УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Усклађивање Блокчејн технологије са ГДПР: Правни и технички изазови права на заборав

(мастер рад)

Ментор:
Проф. др Предраг Цветковић

Студент:
Иван Јанковић
М014/23-ИТ

Ниш, 2025.

САДРЖАЈ

I. **УВОД**

Блокчејн технологија представља један од најзначајнијих технолошких напредака у последњих неколико деценија, са потенцијалом да суштински промени начин на који се подаци бележе, верификују и деле међу учесницима у различитим системима. Као децентрализована дигитална књига која омогућава складиштење непроменљивих и транспарентних записа, блокчејн је нашао широку примену у многим индустријама, од финансијског сектора, преко логистике, до здравства и правних система. Његова кључна карактеристика, која га издваја од традиционалних база података, је непроменљивост — подаци забележени у блокчејну не могу се брисати или мењати без сагласности већине учесника у мрежи.

Међутим, са све већим усвајањем блокчејна, јављају се озбиљна правна и регулаторна питања, посебно у вези са заштитом личних података. Европска унија је 2018. године увела Општу уредбу о заштити података – "General Data Protection Regulation" (ГДПР), законодавни оквир који поставља строге стандарде за обраду, прикупљање и чување личних података, као и права грађана у вези са њиховим подацима.[1] Један од централних елемената ГДПР-а је право на заборав, што омогућава појединцима да затраже брисање својих личних података када више не постоје легитимни разлози за њихову обраду. Ово право на брисање, дефинисано чланом 17 ГДПР-а, представља кључни изазов за блокчејн технологију, јер сама природа блокчејна не дозвољава да се подаци једноставно бришу са мреже.

На први поглед, блокчејн и ГДПР делују као две супротстављене идеје — једна технологија која подразумева непроменљивост и трајност података и друга правни оквир који инсистира на флексибилности у обради података и заштити приватности појединаца. Управо овај сукоб између технолошких иновација и регулативе чини сржи истраживања у овом раду. Блокчејн нуди неоспорне предности у смислу безбедности, транспарентности и децентрализације, али представља изазове у погледу поштовања законских обавеза које произилазе из ГДПР-а, посебно у контексту права на заборав.[2]

Због све веће примене блокчејн технологије у различитим секторима и географским подручјима, неопходно је дубље истражити како се ови правни и технолошки принципи могу ускладити. Овај рад ће се бавити кључним питањем — да ли је могуће и како пронаћи равнотежу између техничких карактеристика блокчејна и законских обавеза које намеће ГДПР.

[1] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

[2] Poelman, Michelle, and Sarfraz Iqbal. "Investigating the compliance of the gdpr: Processing personal data on a blockchain." *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*. IEEE, 2021.

1.1. Историјски преглед блокчејн технологије и ГДПР

Блокчејн технологија је први пут представљена као основни механизам за криптовалуту Биткоин (Bitcoin) 2008. године, али се њена примена убрзо проширила на низ других области, укључујући паметне уговоре и транспарентно праћење ланца снабдевања. С друге стране, ГДПР, који је ступио на снагу 2018. године, представља кључни законодавни оквир Европске уније за заштиту личних података. ГДПР поставља строге захтеве у погледу обраде, прикупљања и чувања података, као и права грађана, као што је право на брисање података (право на заборав). Ове две технологије — блокчејн и ГДПР — на први поглед изгледају некомпатибилне, што је тема коју ће овај рад детаљно истражити.

1.2. Проблем и циљеви истраживања

Главни истраживачки проблем у овом раду односи се на очигледан сукоб између непроменљивости података на блокчејну и права на заборав, како је дефинисано у члану 17 ГДПР-а. Циљ овог рада је да анализира како се техничке и правне карактеристике блокчејн технологије могу ускладити са захтевима ГДПР-а, са посебним освртом на право на заборав. Додатни циљ је понудити предлоге за помирење ових сукобљених принципа кроз техничке иновације, као што су "off-chain" решења и псеудонимизација, као и кроз прилагођавање законског оквира.

1.3. Методологија и обим истраживања

Овај рад користи комбинацију правне анализе и прегледа техничких решења. Правни део истраживања обухвата анализу ГДПР-а, релевантних одлука и регулаторних смерница. Технички део се фокусира на различите методе које се могу користити за осигурање приватности на блокчејну, укључујући шифровање података и псеудонимизацију. Обим истраживања је ограничен на правне аспекте и техничке изазове усклађивања блокчејн технологије са ГДПР-ом, где ће главни фокус бити на Европској унији, али ће се разматрати и глобални приступи регулацији блокчејна.

II. ОПШТА УРЕДБА О ЗАШТИТИ ПОДАТАКА (GDPR)

Општа уредба о заштити података, познатија као ГДПР (General Data Protection Regulation), представља један од најзначајнијих законских оквира за заштиту података о личности на глобалном нивоу. Ову уредбу је Европска унија усвојила 27. априла 2016. године, са циљем да замени ранију директиву о заштити података из 1995. године, и да одговори на изазове које доноси све већа дигитализација и глобализација обраде података. ГДПР је ступио на снагу 25. маја 2018. године и од тада је постао неопходан стандард за све организације које обрађују личне податке грађана Европске уније, без обзира на то где се те организације налазе.[3]

[3] European Union. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)." *Europa.eu*, 27 Apr. 2016, eur-lex.europa.eu/eli/reg/2016/679/oj.

С обзиром да се дигитални свет убрзано развија, количина прикупљених личних података значајно се повећала. Са повећањем количине података расте и ризик од њихове злоупотребе, што је резултирало потребом за снажнијим и свеобухватнијим законодавним оквиром. ГДПР је осмишљен да грађанима пружи већу контролу над својим подацима и да осигура права на приватност, истовремено омогућавајући организацијама да одговорно обрађују податке у складу са јасно дефинисаним правилима.

Једна од кључних карактеристика ГДПР-а је његова екстериторијална примена. То значи да се уредба не односи само на компаније и организације унутар Европске уније, већ и на све субјекте који обрађују податке грађана ЕУ, без обзира на њихову географску локацију. Ово укључује мултинационалне корпорације и мала предузећа која нуде робу или услуге грађанима ЕУ или која прате понашање корисника у ЕУ, као што су онлајн платформе и услуге.[4]

Главна сврха ГДПР-а је успостављање јединственог законодавног оквира за све земље чланице ЕУ, чиме се елиминишу недоследности између различитих националних закона о заштити података. Раније су државе чланице имале различите законе који су проистекли из раније Директиве 95/46/ЕЦ, што је створило правну несигурност и сложеност за организације које раде у више држава чланица. ГДПР је, као пропис, директно применљив у свим државама чланицама, без потребе за додатним националним законима, што омогућава уједначеност и доследност у примени.[5]

Поред тога, ГДПР се фокусира на усклађивање права појединаца са потребама савремених привредних субјеката, увођење строжијих услова за сагласност на обраду података, јачање права на приступ, исправку и брисање података, као и увођење нових права, као што су право на преносивост података и право на ограничење обраде. Такође, ГДПР уводи ригорозне захтеве за безбедност података, укључујући обавезу пријављивања повреда података у року од 72 сата надлежним органима за заштиту података.[6]

Један од главних изазова са којима се организације суочавају је усклађеност са ГДПР-ом, јер се његова примена протеже на широк спектар активности обраде података. Без обзира да ли се ради о великим корпорацијама, малим и средњим предузећима или непрофитним организацијама, сви субјекти који обрађују личне податке грађана ЕУ морају осигурати да њихови процеси обраде података буду у складу са ГДПР-ом. То укључује техничке и организационе мере за заштиту података, као што су шифровање, псеудонимизација, благовремено брисање података, као и редовно праћење и ревизија ових мера.

[4] Greze, Benjamin. "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives." *International Data Privacy Law* 9.2 (2019): 109-128.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ L 281, 23.11.1995.

[6] Krystlik, Jocelyn. "With GDPR, preparation is everything." *Computer Fraud & Security* 2017.6 (2017): 5-8.

Важно је истаћи да ГДПР не треба схватити као закон који само поставља ограничења, већ и као законодавни оквир који омогућава безбедну и одговорну обраду података у дигиталној ери. Његова сврха је да уравнотежи права на приватност појединаца са потребом да организације обрађују податке у легитимне пословне сврхе. ГДПР се тако позиционира као кључни закон у заштити података у доба информатичке економије, где подаци представљају једну од најважнијих валута.

2.1. Основни принципи ГДПР-а

Принцип законитости, поштења и транспарентности

Овај принцип налаже да се сви лични подаци морају обрађивати законито, поштено и транспарентно. Законитост обраде значи да сваки поступак обраде мора бити заснован на правном основу, као што је сагласност субјекта података, испуњење уговора, испуњење законске обавезе, заштита виталних интереса или легитимни интерес лица. организација. Поштена обрада подразумева да субјекти података не смеју бити заведени или заведени у вези са сврхом обраде података. Транспарентност захтева од организација да јасно и разумљиво обавесте субјекте података о томе које информације прикупљају, зашто их прикупљају и како ће их користити.

Принцип ограничења сврхе

Према овом принципу, лични подаци морају се прикупљати искључиво у сврхе које су јасно дефинисане и легитимне и не смеју се обрађивати на начин који није у складу са тим сврхама. То значи да организације морају обавестити субјекте података о тачним разлозима за прикупљање података и да се ти подаци не могу користити у било коју другу сврху осим оне за коју су првобитно прикупљени, осим ако субјект података не да додатну сагласност.

Принцип минимизације података

Један од кључних аспеката ГДПР-а је принцип минимизације података, који налаже да се прикупљају само лични подаци који су неопходни за постизање одређене сврхе обраде. Организације не би требало да прикупљају више података него што је потребно, а обрада непотребних података представља кршење прописа. Овај принцип захтева од организација да критички процене које су им информације заиста потребне за њихову активност и да избегавају прикупљање сувишних података.

Принцип тачности

Тачност личних података је још један важан принцип ГДПР-а. Од организација се тражи да обезбеде да подаци које прикупљају и обрађују буду тачни, ажурни и релевантни. Уколико се утврди да су подаци нетачни или неажурни, организације су дужне да их одмах исправе или обришу. Ово је неопходно како би се осигурала тачност информација које се користе за доношење одлука, као и за заштиту права субјеката података.

Принцип ограничења складиштења

Према ГДПР-у, лични подаци се не смеју чувати дуже него што је потребно да би се постигла сврха обраде. Након што се постигне сврха обраде, подаци морају бити избрисани или анонимизовани, осим ако не постоји правни основ за њихово даље чување. Овај принцип помаже у смањењу ризика од злоупотребе података и смањује оптерећење за организације које би морале да управљају великим количинама непотребних информација.

Принцип интегритета и поверљивости

Заштита личних података од неовлашћене или незаконите обраде, губитка, уништења или оштећења је још један основни принцип ГДПР-а. Организације су дужне да спроводе одговарајуће техничке и организационе мере за заштиту података од ризика. Ово може укључивати шифровање података, псеудонимизацију, као и контролу приступа подацима. Поред техничких мера, важно је обезбедити и адекватну обуку запослених како би се обезбедила безбедна обрада података.

Принцип одговорности

Коначно, ГДПР уводи принцип одговорности, који налаже да организације морају бити у стању да покажу своју усклађеност са уредбом. То значи да организације морају да имају документоване процедуре за обраду података, као и да редовно спроводе провере усклађености. Овај принцип захтева од организација да буду проактивне у заштити података и да предузму мере како би осигурале да је обрада података законита и усклађена са ГДПР-ом.[7]

2.2. Лични подаци и права субјекта појединца

Један од кључних аспеката Опште уредбе о заштити података (ГДПР) је заштита личних података појединаца и осигурање њихових права у вези са тим подацима. Према ГДПР-у, лични подаци су свака информација на основу које се може директно или индиректно утврдити идентитет особе. Ово може укључивати различите врсте података као што су име, адреса, број телефона, електронска адреса, подаци о локацији, ИП адреса, као и подаци о физичком, физиолошком, генетском, менталном, економском, културном или друштвеном идентитету појединца.[8]

Шта су лични подаци?

Лични подаци, како их дефинише ГДПР, су широк појам. Они укључују не само очигледне податке као што су име и презиме, већ и податке који могу индиректно идентификовати појединца, као што су ИП адреса или подаци о локацији. Такође, информације које се односе на понашање корисника, као што су подаци прикупљени путем колачића или биометријски подаци који омогућавају директну идентификацију

[7] Општа уредба о заштити података (ГДПР), Службени лист Европске уније, L119, 2016.

[8] Tsesis, Alexander. "Data subjects' privacy rights: regulation of personal data retention and erasure." *U. Colo. L. Rev.* 90 (2019): 593.

појединца, као што су отисци прстију или скенирање мрежњаче, такође потпадају под дефиницију личних података.[9]

Индиректно прикупљање података је такође важно. То значи да чак и ако се појединац не може директно идентификовати на основу доступних података, али постоји могућност идентификације комбиновањем тих података са другим информацијама, та информација се и даље сматра личним подацима. На пример, скуп података који садржи само иницијале особе и њену адресу становања може се сматрати личним подацима ако постоји начин да се на основу тих информација идентификује одређена особа.

Права субјеката података

ГДПР уводи низ права осмишљених да појединцима дају већу контролу над њиховим личним подацима. Ова права омогућавају грађанима ЕУ да одлуче како ће се њихови подаци прикупљати, користити и обрађивати. Најважнија права субјеката података су описана у наставку:

1. **Право на информисање –** Субјекти података имају право да буду информисани о томе које податке организација прикупља, зашто их прикупља, како их користи, колико дуго ће их чувати, као и о правима која им припадају у вези са њиховим подацима. Ове информације морају бити пружене на јасан и разумљив начин пре него што се подаци прикупе.
2. **Право на приступ подацима** – Појединци имају право да затраже копију својих личних података које поседује организација. Ово право омогућава субјектима података да виде које су информације о њима прикупљене и да потврде да се ови подаци обрађују у складу са законом.
3. **Право на исправку** – Ако су подаци које организација чува нетачни или непотпуни, субјект података има право да захтева њихову исправку или допуну. Организације су дужне да брзо одговоре на такве захтеве и да ажурирају информације.
4. **Право на брисање података** – Познато и као „право на заборав“, ово право омогућава појединцима да затраже брисање својих података у одређеним ситуацијама, на пример, када подаци више нису потребни у сврхе за које су коришћени. прикупљени, када је субјект повукао сагласност за обраду или када се подаци незаконито обрађују. Међутим, постоје изузеци од овог права, као што су ситуације у којима организација мора да задржи податке због законских обавеза.
5. **Право на ограничење обраде** – Појединци могу захтевати привремено ограничење обраде својих података, на пример, када оспоравају тачност података или када се подаци обрађују незаконито, али субјект не жели да се подаци обришу.
6. **Право на преносивост података** – ГДПР омогућава субјектима података да затраже копију својих података у машински читљивом формату и да те податке пренесу другом контролору података. Ово право је посебно важно у случајевима када корисници желе да пренесу своје податке са једног дигиталног сервиса на други.
7. **Право на приговор** – Субјекти података имају право приговора на обраду својих података када се обрада заснива на легитимним интересима контролора података,

[9] Finck, Michèle, and Frank Pallas. "They who must not be identified—distinguishing personal from non-personal data under the GDPR." *International Data Privacy Law* 10.1 (2020): 11-36.

на јавном интересу или на вршењу службених овлашћења. Организације морају прекинути обраду података осим ако могу да покажу да имају убедљиве легитимне разлоге за наставак обраде.

8. **Права у вези са аутоматизованим доношењем одлука и профилисањем** – Појединци имају право да не буду предмет одлука донетих искључиво на основу аутоматизоване обраде података, укључујући и профилисање, ако те одлуке имају правне последице по њих или значајно утичу на њих.[10]

Значај права субјеката података у пракси

Права субјеката података чине основу за контролу над њиховим информацијама и дају грађанима ЕУ алате за заштиту њихове приватности. Имплементација ових права у пословну праксу захтева значајне организационе и техничке промене, али је кључна за обезбеђивање усклађености са ГДПР-ом. Свака организација мора да развије процедуре које јој омогућавају да ефикасно одговори на захтеве субјеката података, а у многим случајевима од компанија се тражи да именују службеника за заштиту података који ће надгледати процесе и бити тачка контакта за субјекте података.

2.3. Спровођење ГДПР-а и казне

Општа уредба о заштити података (ГДПР) не само да поставља јасна правила о томе како се лични подаци морају обрађивати, већ и уводи строге механизме спровођења и значајне казне за њихово кршење.

Надлежни органи и спровођење уредбе

Имплементација ГДПР-а поверена је независним надзорним телима сваке земље чланице ЕУ, познатим као „надзорна тела" или „ауторитети за заштиту података". Ова тела играју кључну улогу у обезбеђивању да организације правилно обрађују личне податке и да се придржавају правила уредбе.[11]

Надлежна тела су одговорна за:

- Истрагу притужби које су поднели субјекти података.
- Спровођење инспекција и ревизија унутар организација ради утврђивања усклађености са ГДПР-ом.
- Изрицање санкција и казни у случају кршења правила.

Надзорни органи такође имају задатак да промовишу свест о правима која ГДПР пружа грађанима и да помогну организацијама да схвате своје обавезе. У ситуацијама када дође до прекограничне обраде података, надзорни органи могу да сарађују преко Европског одбора за заштиту података „European Data Protection Board" (ЕДПБ), који олакшава координацију и доследну примену ГДПР-а широм ЕУ.

[10] Voigt, Paul, et al. "Rights of data subjects." *The EU General Data Protection Regulation (GDPR) A Practical Guide* (2017): 141-187.

[11] Voigt, Paul, et al. "Enforcement and fines under the GDPR." *The EU General Data Protection Regulation (GDPR) A Practical Guide* (2017): 201-217.

Механизми имплементације

Један од кључних алата за имплементацију ГДПР-а је механизам доследности, који омогућава координацију између надзорних тела у различитим државама чланицама. Овај механизам је посебно важан за компаније које послују на међународном нивоу и које обрађују податке грађана из више земаља чланица. Када постоји прекогранична обрада података, надзорни органи свих релевантних земаља имају право да учествују у процесу доношења одлука, чиме се обезбеђује доследна примена ГДПР-а широм Европске уније.

Поред тога, ГДПР предвиђа могућност подношења тужби против организација које крше права субјеката података. Субјекти података могу поднети жалбу надлежном органу или директно суду. У случају да организација прекрши права субјекта података, субјекат може захтевати надокнаду. Такође, ГДПР дозвољава колективне тужбе у случајевима када је више ентитета погођено сличним кршењем права.

Казне за непоштовање ГДПР-а

Један од најзначајнијих елемената ГДПР-а је висина новчаних казни које се могу изрећи организацијама које се не придржавају уредбе. Казне за непоштовање ГДПР-а могу бити изузетно високе и зависе од тежине прекршаја. Уредба предвиђа два нивоа казни:

1. До 10 милиона евра или 2% од укупног глобалног годишњег промета – Ова казна се односи на прекршаје у вези са техничким аспектима уредбе, као што је недостатак адекватних мера безбедности података или неправилно вођење евиденције обраде података**.**
2. До 20 милиона евра или 4% укупног глобалног годишњег промета – Ова казна се односи на озбиљнија кршења, као што су кршење основних принципа обраде података, непоштовање права субјеката података или незаконит међународни пренос података**.**[12]

Важно је напоменути да су казне прогресивне и одређују се на основу различитих фактора, укључујући природу, озбиљност и трајање повреде, као и број погођених субјеката података и ниво сарадње организације са надзорним органима. На пример, предузеће које одмах пријави кршење података и предузме кораке за ублажавање штете може добити нижу казну од предузећа које прикрива кршење података или не сарађује са властима.

Примери казни изречених према ГДПР-у

Откако је ГДПР ступио на снагу 2018. године, изречено је неколико значајних новчаних казни, које служе као упозорење организацијама да своје обавезе схвате озбиљно. Неки од најистакнутијих примера укључују:

- Новчана казна против Гугла (Google) – Француска агенција за заштиту података (CNIL) казнила је Гугл са 50 милиона евра због недостатка транспарентности у

[12] Voigt, Paul, et al. "Enforcement and fines under the GDPR." *The EU General Data Protection Regulation (GDPR) A Practical Guide* (2017): 201-217.

вези са обрадом података и незаконитог добијања сагласности корисника за персонализовано оглашавање.[13]

- Новчана казна Британиш Ервејс-у (British Airways) – због велике повреде података која је утицала на више од 400.000 клијената, компромитујући њихове личне и финансијске информације, изречена је казна од 20 милиона фунти.[14]
- Новчана казна против Меријота (Marriott) – Британски „Information Commissioners Office“ (ICO) је такође казнио Marriott International са 18,4 милиона фунти након што је откривено да је преко 300 милиона гостију погођено кршењем података.[15]

Ови примери показују да ГДПР значајно утиче на привредне субјекте, посебно велике корпорације, и да надзорни органи озбиљно схватају примену уредбе. Такође, ови случајеви наглашавају важност улагања у мере заштите података и обезбеђивање усклађености са ГДПР-ом како би се избегле високе казне и заштитио углед компаније.

III. ПРАВО НА ЗАБОРАВ ПРЕМА ГДПР-У

Право на заборав – “Right To Be Forgotten” (РТБФ-RTBF) постало је једна од најважнијих компоненти модерног закона о заштити података о којима се расправљало. Прво артикулисано у оквиру Опште уредбе о заштити података (ГДПР), ово право одражава растућу забринутост око контроле појединаца над њиховим личним подацима у свету који се све више дигитализује. Експлозија праксе прикупљања и складиштења података, коју су покретале и приватне корпорације и јавни субјекти, довела је до огромних складиштења личних података која често трају неограничено. Право на заборав ово решава тако што појединцима даје право да захтевају брисање својих личних података под одређеним условима, чиме се враћа контрола над информацијама које су можда постале застареле, ирелевантне или незаконито обрађене.

