https://doi.org/10.22364/juzk.77.12

BLOKĶĒDES KRIMINĀLTIESISKĀS AIZSARDZĪBAS ASPEKTI

CRIMINAL LAW ISSUES REGARDING LEGAL PROTECTION OF BLOCKCHAIN

Juris Janums, *Mg. iur.*
Latvijas Universitātes Juridiskās fakultātes doktorants

Summary

Considering the significant use of blockchain technology in the field of cryptocurrency, smart contracts and financial services, the author provides definition of blockchain and characterisation of the threats associated with its operation, and examines whether they are protected by Criminal Law. Thus, the publication identifies two main threats related to the operation of the blockchain and the associated individual offenses in the Criminal Law, and finds certain deficiencies in the legal protection of the blockchain in Criminal Law.

Atslēgvārdi: blokķēde, krimināltiesības, datornoziegumi

Keywords: blockchain, criminal law, cybercrimes

Ievads

Kas kopīgs virtuālajai valūtai (kriptovalūtai), vieddarījumiem (angļu val. – *smart contract*) un finanšu pakalpojumu uzskaites sistēmām? Atbilde – blokķēde. Lielākajā interneta vietnē *coinmarketcap.com* tiešsaistē iespējams sekot līdzi vairāk nekā 2000 kriptovalūtu vērtību svārstībām, un dati liecina, ka kopējā kriptovalūtu tirgus vērtība 2019. gada martā sasniegusi jau vairāk nekā 120 miljardus eiro.[1] Vienlaikus Starptautiskais Valūtas fonds savā 2016. gada janvāra pētījumā bija pievērsis uzmanību vieddarījumiem kā potenciālai nākotnes darījumu formai.[2] Savukārt starptautiskā informācijas tehnoloģiju korporācija *International Business Machines Corporation* 2016. gada septembrī informēja, ka globālās bankas un citas finanšu institūcijas ievieš blokķēdes tehnoloģiju ievērojami ātrāk, nekā sākotnēji bija iecerēts.[3] Līdz ar to, ņemot vērā ievērojamo blokķēdes tehnoloģijas pielietojumu kriptovalūtā, vieddarījumos un finanšu pakalpojumos, kā arī citās sfērās, rodas jautājums, – vai Krimināllikumā (turpmāk – KL) ietverta attiecīgi

[1] Cryptocurrencies by Market Capitalization. Pieejams: https://coinmarketcap.com/ [aplūkots 24.03.2019.].

[2] IMF staff discussion note. Virtual Currencies and Beyond: Initial Considerations. January, 2016, SDN/16/03. Pieejams: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf [aplūkots 24.03.2019.].

[3] Kelly J. Banks adopting blockchain 'dramatically faster' than expected: IBM. Pieejams: https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D [aplūkots 24.03.2019.].

nepieciešamā krimināltiesiskā aizsardzība? Lai atbildētu uz šo jautājumu, autors publikācijā piedāvā aplūkot šķietami neviennozīmīgo blokķēdes jēdzienu un divus ar blokķēdi saistītos apdraudējuma gadījumus, proti, vienu, kas ir tieši saistīts ar blokķēdes pastāvēšanas apdraudējumu, un otru, kas ir tieši saistīts ar blokķēdes lietojumu. Visbeidzot, aplūkojot iepriekš minētos gadījumus un atsevišķus KL ietvertos noziedzīgā nodarījuma sastāvus, autors konstatē noteiktus trūkumus blokķēdes tiesiskajā aizsardzībā KL.

1. Blokķēdes jēdziens

Viens no izplatītākajiem blokķēdes tehnoloģijas pielietojumiem ir kriptovalūta.[4] Tā juridiskajā literatūrā ir atzīts, ka "kriptovalūta ir prece ar noteiktu vērtību, kas vienlaikus ir arī maiņas līdzeklis, kas ar kriptogrāfijas metodēm šifrētā veidā pastāv blokķēdē datorsistēmu atmiņā".[5] Savukārt kriptovalūtas legāldefinīcijā Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likuma 1. panta grozījumu 2.[2] punktā blokķēde vispār pat nav pieminēta, tā vietā skaidrojot kriptovalūtu kā "vērtības digitāl[u] atspoguļojum[u], kas var būt digitāli nosūtīts, glabāts vai tirgots un funkcionē kā apmaiņas līdzeklis, bet nav atzīts par likumīgu maksāšanas līdzekli, nav uzskatāms par banknoti un monētu, bezskaidru naudu un elektronisko naudu, kā arī nav monetārā vērtība, kura uzkrāta maksājuma instrumentā, kas tiek izmantots Maksājumu pakalpojumu un elektroniskās naudas likuma 3. panta 10. un 11. punktā minētajos gadījumos".[6] Taču, aplūkojot gan juridiskajā literatūrā piedāvāto definīciju, gan legāldefinīciju, rodas jautājums, kas ir blokķēde, kur vērtības digitālo atspoguļojumu var digitāli nosūtīt.

