

УДК: 343.004.738.5(4-672EU)
Biblid 1451-3188, 24 (2025)
Год XXIV, бр. 89, стр. 51-65
Изворни научни рад
Рад примљен 30. 12. 2024. године
Рад одобрен 24. 1. 2025. године
DOI: https://doi.org/10.18485/iipe_ez.2025.24.89.3
CC BY-SA 4.0

РЕГУЛАТОРНИ ОКВИР ЕУ О КРИПТОВАЛУТАМА И САЈБЕР КРИМИНАЛУ

Срђан МИЧИЋ,
Дијана САВИЋ БОЖИЋ,
Милутин АТЕЉЕВИЋ*

Анстракт: У раду се анализира регулаторни оквир Европске уније (ЕУ) за криптовалуте и мере за сузбијање сајбер криминала повезаног са дигиталним валутама. Са све већом употребом криптовалута као финансијског средства и њиховом привлачношћу за криминалне активности, попут прања новца и напада уцењивачким софтверима (тзв. „рансомвер напада“), ЕУ се суочава са изазовом успостављања ефикасне регулативе која штити потрошаче и одржава стабилност тржишта. Рад обухвата анализу кључних регулаторних аката у области „Тржишта крипто-активе“ (*Markets in Crypto-Assets – MiCA*), провера банкарских клијената (*Know Your Customer – KYC*) и борбе против прања новца (*Anti-Money Laundering – AML*), као и стандарда који су усмерени на побољшање транспарентности у финансијском сектору. Такође, анализирани су механизми као што су дигитална форензика и аналитика дигитално повезаних база података (тзв. „блокчејн аналитика“), које се користе за праћење трансакција и идентификацију криминалних образаца. Поред анализе постојећих мера, рад истиче главне изазове, укључујући анонимност и децентрализацију криптовалута, и предлаже правце за будући развој регулативе који би омогућили ЕУ ефикасније спречавање сајбер криминала уз подстицање

* Федерална управа полиције, Сарајево, БиХ. Е-Mail: srdjan.micic.fup@gmail.com. ORCID iD: <https://orcid.org/0009-0004-1005-4472>; Факултет организационих студија, Београд, Е-Mail: dinabozic@gmail.com. ORCID iD: <https://orcid.org/0009-0008-4315-388X>; Правни факултет, Бијељина, БиХ. Е-Mail: mateljevic@sinergija.edu.ba. ORCID iD: <https://orcid.org/0009-0003-6395-0011>.

иновација. Из предметне анализе аутори закључују да континуирано унапређење регулативе и глобална сарадња представљају кључне елементе у борби против сајбер криминала у криптовалутном сектору.

Кључне речи: Сајбер криминал, криптовалуте, ЕУ, правна регулатива

1) УВОД

Развој дигиталне економије и технолошки напредак утицали су на стварање нових облика валута и финансијских инструмената. Криптовалуте, као што су *Bitcoin* и *Ethereum*, постале су један од најзначајнијих феномена 21. века. У исто време, појава криптовалута допринела је развоју нових могућности у дигиталном финансијском свету, али и нових облика криминалних активности, познатих као сајбер криминал. Ове активности представљају велики изазов за регулаторне и правосудне системе широм света, укључујући ЕУ. Криптовалуте су пружиле корисницима могућност да обављају финансијске трансакције независно од централних банака и традиционалних финансијских система, што их чини атрактивним за широк спектар корисника, укључујући инвеститоре, технолошке ентузијасте, али и криминалце. Захваљујући анонимности коју криптовалуте омогућавају, извршење илегалних активности постало је лакше него икад пре, што доводи до експанзије сајбер криминала у областима као што су прање новца, финансирање тероризма, крађа дигиталне имовине и хаковање. Криптовалуте се одликују децентрализованом природом и брзим технолошким напретком, што ствара изазове у њиховој регулацији. ЕУ настоји да развије свеобухватни регулаторни оквир који би омогућио контролу и праћење крипто активности, истовремено омогућавајући иновације у овој области. Главни изазови у регулацији криптовалута обухватају: потешкоће у идентификацији и праћењу крипто трансакција због анонимности корисника, брз напредак технологија, што отежава правовремено прилагођавање регулаторног оквира, неусклађеност регулатива унутар држава чланица, што омогућава сајбер криминалцима да користе различите регулаторне празнине. Циљ рада је да истражи и анализира регулаторни оквир ЕУ који се односи на криптовалуте и сајбер криминал, те да испита како ове мере утичу на превенцију сајбер криминала. Поред тога, рад настоји да идентификује главне изазове у регулацији криптовалута и да предложи потенцијалне правце за будуће унапређење овог оквира.

