

ДИСРУПТИВНИ ПОТЕНЦИЈАЛ БЛОКЧЕЈН ТЕХНОЛОГИЈЕ ЗА УНАПРЕЂЕЊЕ МЕЂУНАРОДНЕ ПРАВНЕ САРАДЊЕ У КРИВИЧНИМ СТВАРИМА

Апстракт: Блокчејн технологија представља значајан појеницијал за унапређење међународне правне сарадње у домену кривичној правосудја. Ова иновативна технологија нуди решења за неке од најзначајнијих изазова са којима се суочавају правни и правосудни системи, као што су сигурност процеса, разлике у правним системима, високи трошкови, техничка ограничења и језичке баријере. Коришћењем блокчејна може се постићи већа транспарентност, непроменљивост података, брза размена информација и повећана сигурност, чиме се може допринети ефикасности и транспарентности у међународној правосудној сарадњи. Кроз рад се дејствитије истражују конкретне примене блокчејна у међународној сарадњи у кривичним стварима, са посебним освртом на дигитализацију и безбедну размену и извршавање судских одлука, међусобно повезивање националних база података у циљу размене информација, као и коришћење блокчејна за брз и поверљив пренос доказној материјала између држава. Размотрене су и техничке, правне и организационе препреке у имплементацији блокчејна, као и начини њиховој превазилажења. Осим тога, кроз рад ће се анализирати начини на које блокчејн унапређује поверење између правосудних система, ојклањајући ојпребу за посредницима и олакшавајући транснационалну сарадњу. Међу предвиђеним предностима су свакако, убрзање судских процеса, смањење трошкова, унапређења сигурности података и поверљивости, као и олакшана сарадња између земаља са различитим правним системима. На крају, биће истражене појеницијалне баријере за имплементацију, ојоути рејулајорних изазова, техничких ограничења и ијшања приватности, као и мојућа решења за њихово превазилажење.

* Директор Сектора за учеснике на тржишту и дигиталну имовину у Комисији за хартије од вредности Републике Србије, uros.porovic@sec.gov.rs.

Кључне речи: дигитална форензика, блокчејн технологија, ланац кустодија, дигитализација правосуђа, доказни токени, паметни уговори.

1. УВОДНА РАЗМАТРАЊА О БЛОКЧЕЈН ТЕХНОЛОГИЈИ И ЊЕНОМ ПОТЕНЦИЈАЛУ ЗА УНАПРЕЂЕЊЕ САРАДЊЕ У ОБЛАСТИ КРИВИЧНОГ ПРАВОСУЂА

Технолошки напредак последњих деценија драматично је трансформисао начин на који друштво функционише. Дигитализација је прожела готово све аспекте људског живота, укључујући и сферу правосуђа. Међутим, правни и правосудни системи често касне у имплементацији нових технологија, што доводи до проблема у ефикасности и транспарентности. Једна од области у којој су ови изазови посебно изражени јесте међународна сарадња у кривичноправним стварима. Иако је међународна правна помоћ од суштинске важности за борбу против транснационалног криминала, тренутни механизми сарадње су често спори, скупи и подложни грешкама. Питања јурисдикције, различитих правних система и процедуре отежавају благовремену размену информација и доказа неопходних за гоњење кривичних дела.¹ Ово посебно долази до изражаја у дигиталном окружењу где електронски докази могу нестати у делићу секунде.

Савремено кривично правосуђе суочава се са изазовима који произилазе из све комплексније и глобализоване природе савремених злочина. Традиционални правосудни системи често се сусрећу са ограничењима у међународној сарадњи, било да је реч о размени информација, праћењу транснационалних учинилаца кривичних дела или спровођењу пресуда на глобалном нивоу. У таквом контексту, појављују се иновативна технолошка решења као катализатор за трансформацију правних парадигми која обећавају да превазиђу неке од фундаменталних изазова у међународној правосудној сарадњи. Једна од таквих технологија је и блокчејн – децентрализована, непроменљива и транспарентна база података која омогућава учесницима да размењују информације без потребе за централним посредником.²

Ипак, иако је блокчејн технологија иницијално настала као основа за оно што данас зовемо дигитална имовина,³ њен потенцијал се рапидно шири на друге области. Блокчејн мреже могу понудити висок степен сигурности,

1 Congressional Research Service, *Obstruction of Justice: An Overview of Some of the Federal Statutes That Prohibit Interference with Judicial, Executive, or Legislative Activities*, 2014, 13–14, <https://crsreports.congress.gov/product/pdf/RL/RL34303>, 24. март 2024.

2 A. Wright, P. De Filippi, „Decentralized Blockchain Technology and the Rise of Lex Cryptographia“, *Social Science Research Network*, 34/2015, 4–8.

3 Као полазна основа за упознавање са појмом и технологијом на којој се заснива дигитална имовина, често се од стране експерата у овој области упућује прво на

ефикасности и проверљивости у размени података између више страна. Те особине чине ову технологију потенцијално револуционарним алатом за унапређење сарадње правосудних органа на међународном нивоу.

Циљ овог рада јесте да се истражи начин на који би се блокчејн технологија могла искористити за решавање проблема односно унапређења међународне правне сарадње и приближи читаоцима могућности које ова технологија пружа. Биће анализирани конкретни изазови за имплементацију блокчејна у правосуђу. Рад ће покушати да пружи целовиту слику о дисруптивном потенцијалу ове технологије за унапређење ефикасности и транспарентности међународне правосудне сарадње у кривичним стварима, као и да отвори могућност за неке нове погледе конкретне технологије у овој правној сфери.

2. ОСВРТ НА ПРЕДНОСТИ И МАНЕ БЛОКЧЕЈН ТЕХНОЛОГИЈЕ

Блокчејн технологија, фундаментална иновација која је основ за дигиталну имовину, представља децентрализовану и дистрибуирану платформу која омогућава сигурну и транспарентну размену дигиталних информација. У овом поглављу пружа се читаоцу увид у дефиницију, основне принципе и кључне карактеристике које ову технологију чини револуционарним инструментом у контексту правосудне сарадње.⁴

Дефиниција блокчејна лежи у основном концепту ланца повезаних блокова података који се чувају на различитим рачунарима, стварајући дистрибуирану мрежу без потребе за посредницима.⁵ Овај децентрализован систем чини један од стубова на којима је заснован блокчејн, пружајући изузетну отпорност на манипулацију подацима, транспарентност и сигурност. Блокови представљају основне јединице података у блокчејну, сваки садржећи информације о трансакцијама, времену и дигитални печат⁶ који

уознавање са првим белим папиром – Bitcoin whitepaper (S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>, 24. март 2024).

4 За више информација и упознавање са основама блокчејна и институтима дигиталне имовине, вид. У. Поповић, *Евалуација ефикасности и поузданости протокола за сиречавање ирања новца у ирфовини дигиталном имовином*, мастер рад одбрањен на Правном факултету Универзитета у Београду, Београд, 2023; J. Banović, „Criminal Law Aspects of Digital Assets- Investigating and Proving Contemporary Forms of Crime: Scientific Approaches“, *Archibald Reiss Days*, University of Criminal Investigation and Police Studies, Belgrade, 2023, И. Радисављевић, „Кривичноправна заштита дигиталне имовине“, *Казнена реакција у Србији* (ур. Ђ. Игњатовић), Универзитет у Београду – Правни факултет, Београд, 2023, 252–314.