Укључивање права на заборав у ГДПР наглашава посвећеност Европске уније да даје приоритет заштити личних података као основном људском праву. Уз брзи раст онлајн услуга, друштвених медија и инфраструктура заснованих на клауд технологији, огромне количине личних података се обрађују и чувају на глобалном нивоу, често без смисленог надзора или контроле од стране самих субјеката података. Право на заборав настоји да ублажи ове забринутости овлашћујући појединце да захтевају брисање података који више не служе својој првобитној сврси или су у супротности са основним принципима ГДПР-а.[16]

[13] European Data Protection Board. “The CNIL’s Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC | European Data Protection Board.” *Www.edpb.europa.eu*, 21 Jan. 2019, www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Преузето 17 Oct. 2024.

[14] Bray, Oliver. “British Airways Slapped with Biggest Ever Fine for Data Breach.” *Lexology*, 15 Jan. 2021, www.lexology.com/library/detail.aspx?g=4a4818a6-2540-4582-81a7-592be99c85b2. Преузето 24 Oct. 2024.

[15] Page, Carly. “Marriott Hit with £18.4 Million GDPR Fine over Massive 2018 Data Breach.” *Forbes*, 30 Oct. 2020, www.forbes.com/sites/carlypage/2020/10/30/marriott-hit-with-184-million-gdpr-fine-over-massive-2018-data-breach/. Преузето 23 Oct. 2024.

[16] Voigt, Paul, et al. "Rights of data subjects." *The EU General Data Protection Regulation (GDPR) A Practical Guide* (2017): 141-187.

Међутим, ово право није без своје сложености. Оно мора бити у равнотежи са другим основним правима, као што је слобода изражавања, а технички изазови који су укључени у обезбеђивање трајног брисања података у дистрибуираним системима не могу се потценити. Ово поглавље ће истражити правне, техничке и практичне импликације права на заборав, почевши са детаљним испитивањем члана 17. ГДПР-а.

3.1. Члан 17: Право на брисање и његове импликације

Члан 17 ГДПР-а је камен темељац права на заборав, који формално уводи „право на брисање“ као правни оквир. Одредба даје појединцима могућност да затраже брисање својих личних података када су испуњени одређени услови, што одражава шире циљеве ГДПР-а за транспарентност, контролу и одговорност у активностима обраде података. Разумевање потпуних импликација овог члана захтева детаљно испитивање специфичних критеријума према којима се може захтевати брисање података, одговорности које се стављају на контролоре података и потенцијалних сукоба са другим правним и друштвеним интересима.

Члан 17 наводи шест кључних основа по којима појединци могу тражити брисање својих личних података:

1. **Подаци више нису потребни за првобитну сврху**. Ово је можда најосновнији аспект права на заборав. Када лични подаци испуне сврху за коју су првобитно прикупљени или обрађени, не постоји легитиман разлог да се они чувају. На пример, ако се корисник претплатио на услугу на мрежи и касније отказао претплату, добављач услуге не би имао законски разлог да задржи личне податке корисника мимо онога што је неопходно за регулаторне или уговорне сврхе. У таквим случајевима појединци имају право да захтевају брисање података.
2. **Појединац повлачи своју сагласност**. Сагласност је кључна правна основа за обраду података према ГДПР-у. Ако се лични подаци обрађују на основу изричитог пристанка појединца, они имају право да повуку ту сагласност у било ком тренутку. Након повлачења сагласности, контролор мора престати са обрадом података осим ако не постоји друга законска основа. Ово право је кључно за обезбеђивање да појединци имају сталну контролу над коришћењем својих података, посебно у ситуацијама када су можда првобитно пристали без потпуног разумевања импликација или када су се њихове личне околности промениле.
3. **Појединачни приговор на обраду**. Према ГДПР-у субјекти података имају право приговора на обраду својих личних података. Ако се приговор уважи и не постоје важни легитимни разлози за обраду, подаци се морају избрисати. Ова одредба признаје да појединци треба да имају право гласа о томе како се њихови подаци користе, посебно када су у питању активности попут профилисања или директног маркетинга, који можда нису у складу са њиховим личним преференцијама или очекивањима.
4. **Подаци су незаконито обрађени**. Незаконита обрада се односи на ситуације у којима обрада личних података крши одредбе ГДПР-а. Ово се може догодити када се подаци прикупљају без законске основе, обрађују на начин који није у складу са њиховом првобитном сврхом или се чувају дуже него што је то законом дозвољено. У таквим случајевима, право на заборав служи као корективни механизам, омогућавајући појединцима да захтевају брисање незаконито обрађених података, чиме се враћају њихова права на приватност.

5. **Подаци се морају избрисати да би се испунила законска обавеза.** Постоје случајеви у којима би даље задржавање личних података довело до кршења других законских обавеза. На пример, промене националног или ЕУ закона могу захтевати од контролора података да избришу одређене врсте информација како би били у складу са ажурираним прописима. ГДПР осигурава да се у таквим случајевима субјекти података могу ослонити на РТБФ да спроведу своје право на брисање својих података
6. **Подаци су прикупљени у вези са понудом услуга информационог друштва детету**. Постоје посебне одредбе за податке који се односе на децу, уважавајући њихову посебну рањивост и потребу за појачаном заштитом. Када се подаци о детету прикупљају у вези са онлајн услугама, примењују се строжа правила, а право на заборав је кључно средство за обезбеђивање да се подаци о деци не чувају дуже него што је потребно, посебно у случајевима када је пристанак дало дете или законски старатељ. који га касније повлачи.[17]

Импликације члана 17 шире се далеко изван непосредног односа између субјекта података и контролора података. Члан 17(2) уводи концепт „права на обавештавање“, који захтева од руковалаца који су објавили личне податке да предузму „разумне кораке“ да обавесте друге контролоре који обрађују податке о захтеву појединца за брисање. Ово је посебно релевантно у контексту онлајн платформи, претраживача и друштвених медија, где се подаци често брзо шире на више платформи и услуга. Одредба „право на обавештавање“ наглашава амбицију ГДПР-а да осигура да је право на заборав ефикасан чак и у међусобно повезаној и дистрибуираној природи интернета.[18]

Међутим, члан 17 такође наводи неколико изузетака који ограничавају примену права на заборав, балансирајући право на приватност са другим друштвеним и правним интересима. Члан 17(3) прецизира да се право на брисање не примењује када је обрада података неопходна за остваривање слободе изражавања и информисања, поштовање законске обавезе, јавни интерес у области јавног здравља, сврхе архивирања у јавном интересу, научно или историјско истраживање, или успостављање, остваривање или одбрана правних захтева. Ови изузеци наглашавају тензије између права на приватност и других супротстављених вредности, захтевајући пажљиво разматрање начина на који право на заборав треба применити у пракси.[19]

Суд правде Европске уније (СПЕУ) је одиграо кључну улогу у тумачењу члана 17, посебно у значајном случају Гугл (Google) Шпанија против АЕПД (“Agencia Espanola de Proteccion de Datos”-AEPD) и Марио Цостеја Гонзалез из 2014. Пресудом СПЕУ у овом случају утврђено је да се претраживачи могу сматрати контролорима података према ГДПР-у и од њих се може захтевати да уклоне везе до личних података ако се сматрају нерелевантним, застарелим или претераним у односу на сврхе обраде. Ова одлука је била

[17] Wolford, Ben. “Everything You Need to Know about the ‘Right to Be Forgotten.’” *GDPR.eu*, 5 Nov. 2018, gdpr.eu/right-to-be-forgotten/. Преузето 24 Oct. 2024.

[18] European Union. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance).” *Europa.eu*, 27 Apr. 2016, eur-lex.europa.eu/eli/reg/2016/679/oj

[19] Ibid.

значајна у обликовању практичне примене права на заборав, посебно у погледу тензије између приватности и права јавности на приступ информацијама.[20]

Члан 17. ГДПР-а предвиђа право на заборав као кључну компоненту модерног закона о заштити података. Он појединцима нуди моћан алат за утврђивање контроле над њиховим личним подацима, осигуравајући да се они избришу када више нису потребни или када је правни основ за обраду повучен. Међутим, право није апсолутно и његова примена мора бити пажљиво избалансирана са другим правима и интересима.

3.2. Технички аспекти трајног брисања података

Право на заборав, како је дефинисано у члану 17. Опште уредбе о заштити података (ГДПР), захтева да се лични подаци трајно бришу на захтев под одређеним околностима. Међутим, техничка имплементација таквог мандата је далеко од једноставног. Подаци се чувају, обрађују и деле кроз све сложеније и међусобно повезане дигиталне екосистеме, што технички процес обезбеђивања потпуног и неповратног брисања личних података чини изазовним задатком. Овај одељак истражује техничке методологије за брисање података, укључујући изазове које постављају дистрибуирана рачунарска окружења, системи резервних копија и нове технологије као што је блокчејн.

3.2.1 Врсте брисања података

Трајно брисање података укључује више од пуког уклањања приступа подацима; мора осигурати да се сами подаци више не могу повратити ни на који начин. Да бисмо разумели техничке детаље овога, неопходно је разликовати различите методе брисања података:

- Меко брисање: У неким системима, подаци су само означени као „избрисани“, али остају на медијуму за складиштење. Ово је слично уклањању уноса из директоријума без брисања основне датотеке. Меко брисање омогућава могућност опоравка података, пошто подаци остају физички присутни док их не пребришу нови подаци. Овај метод је недовољан за испуњавање ГДПР-ових захтева у вези права на заборав.
- Тврдо брисање: Овај метод укључује уклањање података из система, обично преко преписивања или чишћења са локација за складиштење. Међутим, чак и уз тврдо брисање, остаци података могу и даље постојати на тракама за резервне копије, евиденцијама или системским кешовима, што представља додатне изазове за потпуно брисање.
- Безбедно брисање: Безбедно брисање је робуснији метод дизајниран да обезбеди да подаци не могу да се поврате. Ово обично укључује криптографско брисање, где су кључеви за шифровање који штите податке уништени, чинећи податке недоступним. Алтернативно, може укључити вишеструка преписивања физичких сектора складиштења како би се осигурало да су преостали трагови оригиналних података елиминисани. Методе безбедног брисања су критичне за испуњавање

[20] Lynskey, Orla. "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez." *The modern law review* 78.3 (2015): 522-534.

захтева ГДПР одредби, јер обезбеђују да подаци нису само недоступни већ и неповратни.[21]

3.2.2 Изазови у брисању података у дистрибуираним системима

Модерне инфраструктуре за складиштење података често укључују дистрибуиране системе где се подаци складиште на више локација, укључујући окружења у облаку и дата центре. У таквим системима, копирање и дистрибуција података се користе да би се обезбедила доступност, перформансе и поузданост. Иако ова архитектура пружа робусну заштиту података, она ствара значајне техничке потешкоће када је у питању усклађеност са правом на заборав.

- **Преобилност и репликација података**: Подаци се често реплицирају преко сервера или чак у другим земљама како би се осигурала отпорност на грешке. Као резултат тога, брисање података из једног система не осигурава аутоматски њихово брисање са свих реплицираних локација. Штавише, због географске дисперзије, различите копије истих података могу бити предмет различитих правних надлежности и стандарда за брисање података, што компликује усклађеност са ГДПР-ом.
- **Складиштење у облаку и пресликавање података**: У окружењима у облаку, добављачи услуга често пресликавају податке како би осигурали да корисници имају приступ својим датотекама без обзира на географску локацију. Док се примарна копија података може избрисати на захтев, пресликане верзије могу да опстану у секундарним центрима података. Na primer, Amazon Web Services (AWS) ili Google Cloud Platform (GCP) обезбеђују дистрибуирана решења за складиштење где се подаци аутоматски пресликавају на различите локације, што отежава обезбеђивање потпуног брисања на свим инстанцама.[22]
- **Системи резервних копија**: Организације често одржавају резервне копије података како би спречиле губитак у случају квара система. Ове резервне копије могу да се чувају ван изворне локације или на архивским системима заснованим на тракама, којима се приступа само током хитних случајева или обнове система. Брисање података из активних система не обухвата нужно ове резервне копије, а многе организације се суочавају са техничким препрекама у идентификацији и брисању одређених података из старих система. Политике задржавања резервних копија морају бити усклађене са ГДПР-ом како би се осигурало да се лични подаци у резервним копијама бришу или анонимизирају на захтев, што је задатак који је посебно сложен с обзиром на то да ове резервне копије често нису одмах доступне.[23]

3.2.3 Преписивање и криптографске технике

Да би били у складу са захтевом права на заборав, контролори података морају да обезбеде да подаци не буду само избрисани већ и да буду неповратни. Да би се то

[21] Reardon, Joel, David Basin, and Srdjan Capkun. "Sok: Secure data deletion." *2013 IEEE symposium on security and privacy*. IEEE, 2013.

[22] Amazon. “Amazon Web Services (AWS) - Cloud Computing Services.” *Amazon Web Services, Inc.*, 2024, aws.amazon.com/. Accessed 9 Sept. 2024.

[23] Politou, Eugenia, Efthimios Alepis, Maria Virvou, and Constantinos Patsakis. *Privacy and data protection challenges in the distributed era*. Vol. 26. Heidelberg, Germany: Springer, 2022.

постигло могу се користити две основне техничке методе: преписивање података и криптографско брисање.

- **Преписивање података**: Овај процес укључује писање нових, насумичних података преко сектора у којима су оригинални подаци ускладиштени, чинећи оригиналне податке неповратним. Да би се испунили стандарди безбедног брисања, овај процес се често понавља више пута како би се осигурало да не остану преостали магнетни трагови, који би потенцијално могли да се реконструишу коришћењем специјализованих алата. Стандард Министарства одбране САД (DoD) 5220.22-M, на пример, препоручује вишеструко преписивање како би се осигурало да подаци не могу да се поврате.[24]
- **Криптографско брисање**: У системима где су подаци шифровани, безбедно брисање се може постићи уништавањем кључева за шифровање који су потребни за приступ подацима. Када се ови кључеви униште, подаци постају неповратни. Овај метод је посебно користан у окружењима у облаку или дистрибуираним системима, где је физичко брисање свих копија података технички непрактично или немогуће. Криптографско брисање је скалабилно решење за усаглашеност са ГДПР-ом, посебно када се примењује са јаким алгоритмима за шифровање који испуњавају индустријске стандарде као што је AES-256.[25]

3.2.4 Анонимизација и псеудонимизација података

У неким случајевима, трајно брисање можда неће бити изводљиво или пожељно, посебно када су дотични подаци и даље потребни за сврхе попут статистичке анализе, истраживања или архивирања. У таквим случајевима, анонимизација или псеудонимизација могу пружити алтернативу која задовољава захтеве ГДПР-а уз очување корисности података.

- **Анонимизација**: Анонимизација се односи на процес неповратне измене личних података тако да се више не могу приписивати појединцу. Правилно анонимизирани подаци не спадају у опсег ГДПР-а, јер се више не сматрају личним подацима. Међутим, постизање истинске анонимизације може бити технички изазовно, посебно када се ради о великим скуповима података који могу садржати индиректне идентификаторе или када се анонимизовани подаци могу поново идентификовати унакрсним референцама са другим скуповима података. Технике као што су к-анонимност и диференцијална приватност се често користе да би се смањио ризик од поновне идентификације, али се морају пажљиво применити како би се обезбедила усклађеност.[26]
- **Псеудонимизација**: Псеудонимизација, са друге стране, подразумева замену информација које могу да идентификују личности вештачким идентификаторима (псеудонимима) који се могу користити за праћење података до појединца само коришћењем додатних информација које се чувају одвојено. За разлику од анонимизације, псеудонимизација је реверзибилна, али нуди побољшану заштиту

[24] Joshi, Seema B. "Standards and techniques to remove data remanence in cloud storage." *2018 IEEE Punecon*. IEEE, 2018.

[25] ibid.

[26] Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation." *Computer law & security review* 33.2 (2017): 171-181.

тако што осигурава да се подаци не могу приписати одређеној особи без приступа засебном кључу или скупу података. ГДПР подстиче употребу псеудонимизације као технике за побољшање приватности, посебно када потпуно брисање није изводљиво или када подаци морају да се чувају у легитимне пословне сврхе.[27]

3.2.5 Нове технологије и брисање података

Нове технологије, као што су блокчејн и Интернет ствари (Internet of Things - ИоТ), представљају јединствене изазове за имплементацију права на заборав, јер су засноване на децентрализованим или непроменљивим архитектурама где се традиционалне методе брисања података можда не примењују.

- **Блокчејн технологија**: непроменљива књига Блокчејн-а, која осигурава да када се подаци једном запишу, не могу се мењати или брисати, ствара конфликте са правом на заборав. Иако блокчејн нуди робусну сигурност и транспарентност, није дизајниран да омогући трајно брисање појединачних трансакција или уноса података. Једно потенцијално решење је употреба складиштења ван ланца (off-chain) или доказа о нултом знању (zero-knowledge proof), који омогућавају да се одређени елементи података уклоне или прикрију без угрожавања интегритета блокчејна.[28] [29]
- **ИоТ уређаји**: Раст броја ИоТ уређаја, који прикупљају и преносе огромне количине личних података у реалном времену, ствара додатне компликације за брисање података. Многи ИоТ уређаји су уграђени у свакодневне објекте, од паметних термостата до носивих уређаја за праћење здравља, и често немају капацитет складиштења или интерфејс неопходан за управљање захтевима за брисање. Осигурати да се лични подаци прикупљени помоћу ових уређаја могу избрисати или анонимизирати у складу са ГДПР-ом је све већи технички изазов, посебно пошто се обим и разноврсност података које прикупљају ИоТ системи настављају ширити.[30]

Технички аспекти трајног брисања података су сложени и вишеструки, укључујући низ метода, од безбедних алгоритама за брисање до криптографског брисања и техника анонимизације. Ови процеси морају бити пажљиво имплементирани како би се осигурала усклађеност са ГДПР-ом, док се истовремено баве специфичним изазовима које постављају дистрибуирани системи, инфраструктура за резервне копије и нове технологије као што су блокчејн и ИоТ. Како се дигитални пејзаж развија, предузећа и организације морају стално да ажурирају своје праксе управљања подацима како би

[27] Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation." *Computer law & security review* 33.2 (2017): 171-181.

[28] Molina, Fernanda, Gustavo Betarte, and Carlos Luna. "Design principles for constructing GDPR-compliant blockchain solutions." *2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*. IEEE, 2021.

[29] Sun, Xiaoqiang, F. Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. "A survey on zero-knowledge proof in blockchain." *IEEE network* 35, no. 4 (2021): 198-205.

[30] Bastos, Daniel, Fabio Giubilo, Mark Shackleton, and Fadi El-Moussa. "GDPR privacy implications for the Internet of Things." In *4th Annual IoT Security Foundation Conference*, vol. 4, pp. 1-8. 2018.

осигурале да могу да испуне техничке захтеве трајног брисања података, док регулатори морају остати опрезни у процени ефикасности ових метода.

3.3 Етички аспекти и потенцијалне злоупотребе права на заборав

Право на заборав, у теорији замишљено као средство заштите приватности појединца, у пракси доноси и бројне етичке дилеме и ризике од злоупотребе. Експоненцијални раст дигиталних података и стално присуство информација у онлајн простору значајно су повећали вредност овог права, али и изазвали потребу за етичким разматрањем његовог ефекта на право јавности на информисање, као и на очување историјске истине. Овај сегмент истражује сложеност балансирања између права на приватност и јавног интереса, ризике од злоупотребе у правној и друштвеној сфери, као и дилеме у примени права на заборав у дигиталном добу.

3.3.1. Балансирање приватности и права на информисање

Уставни и законски оквири земаља ЕУ, као и Европска конвенција о људским правима, истичу право на приватност и слободу информисања као два основна људска права.[31] У случају права на заборав, ова права су често у сукобу. На пример, брисање одређених информација које се односе на јавне личности може утицати на слободу изражавања и слободу медија, јер би ограничавало способност новинара, истраживача и јавности да приступе информацијама од јавног значаја. Пресуда у случају Google Spain v. AEPD (2014), као што сам раније навео, подвукла је значај балансирања ових права, јер је Европски суд правде препознао право појединаца да захтевају брисање одређених резултата претраге, али само у случајевима када је информација непотребна, ирелевантна или застарела у односу на сврху за коју се обрађује.[32] Иако је ова пресуда дефинисала оквир за примену права на заборав, она је отворила многа питања у погледу одређивања граница између личног права на приватност и права јавности на приступ релевантним информацијама.

3.3.2. Могућности злоупотребе и угрожавање транспарентности

Један од највећих етичких ризика права на заборав је могућност да појединци искористе ово право како би уклонили информације које су од јавног интереса, али су потенцијално штетне по њихов углед или позицију. У случају јавних личности, политичара или пословних лидера, ова пракса може довести до брисања информација о етичким прекршајима, злоупотреби службеног положаја, финансијским неправилностима или других података који су од значаја за јавност. Овакво брисање може угрозити транспарентност и онемогућити јавност да има увид у важне друштвене информације, посебно када је у питању одговорност и интегритет оних који обављају јавне функције. Док ГДПР пружа изузетке за брисање података у случајевима када су у питању историјски, научни или јавни интереси, не постоји јасан механизам који би

[31] European Court of Human Rights. *European Convention on Human Rights*. 1950, p. 11, www.echr.coe.int/documents/d/echr/Convention_ENG. Преузето 26 Oct. 2024.

[32] Lynskey, Orla. "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez." *The modern law review* 78.3 (2015): 522-534.