Tā Latvijas Zinātņu akadēmijas Terminoloģijas komisijas Informācijas tehnoloģijas, telekomunikācijas un elektronikas terminoloģijas apakškomisija 2017. gada 2. jūnijā (prot. Nr. 499) oficiāli ir atzinusi terminu "blokķēde", saistot to ar angļu valodas terminu *blockchain*, kas aizgūts no informācijas tehnoloģiju kompānijas *Microsoft Corporation* terminoloģijas datubāzes:[7] "blokķēde ir datu struktūra, kas tiek izmantota, lai izveidotu digitālo darījumu virsgrāmatu, kas tā vietā, lai būtu pakļauta vienam avotam, tiek kopīgi izvietota izkliedētā datoru tīklā. Rezultāts ir atvērtāka, pārredzamāka un publiski pārbaudāma sistēma digitālajiem darījumiem".[8]

Savukārt, ielūkojoties Eiropas Savienības terminoloģijas sistēmā *IATE* (*iate.europa.eu*), redzam, ka jēdziena *blockchain* skaidrojums aizgūts no *Oxford* skaidrojošās vārdnīcas – "blokķēde ir sistēma, kurā ieraksta ar bitkoinu (*bitcoin*) vai citu

[4] Blockchain Top Trends in 2017. Pieejams: https://channels.theinnovationenterprise.com/articles/blockchain-top-trends-in-2017 [aplūkots 24.03.2019.].

[5] Janums J. Jaunas kriptovalūtas emisija un tās kolektīvās finansēšanas krimināltiesiskie aspekti. Grām.: LU 76. starptautiskās zinātniskās konferences rakstu krājums. Rīga: Latvijas Universitāte, 2018, 417. lpp.

[6] Grozījumi Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likumā: LV likums. 26.10.2017. Pieejams: https://likumi.lv/ta/id/294868-grozijumi-noziedzigi-iegutu-lidzeklu-legalizacijas-un-terorisma-finansesanas-noversanas-likuma [aplūkots 24.03.2019.].

[7] LZA terminu datubāze AkadTerm. Pieejams: http://termini.lza.lv/term.php?term=blokķēde&list=blokķēde &lang=LV [aplūkots 24.03.2019.].

[8] Ibid.

kriptovalūtu veiktos darījumus, kas glabājas vairākos datoros, kuri ir savstarpēji saistīti vienādranga tīklā".[9]

Savu skaidrojumu jēdzienam "blokķēde" piedāvā arī Eiropas Savienības Tīklu un informācijas drošības aģentūra, proti: "Blokķēžu tehnoloģija ir saistīta ar publisku reģistru, kurā tiek uzglabāta informācija par visiem darījumiem, kas ir veikti vienādranga tīklā. Tā ir decentralizēta tehnoloģija, kas viena ranga tīklu dalībniekiem ļauj veikt darījumus, piemēram, tiešsaistes maksājumus, neizmantojot uzticamas centrālas iestādes ("starpnieka") pakalpojumus."[10]

Tādējādi, jau aplūkojot vien trīs dažādus avotus, pirmšķietami saskatāmas atšķirības blokķēdes skaidrojumā. Tomēr, salīdzinot šos skaidrojumus, redzam – lai arī tie ir dažādi, tomēr to saturs ietver būtiskākās blokķēdes pazīmes, proti:

1) strukturēta datu sistēmas uzbūve (reģistrs vai virsgrāmata);
2) satur ziņas par divpusējiem vai daudzpusējiem darījumiem (tai skaitā *bitcoin*, kriptovalūtu u. c. darījumiem);
3) glabājas vienādranga izkliedētā datoru tīklā (*Peer-to-peer*).