5 R. Berto, „Blockchain records: is the evidence admissible? A challenge for European Member States“, *Civil Procedure Review*, 3/2019, 57.

6 Ради се о јединственом криптографском потпису који гарантује аутентичност и интегритет података, користећи се алгоритмима за хаширање и енкрипцију да би се осигурало да су подаци непромењени и веродостојни од тренутка њиховог стварања.

га јединствено идентификује. Блокчејн се повезују у низ познат као ланац, чиме се ствара непрекинут и непроменљив низ података.⁷

Основни принцип блокчејна је децентрализација података. Информације нису смештене на централном серверу, већ се дистрибуирају на различите рачунаре у мрежи (чворови⁸). Ова децентрализација елиминира потребу за централним ауторитетом и повећава сигурност система. Криптографски алгоритми⁹, такође имају важну улогу у осигуравању безбедности података у блокчејн технологији. Кроз употребу приватних и јавних кључева,¹⁰ омогућава се енкрипција података, чиме се гарантује приватност и интегритет информација.

Транспарентност блокчејн технологије произлази из чињенице да су сви учесници у мрежи увек ажурирани са истим сетом података. Свака трансакција је видљива свим члановима мреже, пружајући потпуну транспарентност у раду система. Иако све блокчејн мреже деле кључне особине попут децентрализације, непромењивости и транспарентности, постоје различити типови мрежа који се разликују по нивоу приступа и правилима валидације трансакција. Свакако, могло би се рећи да је основна подела, на јавне (*public*), приватне (*private*) и конзорцијумске (*consortium*) блокчејн мреже.

Јавне блокчејн мреже карактерише њихова отвореност и доступност за учешће без ограничења, што омогућава било ком појединцу да се прикључи и учествује у мрежи без претходног одобрења. Примери таквих мрежа укључују *Bitcoin* и *Ethereum*, који су пионири у области криптовалута¹¹ и децентрализованих апликација¹². Ове мреже користе иновативне механизме

7 К. Wüst, A. Gervais, „Do you need a Blockchain?“, *Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, 1.

8 Чворови (*нодови*) представљају основне компоненте мреже које одржавају дистрибуирану књигу, валидирајући и снимајући све трансакције у блоковима. Сваки чвор функционише као аутономна јединица која приступа, чува и ажурира копију комплетног ланца блокова, чиме се осигурава децентрализација, интегритет података и отпорност мреже на манипулације и нападе.

9 Криптографски алгоритми представљају математичке процедуре коришћене за обезбеђивање података, омогућавајући шифровање и дешифровање информација са циљем заштите приватности, интегритета и аутентичности комуникације у дигиталном свету, чиме се гради поверење међу корисницима без потребе за централним посредником.

10 Приватни и јавни кључеви су основни елементи асиметричне криптографије, где приватни кључ остаје тајна коју познаје само власник, док је јавни кључ доступан свима за шифровање порука или верификацију потписа. Ова два кључа раде у пару тако да оно што је шифровано јавним кључем може бити дешифровано само одговарајућим приватним кључем, што омогућава сигурну комуникацију и аутентификацију у дигиталном простору.

11 Дигиталне или виртуелне валуте које користе криптографију за обезбеђивање трансакција и контролу стварања нових јединица, а функционишу применом блокчејн технологије.

12 Апликације које функционишу на блокчејн технологији омогућавајући корисницима да извршавају трансакције или користе услуге без потребе за централним ауторитетом.

за постизање дистрибуираног консензуса међу учесницима, што је основни услов за одржавање интегритета и сигурности блокчејна без централног ауторитета. Консензус механизам *Proof-of-Work (PoW)*,¹³ представља један облик правила валидације трансакција, а који се и даље широко користи у многим јавним блокчејн мрежама и захтева од учесника (познатих као рудари или *miners*¹⁴) да изврше велику количину рачунарских операција како би решили криптографске загонетке. Овај процес не само да помаже у верификацији и додавању нових трансакција у блокове ланца, већ и штити мрежу од злонамерних напада и покушаја манипулације. По успешном решавању загонетке, рудар који је то учинио има право да дода нови блок у ланац и као награду добија одређену количину дигиталне имовине.¹⁵

Приватне или затворене блокчејн мреже су дизајниране тако да функционишу унутар строго дефинисаних параметара, где приступ и учешће захтевају експлицитно одобрење или позивницу. Овај модел пружа организацијама могућност да имплементирају блокчејн технологију унутар својих система са већим степеном контроле над трансакцијама и подацима који се размеђују. Приватним блокчејн мрежама¹⁶ обично управља једна организација која одлучује о правилима, протоколима и учесницима мреже, што омогућава брже трансакције и повећану приватност.¹⁷

С друге стране, конзорцијумске блокчејн мреже¹⁸ представљају хибрид између јавних и приватних мрежа. У овом моделу, управљање мрежом је

-
- 13 Консензусни механизам који се користи у блокчејн технологији да би се омогућило договарање међу свим чворовима у мрежи око јединственог стања дистрибуиране књиге, без потребе за централним ауторитетом. PoW захтева од учесника (рудара) да изврше велику количину рачунарског рада да би решили комплексан математички задатак.
- 14 Представљају учеснике мреже који користе своју рачунарску снагу за решавање комплексних математичких задатака који омогућавају додавање нових блокова трансакција у блокчејн. За свој труд и уложену енергију, рудари се награђују блок наградама и трансакцијским провизијама.
- 15 У. Поповић, *op. cit.*, 33–34.
- 16 Један од најпознатијих примера овакве врсте блокчејна јесте отворени пројекат под окриљем *Linux Foundation*, дизајниран као основа за развој блокчејн апликација са модулрном архитектуром, који омогућава компанијама да креирају децентрализоване апликације које подржавају специфичне пословне потребе са високим степеном конфиденцијалности, скалабилности и ефикасности. *Fabric* је усмерен на приватне блокчејн мреже, где учесници морају да имају дозволу за учешће, чиме се обезбеђује већи контролни ниво над трансакцијама и члановима мреже. За више вид, <https://www.oak-tree.tech/blog/hyperledger-overview>, 12. март 2024.
- 17 D. Guegan, „Public Blockchain versus Private Blockchain“, *Documents de travail du Centre d’Economie de la Sorbonne*, 2017, 2, 3.
- 18 Најпознатији пример конзорцијумског блокчејна је *Enterprise Ethereum Alliance* (ЕЕА). ЕЕА обједињује компаније, организације и академске институције са циљем развоја стандарда и архитектуре за примену Ethereum технологије у пословном контексту. Овај конзорцијум ради на развијању отворених и персонализованих блокчејн решења која омогућавају ефикасну, транспарентну и сигурну пословну

подељено међу више организација које чине конзорцијум. Овакав приступ обезбеђује већу децентрализацију у односу на приватне мреже, док истовремено омогућава учесницима да одрже контролу над правилима мреже, њеном функционалношћу и безбедношћу. Конзорцијумске мреже су идеалне за пословне апликације где различите организације треба да сарађују и размењују податке у безбедном и транспарентном окружењу, али са строгим контролама приступа и већим степеном приватности.¹⁹

Оба модела, приватне и конзорцијумске блокчејн мреже, нуде специфичне предности за корпоративне и регулисане околине, укључујући ефикасније управљање ланцем снабдевања, унапређење процеса верификације идентитета, повећање степена безбедности трансакција и података, као и олакшавање сарадње међу различитим *stakeholderima*²⁰. Кроз коришћење ових мрежа, организације могу значајно побољшати ефикасност и транспарентност својих операција, док се истовремено осигурава да се поштују прописи и стандарди приватности и безбедности. Избор типа блокчејн мреже зависи од конкретне намене и захтева у погледу нивоа децентрализације, скалабилности²¹ и контроле приступа. У правосудним применама обично је потребан баланс између транспарентности јавних мрежа и контролисаних права приступа, те би можда највише и одговарао пример конзорцијумске мреже. Анализа предности и мана блокчејн технологије кључна је за сагледавање ширег контекста њеног потенцијала и ограничења.