обезбедио да се сви случајеви потенцијалне злоупотребе правилно процене. Ово оставља простор за несавесну примену права на заборав.[33]

3.3.3. Последице на правни систем и истраживање

У правном систему, право на заборав може утицати на преседане и приступ подацима о ранијим судским случајевима који су често корисни у процесу истраживања и анализе будућих случајева. Правни аналитичари и истраживачи ослањају се на приступ историјским подацима и судским одлукама као моделима за проучавање правних трендова, одлука и еволуције правних тумачења. Уклоњени подаци могу довести до "празнина у знању", што може негативно утицати на разумевање историјских и правних промена и ограничити квалитет правног истраживања. Такође, право на заборав поставља изазове за архивистичке и историјске институције које се ослањају на комплетне и тачне податке ради документовања историје. Уклањање појединачних података из историјског контекста може утицати на истинитост историјских извора и ограничавање истраживача у анализи друштвених и културолошких трендова. Овде настаје феномен дигиталне амнезије – процеса у коме се важне информације губе услед брисања података, што може имати дугорочне негативне последице на друштво.[34]

3.3.4. Потреба за етичким смерницама и регулисањем

Иако право на заборав представља значајан напредак у правима на приватност појединаца, његова практична примена намеће низ изазова који захтевају пажљиво разматрање етичких импликација и правних оквира. Потреба за етичким смерницама и бољим регулисањем у овом контексту постаје све израженија, јер су правна решења тренутно недовољна да у потпуности предвиде или спрече злоупотребе овог права, као и последице по друштво у целини.

Прецизна дефиниција јавног интереса: Смернице и регулатива морају детаљно дефинисати појам јавног интереса како би се обезбедило да се ово право не користи за прикривање информација које су важне за друштво. Јавни интерес може обухватати све од историјских чињеница и правних случајева до етичких и пословних прекршаја јавних личности. Без јасне дефиниције овог појма, постоји ризик да право на заборав буде примењено на начин који угрожава приступ јавности информацијама од значаја за друштвени надзор и транспарентност.

Побољшање регулаторног надзора: Регулаторна тела морају бити оспособљена и опремљена ресурсима да доследно и правично спроводе закон и одређују случајеве у којима право на заборав може, или не може, бити примењено. Потребна је и интернационална координација, јер се подаци често чувају у различитим јурисдикцијама које могу имати различите приступе и стандарде у погледу права на заборав и приватност података. Само на овај начин се могу превазићи правне празнине које настају због географске распршености података и различитих националних законодавстава.

[33] Brimblecombe, Fiona. "The public interest in deleted personal data? The right to be forgotten's freedom of expression exceptions examined through the lens of Article 10 ECHR." *Journal of Internet Law* 23.10 (2020): 1-29.

[34] Stainforth, Elizabeth. "Collective memory or the right to be forgotten? Cultures of digital memory and forgetting in the European Union." *Memory Studies* 15.2 (2022): 257-270.

Етичке смернице за примену технологија усклађених са правом на заборав: С обзиром на све сложеније дигиталне екосистеме, потребне су смернице за примену технологија које омогућавају брисање података на начин који је компатибилан са правом на заборав. На пример, развој напредних алгоритама за сигурно брисање података, као и криптографске методе, могао би да обезбеди да се подаци избришу на одговарајући начин, али је важно развити и етичке смернице које би спречиле злоупотребу таквих технологија у сврхе манипулације или прикривања истине.

Образовање јавности и етичка одговорност појединаца: Поред регулативе, важно је едуковати јавност о правима и одговорностима које носи право на заборав. Етичка одговорност не лежи само на институцијама и компанијама, већ и на појединцима који могу покушати да искористе ово право ради прикривања чињеница које би могле бити од јавног значаја. Образовање о томе како се право на заборав примењује и етичка свест о његовој злоупотреби могу допринети смањењу злоупотребе и очувању равноправног приступа информацијама.

Подстицање транспарентности у примени права на заборав: Иако је циљ овог права заштита приватности, неопходно је створити механизме који ће осигурати транспарентност у његовој примени, нарочито када су у питању јавне личности или случајеви од ширег значаја. Овај приступ би могао да укључи стварање јавних регистара или посебних извештаја у којима би били забележени захтеви за брисање одређених података и разлози за одобрење или одбијање тих захтева, у случајевима када су информације од јавног интереса. Овакве мере омогућиле би да се право на заборав користи сврсисходно, без угрожавања права јавности на информисање.

У светлу изазова које поставља право на заборав, потреба за етичким смерницама и регулаторним побољшањима постаје кључна за очување равнотеже између приватности и јавног интереса. Само кроз инклузиван и пажљив приступ који подразумева јасне дефиниције, одговарајући надзор и транспарентност, право на заборав може постати ефикасан механизам заштите приватности, а да притом не угрози принципе транспарентности и друштвене одговорности.

IV. БЛОКЧЕЈН ТЕХНОЛОГИЈА

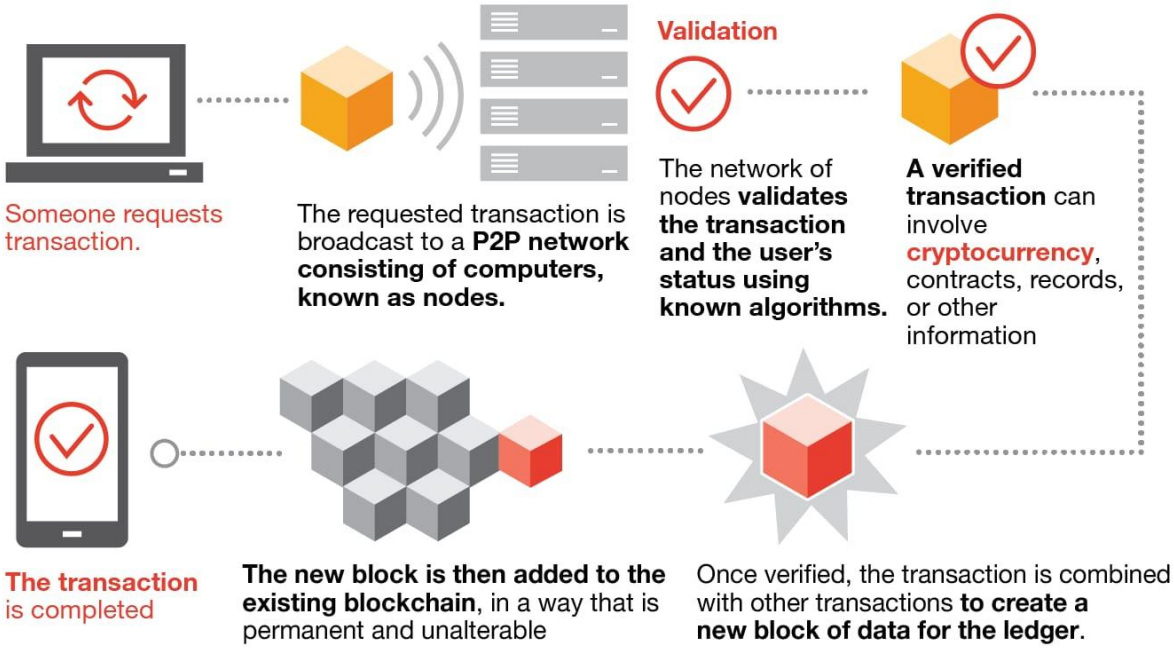
Блокчејн технологија, коју је 2008. године представио псеудонимни креатор Сатоши Накамото као окосницу Биткоина (Bitcoin), од тада је еволуирала у револуционарну дигиталну инфраструктуру.[35] Далеко изван своје почетне примене у криптовалутама, блокчејн сада служи као свестрано решење за широк спектар индустрија. У својој сржи, блокчејн је технологија дистрибуиране књиге ("Distributed Ledger Technology"-ДЛТ) која омогућава безбедно, транспарентно и отпорно вођење евиденције у оквиру децентрализоване мреже. Његова привлачност лежи у могућности успостављања поверења у дигиталним окружењима у којима учесници можда немају већ постојеће односе поверења, што га чини технологијом каменом темељцем за будућност сигурних и транспарентних трансакција.

Структура блокчејна се састоји од низа међусобно повезаних блокова података, од којих сваки садржи листу трансакција, временску ознаку и јединствени криптографски хеш. Сваки блок је повезан са својим претходником преко своје хеш вредности, формирајући непроменљиви ланац који чува хронолошки ред и интегритет података. Ова

[35] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Satoshi Nakamoto* (2008).

јединствена конфигурација осигурава да када се информације додају у ланац блокова, оне се не могу ретроактивно мењати без промене свих наредних блокова, чинећи манипулисање подацима компјутерски недовољно. Концепт непромењивости, заједно са децентрализованом архитектуром, обезбеђује да ниједан ентитет или учесник не може једнострано да контролише или манипулише књигом, обезбеђујући ниво транспарентности и безбедности који је тешко постићи традиционалним централизованим базама података.[36]

Slika 1.



https://blog.college.ch/blockchain-technology/all-you-need-to-know-about-cryptocurrency-and-blockchain-technology/

Једна од најкарактеристичнијих карактеристика блокчејн технологије је њен механизам консензуса, који је фундаменталан за постизање договора о стању књиге у дистрибуираној мрежи. Уобичајени консензусни алгоритми укључују Доказ о Раду ("Proof of Work"-PoW), где се чворови такмиче у решавању сложених математичких проблема за валидацију трансакција, и Доказ о Улогу ("Proof of Stake"-PoS), који додељује снагу валидације на основу броја токена које држи учесник. Ови механизми консензуса елиминишу потребу за централним ауторитетом од поверења, смањујући ризик од појединачних тачака квара и повећавајући отпорност и поузданост мреже.[37]

Са техничког становишта, капацитет блокчејна да омогући децентрализоване равноправне трансакције се ослања на комбинацију криптографских алгоритама и мрежних протокола. Крипографија са јавним кључем, на пример, осигурава да само појединци са исправним приватним кључевима могу да овласте трансакције, чиме се одржава поверљивост података. Поред тога, дигитални потписи обезбеђују непорицање, обезбеђујући да се трансакција не може одбити након што је потписана и забележена у књизи. Децентрализована природа блокчејна такође побољшава његову доступност и

[36] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

[37] Cao, Bin, Zhenghui Zhang, Daquan Feng, Shengli Zhang, Lei Zhang, Mugen Peng, and Yun Li. "Performance analysis and comparison of PoW, PoS and DAG based blockchains." *Digital Communications and Networks* 6, no. 4 (2020)

робусност, јер архитектура дистрибуиране мреже значи да чак и ако део мреже откаже, целокупни систем остаје оперативан и доступан.[38]

Случајеви употребе блокчејн технологије су се значајно проширили последњих година, вођени њеним јединственим својствима као што су децентрализација, транспарентност и безбедност.[39] Индустрије у распону од финансија и управљања ланцем снабдевања до здравства и јавне администрације користе блокчејн за решавање изазова, као што су превенција превара, интегритет података и неефикасност процеса. На пример, у финансијском сектору, блокчејн олакшава прекогранична плаћања у реалном времену, смањујући потребу за посредницима и смањујући трошкове трансакције. У ланцима снабдевања, блокчејн обезбеђује видљивост робе од почетка до краја, омогућавајући заинтересованим странама да прате производе од порекла до одредишта, чиме се обезбеђује аутентичност производа и усклађеност са регулаторним стандардима. Ове различите апликације наглашавају потенцијал блокчејна да не само поједностави операције већ и редефинише механизме поверења у дигиталним екосистемима.

Упркос свом трансформативном потенцијалу, блокчејн технологија није без ограничења и изазова. Скалабилност остаје значајна брига, јер се величина и сложеност главне књиге повећавају са сваком новом трансакцијом. Велика потрошња енергије, посебно у мрежама које користе PoW, и регулаторна несигурност такође представљају препреке за широко усвајање.

Блокчејн технологија представља промену парадигме у начину на који се подаци чувају, верификују и деле. Његова способност да подстакне поверење у децентрализована окружења, елиминише потребу за посредницима и обезбеди транспарентан ревизорски траг позиционирала га је као темељну технологију за следећу генерацију дигиталних инфраструктура. Као такво, разумевање његових техничких основа, потенцијалних апликација и изазова је од суштинског значаја за разумевање ширег утицаја блокчејна на савремене дигиталне и економске системе.

4.1 Основе блокчејна: децентрализација и непроменљивост

Блокчејнови најважнији атрибути — децентрализација и непроменљивост — разликују га од конвенционалних система дигиталних књига и централизованих база података. Да бисмо у потпуности схватили трансформативну природу блокчејна, неопходно је разумети како ови основни принципи подупиру његову архитектуру, функционалност и безбедност. Овај одељак се бави концептуалним основама и техничким компонентама блокчејна које му омогућавају да постигне ова својства, постављајући основу за његову примену у различитим секторима.

4.1.1 Децентрализација: Помак од централизованих система

Децентрализација је у срцу блокчејн технологије, која се односи на дистрибуцију података и контроле преко мреже независних чворова, а не централизованог система. У традиционалним системима, централни ентитет, као што је банка или владина институција, служи као чувар података и спроводи правила. Ова концентрација моћи не само да ствара потенцијалне појединачне тачке квара, већ и чини ове системе подложним корупцији, цурењу података и неовлашћеним изменама. Блокчејн решава ове рањивости

[38] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

[39] Merrell, Ian. "Blockchain for decentralised rural development and governance." *Blockchain: Research and Applications* 3.3 (2022)

ширењем одговорности за одржавање и валидацију књиге међу мрежом учесника, такође познатим као чворови.

Децентрализована природа блокчејна ради кроз пеер-то-пеер („Peer-To-Peer”-П2П) мрежну архитектуру. Сваки чвор у мрежи одржава комплетну копију књиге, а промене у блокчејну се врше кроз процес консензуса. Ово осигурава да ниједан чвор нема овлашћење да једнострано модификује податке, а квар једног или више чворова не утиче на укупан интегритет и доступност књиге. Овај дизајн веома повећава толеранцију на грешке и смањује вероватноћу системских поремећаја, јер мрежа може да настави да ради чак и ако подскуп чворова постане угрожен или неактиван.[40]

Децентрализација такође има импликације на управљање и доношење одлука унутар блокчејн екосистема. Различите блокчејн мреже примењују различите нивое децентрализације у зависности од њихових механизама консензуса и структура управљања. Јавни блокчејни, као што су Биткоин и Етереум (Bitcoin, Ethereum), сматрају се потпуно децентрализованим, јер свако може учествовати у мрежи и допринети процесу консензуса. Насупрот томе, дозвољени блокчејни, као што је Хиперледжер Фабрик (Hyperledger fabric), одржавају полудецентрализован модел, где само одобрени учесници могу да потврђују трансакције.[41] Ове разлике наглашавају флексибилност блокчејн технологије за подршку широком спектру случајева употребе, од отворених окружења без поверења до више контролисаних апликација оријентисаних на предузећа.[42]

4.1.2. Непроменљивост: Обезбеђивање интегритета података и поверења

Непроменљивост се односи на способност блокчејн књиге да се одупре неовлашћеним променама или брисањем снимљених података. Ово својство се постиже комбинацијом криптографског хеширања и структурног дизајна самог блокчејна. Сваки блок у ланцу блокова садржи јединствени криптографски хеш који се генерише на основу садржаја блока, укључујући податке о трансакцији, временску ознаку и хеш претходног блока. Сваки покушај измене података у једном блоку би променио његову хеш вредност, чиме би се прекинуле везе ланца и учинио цео ланац неважећим[43].

Принцип непромењивости служи као моћан алат за обезбеђивање интегритета података и поверења у окружењима у којима више страна има интеракцију. У традиционалним базама података, уносе могу модификовати администратори базе података или злонамерни актери, што доводи до потенцијалних проблема са аутентичношћу података. Насупрот томе, непромењивост блокчејна значи да када се трансакција сними и потврди од стране мреже, она постаје стални део историје књиге. Ово је посебно драгоцено у контекстима као што су финансијске услуге, управљање ланцем снабдевања и здравствена заштита, где је вођење евиденције која се може проверити и не мењати кључно.

Међутим, непроменљивост није апсолутна, технички је могуће, иако веома непрактично и скупо, изменити историјске податке кроз оно што је познато као напад од

[40] Tasatanattakool, Pinyaphat, and Chian Techapanupreeda. "Blockchain: Challenges and applications." In *2018 international conference on information networking (ICOIN)*, pp. 473-475. IEEE, 2018.

[41] Hyperledger Foundation. “Hyperledger Fabric.” *Lfdecentralizedtrust.org*, The Linux Foundation, 31 July 2023, www.lfdecentralizedtrust.org/projects/fabric. Accessed 12 Sept. 2024.

[42] Beck, Roman, Christoph Müller-Bloch, and John Leslie King. "Governance in the blockchain economy: A framework and research agenda." *Journal of the association for information systems* 19.10 (2018): 1.

[43] Hofmann, Frank, Simone Wurster, Eyal Ron, and Moritz Böhmecke-Schwafert. "The immutability concept of blockchains and benefits of early standardization." In *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, pp. 1-8. IEEE, 2017.

51%. У јавним блокчејновима, ако злонамерни актер добије контролу над више од 50% рачунарске снаге или удела мреже, он би теоретски могао да препише делове књиге тако што ће поништити трансакције или искључити нове. Иако су такви напади ретки и захтевају огромне ресурсе, они наглашавају важност одржавања добро дистрибуиране мреже са робусним механизмима консензуса како би се очувала непромењивост блокчејна.

4.1.3. Механизми консензуса: постизање споразума у децентрализованој мрежи

Да би се постигла децентрализација и непромењивост, мреже блокова користе механизме консензуса који омогућавају дистрибуираним учесницима да се договоре о валидности трансакција и стању књиге. Два најшире коришћена консензус алгоритма су **Proof of Work (PoW)** и **Proof of Stake (PoS)**, сваки са одређеним предностима и компромисима.

Proof of Work (PoW) – доказ о раду: Користе га Биткоин и многе друге криптовалуте, PoW захтева чворове (рударе) за решавање сложених криптографских загонетки како би додали нове блокове у ланац. Овај процес је рачунарски интензиван и троши пуно електричне енергије, али осигурава да је измена главне књиге економски неизводљива. Сигурност PoW-а је укорењена у чињеници да би сваки покушај да се манипулише блокчејн-ом захтевао поновно рударење неовлашћеног блока и свих наредних блокова, што захтева претерано високу количину рачунарске снаге.[44]

Proof of Stake (PoS) – доказ о улогу: PoS, који су усвојиле новије блокчејн мреже као што је Етереум 2.0, додељује права валидације блока на основу количине криптовалуте коју учесник држи и спреман је да „уложи“ као колатерал. За разлику од PoW-а, који се ослања на рачунарску снагу, PoS подстиче поштено понашање тако што тера непоштене валидаторе да одузму своје уложене токене. Овај механизам значајно смањује потрошњу енергије и побољшава скалабилност, чинећи PoS одрживијом алтернативом за будуће имплементације блочејна.[45]

4.1.4. Улога криптографије у осигурању сигурности блокчејна

Криптографија је фундаментална за одржавање безбедности блокчејн мреже. Крипографија са јавним кључем, посебно, подупире аутентификацију и интегритет трансакција. Сваком учеснику у блокчејн мрежи је додељен пар јавних и приватних кључева. Приватни кључ се чува као поверљив и користи се за потписивање трансакција, док се јавни кључ дели отворено и служи као адреса примаоца. Овај криптографски потпис обезбеђује да само власник приватног кључа може да покрене трансакције са дате адресе, док свако у мрежи може да провери аутентичност трансакције користећи придружени јавни кључ.[46]

Поред тога, криптографске хеш функције играју кључну улогу у обезбеђивању непроменљивости и интегритета података. Хеш функције узимају улаз (нпр. податке о трансакцији) и генеришу излаз фиксне величине (хеш), који делује као дигитални отисак прста улаза. Чак и мања промена у уносу резултира драстично различитом хеш вредношћу, што олакшава откривање било каквог неовлашћеног приступа. Ова

[44] Lepore, Cristian, Michela Ceria, Andrea Visconti, Udai Pratap Rao, Kaushal Arvindbhai Shah, and Luca Zanolini. "A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS." *Mathematics* 8, no. 10 (2020)

[45] ibid.

[46] ibid.

криптографска карактеристика се користи у креирању хешова блокова, повезивању блокова заједно и верификацији интегритета целог блокчејна[47].

Основни принципи децентрализације и непроменљивости чине блокчејн јединственом и моћном технологијом за креирање безбедних и транспарентних дигиталних екосистема. Дистрибуцијом контроле преко мреже и осигуравањем да се подаци не могу мењати без консензуса, блокчејн нуди робустан оквир за широк спектар апликација где су интегритет, транспарентност и отпорност на манипулацију најважнији.

4.2. Употреба блокчејна у различитим индустријама

Блокчејн технологија, првобитно развијена да подржи трансакције криптовалута, постепено се проширила на бројне индустрије, трансформишући традиционалне системе и процесе повећањем транспарентности, сигурности и ефикасности. Његова јединствена својства — децентрализација, непромењивост и следљивост — чине блокчејн свестраним решењем за решавање различитих изазова у секторима као што су финансије, ланац снабдевања, здравство, јавна управа и шире.

4.2.1. Финансијске услуге: Револуција у плаћањима и трансакцијама

Сектор финансијских услуга је био први који је препознао потенцијал блокчејна, користећи га за поједностављење прекограничних плаћања, побољшање безбедности и увођење нових финансијских инструмената. Традиционални банкарски системи се ослањају на посреднике за прекограничне трансакције, што резултира високим накнадама, дугим временима обраде и потенцијалним грешкама. Блокчејн решава ове проблеме тако што омогућава једноставне трансфере дигиталне имовине, смањујући ослањање на треће стране и осигуравајући скоро тренутно извршење трансакција.

Прекогранична плаћања - Једна од најзначајнијих употреба блокчејна је у прекограничним плаћањима, где блокчејн значајно смањује трошкове трансакције и време обраде. Платформе као што су Рипл (Ripple) и Стелар (Stellar) користе блокчејн да би олакшале скоро тренутне трансфере између различитих валута, заобилазећи традиционалну СВИФТ (SWIFT) мрежу. На пример, Рипл технологија омогућава финансијским институцијама да обрађују међународна плаћања у року од неколико секунди, за разлику од дана, чиме се повећава ликвидност и оперативна ефикасност.[48]

Паметни уговори за финансијске услуге - Поред плаћања, блокчејн омогућава креирање паметних уговора који се самостално извршавају, који аутоматизују примену уговора на основу унапред дефинисаних услова[49]. Ови уговори се широко користе у трговању дериватима, осигурању и исплати кредита.