2) РЕГУЛАТОРНИ ОКВИР ЕУ ЗА КРИПТОВАЛУТЕ

ЕУ настоји да обезбеди свеобухватни регулаторни оквир за криптовалуте и друге дигиталне имовине, што је нарочито важно у светлу брзог раста ове

индустрије. Неки од кључних регулаторних аката укључују: *Markets in Crypto-Assets Regulation* – MiCA представља једну од најобухватнијих иницијатива ЕУ која је усмерена на регулисање криптовалутних активности.¹ Донесен у циљу успостављања јасних и униформних правила за тржиште дигиталних имовина у Европи, MiCA покрива неколико кључних области. Све крипто платформе које послују унутар ЕУ морају бити лиценциране и усклађене са правилима MiCA, што подразумева транспарентност пословања и одговорност према корисницима. MiCA захтева да компаније пруже потрошачима јасне информације о природи ризика везаних за крипто активности, што укључује и упозорења на могућност губитка имовине. MiCA регулише питања манипулације и злоупотребе тржишта, што је значајно у контексту криптовалута због честих манипулативних пракси на неким платформама. Пета директива о спречавању прања новца у ЕУ, позната као 5AMLD, обавезује крипто размене и дигиталне новчанике да примењују мере које су већ дуго обавезне за традиционалне финансијске институције. 5AMLD захтева идентификацију корисника и спровођење процедура за борбу против прања новца.² Све крипто компаније морају сакупљати и чувати податке о клијентима како би спречиле криминалне активности. Пружаоци крипто услуга у ЕУ морају пријављивати сумњиве активности надлежним органима, што олакшава праћење и истрагу сајбер криминала. ЕУ настоји да заштити инвеститоре и кориснике криптовалута од превара и злоупотребе личних података. Регулаторни механизми укључују право на информисаност (пружаоци услуга крипто имовине дужни су да јасно обавесте кориснике о ризицима који могу бити укључени у њихове услуге) и гаранције заштите средстава (компаније морају осигурати одређени ниво заштите средстава корисника и преузети одговорност у случају нестанка или крађе имовине). Ове мере представљају темељни оквир за регулисање криптовалута у ЕУ, али их је потребно редовно ажурирати како би биле у корак са иновацијама у крипто индустрији. Регулаторни приступ ЕУ је значајно другачији од приступа других јурисдикција. Кључне разлике су видљиве у приступима Сједињених Америчких Држава, Јапана, Кине и других земаља. Регулација криптовалута у САД је подељена између различитих федералних агенција, попут SEC (Комисије за хартије од вредности и берзу) и CFTC (Комисије за

¹ "European Commission. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets (MiCA)", COM(2020) 593 final. Brussels: European Commission, 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>.

² Robby Houben, Alexander Snyers, *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*, European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Brussels, 2018.

трговину робним фјучерсима). SEC захтева да криптовалутне платформе које нуде хартије од вредности буду регистроване, што укључује и ICO пројекте.³ Ово је значајно строжији приступ од оног који ЕУ примењује. У САД постоје и појединачне државне регулативе, попут „BitLicense“ лиценце у Њујорку, што ствара фрагментиран регулаторни оквир који је у појединим случајевима ригиднији од приступа ЕУ. Јапан је убрзо након појаве криптовалута створио легалан оквир који регулише њихову употребу. Закони попут Закона о платним услугама одређују услове под којима крипто размене могу легално пословати. Све крипто размене морају добити дозволу за рад од Јапанске агенције за финансијске услуге (FSA), што је допринело стабилности и транспарентности тржишта криптовалута у Јапану. Јапан захтева од размена да осигурају корисничке фондове, што значајно смањује ризик за инвеститоре и минимизира последице хаковања. Кина има строгу политику према криптовалутама и постоје строга ограничења на активности везане за криптовалуте. Потпуна забрана рударења и трговања криптовалутама, при чему овај приступ представља потпуно супротан приступ у односу на ЕУ, јер Кина настоји да онемогући употребу криптовалута на својој територији, што је део шире стратегије економске контроле и сигурности. Поређење показује да је регулаторни приступ ЕУ уравнотеженији и омогућава већи степен иновација у поређењу са строжим политикама неких других земаља. Европска централна банка (ЕЦБ) и Европска агенција за тржишта и хартије од вредности (ЕСМА) имају кључну улогу у надзору и имплементацији регулативе за криптовалуте унутар ЕУ. ЕЦБ има задатак да обезбеди стабилност и сигурност у еврозони и на европском финансијском тржишту.⁴ Она истражује могућност издавања дигиталног евра као стабилне дигиталне валуте која би могла да смањи зависност од нестабилних криптовалута и игра важну улогу у надзору и процени ризика које криптовалуте могу представљати за стабилност еврозоне, што укључује и истраживање утицаја дигитализације финансијског сектора. Европска агенција за тржишта и хартије од вредности (ЕСМА) има задатак да координише регулативу и обезбеди усаглашеност међу државама чланицама. ЕСМА пружа смернице које имају за циљ да стандардизују активности крипто компанија у ЕУ. ЕСМА такође врши надзор над ICO-овима како би осигурала да пројекти који нуде дигиталну имовину испуњавају стандардне прописе. Она поставља стандарде за спречавање

³ Michael Casey, Paul Vigna, *The Truth Machine: The Blockchain and the Future of Everything*, St. Martin's Press, New York, 2018.

