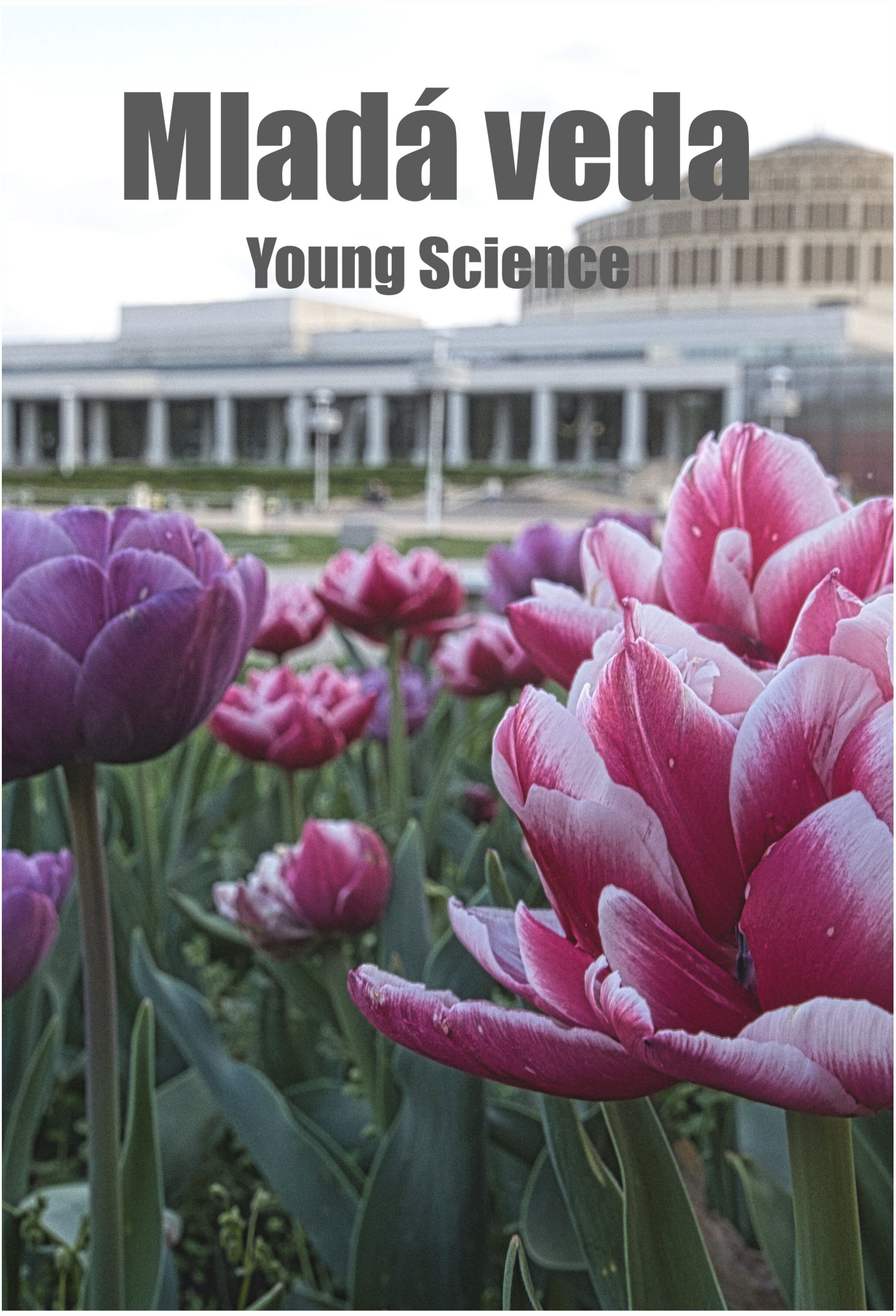
ISSN 1339-3189 1/2026

Mladá veda

Young Science



www.mladaveda.sk

Mladá veda
Young Science

MEDZINÁRODNÝ VEDECKÝ ČASOPIS MLADÁ VEDA / YOUNG SCIENCE

Číslo 1, ročník 14., vydané v marci 2026
ISSN 1339-3189, EV 167/23/EPP
Kontakt: info@mladaveda.sk, tel.: +421 908 546 716, www.mladaveda.sk
Fotografia na obálke: Wrocław. © Branislav A. Švorc, foto.branisko.at