Токенизација имовине - Токенизација имовине, као што су некретнине, акције и роба, је још једна велика иновација коју покреће блокчејн. Представљањем физичке имовине као дигиталних токена на блокчејну, инвеститори могу да тргују деловима имовине високе вредности, побољшавајући ликвидност и доступност. Овај приступ је посебно повољан за традиционално неликвидна тржишта, јер омогућава делимично

[47] Lepore, Cristian, Michela Ceria, Andrea Visconti, Udai Pratap Rao, Kaushal Arvindbhai Shah, and Luca Zanolini. "A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS." *Mathematics* 8, no. 10 (2020)

[48] Ripple. “Cross-Border Payment Settlement Solution | Ripple.” *Ripple.com*, ripple.com/solutions/cross-border-payments/. Преузето 30 Oct. 2024.

[49] Khan, Shafaq Naheed, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. "Blockchain smart contracts: Applications, challenges, and future trends." *Peer-to-peer Networking and Applications* 14 (2021)

власништво, повећава ефикасност тржишта и смањује баријере за улазак за мање инвеститоре.[50]

4.2.2. Управљање ланцем снабдевања: побољшање транспарентности и праћења робе

Управљање ланцем снабдевања је сложено, укључује више заинтересованих страна, логистику и регулаторне захтеве. Способност блокчејна да обезбеди транспарентну евиденцију сваке трансакције у ланцу снабдевања која је заштићена од неовлашћеног приступа решава кључне проблеме, као што су недостатак видљивости, фалсификовање и неефикасност у праћењу робе.

Порекло и праћење производа - Једна од примарних примена блокчејна у управљању ланцем снабдевања је порекло производа, које обезбеђује да се роба може пратити до њеног порекла, обезбеђујући непрекинути ланац надзора. Ово је кључно за индустрије попут производње хране и фармацеутских производа, где је порекло директно повезано са безбедношћу и усклађеношћу са прописима. На пример, блокчејн ИБМ-овог Фуд Траст-а (IBM Food Trust) омогућава компанијама да прате пут прехрамбених производа од фарме до стола, побољшавајући безбедност хране и минимизирајући утицај повлачења робе[51].

Борба против фалсификовања - Фалсификовање је значајан проблем у индустријама као што су луксузна роба, електроника и фармацеутски производи. Блокчејн се може користити за креирање дигиталног близанца физичког производа, са сваким преносом или модификацијом снимљеним на блокчејну. Ово ствара непроменљиву историју производа, омогућавајући потрошачима и предузећима да провере аутентичност робе у свакој фази ланца снабдевања. ВиЧејн (VeChain), на пример, користи верификацију производа засновану на блокчејну да заштити врхунске производе од фалсификовања обезбеђујући јединствене идентификаторе који се могу скенирати да би се приступило целокупној историји животног циклуса производа.[52]

Рационализација логистике и смањење трошкова - Блокчејн такође оптимизује логистику аутоматизацијом различитих аспеката ланца снабдевања, као што су управљање залихама, обрада поруџбина и документација. Паметни уговори могу покренути аутоматизоване радње када се испуне унапред дефинисани услови, као што је аутоматско ослобађање плаћања када пошиљка стигне на одредиште. Ово смањује административне трошкове, убрзава процесе и минимизира потенцијал за људске грешке.

4.2.3. Здравство: Обезбеђивање података о пацијентима и обезбеђивање интегритета података

Сектор здравствене заштите суочава се са значајним изазовима у управљању и обезбеђивању осетљивих података о пацијентима, придржавању строгих регулаторних захтева и обезбеђивању интероперабилности података међу различитим пружаоцима

[50] Team, Chainalysis. "Asset Tokenization Explained." *Chainalysis*, 22 Mar. 2024, www.chainalysis.com/blog/asset-tokenization-explained/. Преузето 9 Oct. 2024.

[51] IBM. "IBM Supply Chain Intelligence Suite - Food Trust." *Www.ibm.com*, 2023, www.ibm.com/products/supply-chain-intelligence-suite/food-trust. Преузето 28 Oct. 2024.

[52] Gathecha, James M. "Transforming Industries: VeChain's Impact on Luxury, Food Safety, and Sustainability." *Crypto News Flash*, 4 July 2024, www.crypto-news-flash.com/vechains-impact-on-luxury-food-safety-and-sustainability/. Преузето 28 Oct. 2024.

здравствених услуга. Блокчејн пружа робусно решење омогућавајући безбедно, интероперабилно управљање здравственим информацијама усмерено на пацијента.

Електронски здравствени картони - Блокчејн омогућава креирање безбедних и интероперабилних Електронских Здравствених Записа (ЕЗЗ), омогућавајући пацијентима да контролишу приступ својим медицинским подацима. Коришћењем ЕЗЗ система заснованог на блокчејну, здравствени радници могу безбедно и ефикасно да деле информације о пацијентима, смањујући потребу за понављајућим тестовима и побољшавајући координацију неге пацијената. Пројекти као што је МедРец (MedRec) користе блокчејн за креирање децентрализованих здравствених записа који су доступни само уз пристанак пацијената, осигуравајући приватност и усклађеност са прописима о заштити података као што је ХИПАА (HIPAA).[53]

Клиничка испитивања и истраживања - Блокчејн такође може побољшати транспарентност и интегритет клиничких испитивања и истраживачких података. Снимањем свих истраживачких података и споразума о сагласности на блокчејну, заинтересоване стране могу осигурати да подаци остану неизмењени, чиме се повећава поверење у клиничке исходе. Штавише, пристанком пацијената за учешће у истраживању може се управљати путем паметних уговора, осигуравајући усклађеност и етичко управљање подацима о пацијентима..

4.2.4. Јавна управа: Јачање транспарентности и смањење корупције

Јавна управа је спремна за усвајање блокчејна због потенцијала технологије да побољша транспарентност, смањи бирократску неефикасност и бори се против корупције. Државни субјекти све више истражују блокчејн за коришћење у гласању, земљишним књигама и дигиталним идентитетима.

Системи гласања - Блокчејн-ова способност да креира непроменљиве записе чини га идеалним за сигурне и транспарентне системе гласања. Гласање засновано на блокчејну може смањити ризик од преваре бирача, повећати доступност и омогућити пребројавање гласова у реалном времену.

Естонија је већ имплементирала систем електронског гласања заснован на блокчејну који омогућава грађанима да дају своје гласове безбедно и проверљиво са било ког места у свету.[54]

Земљишне књиге - Употреба блокчејна за земљишне књиге и управљање имовином обезбеђује непроменљивост имовинских записа, смањујући спорове и спречавајући лажне трансакције са земљиштем. У земљама са историјом непоузданих земљишних записа, блокчејн може да обезбеди јединствен извор за власништво и имовинска права. Пројекти као што је иницијатива за блокчејн Шведског земљишног регистра имају за циљ да елиминишу документе на папиру и смање време трансакција са месеци на дане.[55]

Управљање дигиталним идентитетом - Дигитални идентитет је критична област у којој блокчејн може да обезбеди сигурне идентитете које контролишу појединци, а не централизоване власти. Са системима идентитета заснованим на блокчејну, појединци могу да управљају и деле своје акредитиве са различитим провајдерима услуга без

[53] Ekblaw, Ariel. "MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis." *MIT Media Lab*, 2017, www.media.mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis/. Преузето 29 Oct. 2024.

[54] e-Estonia. "E-Democracy & Open Data." *E-Estonia*, e-estonia.com/solutions/e-governance/e-democracy/. Преузето 30 Oct. 2024.

[55] Proskurovska, Anetta, and Sabine Dörry. "The Blockchain Challenge for Sweden's Housing and Mortgage Markets." *Environment and Planning A: Economy and Space*, Aug. 2022, p. 0308518X2211168, https://doi.org/10.1177/0308518x221116896. Преузето 30 Oct. 2024.

угрожавања приватности. Концепт децентрализованог идентитета добија на снази иницијативама попут Микрософт-овог ИОН-а (Microsoft ION), који користи Биткоин блокчејн за креирање мреже за децентрализоване идентификаторе.[56]

V. СУКОБИ ИЗМЕЂУ БЛОКЧЕЈНА И ГДПР-А

Брзи напредак и усвајање блокчејн технологије донели су значајну правну и регулаторну контролу, посебно у контексту закона о заштити података. Као децентрализовани, систем дистрибуиране књиге, блокчејн се разликује по својој транспарентности, непроменљивости и безбедности – атрибутима који представљају нове могућности за индустрије у распону од финансија и управљања ланцем снабдевања до здравствене заштите и јавне управе. Међутим, ови исти атрибути представљају значајне изазове када се примењују у оквиру Опште уредбе о заштити података (ГДПР), камена темељца режима заштите података Европске уније.

ГДПР, који је ступио на снагу 25. маја 2018. године, један је од најстрожих закона о заштити података на глобалном нивоу, који поставља свеобухватан регулаторни оквир који има за циљ заштиту личних података и заштиту права на приватност појединаца. Увео је неколико кључних принципа, укључујући минимизирање података, ограничење сврхе и права субјеката података, као што су право на приступ, исправку и, што је критично, право на брисање (које се често назива „право на заборав“). Ови принципи успостављају динамичан и флексибилан приступ управљању подацима, осигуравајући да организације могу да рукују личним подацима на начин који поштује аутономију и преференције појединаца. [57]

Међутим, суштинска природа блокчејн технологије је у супротности са многим од ових ГДПР захтева. Већина блокчејна је дизајнирана да буде непроменљива, што значи да када се подаци забележе на блокчејну, не могу се мењати или брисати. Ова непроменљивост је и снага и ограничење. Осигурава интегритет и следљивост записа, чинећи технологију идеалном за апликације као што су финансијске трансакције, правни уговори и праћење ланца снабдевања. Ипак, ова иста карактеристика чини скоро немогућим прилагођавање ГДПР-а „праву на заборав“ и принципу минимизације података, где подаци не би требало да се чувају дуже него што је потребно за њихову намену. Другим речима, непромењивост блокчејн података је у супротности са захтевом ГДПР-а за флексибилно и реверзибилно управљање подацима.

Децентрализована природа блокчејна компликује примену ГДПР механизама одговорности и управљања. У традиционалним, централизованим системима, постоји јасно дефинисан „контролор података“ или „обрађивач података“ који је одговоран за поштовање прописа и осигурање права субјеката података. Блокчејн, насупрот томе, расподељује одговорности за управљање подацима на бројне чворове у мрежи, што отежава утврђивање који ентитет (или ентитети) сноси законску одговорност за обезбеђивање усклађености. Ова фрагментација одговорности поставља дубока питања о томе како се традиционалне правне конструкције примењују у контексту блокчејн

[56] Dingle, Pamela. “ION – We Have Liftoff!” *MICROSOFT.COM*, 25 Mar. 2021, techcommunity.microsoft.com/blog/microsoftsecurityandcompliance/ion-%E2%80%93-we-have-liftoff/1441555. Преузето 31 Oct. 2024.

[57] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

технологије, посебно у јавним блокчејнима без дозволе где учесници могу бити анонимни или псеудонимни.[58]

ГДПР такође захтева да субјекти података буду обавештени о томе како се њихови лични подаци обрађују и деле, и намеће ограничења на прекогранични пренос личних података. Са блокчејном, реплицирана и дистрибуирана природа књиге значи да се једна трансакција може ускладиштити на чворовима у више јурисдикција, од којих је свака регулисана различитим правним стандардима. Ово ствара значајне компликације за одређивање важећих закона о заштити података и обезбеђивање усклађености са строгим правилима о прекограничном преносу података ГДПР-а.[59]

Још једна фундаментална тачка спора је третман личних података на блокчејн мрежама. Према ГДПР-у, лични подаци су широко дефинисани тако да укључују све информације које се односе на идентификовано физичко лице или физичко лице које се може идентификовати. Ово укључује не само директне идентификаторе као што су имена и адресе, већ и индиректне идентификаторе као што су историја трансакција или дигитални потписи. На блокчејновима, чак и ако су подаци псеудонимизовани – као што су повезани са хешираном адресом или криптографским кључем – они се и даље могу сматрати личним подацима према ГДПР-у ако се подаци могу повезати назад са појединцем, било директно или комбиновањем са другим информацијама. Ово тумачење значи да би многи облици података који се чувају на блокчејну могли бити подвргнути читавом скупу ГДПР захтева, доводећи у питање перцепцију да блокчејни могу постићи усклађеност само путем псеудонимизације.

За навигацију у овим конфликтима, предложене су различите техничке и правне стратегије, као што је употреба складиштења ван ланца (Off-Chain), хибридне архитектуре и напредне криптографске технике као што су Докази са нултим знањем (Zero Knowledge Proofs).[60] Иако ова решења обећавају, често долазе са компромисима у погледу сложености, цене и употребљивости. Темпо технолошких иновација у блокчејну наставља да надмашује развој регулаторних оквира, што доводи до фрагментираног и неизвесног правног пејзажа.

Интеракција између ГДПР-а и блокчејна симбол је шире тензије између иновација и регулативе у дигиталном добу. Како блокчејн технологија сазрева и постаје све више интегрисана у критичне инфраструктуре, потреба за целовитим приступом који усклађује њена техничка својства са правним мандатима заштите података постаје све хитнија. Постизање ове равнотеже ће захтевати стални дијалог и сарадњу између технолога, регулатора и правника како би се развила решења која чувају предности блокчејна, истовремено подржавајући основна права појединаца према ГДПР-у.

5.1. Непроменљивост наспрам права на заборав

Једно од најспорнијих питања на раскрсници технологије блокчејна и ГДПР-а је сукоб између непроменљивости блокчејна и „права на заборав“ ГДПР-а, формално познатог као право на брисање. Члан 17 ГДПР-а даје појединцима право да затраже брисање личних података под одређеним условима, као што су када подаци више нису потребни за њихову првобитну сврху, када је сагласност повучена или када су подаци незаконито обрађени. Ово право је изграђено на основном принципу да појединци треба

[58] Politou, Eugenia, Efthimios Alepis, Maria Virvou, and Constantinos Patsakis. *Privacy and data protection challenges in the distributed era*. Vol. 26. Heidelberg, Germany: Springer, 2022.

[59] ibid.

[60] Sun, Xiaoqiang, F. Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. "A survey on zero-knowledge proof in blockchain." *IEEE network* 35, no. 4 (2021)

да имају контролу над својим личним подацима и могућност да елиминишу свој дигитални отисак када је то потребно.[61] Насупрот томе, принцип непромењивости блокчејна, који обезбеђује да када се подаци забележе, не могу да се мењају или бришу, је камен темељац технологије која подупире њену веродостојност, сигурност и транспарентност. Овај сукоб између правне и технолошке парадигме покреће сложена питања која сежу даље од пуке усклађености, дотичући се филозофске основе управљања подацима и дигиталних права.

5.1.1. Разумевање некомпатибилности: ГДПР права субјекта података у односу на Блокчејн архитектуру

Право на заборав је само једно од неколико права носилаца података садржаних у ГДПР-у. Остала права укључују право на исправку, право на ограничење обраде и право на приговор на одређене врсте коришћења података.[62] Сва ова права су заснована на принципу да лични подаци треба да буду динамични, зависни од контекста и подложни промени или уклањању у складу са преференцијама појединца. Из правне перспективе, ГДПР предвиђа податке као нешто чиме се може управљати и контролисати како би одражавало еволуирајуће околности у животу појединца. На пример, особа која је променила каријеру можда жели да се застареле професионалне информације уклоне са дигиталних платформи, или корисник који је једном делио личне податке у замену за услугу може касније одлучити да повуче те податке ако више не жели да се бави тим услуга.[63]

Насупрот томе, архитектонски дизајн блокчејна третира податке као статичан, непроменљив ентитет. Подаци снимљени на блокчејну се трајно додају на начин који има за циљ да створи непроменљив историјски запис. Ова непромењивост се постиже низом међусобно зависних блокова, од којих сваки садржи криптографски хеш који упућује на претходни блок, стварајући ланац трансакција који је рачунарски неизводљиво мењати ретроактивно без консензуса мреже. Ова структура је критична за осигурање сигурности и интегритета књиге, јер би се чак и мање промене у једном блоку ширile кроз цео ланац, поништавајући све наредне блокове. Дакле, појам „брисања“ или „модификовања“ података у оквиру блокчејн оквира није само у супротности са његовом основном функционалношћу, већ би такође могао да угрози интегритет и стабилност целог система.[64]

Ова тензија је посебно изражена у јавним блокчејнима, где нема централног органа или одређеног контролора података који је одговоран за управљање подацима. У овим децентрализованим мрежама, било какве промене би захтевале консензус већине међу свим чворовима, ситуацију коју је практично немогуће постићи. Чак и у приватним или одобреним блокчејновима, где конзорцијум учесника контролише мрежу, примена таквих промена би била у супротности са примарном сврхом коришћења блокчејна за одржавање транспарентне књиге која је отпорна на неовлашћено коришћење. Сходно томе, када се лични подаци забележе на блокчејн, они постају „закључани“ у књизи, што доводи у питање захтеве ГДПР-а за реверзибилно управљање подацима.

[61] Wolford, Ben. “Everything You Need to Know about the ‘Right to Be Forgotten.’” *GDPR.eu*, 5 Nov. 2018, gdpr.eu/right-to-be-forgotten/. Преузето 24 Oct. 2024.

[62] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

[63] ibid

[64] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

5.1.2. Врсте података и њихове импликације

Друга димензија овог сукоба укључује категоризацију података у блокчејну и њихову квалификацију као личних података према ГДПР-у. Уредба дефинише личне податке широко као „сваку информацију која се односи на идентификовано или физичко лице које се може идентификовати“. Ова дефиниција обухвата широк спектар идентификатора, укључујући не само експлицитне идентификаторе као што су имена и адресе е-поште, већ и друге идентификаторе као што су ИП адресе, подаци о понашању или чак јединствени хешови трансакција, ако се они могу повезати са одређеном особом.

На блокчејн мрежама, подаци се често чувају у облицима који на први поглед не изгледају као лични. На пример, типична блокчејн трансакција може да садржи само јавни кључ (псеудонимизовани идентификатор), временску ознаку и детаље саме трансакције. Међутим, због транспарентне природе многих блокова, где су све трансакције јавно доступне и следљиве, чак и псеудонимизовани подаци се често могу деанонимизовати помоћу техника као што су напад повезивањем, анализа шаблона или повезивањем са другим изворима података. На пример, студије су показале да је, упркос псеудонимној природи Биткоин адреса, могуће повезати ове адресе са идентитетима у стварном свету анализом образаца трансакција и коришћењем спољних тачака података као што су ИП адресе или записи размене.[65]

Ово поставља питање: ако се чак и наизглед анонимни или хеширани подаци могу повезати са појединцем, да ли цео блокчејн потпада под делокруг ГДПР-а? Ако је тако, сваки чвор и учесник у мрежи потенцијално би се могли сматрати контролором или обрађивачем података, који је одговоран за очување права субјекта података, укључујући право на брисање. Ово тумачење би наметнуло неодржив терет усклађености блокчејн системима, потенцијално гушивши иновације и негирајући предности децентрализације.

5.1.3. Потенцијални сукоби: Трајност података и правне обавезе

Још један изазов у помирењу права на заборав са непроменљивошћу блокчејна је потенцијални сукоб између различитих законских обавеза. Сам ГДПР није једини правни оквир који утиче на задржавање и обраду личних података. У многим случајевима, од организација се тражи да задрже одређене врсте података ради усклађивања са прописима, као што су финансијске евиденције за сврхе борбе против прања новца (AML) или подаци о клијентима за потребе познавања свог клијента (KYC). Ове обавезе често захтевају вођење евиденције за одређене периоде, што може бити у супротности са захтевом појединца да се њихови подаци избришу према ГДПР-у.

Непроменљивост блокчејна додатно компликује ове сценарије. Када се лични подаци унесу у блокчејн, они постају део трајног записа који се не може селективно мењати или уклањати. Ово ствара ситуацију у којој усаглашеност са једним скупом законских захтева (нпр. ГДПР) може довести до неусаглашености са другим скупом захтева (нпр. финансијским прописима). На пример, брисање трансакције која садржи личне податке на блокчејну може да поништи ревизијски траг, потенцијално поткопавајући могућност да се демонстрира усклађеност са AML или KYC обавезама.[66]

Сукоб између непроменљивости и брисања података није ограничен само на техничку изводљивост, већ се дотиче и ширих етичких и филозофских разматрања о

[65] Khalilov, Merve Can Kus, and Albert Levi. "A survey on anonymity and privacy in bitcoin-like digital cash systems." *IEEE Communications Surveys & Tutorials* 20.3 (2018): 2543-2585.

[66] Politou, Eugenia, Francisco Casino, Efthymios Alepis, and Constantinos Patsakis. 2019. “Blockchain Mutability: Challenges and Proposed Solutions.” *IEEE Transactions on Emerging Topics in Computing* 9 (4). https://doi.org/10.1109/tetc.2019.2949510

природи трајности података. Док је право на заборав укорењено у концепту личне аутономије и способности да се контролише нечији дигитални отисак, непроменљивост блокчејна је укорењена у принципу стварања транспарентног и поузданог историјског записа. Ови принципи служе различитим друштвеним сврхама – један даје приоритет индивидуалним правима и приватности, док други даје приоритет колективној безбедности и одговорности. Успостављање равнотеже између ових конкурентских вредности није само питање развоја нових техничких алата, већ и поновног промишљања темељних претпоставки дигиталног управљања у ери децентрализованих технологија.[67]

5.1.4. Управљање мрежом и одговорност

Структура управљања блокчејн мрежама додатно компликује спровођење права на заборав. У централизованим системима, јасно дефинисани контролор или обрађивач података може доносити одлуке у вези са брисањем или исправљањем података и сносити одговорност за усклађеност. Блокчејн, међутим, функционише као децентрализована мрежа у којој се подаци дистрибуирају преко бројних чворова, од којих се сваки може налазити у различитим јурисдикцијама. Ова децентрализација поставља питања о томе ко има овлашћења да доноси одлуке у вези са управљањем подацима и ко је одговоран у случају непоштовања.