⁴ "Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures", *Occasional Paper Series*, No. 223, European Central Bank, 2019. Интернет: <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf>.

злоупотребе тржишта и промовише транспарентност, чиме се значајно смањују шансе за преваре.⁵ Криптовалуте су децентрализоване и углавном нису под контролом било ког појединца или централизоване институције. Ово доноси низ изазова у примени регулаторног оквира. Један од највећих изазова је праћење актера који стоје иза крипто трансакција. Анонимност корисника спречава регулаторе да идентификују криминалце који користе криптовалуте за нелегалне активности. Индустрија криптовалута се брзо развија, што чини да је регулаторима тешко да одрже корак са новим технологијама, попут децентрализованих финансија (DeFi) и NFT-ова. Неусклађеност регулативе између различитих земаља ЕУ омогућава сајбер криминалцима да користе празнине и проналазе „сигурна уточишта“. ЕУ тежи већем усаглашавању, али постоје изазови у уклапању интереса свих земаља чланица.

3) САЈБЕР КРИМИНАЛ И КРИПТОВАЛУТЕ

Криптовалуте, због своје децентрализоване природе и степена анонимности који пружају корисницима, значајно привлаче сајбер криминалце који траже нове начине за извођење нелегалних активности. Праће новца је једна од најраспрострањенијих криминалних активности повезаних са криптовалутама. Преступници користе разне технике за „чишћење“ нелегално стеченог новца претварањем у криптовалуте и затим враћањем у легалне финансијске системе. Криминалци често користе миксере – услуге које раздвајају и спајају различите крипто трансакције како би се сакрио извор средстава, а затим их шаљу на адресе које нису повезане са оригиналним средствима. Поред миксера, на „тамном вебу“ постоје и анонимне размене које омогућавају криминалцима да трансформишу крипто новац у фиат валуту, чиме завршавају процес прања новца без откривања идентитета. Рансомваре напади, у којима нападачи шифрују податке жртве и захтевају откуп, постали су учестала претња. Захтеви за плаћање откупнине у криптовалутама су најпопуларнији, јер оваква плаћања не захтевају откривање идентитета. Током 2020. и 2021. године забележен је пораст у броју рансомваре напада, укључујући нападе на велике корпорације и институције, где су хакери захтевали криптовалуте као метод исплате, како би избегли откривање и омогућили лако скривање трага трансакције.⁶ Хакери често користе више крипто адреса и служе се миксерима и разним

⁵ “Advice on Initial Coin Offerings and Crypto-Assets”, European Securities and Markets Authority (ESMA), ESMA50-157-1391. Paris, 2019. Интернет: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

⁶ Malcolm Campbell-Verduyn, ed., *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. Routledge, Abingdon, 2023.

разменама како би онемогућили праћење средстава, што значајно отежава напоре регулаторних агенција у идентификацији злочинаца. Хаковање крипто размена је још једна значајна претња сајбер криминала у контексту криптовалута. С обзиром на то да крипто размене управљају великим количинама дигиталне имовине корисника, често су мета хакера. Примери укључују нападе на размене попут Mt. Gox (2014) и Coincheck (2018), где је изгубљено преко 500 милиона долара у криптовалутама.⁷ Ови инциденти су довели до захтева за унапређењем безбедносних протокола и приморали регулаторе на строже захтеве за заштиту података и дигиталне имовине. Криминалци користе различите технике хаковања, укључујући софистициране малвере, фишинг нападе и експлоатацију софтверских рањивости размена. Ове методе омогућавају приступ новчаницима и приватним кључевима корисника, што доводи до директне крађе имовине. Преваранти често користе ICO-ове (*Initial Coin Offering*) како би привукли инвеститоре у лажне пројекте. Они обећавају значајан повратак на инвестицију и користе убедљиве маркетиншке кампање да привуку капитал, а затим напуштају пројекат и задржавају новац инвеститора. У периоду 2017–2018. ICO преваре су биле учестале, што је навело регулаторе да успоставе строже захтеве за ICO пројекте, као и мере транспарентности које подразумевају откривање идентитета и намере пројеката пре него што се понуде инвеститорима.⁸ Анонимност и децентрализација су кључне карактеристике криптовалута, али истовремено представљају значајне изазове за регулацију и борбу против сајбер криминала. Традиционални финансијски системи имају јасан приступ идентификацији корисника, што значи да регулатори могу да открију учеснике у трансакцијама. Код криптовалута корисници могу да остану анонимни, што значи да криминалци могу сакрити свој идентитет и лако избегавати правду. Непостојање централног органа за надзор, као што је банка или друга институција, значи да регулатори морају користити иновативне технологије попут блокчејн аналитике како би пратили токове новца, али и поред тога често наилазе на изазове у идентификацији актера. Криминалци се ослањају на услуге попут миксера и тумблера, који додатно замагљују порекло средстава. Ови сервиси омогућавају корисницима да комбинују своја крипто средства са другим корисницима и поделе их на нове адресе, чиме се знатно отежава праћење токова новца. Поред тога, постоје новчаници и криптовалуте које су специјално дизајниране за анонимност, као што је *Monero*, који користи напредне технике шифровања да сакрије информације