Укратко предности блокчејн технологије су транспарентност, непроменљивост података, сигурност, смањење трошкова, децентрализација и ефикасност размене информација.²² Са друге стране поред усаглашености регулаторног статуса и законске примењивости, техничке комплексности и енергетске ефикасности, као проблеми најчешће се спомињу:

- 1) **Скалабилност блокчејн технологије** представља значајан изазов, посебно када се суочи са великим бројем трансакција које се обрађују симултано. Како се број учесника и трансакција у мрежи повећава, многе блокчејн платформе се суочавају са тешкоћама у одржавању брзине и ефикасности обраде података. Ово је нарочито изражено

комуникацију и трансакције међу члановима, при чему се одржава висок ниво приватности и испуњавају специфични пословни захтеви. За више вид. <https://entethalliance.org/about-enterprise-ethereum-alliance/>, 11. фебруар. 2024.

- 19 А. Hofmann et al., „Security Implications of Consortium Blockchains: The Case of Ethereum Networks“, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, 4/2021, 347–353.
- 20 Овај појам обухвата широк спектар учесника, укључујући, али не ограничавајући се на, запослене, клијенте, добављаче, инвеститоре, заједницу и владине агенције.
- 21 Способност мреже да обрађује велики број трансакција у реалном времену и да се прошири тако да подржи растући број корисника, уређаја и трансакција без деградације учинка.
- 22 За више вид. М. Vukolić, „The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication“, *Open Research Problems in Network Security* (J. Camenisch, D. Kesdoğan, eds.), Springer, 2015, 115–116.

- у случају механизма консензуса као што је *Proof-of-Work (PoW)*, који захтева значајну количину рачунарске снаге и времена за обраду сваког блока.²³
- 2) Имплементација блокчејна у правосудним системима захтева, такође и постизање **глобалног консензуса** око стандарда и правила. Различити правни оквири и културне разлике могу представљати препреку постизању овог консензуса, што може утицати на хомогеност система.
 - 3) Изазови **приватности и заштите података** које носи блокчејн технологија су мултидимензионални и захтевају детаљно разматрање. Док блокчејн омогућава непроменљивост и транспарентност трансакција, што доприноси поверењу и интегритету система, ове карактеристике такође могу створити потенцијалне ризике за приватност корисника и заштиту њихових података. На пример, једном када се информација унесе у блок, а блок постане саставни део ланца, она постаје трајно доступна свим учесницима мреже, што може олакшати неауторизовани приступ осетљивим подацима.

Проблеми се јављају и у контексту „права да будеш заборављен“ (*Right to be Forgotten*),²⁴ које је заштићено у општим регулативама о заштити података попут GDPR²⁵ у Европској унији. Блокчејн технологија, са својом основном карактеристиком непроменљивости, изазива питања о томе како се могу испунити захтеви за брисањем података. Да би се решили ови изазови, предложена су различита техничка и правна решења. На техничком нивоу, решења попут примене технологије енкрипције и псеудонимизације података могу помоћи у заштити идентитета корисника и осетљивих информација у блокчејн трансакцијама. Ово укључује технике као што су енкрипција пре снимања података у блокчејн, као и употреба доказа нултог знања (*Zero Knowledge Proofs*)²⁶ који омогућавају верификацију трансакција без откривања самог садржаја података.

Са правног аспекта, потребно је развити и имплементирати правне оквири који ће регулисати употребу блокчејна, посебно у односу на заштиту

23 На пример, Visa евидентира до 65.000 трансакција по секунди, док се на биткоин блокчејну изврши између 5 и 15 трансакција по секунди.

24 „Право да будеш заборављен“, како је утврђено у оквиру GDPR, омогућава појединцима да њихови лични подаци буду избрисани из одређених база података, обезбеђујући приватност и контролу над личним информацијама. За више вид. <https://gdpr-info.eu/issues/right-to-be-forgotten/>, 26. март 2024.

25 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504>, 26. март 2024.

26 Революционарна технологија у области криптографије и приватности података, омогућавајући једној страни (проверавајућој) да потврди истинитост тврдње друге стране без откривања било каквих конкретних информација о самој тврдњи. Концепт је први пут предложен 1985. године, од стране истраживача Шафи Голдвасер (*Shafi Goldwasser*), Силвио Микали (*Silvio Micali*) и Чарлс Ракоф (*Charles Rackoff*) у раду „Познавање тајни за дозвољени систем стварних идентитета“.

података. Ово укључује стварање смерница које ће обезбедити да се употреба блокчејн технологије усклађује са постојећим законима о заштити података и приватности. Такође, постоји потреба за развојем механизма који ће омогућити усклађивање блокчејна са захтевима за брисањем података, без компромитовања непроменљивости и транспарентности које технологија нуди. Изазов у имплементацији блокчејна лежи у налажењу праве равнотеже између транспарентности и приватности, која ће омогућити коришћење предности које ова технологија пружа, док се истовремено штите основна права и слободе појединаца. Ово захтева сарадњу између технолошких експерата, правника, регулаторних тела и других заинтересованих страна у процесу развоја и примене блокчејн технологије.

3. МЕЂУНАРОДНО КРИВИЧНО ПРАВО У ДИГИТАЛНОМ ДОБУ

3.1. Изазови и ограничења тренутног система правне сарадње

Дигитализација правосудних система у контексту међународног кривичног права доноси са собом низ изазова који ограничавају ефикаснију правну сарадњу између различитих правосудних система. У овом делу се анализира идентификација битних ограничења како би се сагледао контекст у којој блокчејн технологија може интервенисати и унапредити тренутни систем правне сарадње. Иако је међународна правна помоћ од фундаменталног значаја за ефикасно функционисање кривичног правосудја, постоје бројни изазови у остваривању делотворне сарадње између држава са различитим правним системима. Неки од кључних проблема и ограничења су:

- Спорост процеса - захтеви за међународну правну помоћ, који су често кључни за истраге које прелазе националне границе, могу бити посебно осетљиви на ове замке. Бирографија и неефикасне процедуре, као и разлике у правним системима и језичке баријере, додатно компликују ове процесе. Одсуство стандардизованих процедура за обраду и одобравање међународних захтева за правном помоћи може довести до дугих периода чекања, током којих докази могу постати мање релевантни или се сведоци могу повући. Оваква кашњења не само да одлажу истраге и судске процесе, већ могу и угрозити правду, омогућавајући осумњиченима да избегну казну и лишвавајући жртве правичног решења. У том контексту, постоји све већи позив на реформе које би убрзале процесе и побољшале међународну сарадњу у правосудним питањима, укључујући увођење технолошких иновација за ефикаснију размену информација и доказа.²⁷