Līdz ar to var izdarīt secinājumu, ka blokķēdes skaidrojumu neviennozīmīgums ir šķietams un ka, identificējot noteiktas pazīmes, ir iespējams konstatēt, kas ir blokķēde.

Vienlaikus tiesiskās noteiktības labad nākotnē būtu nepieciešams izstrādāt vienotu legāldefinīciju, jo aplūkotajiem blokķēdes skaidrojumiem ir katram savas īpatnības, proti:

1) Latvijas Zinātņu akadēmijas termins ir savā ziņā universāls, jo nesaista blokķēdi tikai ar kriptovalūtu, atstājot jēdzienā vietu inovācijām – tas ir, citiem blokķēdes pielietojumu veidiem;
2) Eiropas Savienības Tīklu un informācijas drošības aģentūras skaidrojums ietver apgalvojumu, ka darījumu apstrādē uzticama ir tikai tāda darījumu sistēma, kurā ir viena centrālā iestāde, taču tas vienlaikus ir pretrunā ar blokķēdes decentralizēto raksturu, kur drošība tiek garantēta, pamatojoties nevis uz centrālo autoritāti, bet gan uz pašu informācijas uzglabāšanas veidu – šifrētu informāciju, gan publisku ticamību, ko ikviens var pārbaudīt, publiski redzot, kā blokķēdē tiek reģistrēti visi darījumi;
3) Oksfordas vārdnīcas skaidrojums, savukārt, ir par šauru, jo apraksta blokķēdi vien kā ar kriptovalūtas darījumiem saistītu uzskaites sistēmu, taču tam var saskatīt zināmu pamatu, proti, tas ir pietuvināts blokķēdes autoru viedoklim, kuri paši savā darbā blokķēdi sauc par "*Bitcoin*: vienādranga elektroniskās naudas sistēmu".[11]

2. Ar blokķēdes darbību saistītie apdraudējumi

2.1. Blokķēdes pastāvēšanas apdraudējumi

Kā pirmo blokķēdes pastāvēšanas apdraudējumu blokķēdes tehnoloģijas izstrādātāji min nevis pašas izkliedētās datu glabāšanas sistēmas graušanu, bet gan tās

[9] Oxford dictionaries. Pieejams: https://en.oxforddictionaries.com/definition/blockchain [aplūkots 24.03.2019.].

[10] The European Union Agency for Network and Information Security (ENISA): Blockchain. Pieejams: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/blockchain [aplūkots 24.03.2019.].

[11] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Pieejams: https://bitcoin.org/bitcoin.pdf [aplūkots 24.03.2019.].

pastāvēšanai nepieciešamās infrastruktūras apdraudējuma riskus.[12] Proti, kā jau norādīts iepriekš – viena no blokķēdes pazīmēm ir tā, ka sistēma glabā datus decentralizēti vienādranga izkliedētā datoru tīklā, līdz ar to – apdraudot tīkla darbību un tajā esošo datoru darbību, it sevišķi to pieejamību datoru tīklam, tiek apdraudēta arī pati blokķēde. Tāpat blokķēdes sistēmas darbībai ir nepieciešama stabila datoru darbība, tātad arī pašu blokķēdes tīkla datoru darbība pati par sevi ir apdraudējuma objekts.

Tādējādi, vērtējot blokķēdes pastāvēšanas apdraudējuma riskus, ir jāanalizē ar to saistītā datoru un datoru tīklu tiesiskā aizsardzība.

2.2. Apdraudējumi saistībā ar blokķēdes lietojumu

Otrs apdraudējuma gadījums, savukārt, ir juridiski ievērojamāks, jo ir tieši saistīts ar blokķēdes pielietojumu, piemēram, kriptovalūtā vai kādā blokķēdē esoša finanšu pakalpojuma gadījumā (piemēram, bankas klientu depozītu kontu un darījumu uzskaites sistēma).

Tā ekspertu publikācijās internetā aprakstīti šādi apdraudējumi saistībā ar blokķēdes lietojumu:[13]

1) drošajā blokķēdē – secīgā darījumu ieraksta sistēmā – tiek ierakstīts nelikumīgs darījums, ar to saprotot gan tādus darījumus, kuru priekšmets nav atļauts, piemēram, narkotiku iegādi par kriptovalūtu *Dark Net* (tumšais tīkls – vienādranga datoru tīkls ar savstarpēji ierobežotu un anonīmu piekļuvi),[14] vai ar noziedzīgi iegūtu līdzekļu legalizāciju saistītus darījumus, gan tādus darījumus, kuru pamatā ir bijusi, piemēram, krāpšana, piesavināšanās u. c. prettiesiskas darbības;
2) kādus datus un cik plaši izkliedētā datoru tīklā glabāt.