⁷ Fergal Reid, Martin Harrigan. "An Analysis of Anonymity in the Bitcoin System", In *Security and Privacy in Social Networks*, edited by Yaniv Altshuler et al., Springer, New York, 2019, pp. 197–223.

⁸ Michael Casey, Paul Vigna, *op. cit.*

о корисницима и трансакцијама, чинећи их практично непролазним за стандардне регулаторне методе праћења.⁹ Криптовалуте су постале средство плаћања на „тамном вебу“, где се користе за куповину нелегалних производа и услуга, као што су дроге, оружје и украдени подаци. Ове платформе омогућавају анонимну куповину и продају, користећи криптовалуте као метод који не оставља траг. Сајбер криминалци често користе неколико крипто новчаника и праве сложене мреже трансакција како би сакрили свој идентитет. Ово додатно компликује истраге и праћење криминалних активности од стране полицијских агенција и регулатора. Регулаторни оквир ЕУ има значајну улогу у борби против сајбер криминала, али његова ефикасност у великој мери зависи од начина примене и усаглашености међу државама чланицама. Захтеви за KYC и AML процедуре наметнути разменама и провајдерима новчаника помажу у идентификацији корисника и смањују ризик од криминалних активности. Обавезно прикупљање података о клијентима омогућава регулаторима бољи увид у учеснике у тржишту и отежава извршење криминала. Стандарди за KYC процедуре посебно се примењују на платформе које послују унутар ЕУ, али се јављају изазови у примени уколико платформе нису регулисане у другим државама и послују на глобалном нивоу.¹⁰ Дигитална форензика и блокчејн аналитика постали су неопходни алати у борби против сајбер криминала у крипто простору. Ове технологије омогућавају регулаторима и истражитељима да прате токове новца унутар блокчејн мреже, чак и ако су укључене анонимне адресе. Иако блокчејн аналитика не може открити директан идентитет корисника, може помоћи у стварању „токова новца“ који повезују различите адресе, олакшавајући идентификацију образаца криминалних активности.¹¹ Иако регулаторне мере ЕУ значајно доприносе борби против сајбер криминала, децентрализована природа криптовалута и појављивање нових технологија често представљају изазове у имплементацији мера. Неусклађеност регулатива међу чланицама ЕУ може довести до „регулаторних рупа“ које криминалци могу искористити. Сталне иновације у криптовалутном сектору захтевају ажурирање регулативе како би се ефикасно сузбиле нове врсте сајбер криминала, попут злоупотребе NFT-ова и децентрализованих финансија (DeFi).¹² Због глобалне природе криптовалута неопходна је

⁹ Fatf-Gafi, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Financial Action Task Force, 2023. Интернет: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>.

¹⁰ Aviv Zohar, "Bitcoin: An Innovative Alternative Digital Currency". *Communications of the ACM*, 56, no. 3 2019, pp. 12–14.

¹¹ Fatf-Gafi. *op. cit.*

¹² Robby Houben, Alexander Snyers, *op. cit.*

сарадња међу државама на разменама информација и заједничком решавању сајбер криминала. Са порастом DeFi-а, NFT-ова и нових облика дигиталне имовине, потребно је увести прилагођене регулаторне мере које би спречиле њихову злоупотребу. Додатно побољшање KYC и AML стандарда може значајно смањити простор за криминалне активности, као и обавезати размене да у потпуности спроводе праксе идентификације корисника.