На пример, у јавном блокчејну као што је Етереум, не постоји ниједан ентитет који контролише мрежу. Сваки покушај модификације података захтевао би "хард форк" (Hard Fork) — фундаменталну промену блокчејн протокола са којом би требало да се сложи већина учесника мреже. Овај процес није само технички сложен, већ је препун политичких и друштвених изазова, што се показало након хаковања Етереума 2016. године, што је довело до контроверзног хард форка који је мрежу поделио на два ланца: Етереум (ETH) и Етереум Класик (ETC).[68]

Недостатак јасних механизама одговорности у децентрализованим мрежама отежава спровођење ГДПР захтева, јер не постоји јединствена контролна тачка која се може сматрати одговорном. Ова фрагментација овлашћења је у потпуној супротности са очекивањима ГДПР-а о јасно идентификованом контролору или обрађивачу података који је одговоран за осигурање усклађености и поштовање права носилаца података. Овај јаз у управљању је једна од кључних препрека за постизање усклађености са ГДПР-ом у блокчејн екосистемима и наглашава потребу за поновним размишљањем о томе како се одговорност дефинише у децентрализованим системима.

5.2. Ограничења складиштења и преносивости података

Децентрализована и дистрибуирана природа блокчејн технологије поставља јединствене изазове у вези са складиштењем података и преносивости личних информација, посебно у светлу принципа и захтева ГДПР-а. У суштини, ГДПР налаже да лични подаци треба да се чувају на начин који обезбеђује сигурност, поверљивост и лакоћу управљања, уз поштовање принципа минимизације података и ограничења сврхе. Ови захтеви су додатно компликовани фундаменталном структуром блокчејна, где се

[67] Politou, Eugenia, Francisco Casino, Efthymios Alepis, and Constantinos Patsakis. 2019. "Blockchain Mutability: Challenges and Proposed Solutions." *IEEE Transactions on Emerging Topics in Computing* 9 (4). https://doi.org/10.1109/tetc.2019.2949510

[68] Frankenfield, Jake. "Ethereum Classic." *Investopedia*, www.investopedia.com/terms/e/ethereum-classic.asp. Преузето 5 Nov. 2024.

подаци реплицирају кроз мрежу чворова, од којих сваки чува идентичну копију блокчејн књиге.

5.2.1. Проблем дистрибуираног складиштења података

Принцип минимизације података према ГДПР-у захтева да организације прикупљају и чувају само минималну количину личних података неопходну за одређену сврху. Слично, принцип ограничења складиштења налаже да се лични подаци чувају у облику који дозвољава идентификацију субјеката података не дуже него што је потребно за сврхе за које се подаци обрађују.[69] Међутим, блокчејн технологија је по дизајну у супротности са овим принципима.

У блокчејн мрежама, сваки чвор задржава комплетну копију блокчејна, која садржи све податке о трансакцијама које су икада забележене у књизи. Ова репликација је фундаментална за безбедност и отпорност блокчејн технологије, обезбеђујући да систем може да настави да функционише чак и ако значајан број чворова оде ван мреже или постане угрожен. У типичној јавној блокчејн мрежи, хиљаде чворова могу постојати у различитим јурисдикцијама, од којих сваки чува идентичан скуп података који стално расте.[70] Као резултат тога, чак и ако се лични подаци користе само у једној трансакцији, они се ефективно дуплирају у свим чворовима у мрежи и чувају на неограничено време, потенцијално кршећи захтеве за ограничење складиштења ГДПР-а.

Проблем прекомерног задржавања података је погоршан чињеницом да податке ускладиштене на блокчејну није лако избрисати или модификовати. У традиционалним базама података, централизовани администратор може обрисати записе или применити правила задржавања података како би осигурао усклађеност са законским захтевима. У блокчејн системима, међутим, подаци се трајно бележе у књизи, па чак и након што трансакција више није релевантна или неопходна, запис остаје у ланцу, настављајући да се шири кроз све чворове који учествују. Ово неограничено задржавање је директно у супротности са очекивањима ГДПР-а да би подаци требало да буду избрисани или анонимизовани када више не буду потребни за првобитну сврху.

5.2.2. Реплицирање података кроз различите јурисдикције

Једна од кључних карактеристика блокчејн технологије је њена дистрибуирана природа, где су чворови често распоређени у више земаља и јурисдикција. Овај прекогранични ток података представља значајан изазов за усклађеност према строгим правилима ГДПР-а у вези са међународним преносом података. Према ГДПР-у, лични подаци се могу пренети ван Европског економског простора (ЕЕП) само ако су испуњени одређени услови, као што је постојање одлуке о адекватности, обавезујућа корпоративна правила или посебна одступања за одређене ситуације.[71] Ови захтеви су дизајнирани да обезбеде да се исти ниво заштите података који се пружа унутар ЕУ одржава када се подаци преносе у треће земље.

[69] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

[70] Uzougbo, Ngozi Samuel, Chinonso Gladys Ikegwu, and Adefolake Olachi Adewusi. "International enforcement of cryptocurrency laws: jurisdictional challenges and collaborative solutions." *Magna Scientia Advanced Research and Reviews* 11.1 (2024): 068-083.

[71] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

Међутим, у јавним блокчејн мрежама, локација чворова је често непозната и стално се мења како се чворови придружују и напуштају мрежу. Овај недостатак контроле над преносом података ствара ситуацију у којој се лични подаци могу чувати и обрађивати у земљама које не пружају адекватну заштиту података према ГДПР-у, као што су Сједињене Државе, Русија или Кина.[72] Пошто се подаци реплицирају у свим чворовима, чак и ако се само мали проценат чворова налази изван ЕУ, може се сматрати да цео блокчејн укључује међународне преносе података, што захтева усклађеност са одредбама ГДПР-а о прекограничном преносу.

Ово питање је додатно компликовано чињеницом да блокчејнови често немају централизовани ентитет који је одговоран за надгледање усклађености.[73] Без јасно одређеног контролора података или обрађивача података, постаје тешко осигурати да постоје одговарајуће заштитне мере за прекогранични пренос података. Чак и ако блокчејн мрежа спроводи одређене мере усклађености, као што је шифровање личних података пре него што их ускладишти у ланцу, то не елиминише захтев да се адресира правни статус самог преноса података. Као резултат тога, блокчејн мреже се често налазе у регулаторно сивој зони, неспособне да у потпуности испуне захтеве ГДПР-а, истовремено задржавајући децентрализовану природу која дефинише технологију.

5.2.3. Сукоб између децентрализованог складиштења и суверенитета података

Још једно критично питање у вези са складиштењем података у блокчејн системима је концепт суверенитета података. Сувереност података односи се на идеју да лични подаци подлежу законима и прописима земље у којој се чувају. ГДПР оличава овај принцип тако што захтева да се подаци грађана ЕУ третирају у складу са стандардима ЕУ, без обзира на то где се чувају или обрађују.[74] Међутим, у контексту блокчејна, подаци се складиште истовремено на више локација у различитим јурисдикцијама, што отежава одређивање који правни режим регулише податке.

Ова дистрибуирана природа складиштења компликује могућност поштовања закона о локализацији података, које све више усвајају јурисдикције широм света. На пример, Уредба о електронској приватности коју је предложила ЕУ укључује одредбе које би захтевале да се одређене врсте података чувају и обрађују унутар граница ЕУ.[75] Слично томе, земље попут Кине и Русије донеле су строге законе о локализацији података који захтевају да се лични подаци прикупљени унутар њихових граница чувају на локалним серверима.[76] Глобална природа блокчејн технологије чини готово немогућим да се осигура да подаци остану унутар одређене јурисдикције, чиме се повећава ризик од неусклађености са прописима и правног сукоба.

На пример, ако блокчејн трансакција укључује личне податке грађанина ЕУ и похрањена је на чвору у јурисдикцији са слабим законима о заштити података, као што

[72] European Commission. "Adequacy Decisions." *Commission.europa.eu*, commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Преузето 2 Nov. 2024.

[73] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

[74] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

[75] European Commission. "EPrivacy Regulation | Shaping Europe's Digital Future." *Digital-Strategy.ec.europa.eu*, digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation. Преузето 2 Nov. 2024.

[76] "Russia Is Weaponizing Its Data Laws against Foreign Organizations." *Brookings*, www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/. Преузето 2 Nov. 2024.

је земља са историјом државног надзора или ограниченим индивидуалним правима на приватност, то би могло условити учеснике мреже на значајне правне обавезе према законима ЕУ. Ова сложеност је отежана чињеницом да су блокчејни фундаментално транспарентни, што значи да када се трансакција евидентира, свако ко има приступ књизи може да је види, без обзира на своју локацију или правни статус.

5.2.4. Изазови преносивости података и интероперабилности

Поред питања складиштења и преноса, ГДПР такође налаже право на преносивост података, омогућавајући субјектима података да примају своје личне податке у структурираном, уобичајено коришћеном и машински читљивом формату и да те податке несметано пренесу другом контролору.[77] Ово право има за циљ да промовише слободан проток личних података и унапреди аутономију потрошача олакшавајући појединцима да прелазе између добављача услуга или преносе своје податке на нове платформе.

Блокчејн, међутим, компликује имплементацију преносивости података на неколико начина. Прво, пошто су блокчејн трансакције непроменљиве и трајно се снимају, није увек могуће издвојити личне податке корисника у облику који се лако може пренети на други систем. Свака трансакција је део већег ланца који упућује на претходне и наредне трансакције, што отежава изоловање одређеног скупа личних података без утицаја на интегритет целог ланца.[78] Штавише, због децентрализоване природе блокчејна, не постоји јединствени контролор података који би олакшао пренос података између платформи.

Још један изазов је недостатак стандардизације и интероперабилности на различитим блокчејн платформама. Док се улажу напори да се створе интероперабилна блокчејн решења, као што су унакрсни протоколи и стандардизовани модели података, већина блокчејна и даље функционише као изоловани екосистеми са сопственим јединственим структурама података и протокола.[79] Овај недостатак интероперабилности значи да чак и када би корисник могао да искористи своје право на преносивост података, не постоји гаранција да би подаци могли бити неприметно пренети на другу блокчејн мрежу или интегрисани са традиционалним централизованим системима. Као резултат тога, фрагментирани пејзаж блокчејна подрива циљ ГДПР-а да омогући лаку и ефикасну преносивост података за субјекте података.

5.3. Псеудонимизација и анонимизација на блокчејну

У контексту Опште уредбе о заштити података (ГДПР), концепти псеудонимизације и анонимизације су кључни за обезбеђивање усклађености приликом обраде личних података. ГДПР дефинише псеудонимизацију као процес који замењује личне идентификаторе вештачким идентификаторима (или псеудонимима) како би се спречила директна идентификација појединаца, док се и даље дозвољава поновна идентификација путем додатних информација које се чувају одвојено.[80] Анонимизација

[77] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

[78] ibid.

[79] Ou, Wei, Shiying Huang, Jingjing Zheng, Qionglu Zhang, Guang Zeng, and Wenbao Han. 2022. "An Overview on Cross-Chain: Mechanism, Platforms, Challenges and Advances." *Computer Networks* 218 (December): 109378. https://doi.org/10.1016/j.comnet.2022.109378.

[80] Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation." *Computer law & security review* 33.2, 2017.

се, с друге стране, односи на неповратну трансформацију личних података тако да се појединац више не може идентификовати, чак ни са додатним скуповима података.[81] Када се правилно имплементирају, анонимни подаци не спадају у опсег ГДПР-а, што их чини пожељним циљем за организације које желе да ублаже ризике усклађености. Међутим, постизање истинске анонимизације у блокчејн окружењима је знатно сложеније него у традиционалним системима, првенствено због транспарентности и непроменљивости технологије.

5.3.1. Псеудонимизација: решење за делимичну усклађеност

Псеудонимизација се широко користи у блокчејн мрежама као средство за побољшање приватности уз одржавање следљивости и транспарентности трансакција. Већина јавних блокчејна, као што су Биткоин и Етереум, користе псеудонимне адресе уместо идентитета из стварног света.[82] Сваки корисник је представљен јединственим јавним кључем (или адресом), који функционише као идентификатор за све трансакције повезане са тим корисником. Иако сама адреса не открива директно идентитет корисника, она је везана за њихове активности на блокчејну, стварајући историју јавних трансакција коју свако може да види.[83]

Псеудонимизација има одређене предности за заштиту приватности. Заменом директних идентификатора (нпр. имена, адресе е-поште) криптографским кључевима, псеудонимизација смањује вероватноћу тренутне идентификације, чиме се обезбеђује одређени ниво приватности за кориснике блокчејна.[84] Међутим, према ГДПР-у, псеудонимизовани подаци се и даље сматрају личним подацима ако се могу поново повезати са појединцем, било путем додатних информација или комбиновањем са другим скуповима података.[85] То значи да иако су блокчејн адресе псеудонимне, оне нису анонимне и стога остају подложне захтевима ГДПР-а, укључујући права и обавезе носилаца података за контролоре података.

Проблем са ослањањем на псеудонимизацију у блокчејн системима је у томе што она не пружа апсолутну заштиту од поновне идентификације. Истраживања су показала да се псеудонимне блокчејн адресе могу повезати са стварним идентитетима кроз различите методе, укључујући анализу графова трансакција, технике груписања и унакрсно референцирање са спољним изворима података као што су ИП адресе или размене где корисници испуњавају процедуре познавања свог клијента (KYC). На пример, иако Биткоин адреса не открива директно идентитет власника, мотивисани истраживач може анализирати обрасце трансакција и повезати их са познатим адресама или активностима ван ланца како би идентификовао корисника.[86]

---

[81] Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation." *Computer law & security review* 33.2, 2017.

[82] Khalilov, Merve Can Kus, and Albert Levi. "A survey on anonymity and privacy in bitcoin-like digital cash systems." *IEEE Communications Surveys & Tutorials* 20.3 (2018): 2543-2585.

[83] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

[84] Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation." *Computer law & security review* 33.2, 2017.

[85] ibid.

[86] Zhang, Yuhang, Jun Wang, and Jie Luo. "Heuristic-Based Address Clustering in Bitcoin." *IEEE Access* 8 (2020): 210582–91. https://doi.org/10.1109/access.2020.3039570.

Штавише, пошто су блокчејн записи трајни и јавно доступни, сви подаци који су данас псеудонимизовани могу потенцијално бити деанонимизовани у будућности како нове технике или скупови података постану доступни. Овај ризик од поновне идентификације представља значајан изазов за усклађеност, јер контролори података морају континуирано да надгледају и процењују да ли се псеудонимизовани подаци и даље могу сматрати безбедним према ГДПР-у. Ако је поновна идентификација могућа, подаци више не би испуњавали стандарде за псеудонимизацију и морали би да се третирају као лични подаци који се могу у потпуности идентификовати, подвргавајући их читавом низу обавеза ГДПР-а.

5.3.2. Анонимизација: изазов постизања потпуне анонимности

Анонимизација, како је дефинисана ГДПР-ом, укључује трансформацију личних података на такав начин да их је немогуће повезати са појединцем, чак и ако су доступне додатне информације. Ако су подаци заиста анонимни, они се више не сматрају личним подацима и не потпадају под опсег ГДПР-а, чиме се елиминише потреба за усклађеношћу са захтевима као што је право на брисање или преносивост података.[87] Међутим, постизање истинске анонимизације у блокчејн системима је изузетно тешко због непроменљиве и транспарентне природе технологије.

Транспарентност блокчејна значи да су све трансакције видљиве сваком учеснику у мрежи. Чак и ако се лични идентификатори уклоне, сами трансакцијски подаци (нпр. временске ознаке, износи, друге уговорне стране) могу пружити довољно информација за закључивање образаца и потенцијалну поновну идентификацију појединаца. Ово је посебно проблематично у случајевима када је историја трансакција дуга и укључује вишеструке интеракције са другим корисницима који се могу идентификовати. На пример, чак и ако је блокчејн адреса анонимизована заменом насумичним идентификатором, низ трансакција повезаних са том адресом и даље може открити јединствене обрасце који, када се комбинују са другим информацијама, могу да идентификују појединца иза адресе.[88]

Концепт к-анонимности, који се обично користи у традиционалним базама података за постизање анонимизације, тешко је применити у блокчејн мрежама јер је књига дизајнирана да буде потпуно транспарентна и следљива. У традиционалним системима, к-анонимност осигурава да се сваки појединац не може разликовати од најмање к-1 других појединаца на основу њихових атрибута.[89] На блокчејну, међутим, транспарентност главне књиге значи да би сваки покушај модификације података да би се постигла к-анонимност био видљив свим учесницима, нарушавајући интегритет књиге.

Други изазов је у томе што, за разлику од традиционалних база података, где се подаци могу трансформисати или брисати да би се постигла анонимност, непроменљивост блокчејна спречава ретроактивну анонимизацију постојећих записа. Једном када је трансакција снимљена на блокчејну, не може се променити или уклонити, што онемогућава истинску анонимност података без подривања непроменљивости

[87] Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation." *Computer law & security review* 33.2, 2017.

[88] Khalilov, Merve Can Kus, and Albert Levi. "A survey on anonymity and privacy in bitcoin-like digital cash systems." *IEEE Communications Surveys & Tutorials* 20.3 2018.

[89] Hameed, Khizar, Mutaz Barika, Saurabh Garg, Muhammad Bilal Amin, and Byeong Kang. "A Taxonomy Study on Securing Blockchain-Based Industrial Applications: An Overview, Application Perspectives, Requirements, Attacks, Countermeasures, and Open Issues." *Journal of Industrial Information Integration* 26 2022.: 100312. https://doi.org/10.1016/j.jii.2021.100312.

ланца. Као резултат тога, чак и софистициране технике анонимизације као што су диференцијална приватност или убризгавање буке, које функционишу додавањем насумичних података у нејасне појединачне записе, тешко је ефикасно применити на блокчејну без угрожавања интегритета и корисности главне књиге.[90]

5.3.3. Правне и техничке импликације псеудонимизације и анонимизације

Правна разлика између псеудонимизације и анонимизације има значајне импликације на усклађеност са ГДПР-ом. Док се псеудонимизовани подаци и даље сматрају личним подацима према ГДПР-у, анонимизовани подаци нису. Стога би постизање истинске анонимности било идеално решење за блокчејн мреже које желе да умање ризике усклађености. Међутим, због техничких ограничења, већина блокчејн мрежа се тренутно ослања на псеудонимизацију, а не на праву анонимизацију.

Употреба псеудонимизације у блокчејн системима уводи неколико правних и оперативних изазова. Прво, од контролора података се тражи да спроведу додатне мере заштите за заштиту псеудонимизованих података, као што је шифровање информација о повезаности које би се могле користити за поновну идентификацију појединаца. Они такође морају осигурати да псеудонимизоване податке не може поново идентификовати ниједна страна, укључујући и њих саме.[91] У децентрализованој мрежи са више учесника, овај захтев је тешко спровести, пошто псеудонимизовани подаци могу бити доступни бројним странама са различитим нивоима техничке софистицираности.

Друго, принцип одговорности ГДПР-а захтева од контролора података да покажу да су предузели одговарајуће мере за заштиту личних података и да су у стању да одговоре на захтеве носилаца података.[92] Ако се псеудонимизовани подаци на блокчејну поново идентификују, контролори података могу бити одговорни за пропуст да заштите податке у складу са захтевима ГДПР-а. Овај ризик је отежан чињеницом да блокчејн мрежама често недостаје централно тело одговорно за надгледање усклађености, због чега није јасно ко треба да буде одговоран у случају повреде података или поновне идентификације.

Из техничке перспективе, примена напредних криптографских техника, као што су докази са нултим знањем или вишестраначко рачунање, нуди извесно обећање за постизање функционалности које побољшавају приватност без угрожавања непроменљивости блокчејна.[93] Ове технике омогућавају верификацију трансакција без откривања основних података, чиме се чува анонимност. Међутим, ови приступи су још увек у експерименталној фази и још увек нису широко прихваћени у већини блокчејн мрежа. Штавише, захтевају значајне рачунарске ресурсе и техничку експертизу, што их чини непрактичним за многе случајеве употребе.

5.3.4. Импликације за будућност усаглашености блокчејна

[90] Ponomareva, Natalia, Hussein Hazimeh, Alexey Kurakin, Zhen-Liang Xu, Carson Denison, McMahan H Brendan, Sergei Vassilvitskii, Steve Chien, and Abhradeep Thakurta. “How to DP-Fy ML: A Practical Guide to Machine Learning with Differential Privacy.” *Journal of Artificial Intelligence Research* 77, 2023.: 1113–1201. https://doi.org/10.1613/jair.1.14649.

[91] Khalilov, Merve Can Kus, and Albert Levi. "A survey on anonymity and privacy in bitcoin-like digital cash systems." *IEEE Communications Surveys & Tutorials* 20.3, 2018.

[92] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

[93] Ishai, Yuval, et al. “Zero-Knowledge Proofs from Secure Multiparty Computation.” *SIAM Journal on Computing*, vol. 39, no. 3, Jan. 2009., https://doi.org/10.1137/080725398. Преузето 5 Nov. 2024.

Ограничења псеудонимизације и анонимизације у блокчејн системима илуструју тешкоће постизања усклађености са ГДПР-ом без суштинске промене природе технологије. Док псеудонимизација пружа привремено и делимично решење, она не елиминише потребу за решавањем основних питања транспарентности и непроменљивости који чине блокчејн некомпатибилним са одређеним принципима ГДПР-а. Постизање праве анонимизације је још изазовније и можда неће бити изводљиво с обзиром на тренутно стање технологије.