27 Europol, Basel Institute of Governance, *Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering*, 2022, 6.

- Неусклађеност правних оквира - Разлике у кривичном законодавству, процесним правилима, као и у стандардима за заштиту права осумњичених и жртава, могу довести до правних препрека које отежавају, а понекад и онемогућавају, ефикасну сарадњу међу земљама. Примери таквих разлика укључују различите дефиниције кривичних дела, различите процедуре за прикупљање доказа, као и различите прагове за доказивање кривице.
- Трошкови - међународна правна сарадња захтева ангажовање преводилаца, путне трошкове, правне таксе и друге трошкове, што представља додатни терет.
- Техничка ограничења - застареле технологије, формат података и канали комуникације успоравају размену информација између држава и њених органа.
- Језичке баријере - превођење захтева за правну помоћ и пратеће документације је често скуп, неопходан и спор процес који изискује укључење већег броја лица, што доводи до потребе за додатним утрошком времена.
- Политички односи - Тензије или неповољни дипломатски односи међу државама могу значајно утицати на спремност за сарадњу, често резултујући одбијањем захтева за правну помоћ или намерним одуговлачењем у обради таквих захтева. Ово може имати директне последице на ефикасност међународних истрага и судских процеса, посебно када су у питању транснационални криминал и тероризам. Осим тога, политичке одлуке могу утицати на интерпретацију међународних уговора и конвенција, као и на постављање и приоритизацију правних стандарда који се примењују у међународним односима. У неким случајевима, државе могу користити правну помоћ као инструмент политичког притиска или уговора, уместо као средство за постизање правде.

Решавање ових проблема захтева комбинацију технолошких, правних и политичких мера како би се унапредила ефикасност међународне правосудне сарадње у кривичним стварима. Међународно кривично право суочава се и са изазовима због хетерогености правних система широм света. Различите јурисдикције имају различите правне стандарде, поступке и дефиниције кривичних дела, што отежава брзу и ефикасну сарадњу између држава.²⁸ На примеру јапанског међународног приватног права, види се да јапански правни систем тренутно не садржи специфичне законе нити пре-суде везане за грађанске парнице који укључују блокчејн технологију.²⁹

28 P. Galvão Teles, „The International Criminal Court and the evolution of the idea of combating impunity: an assessment 15 years after the Rome Conference“, *International Criminal Justice: A Dialogue between two Cultures* (P. Galvão Teles, M. Kowalski, eds.), Lisboa, 2017, 125–128.

29 Јапанско међународно приватно право, као и у многим другим земљама, примарно се бави регулацијом прекограничних приватноправних односа, укључујући

Међутим, идентитет странака и предмет спора су важни у одређивању међународне јурисдикције у поступцима везаним за блокчејн трансакције. Иако постојећи оквири међународне јурисдикције генерално добро функционишу за трансакције засноване на блокчејну, постоји неколико питања, посебно у вези са идентификацијом и лоцирањем одговарајућег туженог због псеудоанонимности. Осим тога, и даље се дискутује о поштовању споразума о јурисдикцији у споровима који произилазе из трансакција које користе блокчејн, где се такви споразуми генерално поштују, под условом да су јасно дефинисани и повезани са специфичним правним односима.³⁰

Правосудни системи имају различите обрасце сарадње, што може довести до спорова око признавања, извршења пресуда или екстрадиције. Оваква дивергенција ствара баријере у брзој размени информација и извршавању правних одлука између држава. Тренутни систем правне сарадње често је обележен спорим процесима размене информација. Ограничења у брзини и ефикасности могу значајно утицати на исходе међународних кривичних поступака, често доводећи до застоја или губитка релевантних информација који могу успорити или отежати ефикасно спровођење истрага и кривичног гоњења транснационалних кривичних дела. Сигурносне и поверљиве информације које се размењују између правосудних система захтевају посебан третман. Постојећи системи нису у потпуности сигурни, а питање поверљивости може представљати озбиљан изазов у осетљивим кривичним случајевима. Захтеви за узајамном правном помоћи могу месецима чекати на обраду због комплексних процедура и неефикасне бирократије. Све ово доводи до застоја у истрагама и отежава правовремено прикупљање електронских доказа који могу бити измењени или избрисани.

Додатно, различити стандарди у погледу прикупљања и чувања доказа стварају проблеме приликом коришћења доказа прикупљених у иностранству у домаћим судским поступцима.³¹ Неусклађеност правних оквира је посебно изражена у дигиталном домену где не постоје глобално усаглашени стандарди. Техничке и технолошке препреке попут некомпатибилних система за управљање предметима и мањка средстава за дигитализацију процеса, такође опструирају сарадњу. Питања кибернетичке безбедности и заштите личних података додатно усложњавају размену осетљивих информација.

питања која се односе на јурисдикцију, избор применљивог права и признавање и извршење страних судских одлука. Међутим, специфични закони који експлицитно укључују блокчејн технологију могу се наћи више у оквиру специјализованих регулација које се односе на финансијске услуге, дигиталне валуте, итд., а не директно у оквиру међународног приватног права.

- 30 T. Morishita, „Blockchain and Japanese Private International Law“, *Blockchain and Private International Law* (A. Bonomi, M. Lehmann, S. Lalani, eds.), Brill–Nijhof, 2023, 768–772.
- 31 E. Jennings, „Proving your cross-border claim – how to collect evidence abroad“, 2016, <https://moulislegal.com/knowledge-centre/proving-your-cross-border-claim-how-to-collect-evidence-abroad/>, 6. март 2024.

Размена информација између националних правосудних органа и међународних тела попут Интерпола или Еуропола представља важан елемент међународне сарадње у кривичним стварима. Међутим, ова област је оптерећена бројним ограничењима и изазовима. Једно од главних ограничења је што се размена информација углавном ослања на спору и скупу формалну правну помоћ између држава, уместо на директну комуникацију између органа, што свакако успорава добијање кључних информација у истрагама.³²

3.2. Како блокчејн може да превазиђе те проблеме

Како је претходно наведено, постојећи системи за размену информација имају значајна ограничења, међутим блокчејн технологија отвара могућности за превазилажење неких изазова. Блокчејн може унапредити међународну размену информација кроз:

- 1) **Транспарентност кроз децентрализацију** – Један од начина на који блокчејн технологија може превазићи изазове тренутног система правне сарадње јесте кроз пружање транспарентности. Ова технологија омогућава свим учесницима система приступ јединственој и неизмењивој књизи трансакција,³³ елиминишући могућност манипулације или скривања информација. Таква транспарентност помаже у отклањању неповерења између различитих правосудних система. Транспарентност блокчејна такође омогућава верификацију аутентичности информација. Свака трансакција забележена на блокчејн мрежи пружа јасну евиденцију о свим променама и приступима подацима, тиме би овај ниво транспарентности могао помоћи у одржавању интегритета правосудних процеса и процедура.
- 2) **Непроменљивост података** - информације креиране на блокчејну су трајно забележене и тешко их је накнадно изменити без детекције,³⁴ чиме се штити интегритет података, и обезбеђује ненарушава база података, где су информације забележене у блоковима који су повезани криптографским хеш функцијама.³⁵ Ова карактеристика елиминише

32 Поред осталог, на Конференцији Комитета експерата Савета Европе о сарадњи у кривичним стварима, која је одржана 2021. године, закључено је да дигитализација међународне сарадње, која је током пандемије корона вируса била интензивирана, треба да се настави и у будућности, вид. L. Breulich, „Strengthening of International Cooperation in Criminal Matters: Extradition and Mutual Legal Assistance, Report of the Council of Europe Online Conference – 5 May 2021“, *EUCRIM*, 4/2021, 283–284, <https://eucrim.eu/articles/strengthening-of-international-cooperation-in-criminal-matters-extradition-mutual-legal-assistance/>, 22. јануар 2024.