VYDAVATEĽ
Vydavateľstvo UNIVERSUM, spol. s r. o.
www.universum-eu.sk
Javorinská 26, 080 01 Prešov
Slovenská republika

Mladá veda
Young Science
ISSN 1339-3189

Vol. 14 (1), pp. 201-206

ANONYMITA V KRYPTOMENÁCH: TECHNIKY UTAJENIA, MOŽNOSTI DEANONYMIZÁCIE A REGULAČNÉ DOPADY

ANONYMITY IN CRYPTOCURRENCIES: TECHNIQUES OF CONCEALMENT, POSSIBILITIES OF DEANONYMIZATION AND REGULATORY IMPACTS

Libor Jakubec [1]

Autor pôsobí ako externý doktorand na Katedre bezpečnostných vied Vysokej školy bezpečnostného manažérstva v Košiciach. Vo svojom výskume (resp. dizertačnej práci) sa venuje problematike bezpečného používania kryptomien v bežnom živote.

The author is an external PhD student at the Department of Security Sciences at the University of Security Management in Košice. His research (i.e., dissertation) focuses on the issue of the safe use of cryptocurrencies in everyday life.

Abstract

Cryptocurrencies are a highly dynamic field, and technological solutions designed to enhance their anonymity are evolving rapidly. This development is driven primarily by three key factors. First, cryptocurrency users increasingly value digital privacy. As more personal and financial activities move online where traditional cryptocurrencies typically provide only pseudonymity there is a growing interest in protecting users' sensitive data from cyberattacks and surveillance. Second, this progress is a response to the capabilities of companies like Chainalysis, Elliptic, and TRM Labs which can deanonymize an increasing proportion of transactions on networks like Bitcoin and Ethereum. Third, regulatory pressure and AML/KYC requirements continue to intensify. As a result, new privacy-enhancing technologies are emerging that preserve user anonymity even within strict regulatory frameworks. The cryptocurrency anonymity field thus combines advanced cryptographic techniques with regulatory efforts aimed at improving transparency and preventing abuse of digital assets. This work seeks to determine the extent to which cryptocurrencies can be considered truly anonymous, to identify the technical and legal tools available for tracking transactions and linking addresses, and to examine their implications for user privacy. Particular attention is paid to the main legal instruments that shape this area, in particular anti-money laundering and KYC obligations, FATF recommendations, the EU MiCA regulation, and procedures related to the seizure of cryptoassets.

[1] Adresa pracoviska: Ing. Libor Jakubec, Ústav humanitných a technologických vied, Vysoká škola bezpečnostného manažérstva v Košiciach, Košťova 1, 040 01 Košice
E-mail: jakubec@itznalec.sk

Existing research suggests that while advanced privacy solutions can significantly hinder the identification of transactions, absolute anonymity cannot currently be guaranteed. The level of privacy depends not only on the underlying technology but also on user behaviour and the availability of forensic tools, and the regulatory environment governing the use of digital assets.
Keywords: cryptocurrencies, anonymity, private transactions, customer experience, regulatory impacts

Abstrakt
Kryptomeny ako také sú dynamickou oblasťou a riešenia v oblasti ich anonymity sa rovnako čoraz viac rozvíjajú. Je to predovšetkým z troch hlavných dôvodov. Prvý dôvod spočíva v tom, že používatelia kryptomien si čoraz viac zakladajú na digitálnom súkromí. Ľudia čoraz viac presúvajú svoje aktivity do online priestoru, kde tradičné kryptomeny poskytujú najčastejšie len pseudonymitu. Avšak napriek tomu vzrastá záujem chrániť citlivé údaje používateľov pred rôznymi kybernetickými útokmi či sledovaním. Druhý dôvod vznikol ako reakcia na firmy ako sú Chainalysis, Elliptic či TRM Labs, ktoré dokážu deanonymizovať čoraz viac transakcií na menách Bitcoine alebo Ethereum. V neposlednom rade tretí dôvod spočíta v regulačnom tlaku a AML/KYC požiadavkách. Čiže je prirodzené, že sa vyvíjajú nové technológie, ktoré umožňujú chrániť súkromie aj v prísnom regulačnom prostredí. V oblasti anonymity kryptomien sa stretávajú pokročilé kryptografické techniky so snahami regulátorov o zabezpečenie transparentnosti a zároveň sa zvyšujú snahy o predchádzanie zneužitiu týchto digitálnych aktív. Cieľom tohto príspevku bude identifikovať, do akej miery sú kryptomeny skutočne anonymné, aké sú technické a právne nástroje na identifikáciu transakcií a spojenia adries a aké dopady na súkromie tu existujú. Taktiež je v tomto príspevku potrebné zohľadniť významné právne nástroje, najmä AML/KYC požiadavky, odporúčania FATF, európska regulácia MiCA a postupy pri zaistení kryptoaktív. Rôzne výskumy ukazujú, že aj napriek tomu, že rôzne pokročilé riešenie orientované na anonymitu kryptomien dokážu výrazne obmedziť identifikáciu transakcií, absolútnu anonymitu v túto chvíľu nie je možné zabezpečiť. Je to ovplyvnené nielen použitou technológiou, ale aj tým, ako sa správa samotný používateľ, aké dostupné sú nástroje a aké sú regulácie v tejto oblasti.
Kľúčové slová: kryptomeny, anonymita, privátne transakcie, regulačné dopady, užívateľská skúsenosť

