps. Among other things this part describes distributed databases, cryptographic keys, wallets, and virtual currency exchanges. This is followed by a description of the evolution of atomic swaps, how atomic swaps work and what are their advantages and disadvantages.

The second part analyses the current regulation against money laundering and terrorist financing from the perspective of FATF, the European Union and the Czech Republic in relation to virtual currencies and atomic swaps. Particularly it focuses on the definition of virtual currencies and obliged entities.

After the explanation how atomic swaps work and the analysis of AML regulation in relation to atomic swaps, it is possible to assess whether atomic swaps pose a risk to AML regulation. This is the focus of the third part of this thesis. It first introduces the issue of money laundering and the use of virtual currencies for illicit purposes in general. Finally, it examines the risks posed by virtual currencies, atomic swaps and the technologies that are gaining popularity thanks to atomic swaps. One of such technologies is DeFi, a software programme that runs on blockchain and provides financial services with virtual assets.

The fourth part examines the changes of AML regulation currently discussed in the European Union. Particularly what impact the changes will have on the regulation of virtual currencies and whether they address the risks associated with atomic swaps.

The fifth section outlines several regulatory approaches to AML regulation of virtual currencies and examines whether and how each approach addresses the risks associated with atomic swaps. It looks at the ban on virtual currencies in China, the obligation to link virtual currency wallets to bank accounts in South Korea, the FATF approach, the regulation of virtual currency wallets in the United States and Switzerland, a method called blacklisting, and finally, the technological solutions.

Keywords: cryptocurrencies, P2P, AML