33 World Bank, *Distributed Ledger Technology (DLT) and Blockchain*, 1–3.

34 Манипулације на блокчејну у теорији су могуће само док информација не постане саставни део блока који се надовезао на претходни блок. Од тог тренутка није могуће мењати саму информацију.

35 У. Поповић, *op. cit.*, 37–40.

могућност непожељних промена или брисања података. У контексту правне сарадње, то значи да једном забележене информације остају непромењене и поуздане током времена. Непроменљивост података на блокчејну смањује могућност манипулације информацијама. У правосудном окружењу, где се тачност података сматра критичном, ова карактеристика блокчејна пружа додатни ниво поверења у интегритет информација које се размењују између правних система.

- 3) **Брзина размене** - размена информација путем блокчејна може бити готово тренутна, за разлику од спорог система правне помоћи између држава. Блокчејн технологија омогућава децентрализовану платформу за брзу размену података у реалном времену. Уместо ослањања на централизоване системе који захтевају сложене процесе верификације, блокчејн омогућава директну и брзу размену информација између правних система. Предност ове технологије јесте у томе што омогућава аутоматизацију процеса размене података. Кроз паметне уговоре, одређене врсте информација могу се размењивати аутоматски када су испуњени одређени услови који су унапред дефинисани.
- 4) **Сигурност** - криптографске методе обезбеђују висок ниво сигурности и штите поверљиве информације од неовлашћеног приступа и злоупотребе. Блокчејн технологија користи криптографске технике заштите информација. Сваки блок података је енкриптован и повезан са претходним блоком путем хеш функција. Ова сигурносна карактеристика штити податке од неовлашћеног приступа и чини их отпорним на нападе.³⁶ Поред криптографске заштите, блокчејн омогућава безбедну размену информација путем децентрализоване мреже. Одсуство централних тачака које се могу напасти чини блокчејн мање подложним сигурносним претњама које често погађају централизоване системе.

Имплементација блокчејн технологије може превазићи изазове везане за хетерогеност правних система. Транспарентност блокчејна омогућава јасно праћење информација и поступака, чиме се смањује ризик од непоразума између различитих јурисдикција. Овај систем чува интегритет података, смањује време потребно за верификацију информација и олакшава аутоматску размену без потребе за дуготрајним процесима. Интероперабилност између различитих правних система захтева глобалне стандарде. На крају, блокчејн технологија може деловати као неутрална платформа која подржава глобалну сарадњу, чиме се превазилази питање неспојивости правних система.³⁷

Иако блокчејн не може у потпуности елиминисати све изазове, велики број његових карактеристика могу значајно унапредити ефикасност, транспарентност и сигурност транснационалне размене информација између органа

36 Више о могућностима напада на блокчејн вид. B. Bartosz, „51% Attack: The Concept, Risks & Prevention“, <https://hacken.io/discover/51-percent-attack/>, 23. март 2024.

37 Europol, Basel Institute of Governance, *op. cit.*, 4.

за спровођење закона и правосудних институција. Треба разумети да блокчејн технологија не представља крајње решење, већ иницијални корак ка иновативним приступима у унапређењу међународне правне сарадње. Комбинација блокчејна са другим технологијама и правним стратегијама може створити холистички приступ решавању изазова и ограничења.

3.3. Конкретне могућности примене блокчејн технологије

3.3.1. Размена доказа (информација) у реалном времену кроз децентрализовану платформу

Како је претходно објашњено, имплементација блокчејн технологије у правосудни систем пружа нове могућности за унапређење сигурности и ефикасности у размени доказа и информација у реалном времену. Коришћење децентрализоване платформе омогућава кључним органима, укључујући полицију, тужилаштва и судове, да на безбедан и непроменљив начин деле критичне податке о кривичним поступцима. Овај вид би могао значајно да унапреди координацију и сарадњу међу различитим органима правосуђа, чиме би се убрзали судски процеси и повећала ефикасност правосудног система. За успешну имплементацију блокчејна у овом контексту, неопходно је размотрити и пратити постојеће правне оквире и стандарде који регулишу обраду и размену доказног материјала. На пример, морају се узети у обзир закони о заштити података о личности попут Опште уредбе о заштити података (GDPR) у Европској унији, који постављају строге захтеве за обраду личних података.³⁸ Поред тога, потребно је обезбедити да се сви докази који се размењују путем блокчејна прикупљају и обрађују у складу са релевантним процедуралним правилима и стандардима за доказе. То укључује осигурање да је доказни материјал релевантан, аутентичан и да није био подложен манипулацији.

Не треба заборавити да и модерне технологије своје упориште имају на старим правилима, па тако, у делу "Vita Neronis", Светоније (Suetonius) наводи да су противмере према фалсификаторима први пут уведене тако што је декретом наложено да документи морају бити пробушени и повезани концем кроз рупе троструко, пре њиховог печатања.³⁹ Због тога је Нерон

38 ГДПР представља правни оквир за заштиту приватности појединаца у контексту обраде личних података у Европској унији, чија имплементација и поштовање постају императив за све органе, организације и друге који послују на територији ЕУ или са грађанима ЕУ, а и шире. Усклађивање са одредбама ове уредбе намеће се као приоритет, с обзиром на далекосежан утицај који има на начине прикупљања, обраде и заштите личних података, као и строге казнене одредбе за случајеве непридржавања истих.

39 У древном Риму, заштита података и спречавање фалсификовања били су од изузетног значаја, о чему сведочи чињеница да су римски владари строго кажњава-

61. године пре нове ере подарио “Senatusconsultum Neronianum Adversos Falsarios”, којим се захтева да споразум мора бити забележен на полиптисима који нису пробушени, везани троструким концем, пре печачења.⁴⁰ Ово одражава континуитет и у приступу европског законодавства према потписивању докумената, наглашавајући три кључна циља: 1) идентификацију аутора, 2) екстерну манифестацију воље аутора за преузимање правних последица чињеница или радњи и 3) очување доказа о правно значајним чињеницама или радњама током времена.

Водећи се истом правном логиком и скоро две хиљаде година касније, Европска унија је кроз Директиву 93/99, која је промовисала технолошки неутралан приступ омогућавајући повезивање аутора са електронским записима путем електронског потписа или идентификације корисника, заменила Уредба Европске уније 910/2014 од 1. јула 2016. Ова нова уредба, позната као е-ИДАС, донела је правила за услуге поверења попут електронских потписа, печата, временских жигова и доставе, усмеравајући се ка унапређењу електронске идентификације и трансакција унутар унутрашњег тржишта.⁴¹

У том смислу, развој међународних стандарда и протокола за коришћење блокчејн технологије у правосудном контексту може помоћи у проналажењу потенцијалних правних и техничких изазова, осигуравајући да се технологија користи на начин који је у складу са међународним правним стандардима и обавезама заштите података. Коначно, за успешну имплементацију и употребу блокчејна у правосудном систему, важно је обезбедити обуку и едукацију за све учеснике у процесу, укључујући полицијске службенике, тужиоце, судије и правне заступнике односно адвокате, како би разумели основе блокчејн технологије и најбоље праксе за њену примену у правосудном контексту.