Као резултат тога, блокчејн пројекти морају пажљиво да размотре како чувају и управљају личним подацима и да ли је могуће постићи усклађеност са ГДПР-ом алтернативним методама, као што су складиштење ван ланца или хибридне архитектуре. Све док се не развију робуснија решења, употреба псеудонимизације и анонимизације у блокчејн контекстима остаће сложена и еволуирајућа област, која захтева континуирано истраживање, иновације и дијалог између технолога и регулатора.

VI. ТЕХНИЧКА И ПРАВНА РЕШЕЊА ЗА УСАГЛАШЕНОСТ ГДПР-А І БЛОКЧЕЈНА

Интеракција између блокчејн технологије и Опште уредбе о заштити података (ГДПР) представља сложен и вишеструки изазов и за правнике и за технологе. Као што је раније речено, децентрализована и непроменљива природа блокчејна често је у сукобу са основним принципима ГДПР-а, као што су право на заборав, минимизација података и обавезе за контролоре и обрађиваче података. Овај сукоб је довео до све веће контроле од стране регулатора и све веће забринутости међу организацијама које користе блокчејн технологију о томе како да обезбеде усклађеност без поткопавања основних карактеристика које чине блокчејн вредним. Како блокчејн постаје све продорнији у секторима као што су финансије, ланци снабдевања, здравствена заштита и јавне услуге, проналажење уравнотеженог приступа који поштује права појединаца уз очување интегритета и корисности децентрализованих система је од кључног значаја.

Постизање усклађености са ГДПР-ом у блокчејн окружењу захтева свеобухватну стратегију која интегрише и техничка и правна решења. Традиционалне праксе управљања подацима, као што је могућност измене или брисања података по вољи, постају неефикасне у блокчејн системима због њихове непроменљиве архитектуре и одсуства централног ауторитета. Стога се морају развити нови приступи како би се премостио јаз између регулаторних захтева и технолошких ограничења система дистрибуираних књига. Ова решења укључују техничке иновације као што су складиштење ван ланца, хибридне архитектуре и напредне криптографске технике, као и истраживање нових правних оквира који прилагођавају постојеће законе о заштити података јединственим карактеристикама блокчејна.

Ово поглавље ће истражити техничка и правна решења која су предложена за решавање изазова усклађености које представља интеракција између блокчејна и ГДПР-а. Анализираћемо потенцијале складиштења ван ланца и хибридних архитектура као средства за ублажавање ризика повезаних са складиштењем личних података на ланцу. Такође, размотрићемо улогу регулаторних приступа у помирењу разлика између закона о заштити података и блокчејн технологије, предлажући потенцијалне путеве за регулаторно прилагођавање и флексибилност који би могли да омогуће хармоничну коегзистенцију ова два оквира.

Циљ није само да се идентификују теоријска решења, већ да се критички процени њихова практичност, скалабилност и делотворност у апликацијама у стварном свету.

6.1. Складиштење ван ланца и хибридна решења

Један од примарних техничких приступа предложених за помирење тензија између непроменљивости блокчејна и захтева ГДПР-а је употреба складиштења ван ланца (Off-Chain) и хибридних решења. Ове методе имају за циљ да минимизирају укључивање личних података у сам блокчејн коришћењем екстерних система за складиштење који могу да прилагоде флексибилно управљање подацима потребно за усаглашеност са ГДПР-ом. Кључна идеја иза ових стратегија је да се осетљиве информације држе ван блокчејна, док се на њему чувају само референтни или криптографски докази, чиме се чува интегритет и корисност блокчејна без излагања пуном обиму ГДПР прописа.

6.1.1. Концепт складиштења ван ланца

Складиштење ван ланца подразумева чување личних података и других осетљивих информација изван мреже блокова у централизованим или дистрибуираним базама података. Уместо да се цео скуп података снима директно на блокчејну, само криптографски хеш или показивач на податке ван ланца се чувају у ланцу. Овај хеш служи као јединствени идентификатор, који доказује да су подаци постојали у одређеном стању у одређеном тренутку, без откривања њиховог садржаја.[94] Ова техника омогућава блокчејн системима да користе својства књиге заштићене од неовлашћеног приступа у сврху верификације без стварног складиштења личних података у ланцу.

На пример, у контексту здравствене заштите, пацијентова медицинска документација може да се чува ван ланца у безбедном, централизованом складишту. Блокчејн би снимио само хеш медицинског картона, заједно са метаподацима као што су временске ознаке или дозволе. Ако пацијент касније затражи брисање или модификацију својих података, запис ван ланца може се лако променити или избрисати у складу са захтевима ГДПР-а, док хеш на ланцу остаје као референца да је запис постојао без икаквих личних података.[95]

Овај приступ нуди неколико предности за усклађеност са ГДПР-ом:

- Брисање и модификација података: Пошто се стварни лични подаци не чувају на блокчејну, они се могу избрисати или изменити без утицаја на интегритет блокчејна. Ова флексибилност је у складу са захтевима ГДПР-а за права носилаца података, као што су право на заборав и право на исправку.[96]
- Минимизирана правна изложеност: Ограничавањем врсте података ускладиштених на блокчејну на неличне податке (нпр. криптографске хешове), организације могу да смање своју правну изложеност према ГДПР-у. Хешови се генерално сматрају мање осетљивим од потпуних скупова личних података и у многим случајевима се можда не квалификују као лични подаци према ГДПР-у ако се не могу повезати са оригиналним подацима.[97]

---

[94] Politou, Eugenia, Francisco Casino, Efthymios Alepis, and Constantinos Patsakis. “Blockchain Mutability: Challenges and Proposed Solutions.” *IEEE Transactions on Emerging Topics in Computing* 9, no. 4 (2019). https://doi.org/10.1109/tetc.2019.2949510.

[95] Jayabalan, Jayapriya, and N. Jeyanthi. "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy." *Journal of Parallel and distributed computing* 164 (2022): 152-167.

[96] Politou, Eugenia, et al. “Blockchain Mutability: Challenges and Proposed Solutions.” *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, 2019, https://doi.org/10.1109/tetc.2019.2949510.

[97] “Introduction to the Hash Function as a Personal Data Pseudonymisation Technique.” *European Data Protection Supervisor*, 2024, www.edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en. Преузето 5 Dec. 2024.

- Побољшана скалабилност: складиштење ван ланца такође може да реши проблеме скалабилности својствене блокчејн мрежама, које могу постати загушене и неефикасне када се велике количине података чувају на ланцу. Премештањем података ван ланца, блокови се могу фокусирати на снимање критичних информација о трансакцијама, побољшавајући укупне перформансе.[98]

6.1.2. Врсте система за складиштење ван ланца

Неколико типова система за складиштење ван ланца може се интегрисати са блокчејн мрежама, у зависности од захтеваног нивоа контроле, безбедности и приватности. Најчешће ванланчане архитектуре складиштења укључују:

Централизоване базе података: Централизовани системи складиштења ван ланца укључују једну базу података или складиште које контролише поуздана страна.[99] Овај приступ је једноставан и лак за имплементацију, али поново уводи многе рањивости и ограничења традиционалних централизованих система, као што су појединачне тачке квара и смањена транспарентност.

Дистрибуиране базе података: Дистрибуиране базе података, као што је Интерпланетарни систем датотека (InterPlanetary File System-IPFS), нуде децентрализованији приступ складиштењу ван ланца. Ови системи користе пеер-то-пеер (P2P) мреже за дистрибуцију података у више чворова, слично самом блокчејну. Чувањем личних података на дистрибуиран начин, ова решења чувају неке од предности децентрализације, као што су редундантност и толеранција грешака.[100] Међутим, они и даље дозвољавају брисање или модификацију података како то захтева ГДПР.

Шифровано складиште ван ланца: Да би се побољшала безбедност и приватност, подаци ван ланца могу се шифровати пре него што буду ускладиштени. Ово осигурава да чак и ако су подаци компромитовани, не могу се прочитати без кључа за дешифровање. Шифровање додаје додатни слој заштите, што отежава злонамерним актерима приступ или злоупотребу података. Употреба криптографских сидара или шема обавеза може повезати шифроване податке са њиховом референцом на ланцу, обезбеђујући да се интегритет података одржава.[101]

Употреба хешева и показивача

Кључна компонента решења за складиштење ван ланца је употреба криптографских хешева и показивача, који служе као референце на стварне податке ускладиштене ван ланца. Криптографски хеш је јединствени низ фиксне дужине генерисан из улаза (у овом случају, података ван ланца). Чак и мања промена података довела би до потпуно другачије хеш вредности, чинећи хешове идеалним алатом за проверу интегритета података без откривања основног садржаја.[102]

Када користите складиште ван ланца, блокчејн трансакција обично укључује хеш података ван ланца заједно са показивачем који показује где се подаци чувају. Показивач може имати облик УРЛ адресе, кључа базе података или децентрализованог идентификатора датотеке, у зависности од система за складиштење који се користи.

---

[98] Jayabalan, Jayapriya, and N. Jeyanthi. "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy." *Journal of Parallel and distributed computing* 164 (2022)

[99] ibid.

[100] ibid.

[101] Goint, Mongetro, Cyrille Bertelle, and Claude Duvallet. "Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems." *Mathematics* 11, no. 7 (March 25, 2023): 1592. https://doi.org/10.3390/math11071592.

[102] "Introduction to the Hash Function as a Personal Data Pseudonymisation Technique." *European Data Protection Supervisor*, 2024, www.edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en. Преузето 5 Dec. 2024.

Комбинација хеша и показивача омогућава блокчејну да одржава трајну евиденцију о постојању и стању података у одређеном тренутку, док се стварним подацима може управљати и контролисати ван ланца.[103]

Међутим, употреба хешева и показивача поставља сопствени скуп правних и техничких изазова. Ако се хеш може повезати са оригиналним подацима, он се и даље може сматрати личним подацима према ГДПР-у, посебно ако подаци ван ланца нису правилно заштићени.[104] Поред тога, ако систем складиштења ван ланца није безбедан или доступан током времена, интегритет и корисност референце на ланцу може бити угрожена, што доводи до проблема са управљањем подацима.

Хибридна решења: комбиновање приступа на ланцу и ван ланца

Хибридна решења представљају средину између система складиштења на ланцу (on-chain) и ван ланца(off-chain). У хибридном моделу, осетљиви подаци се чувају ван ланца, док се неосетљиви метаподаци чувају у ланцу. Овај приступ омогућава организацијама да искористе предности блокчејна (нпр. транспарентност, могућност ревизије и отпорност на неовлашћене промене) без угрожавања усклађености са ГДПР-ом. На пример, у случају коришћења ланца снабдевања, блокчејн може да складишти записе о испорукама производа на ланцу, док се детаљније информације о садржају сваке пошиљке (нпр. информације о клијенту, детаљни подаци о праћењу) чувају ван ланца.[105]

Једно најчешће коришћено хибридно решење је складиштење хеш стабла (Меркле дрво) на блокчејну, које садржи хешеве блокова података ван ланца. Ово омогућава да се цео скуп података верификује без складиштења у блокчејну. Ако субјекат података захтева брисање својих личних података, блок ван ланца који садржи те податке може бити обрисан, а ново Меркле стабло се може генерисати без мењања постојећих записа на ланцу. Овај приступ осигурава да блокчејн остане нетакнут, док се лични подаци могу мењати или брисати по потреби.[106]

6.1.3. Изазови и ограничења ванланчаних и хибридних решења

Упркос свом потенцијалу, складиштење ван ланца и хибридна решења имају неколико ограничења и ризика који се морају узети у обзир:

Повезивање и поновна идентификација: Док хешови и показивачи обезбеђују одређени степен раздвајања између података на ланцу и ван ланца, они и даље могу бити подложни нападима поновне идентификације ако су оригинални подаци или показивач угрожени. Ово би могло учинити ванланчане податке рањивим, излажући их ризицима приватности.

Доступност и постојаност података: Системи складиштења ван ланца морају да обезбеде да подаци остану доступни током времена. Ако се подаци ван ланца избришу

[103] Greenspan, Gideon. "Scaling Blockchains with Off-Chain Data | MultiChain." *Multichain.com*, 13 June 2018, www.multichain.com/blog/2018/06/scaling-blockchains-off-chain-data/. Преузето 6 Nov. 2024.

[104] "Introduction to the Hash Function as a Personal Data Pseudonymisation Technique." *European Data Protection Supervisor*, 2024, www.edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en. Преузето 5 Dec. 2024

[105] Nielson, Bryant. "Bridging On-Chain and Off-Chain Worlds: How Decentralized Oracles Work - the Blockchain Academy." *The Blockchain Academy*, Feb. 2024, theblockchainacademy.com/bridging-on-chain-and-off-chain-worlds-how-decentralized-oracles-work/. Преузето 7 Nov. 2024.

[106] Zhang, Ce, et al. *Authenticated Keyword Search in Scalable Hybrid-Storage Blockchains*. Apr. 2021, https://doi.org/10.1109/icde51399.2021.00091. Преузето 8 Nov. 2024.

или постану недоступни (нпр. због кварова сервера или напуштања чворова), референце на ланцу постају бесмислене, подривајући вредност записа блокчејна.[107]

Регулаторна двосмисленост: Не постоји јасан консензус о томе да ли се хешеви и показивачи ван ланца квалификују као лични подаци према ГДПР-у. Правна тумачења варирају у зависности од тога да ли се подаци ван ланца могу повезати са хешом, стварајући несигурност у погледу регулаторног статуса ових решења.[108]

Поверење и централизација: Централизована решења за складиштење ван ланца представљају тачку централног поверења, потенцијално негирајући предности децентрализоване архитектуре блокчејна. Чак и у дистрибуираним системима као што је IPFS, учесници морају веровати да ће чворови који чувају њихове податке деловати у складу са договореним правилима и да неће мењати или брисати податке без овлашћења.[109]

Складиштење ван ланца и хибридна решења представљају обећавајући приступ помирењу непроменљивости блокчејна са захтевима ГДПР-а за флексибилност и брисање података. Пребацивањем осетљивих података ван ланца и чувањем само проверљивих референци на ланцу, ова решења обезбеђују пут ка усклађености уз очување предности блокчејн технологије. Међутим, њихова ефикасност зависи од пажљиве примене, чврстих безбедносних мера и јасног разумевања правног статуса резултирајућих структура података.

Како блокчејн технологија наставља да се развија, складиштење ван ланца и хибридна решења ће играти све важнију улогу у развоју блокчејн апликација усклађених са ГДПР-ом**.**

6.2. Шифровање и Докази са нултим знањем (Zero-Knowledge Proofs)

Напредне криптографске технике, као што су шифровање и Докази са нултим знањем (Zero-Knowledge Proofs - ZKP), нуде моћне алате за побољшање приватности и постизање усклађености са прописима о заштити података као што је ГДПР у блокчејн окружењима. Ове технике су дизајниране да обезбеде личне податке у ланцу без угрожавања интегритета или транспарентности главне књиге, обезбеђујући начин да се помире конфликтни захтеви заштите података и непроменљивости блокчејна. У суштини, они омогућавају селективно откривање, омогућавајући верификацију информација без откривања основних података.

6.2.1. Шифровање: Заштита података на ланцу

Шифровање је основна техника за заштиту поверљивости и безбедности података. То укључује трансформацију података отвореног текста у формат који је нечитљив без исправног кључа за дешифровање. У блокчејн системима, шифровање се може користити за заштиту осетљивих података који се морају чувати на ланцу, обезбеђујући да само овлашћене стране могу да приступе или тумаче информације. Постоји неколико типова шема шифровања које се обично примењују у блокчејн контекстима, а свака има различите снаге и случајеве употребе:

Симетрично шифровање: Симетрично шифровање користи исти кључ и за шифровање и за дешифровање. Овај метод је брз и ефикасан, што га чини погодним за

[107] Wang, Xiaojie, Hanxue Li, Ling Yi, Zhaolong Ning, Song Guo, and Yan Zhang. “A Survey on Off-Chain Networks: Frameworks, Technologies, Solutions and Challenges.” arXiv.org, 2023. https://arxiv.org/abs/2311.10298. Преузето 08.11.2024.

[108] ibid.

[109] ibid.

шифровање великих количина података. Међутим, изазов лежи у безбедном дељењу и управљању кључевима међу учесницима. Ако је кључ компромитован, шифровани подаци се могу лако дешифровати, откривајући осетљиве информације. [110] Симетрично шифровање се ретко користи на ланцу због ових безбедносних ризика, али се може применити на решења за складиштење ван ланца**.**

Асиметрично шифровање: Асиметрично шифровање, такође познато као криптографија са јавним кључем, користи пар кључева: јавни кључ за шифровање и приватни кључ за дешифровање. Овај метод побољшава безбедност тако што обезбеђује да само власник приватног кључа може да дешифрује податке, чак и ако је јавни кључ опште познат. [111] У блокчејн системима, асиметрична енкрипција се обично користи за обезбеђење података о трансакцијама, проверу дигиталних потписа и управљање корисничким идентитетима. Међутим, рачунарски је интензивна и може успорити перформансе блокчејн мрежа када се примени на велике скупове података.[112]

Хомоморфно шифровање: Хомоморфно шифровање је напредна техника која омогућава да се изводе прорачуни на шифрованим подацима без потребе за њихово дешифровање. То значи да се осетљиви подаци могу обрадити и анализирати на безбедан начин, чувајући приватност чак и током сложених операција. На пример, блокчејн паметни уговор може да рачуна на хомоморфно шифрованим улазима без откривања основних вредности, осигуравајући да подаци остану поверљиви током целог процеса. Иако обећава, хомоморфно шифровање је још увек у експерименталној фази и захтева значајне рачунарске ресурсе, што га чини изазовним за имплементацију у великим размерама**.**[113]

Хибридно шифровање: Хибридно шифровање комбинује предности симетричне и асиметричне енкрипције коришћењем симетричне енкрипције за обезбеђење стварних података и асиметричне енкрипције за заштиту симетричног кључа. Овај приступ балансира ефикасност и сигурност, чинећи га погодним за сценарије у којима су и перформансе и поверљивост важни.[114]

Иако шифровање пружа снажну заштиту за податке на ланцу, оно не испуњава све захтеве усклађености са ГДПР-ом. На пример, чак и ако су лични подаци шифровани, ГДПР их и даље сматра личним подацима ако је кључ за дешифровање доступан и подаци се могу вратити у првобитни облик.[115] Стога, само шифровање није потпуно решење за усаглашеност са ГДПР-ом у блокчејн системима. Мора се комбиновати са додатним мерама, као што су управљање кључевима и контрола приступа, како би се осигурало да шифровани подаци не могу да се повежу назад са појединцем који се може идентификовати.

---

[110] Jeeva, A. L., Dr V. Palanisamy, and K. Kanagaram. "Comparative analysis of performance efficiency and security measures of some encryption algorithms." *International Journal of Engineering Research and Applications (IJERA)* 2.3 (2012)

[111] ibid.

[112] Poston, Howard. "Blockchain and Asymmetric Cryptography | Infosec." *Infosecinstitute.com*, 2021, www.infosecinstitute.com/resources/cryptography/blockchain-and-asymmetric-cryptography/. Преузето 4 Dec. 2024.

[113] "What Is Homomorphic Encryption? - Chainlink." *Chain.link*, chain.link/education-hub/homomorphic-encryption. Преузето 9 Nov. 2024.

[114] Shoukat, Ijaz Ali, et al. "A Generic Hybrid Encryption System (HES)." *Research Journal of Applied Sciences, Engineering and Technology*, vol. 5, no. 9, Mar. 2013, pp. 2692–700, https://doi.org/10.19026/rjaset.5.4793. Преузето 9 Nov. 2024.

[115] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

6.2.2. Докази са нултим знањем (Zero-Knowledge Proofs)

Докази са нултим знањем (ДНЗ) представљају револуционарни приступ приватности у блокчејн мрежама, омогућавајући верификацију без откривања било какве основне информације. Овај концепт је посебно вредан у контекстима где је приватност података најважнија, јер омогућава учесницима да докажу знање о вредности или валидности трансакције без откривања самих података. Једноставно речено, доказ са нултим знањем омогућава једној страни (доказивачу) да убеди другу страну (верификатора) да је изјава истинита, без откривања било чега изван истинитости изјаве.

Постоји неколико врста доказа са нултим знањем, сваки са различитим нивоима ефикасности и сигурности:

Интерактивни Докази са нултим знањем: У интерактивним ДНЗ-овима, доказивач и верификатор учествују у низу размена (или „рунди“) да би утврдили валидност изјаве. Верификатор шаље изазове, а доказивач одговара на начин који убеђује верификатора без откривања додатних информација. Интерактивни ДНЗ-ови су ефикасни за верификацију један-на-један, али нису погодни за шире блокчејн апликације због сложених комуникацијских захтева.[116]

Неинтерактивни Докази са нултим знањем (НДНЗ): Неинтерактивни ДНЗ елиминишу потребу за директном интеракцијом између проверавача и верификатора. Уместо тога, доказ се генерише једном и свако може да га провери користећи заједнички референтни низ. НДНЗ-ови су високо ефикасни и скалабилни, што их чини идеалним за блокчејн окружења. Они се широко користе у криптовалутама које су фокусиране на приватност као што је „Zcash“, која користи zk-SNARK-ове (Succinct Non-Interactive Arguments of Knowledge) да прикрије детаље трансакције, а истовремено омогућава јавну верификацију.[117]

zk-SNARK и zk-STARK: „zk-SNARK“ (Succinct Non-Interactive Arguments of Knowledge) и „zk-STARK“ (Scalable Transparent Arguments of Knowledge) су два напредна облика неинтерактивних доказа са нултим знањем. zk-SNARK -ови пружају компактне доказе са минималним рачунским трошковима, али захтевају поуздану фазу подешавања, која може да уведе безбедносне ризике. zk-STARK -ови су, с друге стране, транспарентни и не захтевају поуздано подешавање, што их чини сигурнијим, али рачунарски интензивнијим. Ове технологије се истражују за различите случајеве употребе, укључујући поверљиве паметне уговоре и пренос приватних средстава.[118]

Докази са нултим знањем нуде неколико потенцијалних апликација за усклађеност са ГДПР-ом у блокчејн системима, посебно за балансирање приватности и транспарентности:

Трансакције које чувају приватност: У традиционалним блокчејн трансакцијама, детаљи о пошиљаоцу, примаоцу и износу трансакције су видљиви свим учесницима. Са ДНЗ је могуће сакрити ове детаље док се и даље доказује да је трансакција важећа. Ова могућност је посебно драгоцена у финансијским апликацијама, где је поверљивост кључна. Криптовалуте које су фокусиране на приватност, попут Zcash-a и Monero-a,

[116] Sun, Xiaoqiang, F. Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. "A survey on zero-knowledge proof in blockchain." *IEEE network* 35, no. 4 (2021)

[117] Partala, Juha, et al. “Non-Interactive Zero-Knowledge for Blockchain: A Survey.” *IEEE Access*, vol. 8, 2020, https://doi.org/10.1109/access.2020.3046025. Преузето 9 Nov. 2024.