Úvod

Rozvoj technológií a digitalizácie sa prejavuje aj vo svete kryptomien. Práve toto vyvoláva okrem iného otázky ohľadom súkromia. Kryptomeny boli od začiatku prezentované skôr ako anonymný spôsob prevodu hodnoty, avšak po bližšom preskúmaní odbornou verejnosťou či regulačnými úradmi sa zistilo, že väčšina bežne používaných digitálnych aktív, ako je Bitcoin či Etherneum poskytujú iba psedonymitu. Pod pseudonymitou možno chápať stav, kedy je identita používateľa nahradená nejakým pseudonymom. Môže ísť napríklad o alfanumerickú adresu, ktorá neobsahuje žiadne osobné údaje. Hoci takáto adresa na prvý pohľad neodhaľuje meno či inú priamo identifikovateľnú informáciu, všetky transakcie s ňou spojené sú trvalo a verejne zaznamenané v blockchaine. Tým pádom používateľ nie je úplne anonymný, ale skrytý za týmto pseudonymom. V prípade, že sa tento pseudonym podarí priradiť ku konkrétnej osobe

napríklad cez burzu s KYC, IP adresu, chybný postup pri práci s peňaženkou alebo analytické nástroje, znamená to, že je potenciálne odhalená aj história jeho transakcií.

V súčasnosti sa teda kladie veľký dôraz na riešenia, ktoré sú zamerané na anonymitu kryptomien a tie sa v posledných rokoch rozvíjajú vo viacerých smeroch, pretože rastie dopyt používateľov po vyššej úrovni ochrany súkromia. Zároveň presun finančných aktivít do online prostredia prirodzene zvyšuje tiež citlivosť na možné kybernetické útoky, sledovanie správania užívateľov a tiež sa zvyšuje motivácia chrániť transakcie a údaje v nich.

Výrazný posun možno vidieť v oblasti blockchainovej forenziky (proces analýz na blockchaine). Mnohé spoločnosti vyvíjajú čoraz výkonnejšie nástroje, ktoré dokážu identifikovať transakčné vzory, prepájať adresy a deanonymizovať používateľov aj v zložitejších transakčných štruktúrach. Tým pádom rastie aj tlak na vývojárov privátnych kryptomien, aby neustále inovovali techniky na zabezpečenie anonymity a zvyšovali ich odolnosť voči analýze.

Všetko toto postupne viedlo ku vzniku privátnych kryptomien, ktoré využívajú extrémne zložité kryptografické prístupy, ako sú zero-knowledge proofs, ring signatures či stealth addresses. Cieľom týchto techník je skryť informácie o odosielateľovi, prijímateľovi a výške prevádzanej sumy. Tu je však otázka, do akej miery dokážu odolať postupom blockchainovej forenziky a zároveň spĺňať legislatívne požiadavky.

V súčasnosti je otázka anonymity kryptomien úzko previazaná aj s právom, najmä s medzinárodnými štandardami, Európskou legislatívou a nariadeniami, ktoré sprísňujú požiadavky s cieľom prevencie voči praniu špinavých peňazí a financovania terorizmu, na čo sa kryptomeny môžu často zneužívať. Služby kryptoaktív sú nútené implementovať komplikované procesy (KYC/AML) na ochranu anonymity.