3.3.2. Повезивање база података

У контексту правног система, блокчејн технологија, такође нуди значајне могућности за унапређење управљања и размене правних информација кроз стварање повезаних база података.⁴² Имплементација блокчејна у правне базе података о осуђеним лицима, пресудама и примењеним правним санкцијама, омогућава стварање централизованог система за праћење

ли оне који би фалсификовали званичне исправе и податке. Штавише, постојали су посебни службеници задужени за верификацију аутентичности докумената, што указује на развијену свест о важности очувања интегритета података и у том периоду.

40 R. Berto, *op. cit.*, 55.

41 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910>, 16. јануар 2024.

42 Polkadot блокчејн, као мултичејн архитектура, могао би бити идеално средство за ове сврхе. За више о могућностима и идејама иза ове технологије вид. <https://polkadot.network/>.

који је истовремено транспарентан, сигуран и отпоран на неправилности. Са правног становишта, овакве иновације захтевају строгу усклађеност са домаћим и међународним прописима који регулишу заштиту података, приступ информацијама и процедуре у правосудном систему.

Поред тога, међународне конвенције и споразуми о правосудној сарадњи, као што су Хашка конвенција о признавању и извршењу страних пресуда у грађанским или трговачким стварима, постављају основе за међународну размену правних информација. Увођење блокчејн технологије у овај процес могло би да обезбеди ефикаснији и сигурнији начин за спровођење ових принципа, али такође захтева развој нових правних оквира и техничких стандарда који ће осигурати њихову компатибилност. Успостављање правних механизма за верификацију и признавање електронских докумената и записа на блокчејну као законитих доказа у судским процесима представља додатни проблем. То захтева измене постојећих закона о доказивању и увод нових норми које ће признати блокчејн као валидну технологију за чување и размену доказних материјала. Даље, неопходно је обезбедити да се процеси размене и чувања информација путем блокчејна спроводе у складу са стандардима који гарантују права окривљеног, правично суђење и права одбране односно право на одбрану, укључујући право на приступ доказима и право на жалбу.⁴³ Повезивање информација о спроведеним мерама и казнама помоћу блокчејн технологије пружа транспарентан преглед над примењеним правним санкцијама, чиме се побољшава праћење успешности спровођења правних мера и доприноси бољем управљању кривичним поступцима.

3.3.3. *Дигитализација судских одлука*

Дигитализација судских одлука путем блокчејн технологије представља револуционарни корак у правосудном сектору, који нуди значајне дисруптивне предности у смислу сигурности, транспарентности и ефикасности. Стварањем дигиталних, неизмењивих записа судских одлука, блокчејн осигурава да су документи аутентични и заштићени од било каквих покушаја неовлашћених измена или брисања. Правни оквир који регулише дигитализацију судских одлука мора да узме у обзир више аспеката, укључујући заштиту података, приступ информацијама и међународну сарадњу. Да би се осигурала правна ваљаност и признавање дигитализованих судских одлука, неопходно је усвојити одговарајуће законодавство које ће прецизирати услове под којима се блокчејн може користити за ову сврху. То укључује одредбе о верификацији дигиталних потписа, интегритету записа, као и о процедурама за регистрацију и чување судских одлука у блокчејн мрежи.

43 Претходно наведена гарантована права представљена су као једна од фундаменталних људских права, утемељена у најзначајнијим међународним начелима, документима и другим правним актима.

Међународна правна сарадња је такође важна за осигуравање униформности и компатибилности система дигитализације судских одлука изван националних граница. Међународни споразуми и стандарди, као што су Хашка конвенција о укидању потребе легализације страних јавних исправа⁴⁴ и други релевантни правни инструменти, треба да се ажурирају или допуне како би се укључиле одредбе специфичне за блокчејн технологију. Осим тога, важно је усмерити напоре на образовање и обуку правосудног особља о блокчејн технологији и њеној примени у контексту судских одлука. То обухвата разумевање техничких аспеката, као и правних импликација употребе блокчејна у овом домену. У закључку, дигитализација судских одлука путем блокчејна представља велики потенцијал за унапређење правосудног система, али њена успешна имплементација захтева развој чврстог правног и техничког оквира који ће осигурати законитост, сигурност и међународну сарадњу.

3.3.4. Чување форензичких доказа

Примена блокчејна у чувању форензичких доказа уводи нову димензију у обезбеђивању и управљању дигиталним доказима у правосудном систему. Један од аспеката ове иновације јесте гаранција интегритета и поузданости доказног материјала, који је критичан за поштен, правичан и ефикасан правосудни процес. Законски оквири који регулишу употребу и чување форензичких доказа морају бити ажурирани како би се укључиле спецификације и стандарди везани за блокчејн технологију. То укључује усвајање одредаба које обезбеђују да је сваки дигитални запис, једном унет у блокчејн, заштићен од неовлашћеног приступа, измена или брисања.⁴⁵ Поред тога, правни оквири треба да регулишу питања повезана са верификацијом и признавањем дигиталних доказа који су чувани у блокчејну, као валидних у судским поступцима. Ово подразумева развој протокола за проверу аутентичности и целовитости доказа који користе криптографске методе и дигиталне потписе за осигурање веродостојности информација. Међународна сарадња и стандардизација су такође кључни за успех у овој области. Сарадња међу земљама и релевантним међународним организацијама може допринети усвајању јединствених стандарда за употребу блокчејна у чувању и размени форензичких доказа, осигуравајући њихову међународну прихватљивост и употребљивост. Кључно је, такође, обезбедити образовање и обуку за правосудне органе, форензичке експерте и друге учеснике у правосудном процесу о предностима, могућностима и ограничењима блокчејн технологије. Такве образовне иницијативе би требале да обухвате

44 Уредба о ратификацији конвенције о укидању потребе легализације страних јавних исправа, *Сл. листић ФНРЈ – Међународни ујговори и групи споразуми*, бр. 10/62).

45 Н. Patil et al., „Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework“, *Egyptian Journal of Forensic Sciences*, 14/2024, 4.

техничке аспекте блокчејна, као и правне импликације његове примене у контексту форензичких истрага и судских поступака.

3.3.5. Ланац кустодија (*Chain of Custody – CoC*)

Ланац бележења стања доказа у контексту блокчејн технологије би могао да представља значајан корак напред у обезбеђивању веродостојности и транспарентности у процесу руковања доказима.⁴⁶ Овај ланац је важан за потврду аутентичности доказа и убедљивост судије у доказном поступку, међутим често традиционални системи (писмени докази) не могу адекватно гарантовати порекло и интегритет дигиталних доказа. Развој оквира за ефикасније достављање и очување дигиталних доказа представља важан изазов у форензичкој науци. Овакав ланац би има битну улогу током читаве истраге, при чему се интегритет доказа мора одржавати од момента првог открића све до каснијег предавања суду. Уколико је процес надзора контаминиран (нарушен), тешко стечени докази неће бити прихваћени.⁴⁷ Стога, овај ланац мора документовати доказе у свакој фази процеса истраге, почевши од стицања, прикупљања, анализе доказа, преко јединица које достављају доказе лабораторији, па све до информација о времену, месту, узроку и начину употребе доказа.⁴⁸ Примена блокчејна у ланцу кустодија дозвољава прецизно праћење путање доказа, почевши од момента њиховог прикупљања, преко различитих фаза обраде и складиштења, све до њиховог представљања у судском процесу⁴⁹. Ова методологија има потенцијал да значајно смањи могућност људске грешке, намерне манипулације или губитка доказа, што је свакако од великог значаја и представљало би напредак у фазама прикупљања доказа и њиховом чувању.⁵⁰

3.3.6. Доказни токени

Доказни токени⁵¹ представљају револуционарни корак у управљању и верификацији доказа у правним и другим формалним контекстима. Усвајањем

46 B. Flannigan, K. Doubleday, „How blockchain can improve digital evidence collection and collaboration“, 2023, <https://www.route-fifty.com/emerging-tech/2023/03/how-blockchain-can-improve-digital-evidence-collection-and-collaboration/383756/>, 23. март 2024.