[118] Guan, Zhangshuang, et al. “BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on Zk-SNARKs.” *IEEE Transactions on Dependable and Secure Computing*, 2020, https://doi.org/10.1109/tdsc.2020.3025129. Преузето 10 Nov. 2024.

користе ДНЗ како би омогућиле корисницима да обављају приватне трансакције без угрожавања сигурности и интегритета блокчејна.[119][120]

Селективно откривање информација: ДНЗ омогућавају селективно откривање, при чему се откривају само специфични атрибути скупа података без излагања целог скупа података. На пример, корисник може доказати да има више од 18 година, а да не открије тачан датум рођења. Ово селективно обелодањивање је веома релевантно за принцип минимизације података ГДПР-а, омогућавајући организацијама да покажу усклађеност уз одржавање поверљивости корисничких података.[121]

Управљање идентитетом и аутентификација: У системима за управљање идентитетом, ДНЗ могу се користити за верификацију аутентичности идентитета корисника без откривања личних података. Ова могућност омогућава безбедну аутентификацију и ауторизацију без угрожавања приватности корисника, што је чини моћним алатом за децентрализована решења идентитета.[122]

Извештавање о усклађености и ревизија: ДНЗ се могу применити на извештавање о усклађености, где се од организација захтева да докажу да су поштовале захтеве ГДПР-а без откривања осетљивих оперативних података. На пример, компанија би могла да користи ДНЗ да покаже да су лични подаци обрађени у складу са ГДПР принципима без излагања основних података.[123]

Упркос свом потенцијалу, Докази са нултим знањем нису без ограничења. Генерисање и верификација ДНЗ-а може бити рачунарски интензивна, посебно за сложене процесе. Ови трошкови могу утицати на перформансе и скалабилност блокчејн мрежа, што отежава имплементацију ДНЗ-а у окружењима високе пропусности података.

Неки типови ДНЗ-а, као што су zk-SNARK, захтевају фазу поузданог подешавања, где се одређени параметри генеришу на безбедан начин. Ако је подешавање угрожено, безбедност целог система може бити угрожена. Овај захтев представља потенцијалну тачку неуспеха и компликује примену решења.[124]

Докази са нултим знањем су и даље технологија у настајању, а недостаје стандардизација и најбоље праксе за њихову примену. Као резултат тога, организације морају да управљају сложеним пејзажом различитих система доказа, од којих сваки има своје компромисе и ограничења.

Шифровање и Докази са нултим знањем обезбеђују робусне криптографске алате за побољшање приватности и постизање усаглашености са ГДПР-ом у блокчејн системима. Омогућавањем безбедног складиштења података, приватних трансакција и селективног откривања, ове технике нуде начин да се уравнотежи транспарентност и непроменљивост блокчејна са потребом за заштитом личних података.

---

[119] "Privacy-Protecting Digital Currency | Zcash." *Zcash*, z.cash/. Преузето 10 Nov. 2024.

[120] Monero. "Monero: Home." *Getmonero.org, the Monero Project*, 2019, www.getmonero.org/. Преузето 10 Nov. 2024.

[121] Sun, Xiaoqiang, F. Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. "A survey on zero-knowledge proof in blockchain." *IEEE network* 35, no. 4 (2021)

[122] Abebe Diro, et al. "Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities." *Journal of Information Security and Applications*, vol. 80, Elsevier BV, Feb. 2024, https://doi.org/10.1016/j.jisa.2023.103678.

[123] ibid.

[124] Abebe Diro, et al. "Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities." *Journal of Information Security and Applications*, vol. 80, Elsevier BV, Feb. 2024, https://doi.org/10.1016/j.jisa.2023.103678.

6.3. Регулаторни приступи

Док техничка решења као што су складиштење ван ланца, енкрипција и Докази са нултим знањем нуде могућности за усклађивање блокчејна са захтевима ГДПР-а, она сама по себи нису довољна за решавање ширих регулаторних изазова који произилазе из пресека ова два оквира. Блокчејнова децентрализована природа, недостатак контролора података који се јасно могу идентификовати и његова фундаментална непроменљивост представљају регулаторне сложености које се не могу у потпуности решити само технологијом. Сходно томе, свеобухватан регулаторни приступ је од суштинског значаја како би се осигурало да блокчејн системи могу да буду у складу са законима о заштити података без гушења иновација или подривања основних принципа блокчејн технологије.

6.3.1. Прилагођавање постојећег правног оквира

Један приступ постизању усклађености је реинтерпретација и прилагођавање постојећих прописа о заштити података како би се прилагодили специфичностима блокчејн технологије. ГДПР, иако један од најобухватнијих прописа о заштити података на глобалном нивоу, није дизајниран имајући на уму децентрализоване технологије. Као резултат тога, многе његове одредбе—као што су оне које се односе на контролоре података, права носилаца података и брисање података—тешко је применити у контексту дистрибуираних књига. Да би се позабавила овим проблемима, регулаторна тела као што је Европски одбор за заштиту података - „European Data Protection Board" (EDPB) и национална тела за заштиту података могла би да издају прилагођеније смернице о томе како би блокчејн технологија требало да буде регулисана према ГДПР-у.

Појашњавање улоге контролора и обрађивача података

Један од примарних регулаторних изазова у блокчејну је одређивање ко се квалификује као контролор или обрађивач података према ГДПР-у. У традиционалним централизованим системима, ове улоге су јасно дефинисане, са једним ентитетом одговорним за прикупљање, чување и управљање личним подацима.[125] У децентрализованим блокчејн мрежама, међутим, подацима заједнички управља дистрибуирани скуп учесника, што отежава идентификацију једног ентитета који се може сматрати одговорним за усклађеност са ГДПР-ом.

Неки регулаторни истраживачи су предложили да се блокчејн чворови могу заједно сматрати заједничким контролорима, који деле одговорност за усклађеност. Међутим, ово тумачење је проблематично јер намеће значајна оптерећења усклађености појединачним учесницима, од којих многи можда немају ресурсе или стручност да испуне обавезе према ГДПР-у.[126] Други приступ је одређивање одређених ентитета унутар мреже (нпр. рудари, програмери или добављачи услуга) као контролори или процесори на основу њихове улоге у управљању подацима.[127] Ипак, такве разлике нису увек јасне и могу значајно да варирају између различитих типова блокчејна (нпр. јавни наспрам приватних, дозвољених или без дозволе).

[125] Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.

[126] Buocz, Thomas, et al. "Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks." *Computer Law & Security Review*, vol. 35, no. 2, Apr. 2019, https://doi.org/10.1016/j.clsr.2018.12.003. Преузето 11 Nov. 2024.

[127] ibid.

Да би одговорили на ове нејасноће, регулатори би могли да обезбеде детаљније критеријуме за одређивање статуса контролора података и процесора у блокчејн системима. На пример, могла би се издати упутства о специфичним околностима под којима оператери чворова, програмери паметних уговора или издаваоци токена треба да се сматрају контролорима података, узимајући у обзир факторе као што су њихов утицај на активности обраде података и њихова способност да се придржавају ГДПР захтева.[128]

Прилагођавање права на заборав

Критична област у којој је потребна регулаторна адаптација је право на заборав, што је суштински у супротности са непроменљивошћу блокчејна. Једно потенцијално решење је реинтерпретација права на заборав у контексту блокчејна, омогућавајући алтернативне механизме усклађености који не захтевају физичко брисање података. На пример, регулатори би могли да препознају методе „логичког брисања“, као што је приказивање података недоступним или коришћење криптографских техника попут „камелеонских хешева“ које омогућавају контролисане модификације одређених блокова без угрожавања читавог ланца.[129]

Алтернативно, право на заборав се може преобличити у право на забрану или ограничење приступа, а не у апсолутно право на брисање. Овај приступ би омогућио блокчејн мрежама да буду у складу са ГДПР-ом омогућавајући субјектима података да минимизирају свој дигитални отисак без потребе за стварним уклањањем историјских записа.[130] Такво тумачење би требало да буде пропраћено јасним смерницама о томе како применити ова ограничења у пракси.

6.3.2. Креирање нових регулаторних категорија за децентрализоване технологије

С обзиром на јединствена својства блокчејна, неки научници и креатори политичке регулативе тврде да постојећи оквири заштите података попут ГДПР-а могу бити неприкладни за регулисање децентрализованих технологија. Уместо тога, они предлажу стварање нових регулаторних категорија које препознају специфичне карактеристике блокчејна и других технологија дистрибуиране књиге. Овај приступ би укључивао развој посебног правног оквира који се посебно бави потребама усклађености и изазовима децентрализованих система, уместо да покушава да их уклопи у постојеће парадигме.

Успостављање улоге „управник децентрализованих података“.

Једна могућа регулаторна иновација је увођење нове улоге, као што је управник децентрализованих података, који би био одговоран за надгледање усклађености са ГДПР-ом у децентрализованим мрежама. Управник података би деловао као посредник између регулатора и блокчејн заједнице, пружајући смернице о стратегијама усклађености, координирајући одговоре на захтеве субјекта података и осигуравајући да се мрежа придржава најбољих пракси за заштиту података. Ову улогу може попунити именовани ентитет унутар мреже (нпр. фондација или конзорцијум) или независна трећа страна са експертизом у области блокчејна и закона о заштити података.[131]

---

[128] Buocz, Thomas, et al. “Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks.” *Computer Law & Security Review*, vol. 35, no. 2, Apr. 2019, https://doi.org/10.1016/j.clsr.2018.12.003. Преузето 11 Nov. 2024.

[129] Haque, AKM Bahalul, A.K.M. Najmul Islam, Sami Hyrynsalmi, Bilal Naqvi, and Kari Smolander. “GDPR Compliant Blockchains – a Systematic Literature Review.” *IEEE Access* 9 (2021). https://doi.org/10.1109/access.2021.3069877.

[130] ibid.

[131] Heleen Janssen, Jennifer Cobbe, Chris Norval, Jatinder Singh, Decentralized data processing: personal data stores and the GDPR, *International Data Privacy Law*, Volume 10, Issue 4, November 2020.

Креирање „Уговора о обради података о блокчејну“

Друго предложено решење је развој стандардизованих споразума о обради података у блокчејну (Blockchain Data Processing Agreements-BDPA) који оцртавају одговорности и обавезе сваког учесника у мрежи. Ови споразуми би служили као уговорни оквир, прецизирајући ко се сматра контролором података, ко је обрађивач и како ће принципи заштите података бити имплементирани у оквиру мреже. BDPA би могао да пружи правну јасноћу и олакша усаглашеност успостављањем јасних правила и процедура за управљање подацима у децентрализованим окружењима.[132]

6.3.3. Регулаторни сандбоксови и колаборативни приступи

С обзиром на брзу еволуцију блокчејн технологије и сложеност усклађености са ГДПР-ом, флексибилан и колаборативни регулаторни приступ је од суштинског значаја. Регулаторни сандбоксови (Regulatory Sandboxes) — контролисана окружења у којима се иновативне технологије могу тестирати уз регулаторни надзор — обезбеђују обећавајући пут за истраживање стратегија усаглашености блокчејна у окружењу ниског ризика. Сандбоксови омогућавају регулаторима и програмерима блокчејна да експериментишу са новим приступима, прикупљају податке о њиховој ефикасности и прецизирају регулаторне оквире на основу практичног искуства.[133]

Предности регулаторних сандбоксова

Регулаторни сандбоксови нуде неколико предности за усаглашеност са блокчејном:

- Правна сигурност: Учешћем у сандбоксу, блокчејн пројекти могу да добију смернице и повратне информације од регулатора, смањујући ризик од неусаглашености и обезбеђујући већу правну сигурност.
- Иновативна решења: Сандбоксови подстичу развој иновативних решења, као што су нове криптографске технике или хибридне архитектуре, што можда није могуће под традиционалним регулаторним ограничењима.
- Сарадња са заинтересованим странама: Сандбоксови олакшавају сарадњу између регулатора, програмера и правних стручњака, промовишући заједничко разумевање изазова и могућности које представља блокчејн технологија.[134]

Земље као што су Уједињено Краљевство, Сингапур и Швајцарска су већ успоставиле регулаторне сандбоксове за финтек и блокчејн пројекте, омогућавајући им да истраже нове стратегије усклађености у окружењу које подржава иновације.[135] Европска унија би могла размотрити имплементацију сличне иницијативе посебно фокусиране на усклађеност са ГДПР-ом за блокчејн, окупљајући регулаторе, блокчејн програмере и органе задужене за заштиту података како би развили најбоље праксе и нова решења за усклађеност.

---

[132] “Blockchain and Data Protection – an FAQ Guide | Perspectives | Reed Smith LLP.” *Www.reedsmith.com*, www.reedsmith.com/en/perspectives/2022/11/blockchain-and-data-protection--an-faq-guide. Преузето 12 Nov. 2024.

[133] hakia. “Unlocking Innovation: Regulatory Sandboxes for Blockchain & Cryptocurrency.” *Hakia: Covering All Angles of Technology*, 23 Mar. 2022, hakia.com/regulatory-sandboxes-for-blockchain-and-cryptocurrency-innovation/. Преузето 12 Nov. 2024.

[134] ibid.

[135] Goo, Jayoung James, and Joo-Yeun Heo. “The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation.” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 6, no. 2, June 2020.

Подстицање саморегулације и индустријских стандарда

Други приступ сарадње је промоција саморегулације и развој индустријских стандарда за заштиту података блокчејна. Саморегулаторна тела, као што су Међународно удружење за поуздане блокчејн апликације (International Association for Trusted Blockchain Applications-INATBA) и Ентерпрајз Етереум Алијанса (Enterprise Ethereum Alliance-EEA), могу да играју кључну улогу у успостављању добровољних кодекса понашања, најбољих пракси и техничких стандарда који се односе на захтеве ГДПР-а.[136] [137] Ове стандарде затим могу усвојити блокчејн мреже како би демонстрирали своју посвећеност заштити података и повећали поверење међу корисницима и регулаторима.

Регулаторни приступи су витална компонента постизања усклађености са ГДПР-ом у блокчејн системима. Док техничка решења могу да ублаже неке ризике усклађености, потребан је јасан и прилагодљив регулаторни оквир за решавање јединствених изазова које представљају децентрализоване технологије. Прилагођавајући постојеће законе, креирајући нове регулаторне категорије и подстичући иницијативе за сарадњу, регулатори могу да обезбеде правну јасноћу и флексибилност потребну за подршку одговорном развоју блокчејн технологије. На крају, уравнотежен приступ који интегрише техничку иновацију са промишљеном регулацијом је од суштинског значаја како би се осигурало да блокчејн може коегзистирати са ГДПР-ом без жртвовања његових основних принципа транспарентности, безбедности и децентрализације.

VII. ЗАКЉУЧНА РАЗМАТРАЊА

Испитивање раскрснице између блокчејн технологије и Опште уредбе о заштити података (ГДПР) открива неколико значајних тачака сукоба, укорењених првенствено у фундаменталним разликама између природе блокчејна и регулаторних мандата ГДПР-а. Ови налази наглашавају да, иако блокчејн нуди трансформативне предности у смислу интегритета података, безбедности и транспарентности, његове основне карактеристике представљају озбиљне изазове када се процене у односу на строге захтеве ГДПР-а за заштиту података. У претходним поглављима појавило се неколико критичних области од којих свака илуструје сложеност помирења децентрализованих, непроменљивих система са флексибилним оквиром ГДПР-а заснованим на правима.

Непроменљивост наспрам права на заборав

Једно од централних идентификованих проблема је контрадикција између непроменљивости блокчејна и члана 17 ГДПР-а, који утврђује „право на заборав“ или право на брисање. Непроменљивост, основна карактеристика блокчејна, осигурава да се подаци, када се сниме, не могу мењати или брисати без угрожавања интегритета целог ланца. Ово је директно у супротности са очекивањима ГДПР-а да субјекти података треба да имају могућност да затраже уклањање својих личних података када то више није неопходно, када је сагласност повучена или када су подаци незаконито обрађени. Крута природа блокчејна чини скоро немогућим испуњавање таквих захтева за брисањем без поткопавања самих својстава која чине блокчејн сигурним и поузданим. Овај сукоб

[136] “INATBA - International Association for Trusted Blockchain Applications.” *INATBA*, 2017, inatba.org/. Преузето 13 Nov. 2024.

[137] Evander Pierre. “Enterprise Ethereum Alliance.” *Enterprise Ethereum Alliance*, entethalliance.org/. Преузето 13 Nov. 2024.

наглашава напетост између заштите индивидуалних права и очувања безбедности и транспарентности мреже блокчејна.

Ограничења складиштења и преноса података

Блокчејнова децентрализована и дистрибуирана архитектура, где се подаци реплицирају у бројним чворовима широм света, поставља значајна питања усклађености са одредбама ГДПР-а о складиштењу и преносу података. Уредба захтева да се лични подаци чувају на начин који омогућава лако управљање, исправљање и брисање, истовремено осигуравајући да су преноси података у треће земље у складу са строгим условима. У блокчејн мрежама, подаци се често чувају на чворовима који се налазе у више јурисдикција, што отежава контролу или ограничавање токова података у складу са правилима прекограничног преноса ГДПР-а. Поред тога, репликација података преко чворова доводи до ситуације у којој чак и мали делови личних информација постају широко дистрибуирани, што компликује напоре да се имплементирају принципи минимизације података и ограничења задржавања. Ове карактеристике чине изазовом спровођење управљања подацима у складу са ГДПР-ом у блокчејн окружењима.

Изазови псеудонимизације и анонимизације

Док су псеудонимизација и анонимизација широко коришћене технике за заштиту личних података и ублажавање ризика усклађености, њихова примена у блокчејн системима је пуна ограничења. Псеудонимизација, као што је коришћење криптографских адреса или јавних кључева уместо идентификатора из стварног света, не пружа потпуну заштиту према ГДПР-у јер се често може поништити анализом трансакција или повезивањем података. Чак је и анонимизацију, која идеално чини податке неповратно неидентификованим, тешко постићи у блокчејн контекстима због транспарентности и следљивости трансакција. То значи да чак и наизглед анонимни подаци о блокчејну могу бити предмет поновне идентификације, што изазива забринутост у вези са адекватношћу ових техника за усклађеност са ГДПР-ом.

Техничка решења: складиштење ван ланца и докази са нултим знањем

За решавање изазова које представља складиштење личних података на ланцу, предложена су техничка решења као што су складиштење ван ланца и хибридне архитектуре. Чувањем осетљивих података ван ланца и само снимањем криптографских доказа или хешова на блокчејну, ова решења омогућавају поштовање права на брисање и принципа минимизације података без угрожавања непроменљивости главне књиге. Слично томе, напредне криптографске технике као што су докази са нултим знањем (Zero-Knowledge Proofs) нуде иновативне начине за верификацију података без откривања основних информација, обезбеђујући средства за балансирање приватности и транспарентности. Међутим, ови приступи су још увек у експерименталној фази и суочавају се са практичним ограничењима, као што су велики трошкови и сложеност имплементације, што омета њихово широко усвајање.

Правне и регулаторне адаптације

Из правне перспективе, постојећи оквир ГДПР-а није дизајниран имајући на уму децентрализовану архитектуру блокчејна. Ово ствара двосмисленост у примени кључних ГДПР концепата, као што је дефиниција контролора и процесора података, на

блокчејн мреже. Недостатак централног органа у многим блокчејн системима отежава утврђивање одговорности за обезбеђивање усаглашености, што доводи до неизвесности о томе ко треба да буде одговоран у случају повреде података или неусаглашености. Предложено је неколико регулаторних адаптација, укључујући развој нових улога као што су управници децентрализованих података и креирање уговора о обради података специфичних за блокчејн. Међутим, ови предлози захтевају даље истраживање и појашњење како би се обезбедио јасан правни пут за блокчејн пројекте.

Регулаторни приступи и препоруке

Да би се премостио јаз између блокчејна и ГДПР-а, неопходна је комбинација техничких, правних и регулаторних стратегија. Регулаторна тела морају да пруже јасније смернице о томе како принципе ГДПР-а треба тумачити у децентрализованим контекстима, док блокчејн програмери треба да усвоје технологије за побољшање приватности и примене најбоље праксе за заштиту података. Регулаторни сандбоксови и иницијативе за сарадњу нуде обећавајуће путеве за тестирање и усавршавање решења усклађености у контролисаном окружењу, подстичући конструктивнији дијалог између регулатора и блокчејн заједнице. Постизање ове равнотеже ће захтевати сталну сарадњу и флексибилност свих заинтересованих страна како би се осигурало да блокчејн може еволуирати на начин који поштује и иновације и права појединца.

Налази овог рада наглашавају значајне изазове и могућности које произилазе из укрштања блокчејн технологије и прописа о заштити података. Док техничка решења и регулаторна прилагођавања нуде потенцијалне путеве за постизање усклађености, не постоји једноставан одговор. Сваки блокчејн пројекат мора бити пажљиво процењен како би се одредила најприкладнија стратегија усклађености, узимајући у обзир специфичне карактеристике технологије и законске захтеве јурисдикције у којој послује. Будућност компатибилности блокчејна са ГДПР-ом зависиће од способности регулатора, програмера и правних стручњака да развију заједничко разумевање технологије и створе уравнотежен оквир који штити права појединца без гушења иновација.