V tomto článku zhodnotíme komplexný vzťah medzi technickými mechanizmami anonymity, možnosťami deanonymizácie a regulačnými zásahmi. Základné výskumné otázky sú: Do akej miery sú anonymné kryptomeny skutočne anonymné? Aké technické a právne nástroje existujú na identifikáciu transakcií a prepájanie adries? Aké dopady má anonymita na ochranu súkromia a dodržiavanie pravidiel KYC/AML? Cieľom je poskytnúť ucelený pohľad na anonymitu v kryptomenách v kontexte súčasného technologického a právneho vývoja.

Anonymita v kryptomenách: princípy a limity

Mnoho ľudí si myslí, že charakter kryptomien je anonymný, ale nie je to úplne tak. Realita je oveľa komplexnejšia. Ako už bolo spomínané, väčšina kryptomien ako je Bitcoin či Ethereum poskytujú iba pseudonymitu. V momente, keď sa adresa spojí s konkrétnou osobou, je možné spätne preskúmať celú jej transakčnú históriu. [8]

V praxi sa anonymita stráca rôzne. Môže to byť na základe analýzy grafu: zhlukovanie adries, detekcia change výstupov, heuristiky peňaženiek. Ďalej network-layer fingerprinting: prvý uzol, ktorý zahliadne transakciu, je možné korelovať s IP; mitigácia cez Tor/I2P, Dandelion++ a transaction broadcast cez mix servery. V neposlednom rade sa často dejú aj dátové úniky nad aplikačnou vrstvou: KYC u zmenární, odtlačky prehliadača/peňaženiek, analytika webu, dusting attacks. U užívateľov, a to hlavne tých začínajúcich je časté chybné používanie peňaženiek: reuse adries, centralizované služby, spájanie fondov z rôznych identít, nedôsledné Coin Control. [6]

Zrejme najčastejší prípad odhalenia identity môže byť zmiešanie adries počas platby. Platby v Bitcoinoch majú tú vlastnosť, že často pozostávajú z viacerých rôznych adries. A ak sa počas platby skombinuje adresa bez identity s adresou s identitou, identita oboch adries je zrazu jasná. V skutočnosti, ak máte jeden bitcoin na adrese A a ďalší bitcoin na adrese B a pošlete 1,1 bitcoinu niekomu na adresu C, zoberie sa jeden bitcoin z adresy A a desatina bitcoinu z adresy B. A keďže je jasné, že túto transakciu vykonáva jedna osoba, stačí, že je známa identita vlastníka adresy A a po transakcii na adresu C je jasné, že adresy A a B patria tej istej osobe. [1]

Aj práve preto sa objavujú ďalšie spôsoby vzniku kryptomien s dôrazom na súkromie. V súčasnosti patria medzi najvýznamnejšie Monero, Zcash a Grin, v ktorých sú implementované rôzne pokročilejšie kryptografické techniky. Monero využíva kombináciu ring signatures, ringCT a stealth addresses, čím skrýva odosielateľa, príjemcu aj výšku transakcie. [7]

Jedna z týchto technológií, konkrétne Zcash dokáže implementovať systém, ktorý umožňuje preukázať platnosť transakcie bez potreby zverejnenia jej detailov. Aj napriek tomu však množstvo používateľov ešte stále vykonáva transakcie v transparentnom režime, čo znižuje mieru anonymity. Aj preto je potrebná edukácia v tejto oblasti. [2]

Ako uvádza Európsky parlament: v súčasnosti sa pri obchodovaní s kryptoaktívami na občanov nevzťahujú pravidlá EÚ o ochrane spotrebiteľa a často nie sú dobre informovaní o rizikách, čo môže znamenať, že môžu prísť o peniaze. Rozšírené používanie kryptoaktív bez regulácie môže viesť k finančnej nestabilite, manipulácii s trhmi a finančnej trestnej činnosti.

Ako uvádza portál fintechhub, s rastúcou komplexnosťou a objemom dát sa tradičné AML systémy stávajú preťaženými. Zločinci sa rýchlo prispôsobujú novým reguláciám a vyvíjajú nové metódy na obchádzanie existujúcich kontrol. Nedostatočná schopnosť systémov učiť sa z nových dát a adaptovať sa na meniace sa hrozby je hlavným dôvodom, prečo je potrebné prejsť na pokročilejšie technológie. Bez pomoci umelá inteligencia bankovníctvo je boj proti praniu špinavých peňazí nerovný.