47 Y. K. Borse et al., „Advantages of Blockchain in Digital Forensic Evidence Management“, *Social Science Research Network*, 2021.

48 S. Rao et al., „A Novel Approach for Digital Evidence Management Using Blockchain“, *Social Science Research Network*, 2020.

49 F.-C. Tsai, „The Application of Blockchain of Custody in Criminal Investigation“, *Procedia Computer Science*, 192/2021, 2780.

50 За више вид. *ibid.*, 2779–2788.

51 Токен на блокчејну описује дигитални запис који представља одређену вредност или право унутар дистрибуираног регистра. Може симболизовати имовину,

блокчејн технологије, доказни токени омогућавају да се сваком физичком или дигиталном доказу додели јединствени дигитални идентитет. Овај идентитет, или токен, садржи потребне информације о доказу, укључујући време стварања, порекло и историју промена или трансфера. Таква технологија обезбеђује неколико значајних предности:

Транспарентност и верификација - Доказни токени омогућавају потпуну транспарентност у процесу руковања доказима, што правосудним органима олакшава верификацију аутентичности и интегритета доказа. Свака промена у статусу доказа, укључујући његово прикупљање, складиштење, или предају, може бити тренутно праћена и ревидирана.⁵²

Непроменљивост и сигурност – Доказни токен би осигуравао да су све записане информације о доказу непроменљиве и отпорне на неовлашћене измене или хаковање, чиме би се повећала сигурност и смањено ризик од манипулације доказима.

Ефикасност и смањење трошкова - Аутоматизација процеса верификације доказа путем доказних токена може смањити време и ресурсе потребне за управљање доказима. Ово укључује смањење потребе за физичким складиштем и олакшавање брзе и ефикасне размене информација међу заинтересованим странама.

Побољшање међународне сарадње - Усвајање стандардизованих доказних токена може олакшати међународну правну сарадњу, омогућавајући лакшу размену доказа међу земљама са различитим правним системима. Токени могу послужити као универзални језик за верификацију и обраду доказа у транснационалним случајевима.

Изазови и регулаторни оквир - Увођење доказних токена такође поставља низ изазова, укључујући потребу за развојем опсежних регулаторних оквира који ће управљати њиховом употребом. Ови оквири морају да реше питања приватности, заштите података, и правну валидност доказних токена. Поред тога, потребно је осигурати широку прихватљивост и разумевање технологије међу правосудним и другим професионалцима.

Усвајање и интеграција доказних токена у постојеће правосудне системе захтеваће време, обуку и значајне инвестиције у технологију. Међутим, потенцијални дугорочни бенефити у погледу повећања веродостојности, транспарентности и ефикасности управљања доказима могло би се рећи да чине овај напор вредним.

3.3.7. Паметни уговори

Паметни уговор је самостални програмски код, који се аутоматски извршава и управља трансакцијама према унапред дефинисаним правилима

идентитет, гласачка права, или приступ услугама. Токени се користе као средство размене, представљајући власништво над дигиталном или физичком имовином, олакшавајући трансакције без посредника путем децентрализоване технологије.

и условима, који су уграђени у код уговора. Ови уговори се обично извршавају на блокчејн платформама, као што је Ethereum, Cardano, Solana, и др., али не и искључиво, која пружа децентрализовану и транспарентну околину за извршење паметних уговора. Паметни уговори садрже детаље трансакције, укључујући услове договорене од стране учесника, са аутоматским извршењем промена чим се ти услови задовоље. Они функционишу као “механизми који обухватају дигиталну имовину и учеснике”, где све или неке од страна улажу и премештају имовину кроз мрежу чворова ради потврде уговореног садржаја. Захваљујући могућности флексибилног пројектовања и развоја помоћу аутоматизованих програма, паметни уговори налазе примену у бројним секторима, укључујући финансије, осигурање и здравствене услуге, проширујући спектар употребе блокчејн технологије.⁵³

Примарна карактеристика паметних уговора је њихова способност да аутоматски извршавају, контролишу или документују правно релевантне догађаје и акције према условима уговора, без потребе за посредницима.⁵⁴ То значи да када се услови уговора испуне, паметни уговор аутоматски извршава договорене акције, као што су трансфер новца, регистрација власништва, или издавање сертификата. Такође, примена паметних уговора у правосудној сарадњи би омогућила аутоматско извршење одређених радњи када се испуне прецизно дефинисани услови. Ово би унапредило ефикасност процеса размене информација и смањило потребу за мануелним интервенцијама. Паметни уговори омогућавају аутоматско извршење дигиталних пресуда или уговора о екстрадицији. Кроз прецизно програмиране услове, ови уговори би допринели бржем спровођењу правних одлука и повећали ефикасност међународне правне сарадње.

3.3.7.1. Аутоматско извршење уговора о екстрадицији

Аутоматско извршење уговора о екстрадицији би могло да представља иновативан приступ у међународној правној пракси, који утиче на ефикасност и транспарентност процеса екстрадиције. Овај метод би укључивао коришћење технологије паметних уговора за аутоматизацију процеса провере и извршења услова екстрадиције, како су дефинисани у двостраним или мултилатералним уговорима. Паметни уговори омогућавају да се правила и услови уговора прецизно кодирају, а њихово испуњење аутоматски прати и верификује, што значајно смањује потребу за ручном обрадом и интерпретацијом од стране правосудних органа. Коришћењем аутоматског извршења уговора о екстрадицији, државе могу значајно убрзати процес екстрадиције, олакшавајући брзу и ефикасну сарадњу у борби против транснационалног криминалитета. Паметни уговори осигуравају да су сви правни услови за екстрадицију аутоматски проверени пре него што се иста одобри,

53 F.-C. Tsai, *op. cit.*, 2781.

54 K. Wüst, A. Gervais, *op. cit.*, 8.

чиме се смањује могућност људских грешака и осигурава да се процес води у складу са међународним стандардима и обавезама.⁵⁵

Поред тога, аутоматско извршење уговора о екстрадицији може значајно повећати транспарентност и одговорност у међународној правној сарадњи. Све трансакције и одлуке биће записане на блокчејну, чинећи их доступним и проверљивим за све заинтересоване стране, укључујући правосудне органе, правне представнике и међународне организације. Ово може допринети већем поверењу међу државама и олакшати сарадњу у комплексним међународним случајевима, доприносећи тиме ефикаснијој и праведнијој глобалној правној пракси.⁵⁶