Pievēršot uzmanību pirmajam punktam, zināmas paralēles attiecībā uz nelikumīgiem darījumiem varam vilkt ar 2017. gada 8. marta Satversmes tiesas spriedumu lietā Nr. 2016-07-01 "Par Kriminālprocesa likuma 356. panta otrās daļas un 360. panta pirmās daļas atbilstību Latvijas Republikas Satversmes 1. pantam, 91. panta pirmajam teikumam, 92. un 105. pantam",[15] kur tika secināts, ka tobrīd attiecīgais Kriminālprocesa likuma regulējums par mantas labticīga ieguvēja aizsardzības principa ierobežojumu atbilst Satversmei, tādējādi faktiski atzīstot, ka labticīgā ieguvēja institūts nav absolūts. Taču blokķēdē, saglabājot gan darījumus saistībā ar kriptovalūtu, gan vieddarījumus, gan jebkuru citu darījumu, visi darījumi tiks saglabāti neatkarīgi no to juridiskā rakstura – labticīgi vai nelabticīgi. No vienas puses, šāda pieeja garantē darījumu drošumu un uzticību, bet, no otras puses, nepieļauj iespēju izslēgt no blokķēdes nelabticīgu darījuma ierakstu, jo blokķēdi (sistēmu) ir iespējams tikai papildināt ar jaunu ierakstu par nākamo darījumu. Šo problēmu gan var novērst ar vieddarījumu palīdzību, paredzot, ka

[12] Bitcoin Developer Guide. Pieejams: https://bitcoin.org/en/developer-guide [aplūkots 24.03.2019.].

[13] Iesalnieks K. Blokķēdes tehnoloģija – mīti un patiesība par kriptorevolūciju. Pieejams: https://www.delfi.lv/news/versijas/kaspars-iesalnieks-blokkedes-tehnologija-miti-un-patiesiba-par-kriptorevoluciju.d?id=49522737 [aplūkots 24.03.2019.].

[14] Šķirklis "darknet". LZA terminu datubāze AkadTerm. Pieejams: http://termini.lza.lv/term.php?term=darknet&lang=EN, arī https://en.oxforddictionaries.com/definition/darknet [aplūkots 24.03.2019.].

[15] Satversmes tiesas spriedums lietā Nr. 2016-07-01. Pieejams: www.satv.tiesa.gov.lv/wp-content/uploads/2016/05/2016-07-01_Spriedums-1.pdf [aplūkots 24.03.2019.].

sistēmā netiek veikts ieraksts par darījumu, kuram nav norādīts darījuma priekšmets un kura priekšmets ir acīmredzami prettiesisks.

Savukārt, pievēršot uzmanību otrajam punktam, pamatoti būtu uzdot jautājumu, kā uz blokķēdē glabātiem datiem varētu attiecināt, piemēram, Vispārīgo datu aizsardzības regulu[16] vai KL 145. pantā paredzēto noziedzīgā nodarījuma sastāvu, ņemot vērā blokķēdes tehnoloģijas pazīmi, ka visi dati tiek glabāti izkliedētā vienādranga datoru tīklā, kurš parasti ir starptautiska mēroga datortīkls. Tajā pašā laikā arī šeit ar vieddarījumu palīdzību varētu paredzēt nepieciešamību iegūt piekrišanu datu apstrādei un šādu piekrišanu uzglabāt blokķēdē līdztekus attiecīgā vieddarījuma ierakstam. Te gan uzreiz rodas jautājums, vai šāds tīkls varētu būt neierobežoti plašs, jo atbilstoši Vispārīgo datu aizsardzības regulai personai jābūt nepārprotami skaidri saprotamam, kur atrodas viņas dati, taču blokķēdes gadījumā – pagaidām datoru tīklā, ja vien attiecīgais tīkls nav izolēts, var iesaistīties ikviens. Tomēr, izmantojot šifrēšanu, noteiktu datu daļu var arī neatklāt, to pieļauj kriptogrāfijas metodes, kuras izmanto kriptovalūtas darījumu šifrēšanā. Tādējādi no krimināltiesību skatpunkta šajā aspektā mūs interesētu ar mantu saistītie jautājumi un satura aizsardzības regulējums.