Ďalšou výzvou je fragmentácia dát. Informácie o transakciách, klientoch a ich aktivitách sú často rozptýlené v rôznych systémoch a oddeleniach, čo sťažuje komplexný pohľad na potenciálne riziká. Táto fragmentácia bráni efektívnej dátovej analýze AML a umožňuje podvodníkom využívať medzery v systéme. Bez integrácie dát a pokročilých analytických nástrojov je pre finančné inštitúcie extrémne náročné držať krok s dynamickým prostredím finančných zločinov. [5]

V závere tejto časti možno konštatovať, že absolútna anonymita kryptomien pre túto chvíľu neexistuje. Vo väčšine prípadov je možné zistiť konečného vlastníka. Pri pseudonymných kryptomenách bude väčšinou jasne vidieť čiastka aj finálna adresa používateľa. [9]

Analýza možností identifikácie transakcií a prepojenia adries a regulácia

Ako sme už spomínali, kryptomeny sa pre laickú verejnosť často spájajú s predstavou anonymity, ale nie je to tak. Dnes je bežnou súčasťou blockchainu vyšetrovanie kybernetickej kriminality, AML kontroly a compliance procesov.

Blockchain si môžeme predstaviť ako „Kataster“. Kto je zapísaný v katastri ako vlastník pozemku, ten ho reálne vlastní. Kto je zapísaný v Blockchaine ako vlastník adresy Kryptomeny, ten ju aj reálne vlastní. Každý NOD zapojený v Bitcoinovej sieti má kópiu Blockchainu. Aktuálne je okolo 10 000 NOD-ov v sieti. To zabezpečuje nefalšovateľnosť a nemožnosť zmeniť alebo nejako upraviť Blockchain, lebo ostatné NOD-y v sieti by to hneď identifikovali. Blockchain je verejne dostupný na internete. Všetky transakcie od vzniku sú tam zapísané až po súčasnosť. [3]

Zároveň kryptomenové burzy vedia o užívateľoch z veľkej časti množstvo osobých údajov, ktoré zdieľajú s firmami, ktoré poskytujú tzv. “blockchain analýzu”. Jedným z dôvodov, prečo to robia je, aby zabránili obchodovaniu s kradnutými kryptomenami, ktoré by burza nemala zmeniť za eurá, doláre a iné fiat meny. Dôsledkom tohto je, že identita užívateľa je sledovaná po blockchaine. Nie je v ňom síce priamo uložená, ale to neznamená, že nákupné správanie tohto užívateľa, je od momentu, kedy kryptomeny opustia burzu anonymné. Práve naopak, je sledované. [2]

Čo sa týka samotných regulácií, technológia smeruje k tomu, aby boli transakcie spracovávané s čo najväčším stupňom súkromia, zatiaľ čo legislatíva EÚ a medzinárodné inštitúcie kladú dôraz transparentnosť a prevenciu voči praniu špinavých peňazí. Práve z tohto dôvodu je pochopiteľné, že prichádza čoraz viac regulácií v tejto oblasti. EÚ pripravila nové pravidlá pod názvom V júni 2022 bola dosiahnutá predbežná dohoda medzi Parlamentom a Radou. Nové pravidlá boli formálne schválené Parlamentom v apríli 2023 a Radou v máji 2023, čo bolo posledným krokom v legislatívnom procese. V apríli 2023 Parlament podporil nové EÚ pravidlá umožňujúce sledovanie a identifikáciu prevodov kryptoaktív s cieľom zabrániť ich využívaniu na pranie špinavých peňazí, financovanie terorizmu a iné trestné činy. Nový zákon tiež umožňuje blokovanie podozrivých transakcií. Pravidlá sa vzťahujú na transakcie s kryptoaktívami nad 1 000 EUR. Nová legislatíva bola formálne schválená Radou v máji 2023. [4] Zároveň sa v právnych systémoch viacerých štátov objavujú konkrétne postupy na zaistenie a spravovanie kryptoaktív.