4. ЗАКЉУЧАК

Кроз овај истраживачки рад анализиран је потенцијал блокчејн технологије за унапређење сарадње у области кривичног правосуђа. У одређеној мери су размотрене специфичне предности блокчејна као што су децентрализација, транспарентност, непромењивост и сигурност података. Предложене су конкретне могућности примене блокчејна за дигитализацију судских одлука, повезивање база података, брзу размену доказа и унапређење опште ефикасности прекограничне правосудне сарадње. Блокчејн технологија, с обзиром на своје карактеристике, могло би се рећи да пружа решења за многе изазове са којима се суочава међународно кривично право. Кроз конкретне примене, попут размене доказа у реалном времену, повезивања база података, дигитализације судских одлука и чувања форензичких доказа, блокчејн технологија обећава револуционарно унапређење ефикасности и транспарентности правне сарадње. Да би се овај потенцијал у потпуности искористио, неопходни су даљи кораци на развоју глобалних стандарда, усаглашавању регулаторних оквира, изградњи техничких капацитета и обуци кадрова. Препорука је свакако да се реализује пилот пројекат који би тестирао примену блокчејна за конкретне потребе размене информација између органа различитих земаља. На основу тих резултата могли би се идентификовати најбољи модели за ширу имплементацију. Мултидисциплинарна сарадња правника, техничких стручњака и представника органа за спровођење закона, такође, биће кључна за успешно коришћење потенцијала ове обећавајуће технологије за јачање правде и владавине права. Остаје свакако да блокчејн технологија има револуционарни потенцијал да трансформише ефикасност, поузданост и транспарентност размене информација у међународном кривичном правосуђу и тиме доприносе већем нивоу сарадње на међународном нивоу.

55 K. Wojdyło, „DAO and criminal law“, *Blockchain, smart contracts and DAO*, Warsaw, 2016, 32–34.

56 V. Schlatt et al., *Blockchain: Grundlagen, Anwendungen und Potenziale*, Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, 2016, 22–25.

ЛИТЕРАТУРА

- Banović J. „Criminal Law Aspects of Digital Assets- Investigating and Proving Contemporary Forms of Crime: Scientific Approaches“, *Archibald Reiss Days*, University of Criminal Investigation and Police Studies, Belgrade, 2023.
- Bartosz B., „51% Attack: The Concept, Risks & Prevention“, <https://hacken.io/discover/51-percent-attack/>.
- Berto R., „Blockchain records: is the evidence admissible? A challenge for European Member States“, *Civil Procedure Review*, 3/2019.
- Borse Y. K. et al., „Advantages of Blockchain in Digital Forensic Evidence Management“, *Social Science Research Network*, 2021.
- Breulich L., „Strengthening of International Cooperation in Criminal Matters: Extradition and Mutual Legal Assistance, Report of the Council of Europe Online Conference – 5 May 2021“, *EUCRIM*, 4/2021, 283–284, <https://eucrim.eu/articles/strengthening-of-international-cooperation-in-criminal-matters-extradition-mutual-legal-assistance/>.
- Congressional Research Service, *Obstruction of Justice: An Overview of Some of the Federal Statutes That Prohibit Interference with Judicial, Executive, or Legislative Activities*, 2014.
- Europol, Basel Institute of Governance, *Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering*, 2022.
- Flannigan B., Doubleday K., „How blockchain can improve digital evidence collection and collaboration“, 2023, <https://www.route-fifty.com/emerging-tech/2023/03/how-blockchain-can-improve-digital-evidence-collection-and-collaboration/383756/>.
- Galvão Teles P., „The International Criminal Court and the evolution of the idea of combating impunity: an assessment 15 years after the Rome Conference“, *International Criminal Justice: A Dialogue between two Cultures* (P. Galvão Teles, M. Kowalski, eds.), Lisboa, 2017.
- Guegan D., „Public Blockchain versus Private Blockchain“, *Documents de travail du Centre d’Economie de la Sorbonne*, 2017.
- Hofmann A. et al., „Security Implications of Consortium Blockchains: The Case of Ethereum Networks“, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, 4/2021.
- Jennings E., „Proving your cross-border claim – how to collect evidence abroad“, 2016, <https://moulislegal.com/knowledge-centre/proving-your-cross-border-claim-how-to-collect-evidence-abroad/>.
- Morishita T., „Blockchain and Japanese Private International Law“, *Blockchain and Private International Law* (A. Bonomi, M. Lehmann, S. Lalani, eds.), Brill–Nijhof, 2023.
- Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>.
- Patil H. et al., „Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework“, *Egyptian Journal of Forensic Sciences*, 14/2024.

- Поповић У., *Евалуација ефикасности и постојећих протокола за сјечавање
прања новца у шјровини дигиталном имовином*, мастер рад одбрањен
на Правном факултету Универзитета у Београду, Београд, 2023.
- Радисављевић И., „Кривичноправна заштита дигиталне имовине“, Казнена
реакција у Србији (ур. Ђ. Игњатовић), Универзитет у Београду – Правни
факултет, Београд, 2023.
- Rao S. et al., „A Novel Approach for Digital Evidence Management Using Block-
chain“, *Social Science Research Network*, 2020.
- Schlatt V. et al., *Blockchain: Grundlagen, Anwendungen und Potenziale*, Projekt-
gruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte
Informationstechnik FIT, 2016.
- Tsai F.-C., „The Application of Blockchain of Custody in Criminal Investigation“,
Procedia Computer Science, 192/2021.
- Vukolić M., „The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT
Replication“, *Open Research Problems in Network Security* (J. Camenisch, D.
Kesdoğan, eds.), Springer, 2015.
- Wojdyło K., „DAO and criminal law“, *Blockchain, smart contracts and DAO*,
Warsaw, 2016.
- World Bank, *Distributed Ledger Technology (DLT) and Blockchain*.
- Wright A., De Filippi P., „Decentralized Blockchain Technology and the Rise of
Lex Cryptographia“, *Social Science Research Network*, 34/2015.
- Wüst K., Gervais A., „Do you need a Blockchain?“, *Crypto Valley Conference on
Blockchain Technology (CVCBT)*, 2018.

Uroš Popović*

THE DISRUPTIVE POTENTIAL OF BLOCKCHAIN TECHNOLOGY FOR ENHANCING INTERNATIONAL LEGAL COOPERATION IN CRIMINAL MATTERS

Summary

Blockchain technology represents significant potential for enhancing international legal cooperation in the context of criminal justice. This innovative technology offers solutions to some of the most significant challenges faced by legal and judicial systems, such as slow processes, differences in legal systems, high costs, technical limitations, and language barriers. By utilizing blockchain, greater transparency, immutability of data, rapid information exchange, and increased security can be achieved, contributing to the efficiency and transparency of international judicial

* Master of Laws and Head of the Market Participants and Digital Assets Department at the Securities Commission of the Republic of Serbia, uros.popovic@sec.gov.rs.

cooperation. The paper explores in detail the specific applications of blockchain in international cooperation in criminal matters, with a particular focus on the digitization and secure exchange of court decisions, the interconnection of national databases for information sharing, as well as the use of blockchain for the rapid and confidential transfer of evidence between states. Technical, legal, and organizational barriers to blockchain implementation will be considered, along with ways to overcome them. Additionally, the paper will analyze how blockchain enhances trust between judicial systems, eliminating the need for intermediaries and facilitating transnational cooperation. The anticipated benefits include accelerated court proceedings, reduced costs, enhanced data security and confidentiality, and facilitated cooperation between countries with different legal systems. Finally, potential barriers to implementation, such as regulatory challenges, technical limitations, and privacy issues, will be explored, along with possible solutions to overcome them.

Keywords: Digital Forensics, Blockchain Technology, Chain of Custody, Digitization of the Judiciary, Evidence Tokens, Smart Contracts.