4) РЕГУЛАТОРНИ МЕХАНИЗМИ ЗА СПРЕЧАВАЊЕ САЈБЕР КРИМИНАЛА

KYC и AML процедуре представљају основу за спречавање криминалних активности у сектору криптовалута. Ове мере се примењују широм финансијског сектора, а увођењем у крипто индустрију омогућавају значајну контролу и надзор. KYC подразумева обавезу идентификације корисника како би се спречило коришћење финансијских услуга у нелегалне сврхе.¹³ KYC процедуре захтевају од крипто размена и других провајдера услуга да сакупљају и чувају податке о корисницима, као што су пуно име, адреса, идентификациони бројеви, и често фотографије или видео записе како би се обезбедила аутентичност података. Коришћењем KYC стандарда крипто размене и новчаници могу боље надгледати и откривати сумњиве активности. Ово је од кључне важности за спречавање прања новца и других криминалних радњи које укључују криптовалуте.¹⁴ Неке земље имају строге KYC процедуре, док друге државе могу имати либералније стандарде. Ова разноликост у примени отежава јединствену борбу против сајбер криминала, јер криминалци могу користити размене које немају обавезне KYC процедуре. AML процедуре имају за циљ да идентификују и спрече прање новца кроз транспарентно прање токова новца. AML стандарди у крипто сектору захтевају од размена и провајдера услуга да пријављују сумњиве трансакције, што омогућава бољу сарадњу са регулаторним агенцијама. На пример, нагли трансфери великих количина криптовалуте или више мањих трансфера на нове адресе могу бити индикације за прање новца. Према AML стандардима, одређени модели активности могу довести до аутоматске блокаде трансакција или захтева за додатну верификацију корисника.¹⁵ Овакве мере обезбеђују додатни слој заштите од криминала и доприносе одржавању сигурности на тржишту криптовалута. Традиционалне AML процедуре често не узимају у обзир децентрализовану природу криптовалута. Увођење

¹³ *The Chainalysis 2022 Crypto Crime Report*, Chainalysis, 2022. Интернет: <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>.

¹⁴ Don Tapscott, Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*, Penguin, New York, 2021.

¹⁵ *The Chainalysis 2022 Crypto Crime Report*, op. cit.

напредних алата за блокчејн анализу омогућава прилагођавање AML мера специфичностима криптовалута, чиме се побољшава ефикасност праћења. У контексту криптовалута, дигитална форензика и блокчејн аналитика постали су кључни алати за праћење и анализу трансакција. Ове технологије су се развиле као одговор на потешкоће у идентификацији и праћењу актера у крипто трансакцијама, а њихова примена значајно доприноси борби против сајбер криминала. Блокчејн аналитика омогућава дубинско праћење токова криптовалуте кроз јавну и непроменљиву евиденцију трансакција, што је кључно у идентификацији образаца који указују на потенцијалне криминалне активности. Применом аналитичких алата истражитељи могу идентификовати обрасце који указују на праће новца, попут одређених циклуса трансакција, коришћења миксера или интензивних трансакција између повезаних новчаника.¹⁶ Иако блокчејн не пружа директну идентификацију корисника, анализом активности могуће је повезати одређене адресе са криминалним активностима и тиме добити индикације о укљученим актерима. Дигитална форензика користи алате и технике за откривање, идентификацију и прикупљање доказа у сајбер простору. Форензички приступи омогућавају законским органима да прикупе и чувају податке који су повезани са криминалним активностима, укључујући трансакционе записе, ИП адресе и податке о корисничким уређајима, чиме се добијају кључни докази за судске процесе. У случајевима рансомваре напада, форензика омогућава идентификацију malware-а који се користи за извођење напада, као и праћење плаћања откупнина, што је често једини начин да се прати трансакција и идентификују актери.¹⁷ Због глобалне природе криптовалута појединачне земље немају довољно ресурса да самостално спрече сајбер криминал на ефикасан начин. Унапређење међународне сарадње је неопходно како би се олакшала размена података и праћење трансакција које укључују више јурисдикција. Многи облици сајбер криминала, укључујући праће новца и хаковање, укључују актере из различитих земаља. Размена информација и заједничке истраге омогућавају регулаторима бољу контролу над тржиштем и пружају ефикаснија решења за идентификацију криминалаца. ЕУ је успоставила размену података са партнерима у САД, Јапану и другим земљама како би се омогућила идентификација актера који извршавају криминалне активности преко граница. Организације попут FATF (*Financial Action Task Force*) и INTERPOL-а развиле су стандарде за борбу против прања новца и сајбер криминала који

¹⁶ Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." *White paper*, 2021. Интернет: <https://bitcoin.org/bitcoin.pdf>.

¹⁷ "ENISA Threat Landscape for 2021: An Overview of Cyber Threat Trends in 2020", European Union Agency for Cybersecurity (ENISA), 2021. Интернет: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.