VIII. ЛИТЕРАТУРА

1. Abebe Diro, Lu Zhou, Akanksha Saini, Shahriar Kaisar, and Pham Cong Hiep "Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities." *Journal of Information Security and Applications*, vol. 80, Elsevier BV, 2024., https://doi.org/10.1016/j.jisa.2023.103678.
2. Amazon. "Amazon Web Services (AWS) - Cloud Computing Services." *Amazon Web Services, Inc.*, 2024, aws.amazon.com/. Преузето 9 Sept. 2024.
3. Bastos, Daniel, Fabio Giubilo, Mark Shackleton, and Fadi El-Moussa. "GDPR privacy implications for the Internet of Things." In *4th Annual IoT Security Foundation Conference*, vol. 4, pp. 1-8. 2018.
4. Beck, Roman, Christoph Müller-Bloch, and John Leslie King. "Governance in the blockchain economy: A framework and research agenda." *Journal of the association for information systems* 19.10.2018.: 1.
5. Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation." *Computer law & security review* 33.2 2017.: pp.171-181.
6. Brimblecombe, Fiona. "The public interest in deleted personal data? The right to be forgotten's freedom of expression exceptions examined through the lens of Article 10 ECHR." *Journal of Internet Law* 23.10.2020.: pp1-29.
7. Cao, Bin, Zhenghui Zhang, Daquan Feng, Shengli Zhang, Lei Zhang, Mugen Peng, and Yun Li. "Performance analysis and comparison of PoW, PoS and DAG based blockchains." *Digital Communications and Networks* 6, no. 4, 2020.: pp.480-485.
8. Finck, Michèle, and Frank Pallas. "They who must not be identified—distinguishing personal from non-personal data under the GDPR." *International Data Privacy Law* 10.1 2020.: pp.11-36.
9. Greze, Benjamin. "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives." *International Data Privacy Law* 9.2 2019.: pp.109-128.
10. Hofmann, Frank, Simone Wurster, Eyal Ron, and Moritz Böhmecke-Schwafert. "The immutability concept of blockchains and benefits of early standardization." In *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, IEEE, 2017. pp. 1-8.
11. Jayabalan, Jayapriya, and N. Jeyanthi. "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy." *Journal of Parallel and distributed computing* 164 2022.: pp.152-167.
12. Jeeva, A. L., Dr V. Palanisamy, and K. Kanagaram. "Comparative analysis of performance efficiency and security measures of some encryption algorithms." *International Journal of Engineering Research and Applications (IJERA)* 2.3 2012.
13. Joshi, Seema B. "Standards and techniques to remove data remanence in cloud storage." *2018 IEEE Punecon*. IEEE, 2018.
14. Khalilov, Merve Can Kus, and Albert Levi. "A survey on anonymity and privacy in bitcoin-like digital cash systems." *IEEE Communications Surveys & Tutorials* 20.3, 2018.
15. Khan, Shafaq Naheed, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. "Blockchain smart contracts: Applications, challenges, and future trends." *Peer-to-peer Networking and Applications* 14, 2021.
16. Lepore, Cristian, Michela Ceria, Andrea Visconti, Udai Pratap Rao, Kaushal

Arvindbhai Shah, and Luca Zanolini. "A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS." *Mathematics* 8, no. 10, 2020.

17. Lynskey, Orla. "Control over Personal Data in a Digital Age: Google S pain v AEPD and Mario Costeja Gonzalez." *The modern law review* 78.3, 2015.: pp522-534.
18. Merrell, Ian. "Blockchain for decentralised rural development and governance." *Blockchain: Research and Applications* 3.3 2022.
19. Molina, Fernanda, Gustavo Betarte, and Carlos Luna. "Design principles for constructing GDPR-compliant blockchain solutions." *2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*. IEEE, 2021.
20. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Satoshi Nakamoto*, 2008.
21. Poelman, Michelle, and Sarfraz Iqbal. "Investigating the compliance of the gdpr: Processing personal data on a blockchain." *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*. IEEE, 2021.
22. Politou, Eugenia, Efthimios Alepis, Maria Virvou, and Constantinos Patsakis. *Privacy and data protection challenges in the distributed era*. Vol. 26. Heidelberg, Germany: Springer, 2022.
23. Reardon, Joel, David Basin, and Srdjan Capkun. "Sok: Secure data deletion." *2013 IEEE symposium on security and privacy*. IEEE, 2013.
24. Stainforth, Elizabeth. "Collective memory or the right to be forgotten? Cultures of digital memory and forgetting in the European Union." *Memory Studies* 15.2 2022.: pp257-270.
25. Sun, Xiaoqiang, F. Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. "A survey on zero-knowledge proof in blockchain." *IEEE network* 35, no. 4, 2021.: pp.198-205.
26. Tasatanattakool, Pinyaphat, and Chian Techapanupreeda. "Blockchain: Challenges and applications." In *2018 international conference on information networking (ICOIN)*, IEEE, 2018., pp. 473-475.
27. Tsesis, Alexander. "Data subjects' privacy rights: regulation of personal data retention and erasure." *U. Colo. L. Rev.* 90, 2019.: pp.593.
28. "Blockchain and Data Protection – an FAQ Guide | Perspectives | Reed Smith LLP." *Www.reedsmith.com*, www.reedsmith.com/en/perspectives/2022/11/blockchain-and-data-protection--an-faq-guide. Преузето 12.11.2024.
29. Bray, Oliver. "British Airways Slapped with Biggest Ever Fine for Data Breach." *Lexology*, 15 Jan. 2021, www.lexology.com/library/detail.aspx?g=4a4818a6-2540-4582-81a7-592be99c85b2. Преузето 24.10.2024.
30. Buocz, Thomas, Tina Ehrke-Rabel, Elisabeth Hödl, and Iris Eisenberger "Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks." *Computer Law & Security Review*, vol. 35, no. 2, Apr. 2019, https://doi.org/10.1016/j.clsr.2018.12.003. Преузето 11.11.2024.
31. "Digital Regulatory Sandbox." *European Commission*, 2023, commission.europa.eu/projects/digital-regulatory-sandbox_en. Преузето 12.11.2024.
32. Dingle, Pamela. "ION – We Have Liftoff!" *MICROSOFT.COM*, 25 Mar. 2021, techcommunity.microsoft.com/blog/microsoftsecurityandcompliance/ion-%E2%80%93-we-have-liftoff/1441555. Преузето 31.10.2024.
33. e-Estonia. "E-Democracy & Open Data." *E-Estonia*, e-estonia.com/solutions/e-

governance/e-democracy/. Преузето 30.10.2024.

34. Ekblaw, Ariel. “MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis.” *MIT Media Lab*, 2017, www.media.mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis/. Преузето 29.10.2024.
35. European Commission. “Adequacy Decisions.” *Commission.europa.eu*, commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Преузето 2 Nov. 2024.
36. European Commission . “EPrivacy Regulation | Shaping Europe’s Digital Future.” *Digital-Strategy.ec.europa.eu*, digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation. Преузето 2.11.2024.
37. European Court of Human Rights. *European Convention on Human Rights*. 1950, p. 11, www.echr.coe.int/documents/d/echr/Convention_ENG. Преузето 26.10.2024.
38. European Data Protection Board. “The CNIL’s Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC | European Data Protection Board.” *Www.edpb.europa.eu*, 21 Jan. 2019, www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Преузето 17.10.2024.
39. European Union. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance).” *Europa.eu*, 27 Apr. 2016, eur-lex.europa.eu/eli/reg/2016/679/oj.
40. Evander Pierre. “Enterprise Ethereum Alliance.” *Enterprise Ethereum Alliance*, entethalliance.org/. Преузето 13.11.2024.
41. Frankenfield, Jake. “Ethereum Classic.” *Investopedia*, www.investopedia.com/terms/e/ethereum-classic.asp. Преузето 5.11.2024.
42. Gathecha, James M. “Transforming Industries: VeChain’s Impact on Luxury, Food Safety, and Sustainability.” *Crypto News Flash*, 4 July 2024, www.crypto-news-flash.com/vechains-impact-on-luxury-food-safety-and-sustainability/. Преузето 28.10.2024.
43. Goint, Mongetro, Cyrille Bertelle, and Claude Duvallet “Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems.” *Mathematics*, vol. 11, no. 7, Mar. 2023, https://doi.org/10.3390/math11071592. Преузето 5.11.2024.
44. Goo, Jayoung James, and Joo-Yeun Heo. “The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation.” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 6, no. 2, 2020.
45. Greenspan, Gideon. “Scaling Blockchains with Off-Chain Data | MultiChain.” *Multichain.com*, 13 June 2018, www.multichain.com/blog/2018/06/scaling-blockchains-off-chain-data/. Преузето 6.11.2024.
46. Guan, Zhangshuang, Zhiguo Wan, Yang Yang, Yan Zhou, and Butian Huang. “BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on Zk-SNARKs.” *IEEE Transactions on Dependable and Secure Computing*, 2020, https://doi.org/10.1109/tdsc.2020.3025129. Преузето 10.11.2024.
47. hakia. “Unlocking Innovation: Regulatory Sandboxes for Blockchain & Cryptocurrency.” *Hakia: Covering All Angles of Technology*, 23 Mar. 2022, hakia.com/regulatory-sandboxes-for-blockchain-and-cryptocurrency-innovation/.

Преузето 12.11.2024.

48. Hameed, Khizar, Mutaz Barika, Saurabh Garg, Muhammad Bilal Amin, and Byeong Kang "A Taxonomy Study on Securing Blockchain-Based Industrial Applications: An Overview, Application Perspectives, Requirements, Attacks, Countermeasures, and Open Issues." *Journal of Industrial Information Integration*, vol. 26, Mar. 2022, https://doi.org/10.1016/j.jii.2021.100312. Преузето 10.11.2024.
49. Haque, AKM Bahalul, A.K.M. Najmul Islam, Sami Hyrynsalmi, Bilal Naqvi, and Kari Smolander "GDPR Compliant Blockchains – a Systematic Literature Review." *IEEE Access*, vol. 9, 2021, https://doi.org/10.1109/access.2021.3069877. Преузето 9.11.2024.
50. Hyperledger Foundation. "Hyperledger Fabric." *Lfdecentralizedtrust.org*, The Linux Foundation, 31 July 2023, www.lfdecentralizedtrust.org/projects/fabric. Преузето 12.9.2024.
51. IBM. "IBM Supply Chain Intelligence Suite - Food Trust." *Www.ibm.com*, 2023, www.ibm.com/products/supply-chain-intelligence-suite/food-trust. Преузето 28.10. 2024.
52. "INATBA - International Association for Trusted Blockchain Applications." *INATBA*, 2017, inatba.org/. Преузето 13.11.2024.
53. "Introduction to the Hash Function as a Personal Data Pseudonymisation Technique." *European Data Protection Supervisor*, 2024, www.edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en. Преузето 5.12.2024.
54. Ishai, Yuval, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai "Zero-Knowledge Proofs from Secure Multiparty Computation." *SIAM Journal on Computing*, vol. 39, no. 3, Jan. 2009, pp. 1121–52, https://doi.org/10.1137/080725398. Преузето 5.11.2024.
55. Monero. "Monero: Home." *Getmonero.org, the Monero Project*, 2019, www.getmonero.org/. Преузето 10.11.2024.
56. Nielson, Bryant. "Bridging On-Chain and Off-Chain Worlds: How Decentralized Oracles Work - the Blockchain Academy." *The Blockchain Academy*, Feb. 2024, theblockchainacademy.com/bridging-on-chain-and-off-chain-worlds-how-decentralized-oracles-work/. Преузето 7.11.2024.
57. Ou, Wei, Shiying Huang, Jingjing Zheng, Qionglu Zhang, Guang Zeng, and Wenbao Han "An Overview on Cross-Chain: Mechanism, Platforms, Challenges and Advances." *Computer Networks*, vol. 218, Dec. 2022, https://doi.org/10.1016/j.comnet.2022.109378. Преузето 3.10.2024.
58. Page, Carly. "Marriott Hit with £18.4 Million GDPR Fine over Massive 2018 Data Breach." *Forbes*, 30 Oct. 2020, www.forbes.com/sites/carlypage/2020/10/30/marriott-hit-with-184-million-gdpr-fine-over-massive-2018-data-breach/. Преузето 23.10.2024.
59. Partala, Juha, Tri Hong Nguyen, and Susanna Pirttikangas "Non-Interactive Zero-Knowledge for Blockchain: A Survey." *IEEE Access*, vol. 8, 2020, https://doi.org/10.1109/access.2020.3046025. Преузето 9.11.2024.
60. Politou, Eugenia, Francisco Casino, Efthymios Alepis, and Constantinos Patsakis "Blockchain Mutability: Challenges and Proposed Solutions." *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, 2019, https://doi.org/10.1109/tetc.2019.2949510. Преузето 9.11.2024.
61. Ponomareva, Natalia, Hussein Hazimeh, Alexey Kurakin, Zhen-Liang Xu, Carson Denison, McMahan H Brendan, Sergei Vassilvitskii, Steve Chien, and Abhradeep

Thakurta “How to DP-Fy ML: A Practical Guide to Machine Learning with Differential Privacy.” *Journal of Artificial Intelligence Research*, vol. 77, AI Access Foundation, July 2023, pp. 1113–201, https://doi.org/10.1613/jair.1.14649. Преузето 5.11.2024.

62. Poston, Howard. “Blockchain and Asymmetric Cryptography | Infosec.” *Infosecinstitute.com*, 2021, www.infosecinstitute.com/resources/cryptography/blockchain-and-asymmetric-cryptography/. Преузето 4.12.2024.
63. “Privacy-Protecting Digital Currency | Zcash.” *Zcash*, z.cash/. Преузето 10.11.2024.
64. Proskurovska, Anetta, and Sabine Dörry. “The Blockchain Challenge for Sweden’s Housing and Mortgage Markets.” *Environment and Planning A: Economy and Space*, Aug. 2022, p. 0308518X2211168, https://doi.org/10.1177/0308518x221116896. Преузето 30.10.2024.
65. Ripple. “Cross-Border Payment Settlement Solution | Ripple.” *Ripple.com*, ripple.com/solutions/cross-border-payments/. Преузето 30.10.2024.
66. “Russia Is Weaponizing Its Data Laws against Foreign Organizations.” *Brookings*, www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/. Преузето 2.11.2024.
67. Shoukat, Ijaz Ali, Kamalrulnizam Abu Bakar, and Subariah Ibrahim “A Generic Hybrid Encryption System (HES).” *Research Journal of Applied Sciences, Engineering and Technology*, vol. 5, no. 9, Mar. 2013, https://doi.org/10.19026/rjaset.5.4793. Преузето 9.11.2024.
68. Team, Chainalysis. “Asset Tokenization Explained.” *Chainalysis*, 22 Mar. 2024, www.chainalysis.com/blog/asset-tokenization-explained/. Преузето 9.10.2024.
69. Uzougbo, Ngozi Samuel, Chinonso Gladys Ikegwu, and Adefolake Olachi Adewusi. "International enforcement of cryptocurrency laws: jurisdictional challenges and collaborative solutions." *Magna Scientia Advanced Research and Reviews* 11.1 2024.: pp.68-83.
70. Voigt, Paul, and Axel von Dem Bussche. *The EU General Data Protection Regulation (GDPR) a Practical Guide*. Cham Springer International Publishing, 2017.
71. Wang, Xiaojie, et al. “A Survey on Off-Chain Networks: Frameworks, Technologies, Solutions and Challenges.” *ArXiv.org*, 2023, arxiv.org/abs/2311.10298. Преузето 8.11.2024.
72. “What Is Homomorphic Encryption? - Chainlink.” *Chain.link*, chain.link/education-hub/homomorphic-encryption. Преузето 9.11.2024.
73. Wolford, Ben. “Everything You Need to Know about the ‘Right to Be Forgotten.’” *GDPR.eu*, 5 Nov. 2018, gdpr.eu/right-to-be-forgotten/. Преузето 24.10.2024.
74. Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078*, 2019.
75. Zhang, Ce, Cheng Xu, Haixin Wang, Jianliang Xu, and Byron Choi *Authenticated Keyword Search in Scalable Hybrid-Storage Blockchains*. Apr. 2021, https://doi.org/10.1109/icde51399.2021.00091. Преузето 8.11.2024.
76. Zhang, Yuhang, Jun Wang, and Jie Luo “Heuristic-Based Address Clustering in Bitcoin.” *IEEE Access*, vol. 8, 2020, https://doi.org/10.1109/access.2020.3039570. Преузето 4.11.2024.

IX. САЖЕТАК И КЉУЧНЕ РЕЧИ

Овај мастер рад истражује правне и техничке изазове усклађивања блокчејн технологије са Општом уредбом о заштити података (ГДПР), са посебним освртом на право на заборав. Главни циљ истраживања је анализа сукоба између непроменљивости података, као једне од основних карактеристика блокчејн технологије, и права на брисање, које је загарантовано чланом 17 ГДПР-а. Рад такође настоји да идентификује могућа решења за премошћавање овог сукоба, кроз техничке иновације и прилагођавање правног оквира.

Методологија рада обухвата анализу релевантних правних докумената, укључујући текст ГДПР-а и судске одлуке које га тумаче, као и техничких аспеката блокчејн архитектуре. Примарни фокус је на примену правних принципа на специфичности блокчејн система, уз разматрање глобалног контекста усклађивања регулатива са технолошким иновацијама.

Резултати истраживања указују да иако блокчејн и ГДПР делују као концептуално супротстављени оквири, постоје техничке и правне мере које могу омогућити њихову коегзистенцију. Техничка решења, попут складиштења ван ланца, псеудонимизације, криптографског брисања и коришћења доказа са нултим знањем (zero-knowledge proofs), омогућавају делимично усклађивање блокчејн система са захтевима ГДПР-а. Правна прилагођавања, као што су изузеци за одређене типове података или успостављање нових регулаторних смерница за децентрализоване системе, могу додатно ублажити регулаторне сукобе.

Закључено је да је неопходна сарадња између технолошких стручњака, законодаваца и регулатора како би се постигла равнотежа између приватности корисника и функционалности блокчејн технологије. Успешна примена ових решења могла би омогућити да се искористи пуни потенцијал блокчејн технологије, уз очување основних права на приватност.

Кључне речи: блокчејн, ГДПР, право на заборав, псеудонимизација, децентрализација, криптографско брисање

SUMMARY AND KEY WORDS

Harmonizing Blockchain Technology with GDPR: Legal and Technical Challenges of the Right to Be Forgotten

This master's thesis explores the legal and technical challenges of aligning blockchain technology with the General Data Protection Regulation (GDPR), with a specific focus on the right to be forgotten. The primary objective of the research is to analyze the conflict between data immutability, a fundamental feature of blockchain, and the right to erasure guaranteed by Article 17 of GDPR. Additionally, the study seeks to identify potential solutions to bridge this gap through technical innovations and legal adaptations.

The methodology includes a review of relevant legal documents, such as GDPR provisions and judicial interpretations, and an examination of the technical aspects of blockchain architecture. The research primarily applies legal principles to the unique characteristics of blockchain systems, while also considering the global context of regulatory alignment with technological advancements.

The findings indicate that, despite the conceptual opposition between blockchain and GDPR, technical and legal measures can enable their coexistence. Technical solutions such as off-chain storage, pseudonymization, cryptographic erasure, and zero-knowledge proofs provide partial compliance pathways. Legal adjustments, including exceptions for certain data types or the establishment of new regulatory guidelines for decentralized systems, can further mitigate conflicts.

The thesis concludes that collaboration among technologists, legislators, and regulators is essential to balance user privacy with blockchain functionality. Implementing these solutions can harness the full potential of blockchain technology while preserving fundamental privacy rights.

Keywords: blockchain, GDPR, right to be forgotten, pseudonymization, decentralization, cryptographic erasure

X. БИОГРАФИЈА

Иван Јанковић рођен је 2. октобра 1987. године у Нишу. Основно и средње образовање стекао је у родном граду, након чега је наставио студије у иностранству. Од 2008. до 2011. године студирао је на Webster University у Женеви, Швајцарска, а 2012. године дипломирао је међународни менаџмент на истом универзитету у Бечу, Аустрија.

Своје академско усавршавање наставио је на мастер студијама Правног факултета Универзитета у Нишу, где је 2024. године завршио постдипломске студије из области "Право и информационе технологије" са средњом оценом 10.

Иван течно говори енглески језик, што је потврдио добијањем Toefl сертификата. Поседује конверзацијски ниво француског језика.

Од 2019. године ради као консултант за швајцарску банку Dukascopy Bank у Женеви, са посебним фокусом на развој блокчејн технологија и паметних уговора. Такође је сувласник компаније Orcas Group у Дижону, Француска, од 2017. године. У оквиру свог рада, Иван је активно учествовао у имплементацији прве дигиталне валуте у оквиру званичне швајцарске банке, као и у усклађивању регулативе са захтевима FINMA, швајцарског регулаторног тела за финансијске институције.

Његово стручно знање обухвата развој блокчејн технологија, пројектовање паметних уговора и примену савремених информационих технологија у финансијском и правном сектору.

ИЗЈАВА О ИСТОВЕТНОСТИ
ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Иван Јанковић

Наслов мастер рада: Усклађивање Блокчејн технологије са ГДПР: Правни и технички изазови права на заборав

Ментор: проф. др Предраг Цветковић

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, 10.01.2025.

Потпис аутора

_____

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом „Усклађивање Блокчејн технологије са ГДПР: Правни и технички изазови права на заборав “
пријављен и одбрањен на Правном факултету Универзитета у Нишу:
• резултат сопственог истраживачког рада;
• да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;
• да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: Иван Јанковић

У Нишу, 10.01.2025.

Потпис аутора

_____