Tieto regulačné zásahy ukazujú, že anonymita v kryptomenách nie je iba otázkou technologického pokroku, ale aj právnou otázkou. Súkromie používateľov, technické limity a právne povinnosti sa prelínajú a vytvárajú tak komplexný systém, v ktorom sa anonymita stáva skutočne dôležitým pojmom a zrejme aj záväzkom do budúcnosti.

Záver

Treba konštatovať, že tento článok má predovšetkým teoretický charakter. Anonymita v kryptomenách je výsledkom toho, aké sú momentálne technologické možnosti, používateľské správanie a regulačné prostredie. Našťastie už v súčasnosti existujú rôzne techniky, ktoré výrazne zvyšujú úroveň súkromia. Tie majú však v súčasnosti stále svoje limity, a to najmä v súvislosti s pokročilými forenznými nástrojmi a databázami prevádzkovanými organizáciami ako Chainalysis či Elliptic.

Úplná anonymita v súčasných kryptomenových systémoch nie je zatiaľ možná. Jej úroveň závisí od konkrétnej kryptomeny, technickej implementácie, nastavenia peňaženky, používania techník, ktoré podporujú anonymitu, ale aj od úrovne vzdelania a prístupu jednotlivých užívateľov či aktuálnych právnych regulácií.

Zároveň je potrebné zdôrazniť potrebu zvyšovania osvety medzi používateľmi, ktorí často preceňujú úroveň ochrany súkromia, ktorú im kryptomeny poskytujú. Kľúčové je, aby používatelia porozumeli rozdielu medzi anonymitou a pseudonymitou, poznali riziká spojené s tým, ak sa odhalí ich identita a v neposlednom rade vedeli správne používať nástroje na ochranu súkromia.

Tento článok odporúčal na publikovanie vo vedeckom časopise Mladá veda:
Dr.h.c. prof. Ing. Josef Reitšpís, CSc., DBA, MSc.

Použitá literatúra

1. Anycoin.sk (2024). "Bitcoin nie je anonymný, jeho používanie zločincami nemá zmysel" Anycoin.sk, 4. 9. 2024. Dostupné online: https://www.anycoin.sk/blog/blog-btc-anonymita
2. Bednár, J. (2020). "Súkromie a KYC v platobných sieťach". Juraj Bednár blog, 13. 10. 2020. Dostupné online: https://juraj.bednar.io/blog/2020/10/13/sukromie-a-kyc-v-platobnych-sietach/
3. Cryptotips.sk (2018). "Všetko čo potrebujete vedieť o kryptomenách". Cryptotips.sk. 1. 1. 2018. Dostupné online: https://cryptotips.sk/co-su-kryptomeny/
4. Európsky parlament (2022). "Riziká kryptomien a prínos legislatívy EÚ". Európsky parlament, 01.4.2022. Dostupné online: https://www.europarl.europa.eu/topics/sk/article/20220324STO26154/rizika-kryptomien-a-prinos-pravnych-predpisov-eu
5. FintechHub.sk (2024). "Umelá inteligencia v boji proti praniu špinavých peňazí (AML)". FintechHub.sk. Dostupné online: https://fintechhub.sk/clanok/umela-inteligencia-v-boji-proti-praniu-spinavych-penazi-aml
6. Gašparík, J. (2025). Bezpečnost a anonymita v blockchainu. EuroEkonóm.sk. Dostupné online: https://www.euroekonom.sk/bezpecnost-a-anonymita-v-blockchainu/
7. Jendrál, M. (2025). „Anonymita za cenu kriminálu: Temná stránka kryptosveta“. Kryptomagazin.sk, 11. 5. 2025. Dostupné online: https://kryptomagazin.sk/anonymita-za-cenu-kriminalu-temna-stranka-kryptosveta/
8. Krause, T. (2018). "Jak funguje anonymita Bitcoinu?". Bitcoinvkapse.cz, 3. 4. 2018. Dostupné online: https://bitcoinvkapse.cz/jak-funguje-anonymita-bitcoinu/
9. Trávnik, P. (2024). "Nezastaviteľnosť anonymných kryptomien pri zaistení a právna zraniteľnosť pseudonymných kryptomien". Paralelná polis. 18. 11. 2020. Dostupné online: https://paralelnapolis.sk/nezastavitelnost-anonymnych-kryptomien-pri-zaisteni-a-pravna-zranitelnost-pseudoanonymnych-kryptomien/

Mladá veda

Young Science

ISSN 1339-3189