укључују криптовалуте. FATF-ови препоручени стандарди налажу усаглашеност процедура за борбу против прања новца и финансирања тероризма у сектору криптовалута, што омогућава државама да боље прате трансакције и идентификују сумњиве активности.¹⁸ Ове организације такође организују обуке и истраживања за регулаторе и институције, чиме подстичу развој нових стратегија за борбу против сајбер криминала. Са порастом комплексности сајбер криминала у крипто сектору регулатори користе нове технологије за бољи надзор и контролу. Вештачка интелигенција (AI) и машинско учење омогућавају напредно откривање сајбер претњи у крипто сектору. Ови системи могу идентификовати обрасце понашања и аномалије у трансакцијама које би могле указати на сумњиве активности. Машинско учење омогућава предиктивну аналитику, где се идентификују потенцијалне претње пре него што постану стварни напади. Овај приступ је посебно важан у раној детекцији рансомваре напада и других врста сајбер криминала. Блокчејн аналитички алати као што су *Chainalysis*, *Elliptic* и *CipherTrace* пружају детаљне податке о токовима новца унутар криптовалута. Ови алати користе напредне алгоритме за праћење сумњивих образаца и олакшавају идентификацију адреса повезаних са криминалним активностима.¹⁹ Софтвери за праћење су кључни у разоткривању сложених мрежа трансакција и идентификацији узорака криминалних активности. Они такође омогућавају сарадњу са регулаторима како би се додатно заштитило тржиште. Криптографија остаје основа заштите криптовалутних трансакција и новчаника, али са развојем технологија као што су *Zero-Knowledge Proofs* (ZKP) и *Multi-Party Computation* (MPC) могуће је постићи већу сигурност уз очување приватности корисника.²⁰ Ове технике омогућавају корисницима да потврде своје трансакције без откривања осетљивих података, што значи да регулатори и даље могу надгледати трансакције без нарушавања приватности.

5) ИЗАЗОВИ И БУДУЋИ ПРАВЦИ РАЗВОЈА

Иако је ЕУ предузела значајне кораке у регулисању криптовалутног сектора и сузбијању сајбер криминала, постоји низ изазова који и даље ограничавају ефикасност регулаторних мера. Криптовалуте попут *Bitcoin* и *Monera* омогућавају висок степен анонимности, чиме се отежава праћење

¹⁸ "Virtual Assets and Virtual Asset Service Providers: FATF Guidance". Financial Action Task Force, 2021. Интернет: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>.

¹⁹ Fergal Reid, Martin Harrigan, *op. cit.*, pp. 197–223.

²⁰ Aviv Zohar, *op. cit.*, pp. 12–14.

трансакција и идентификација учесника. Анонимност и одсуство централног посредника омогућавају корисницима да обављају трансакције без откривања свог идентитета, што отежава регулаторима да ефикасно надзиру тржиште. Користећи технологије као што су миксери и анонимни новчаници, криминалци додатно замагљују траг новца, чиме се отежава откривање злочина и спречавање криминалних активности у реалном времену.²¹ ЕУ настоји да постигне јединствени приступ регулацији криптовалута, али разлике у интерпретацији закона међу државама чланицама доводе до неусклађености регулативе. На пример, неке земље имају либералнији приступ, док друге примењују строге мере, што ствара празнине које криминалци могу искористити. Без јасног и једноликог оквира различите праксе примењене унутар ЕУ могу бити препрека ефикасном спровођењу закона, нарочито у случајевима када сајбер криминал укључује актере из више земаља. Брзи развој нових технологија, попут децентрализованих финансија (DeFi) и NFT-ова (незаменљивих токена), представља додатни изазов за регулаторе. DeFi платформе омогућавају корисницима да размењују криптовалуте без посредника, што додатно смањује могућност надзора и праћења активности. NFT-ови и други нови облици дигиталне имовине такође су постали средство за прање новца и финансирање нелегалних активности, што захтева прилагођавање постојећег регулаторног оквира и увођење нових мера како би се спречила њихова злоупотреба.²² Регулаторне агенције често немају довољно ресурса и специјализованих кадрова који би могли адекватно да се баве комплексним криптовалутним трансакцијама. Технологија криптовалута захтева висок степен техничке експертизе, који није лако доступан у свим регулаторним агенцијама. Без додатне обуке и ресурса, регулатори неће бити у могућности да се суоче са изазовима које доноси иновативан и брзо променљив крипто сектор. Како би се ови изазови превазишли и омогућило адекватно надгледање крипто тржишта, ЕУ ради на унапређењу постојећег регулаторног оквира и усмерава напоре ка новим правцима развоја. Један од кључних правних инструмената за криптовалуте у ЕУ је Markets in Crypto-Assets Regulation (MiCA), који има за циљ да успостави јасне и униформне услове за функционисање крипто тржишта у ЕУ. MiCA представља основу за будуће регулативе и вероватно ће се развијати и прилагођавати новим технологијама. Даљим развојем MiCA регулативе могуће је увести амандмане који би се односили на DeFi, NFT-ове и друге облике дигиталне имовине који тренутно нису покривени основним

²¹ "ENISA Threat Landscape for 2021: An Overview of Cyber Threat Trends in 2020", *op. cit.*

²² "EBA Report with Advice for the European Commission on Crypto-Assets", EBA-Op-2019-08. European Banking Authority, Paris, 2019. Интернет: https://www.eba.europa.eu/sites/default/documents/files/document_library//crypto-assets.pdf.

прописима, чиме би се створила свеобухватнија регулација.²³ Европска централна банка (ЕЦБ) истражује могућност увођења дигиталног евра, који би био дигитални облик стабилне валуте под контролом централне банке. Дигитални евро могао би да омогући сигурну алтернативу криптовалутама и смањи потребу за употребом нестабилних и децентрализованих криптовалута. Увођење дигиталног евра могло би да ограничи простор за сајбер криминалце јер би им омогућило приступ дигиталној валути која је под директним надзором централне банке, чиме би се смањила њихова склоност ка коришћењу анонимних криптовалута. Због глобалне природе криптовалута ЕУ настоји да прошири сарадњу са међународним организацијама попут FATF-а и INTERPOL-а како би се ојачала размена информација и координација у борби против сајбер криминала. Кроз стварање заједничких стандарда и вођење заједничких истрага, ЕУ ће моћи ефикасније да реагује на сајбер криминалце који делују у више јурисдикција и користе различите размене и новчанике за скривање трагова. Вештачка интелигенција и машинско учење све се више користе за откривање сумњивих активности у реалном времену. ЕУ настоји да унапреди своје регулаторне агенције применом ових технологија како би могла да детектује обрасце који указују на потенцијалне криминалне активности пре него што до њих дође. Вештачка интелигенција такође може да помогне у идентификацији нових облика сајбер криминала и омогући регулаторима да брзо прилагоде мере како би одговорили на нове претње.²⁴ Будуће регулаторне мере и иновације које ЕУ планира могу имати значајан утицај на крипто сектор и борбу против сајбер криминала. Ако ЕУ успе да постигне већу транспарентност у крипто сектору и ограничи анонимност корисника, вероватно ће се смањити обим криминалних активности повезаних са криптовалутама. KYC и AML стандарди који су примењени на све размене у ЕУ допринеће бољем надзору тржишта и омогућити лакшу идентификацију актера. Иако ће појачана транспарентност и надзор смањити простор за криминал, може доћи до отпора од стране корисника који су навикли на висок степен приватности, што би могло утицати на популарност одређених криптовалута у ЕУ. Увођење дигиталног евра пружиће корисницима стабилну и сигурну алтернативу криптовалутама, што може смањити потребу за коришћењем нестабилних дигиталних валута. Овај приступ могао би да допринесе развоју иновација у сектору дигиталних финансија, при чему би се смањила зависност од децентрализованих криптовалута и нестабилних тржишта. Дигитални евро такође може подстаћи друге државе да истражују могућност увођења својих дигиталних валута, чиме би се унапредила

²³ Ellie Wroughton, Gareth G. Brown. "The Role of Regulatory Sandboxes in Promoting Innovation in the Fintech Sector." *Journal of Financial Regulation*, vol. 6, no. 2, 2020, pp. 345–368.

²⁴ Malcolm Campbell-Verduyn, *op. cit.*

безбедност дигиталних трансакција и ограничио простор за криминал. Регулаторне мере као што су побољшани стандарди за заштиту инвеститора допринеће смањењу ризика од преваре и злоупотребе, што ће повећати поверење у крипто сектор и привући нове кориснике. Већа сигурност ће подстаћи професионалне инвеститоре и институционалне учеснике да се укључе у тржиште. Уз додатне мере заштите регулатори ће омогућити безбедније окружење за инвестирање у криптовалуте, чиме ће се умањити ризик од манипулације и омогућити одрживији развој тржишта. Док ће појачане регулативе смањити простор за криминал, прекомерна регулација може обесхрабрити иновације у крипто сектору. Балансирање између регулаторних захтева и омогућавања иновација биће кључно за будући развој тржишта. ЕУ настоји да подстакне одрживе иновације које не угрожавају сигурност корисника и интегритет тржишта, али ће бити неопходно пажљиво надгледати утицај регулативе како би се избегло гушење креативних решења у крипто индустрији.

6) ИЗВОРИ

- “Advice on Initial Coin Offerings and Crypto-Assets”, European Securities and Markets Authority (ESMA), ESMA50-157-1391. Paris, 2019. Интернет: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
- Campbell-Verduyn, Malcolm, ed. *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, Routledge, Abingdon, 2023.
- Casey, Michael, Vigna, Paul, *The Truth Machine: The Blockchain and the Future of Everything*, St. Martin's Press, New York, 2018.
- “Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures”, *Occasional Paper Series*, No. 223, European Central Bank, 2019. Интернет: <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf>.
- “EBA Report with Advice for the European Commission on Crypto-Assets”, EBA-Op-2019-08. European Banking Authority, Paris, 2019. Интернет: https://www.eba.europa.eu/sites/default/documents/files/document_library/crypto-assets.pdf.
- “ENISA Threat Landscape for 2021: An Overview of Cyber Threat Trends in 2020”, European Union Agency for Cybersecurity (ENISA), 2021. Интернет: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.
- “European Commission. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets (MiCA)”, COM(2020) 593 final. Brussels: European Commission, 2020. Интернет: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>.

- Fatf-Gafi, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Financial Action Task Force, 2023. Интернет: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>.
- Houben, Robby, Snyers, Alexander, *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*, European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Brussels, 2018.
- Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System". *White paper*, 2021. Интернет: <https://bitcoin.org/bitcoin.pdf>.
- Reid, Fergal, Harrigan, Martin, "An Analysis of Anonymity in the Bitcoin System", In *Security and Privacy in Social Networks*, edited by Yaniv Altshuler et al, Springer, New York, 2019.
- Tapscott, Don, Tapscott, Alex, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*, Penguin, New York, 2021.
- *The Chainalysis 2022 Crypto Crime Report*, Chainalysis, 2022. Интернет: <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>.
- "Virtual Assets and Virtual Asset Service Providers: FATF Guidance". Financial Action Task Force, 2021. Интернет: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>.
- Wroughton, Ellie, Brown, Gareth G., "The Role of Regulatory Sandboxes in Promoting Innovation in the Fintech Sector". *Journal of Financial Regulation*, vol. 6, no. 2, 2020.
- Zohar, Aviv, "Bitcoin: An Innovative Alternative Digital Currency". *Communications of the ACM*, 56, no. 3, 2019.

7) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Промене у технолошком и финансијском сектору, заједно са појавом криптовалута као новог финансијског средства, донеле су нове ризике и изазове за регулаторе, нарочито у контексту спречавања сајбер криминала. Главни налази истраживања показују да ЕУ развија свеобухватни регулаторни оквир за криптовалуте, али да су неки аспекти и даље изазовни, посебно због децентрализоване и анонимне природе криптовалута. Регулаторне мере као што су MiCA, KYC и AML стандарди представљају значајан напредак у осигурању транспарентности и сигурности крипто сектора, али је јасно да постојеће мере захтевају даље усавршавање и прилагођавање новим технологијама. Регулација криптовалута и сајбер криминала је релативно нова област у оквиру финансијске регулативе, али

она постаје све значајнија како се повећава обим и сложеност крипто тржишта. Увођење MiCA регулативе, KYC и AML стандарда представља важан корак у стварању сигурнијег и транспарентнијег тржишта криптовалута у ЕУ. Међутим, пред ЕУ и даље стоје бројни изазови и потреба за континуираним унапређењем регулаторног оквира. Као кључне тачке за будући развој могу се издвојити значајно унапређење сарадње на глобалном нивоу, адаптација регулативе према технолошким променама и успостављање баланса између регулације и подршке иновацијама. Уколико ЕУ успе да ефикасно усклади ове циљеве, може постати глобални лидер у регулацији криптовалута и заштити од сајбер криминала, чиме би се допринело сигурнијем и одрживијем финансијском тржишту у будућности.

EU REGULATORY FRAMEWORK ON CRYPTOCURRENCY AND CYBERCRIME

Srdan MIČIĆ, Dijana SAVIĆ BOŽIĆ, Milutin ATELJEVIĆ*

Abstract: This paper analyses the European Union (EU) regulatory framework for cryptocurrencies and measures to combat cybercrime related to digital currencies. With the increasing use of cryptocurrencies as a means of payment and their attractiveness for criminal activities, such as money laundering and ransomware attacks, the EU faces the challenge of establishing effective regulation that protects consumers and maintains market stability. The paper includes an analysis of key regulatory acts in the areas of Markets in Crypto-Assets (MiCA), Know Your Customer (KYC), and Anti-Money Laundering (AML), as well as standards aimed at improving transparency in the financial sector. It also analyses mechanisms such as digital forensics and analytics of digitally linked databases (so-called “blockchain analytics”) used to track transactions and identify criminal patterns. In addition to analysing existing measures, the paper highlights key challenges, including anonymity and decentralisation of cryptocurrencies. It suggests directions for future regulatory developments that would enable the EU to prevent cybercrime more effectively while encouraging innovation. From the analysis, the authors conclude that continuous regulatory improvement and global cooperation are key elements in the fight against cybercrime in the cryptocurrency sector.

Keywords: Cybercrime, cryptocurrencies, EU, legal regulation.

* Federal Police Administration, Sarajevo, Bosnia and Herzegovina. E-Mail: srdjan.micic.fup@gmail.com. ORCID iD: <https://orcid.org/0009-0004-1005-4472>; Faculty of Organizational Studies, Belgrade. E-Mail: dinabozic@gmail.com. ORCID iD: <https://orcid.org/0009-0008-4315-388X>; Faculty of Law, Bijeljina, Bosnia and Herzegovina. E-Mail: mateljevic@sinergija.edu.ba. ORCID iD: <https://orcid.org/0009-0003-6395-0011>.