3. Blokķēdes darbības krimināltiesiskā aizsardzība

Ņemot vērā aplūkotos ar blokķēdes darbību saistītos apdraudējuma gadījumus, ar blokķēdes darbību saistīto interešu aizsardzības jomā Krimināllikumā galvenokārt varam analizēt četras noziedzīgu nodarījumu grupas.

3.1. Noziedzīgi nodarījumi pret personas pamattiesībām un pamatbrīvībām

Vērtējot, kādus datus un cik plaši izkliedētā datoru tīklā glabāt, kā arī kādā veidā tos pārsūtīt un glabāt, būtu jāņem vērā gan KL 144. pants, kurā paredzēta kriminālatbildība, ja pārkāpts pa elektronisko sakaru tīkliem pārraidāmās informācijas noslēpums, gan KL 145. pantā paredzētā fiziskas personas datu apstrādes aizsardzība. Tā autors jau iepriekšējā nodaļā iezīmēja izaicinājumus saistībā ar Vispārīgo datu aizsardzības regulu[17] un ar to saistīto KL 145. pantu. Tāpat varētu uzdot jautājumu, vai KL 144. panta priekšmets aptver arī tādus datus kā patērētāja paradumi, piemēram, latviešu uzņēmēju jaunuzņēmums *Monetizr*, kas reģistrēts ASV, glabā blokķēdē datus par datorspēļu spēlētāju spēļu paradumiem ASV, lai šo informāciju piedāvātu datorspēļu izplatītājiem un veidotājiem;[18] tas attiecas arī uz datiem par vēlētāju politiskajiem uzskatiem, kā tas notika skandalozajā *Cambridge Analytica* gadījumā,[19] kad šāda informācija tika neatļauti nodota politisko konsultāciju uzņēmumiem.

---

[16] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula). Pieejams: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32016R0679 [aplūkots 24.03.2019.].

[17] Ibid.

[18] Zoldnere T. Latvieši Silīcija ielejā: ar blokķēdes tehnoloģiju pēta datorspēlētājus. Pieejams: https://www.delfi.lv/bizness/tehnologijas/latviesi-silicija-ieleja-ar-blokkedes-tehnologiju-peta-datorspeletajus.d?id=50818225 [aplūkots 24.03.2019.].

[19] Ted Cruz using firm that harvested data on millions of unwitting Facebook users. Pieejams: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data [aplūkots 24.03.2019.].

3.2. Noziedzīgi nodarījumi pret īpašumu

Ņemot vērā to, ka blokķēdē var tikt glabāta gan manta – kriptovalūta, gan arī tiesības uz šādu mantu, ir pamats aplūkot KL 175. pantā paredzēto zādzības regulējumu, KL 177. pantā paredzēto krāpšanas regulējumu, KL 177.[1] pantā paredzēto regulējumu par krāpšanu automatizētā datu apstrādes sistēmā, kā arī KL 179. pantā paredzēto regulējumu par piesavināšanos. Tā, piemēram, blokķēdi un tās ierakstus nav iespējams nozagt, tādēļ uz to nebūtu attiecināms KL 175. pantā paredzētais zādzības sastāvs. Līdzīgi blokķēdes tehnoloģijas būtība izslēdz nepatiesu datu ievadi, lai ietekmētu blokķēdi, jo blokķēdes sistēma pieļauj veikt ierakstu tikai pēc tam, kad automatizēta sistēma ir pārliecinājusies par datu patiesumu, līdz ar to KL 177.[1] pantā paredzētā datorkrāpšana pēc būtības uz blokķēdi pat nav attiecināma. Savukārt, ņemot vērā, ka ir nepieciešama šifrēšanas atslēga, lai reģistrētu ierakstu par darījumu veikšanu blokķēdē – to var uzskatīt par piekļuves tiesībām katram konkrētam ierakstam –, pamatoti varētu runāt par krāpšanu. Te gan vietā ir jautājums par finanšu identitātes zādzību un tās kopību ar krāpšanu (KL 177. p.). Tāpat var runāt par krāpšanu arī attiecībā uz sistēmas uzturētājiem, kas "rokot" uztur blokķēdi, piemēram, kompānija *BitFury*, kura par "rakšanu" saņem atlīdzību kriptovalūtā un kuras uzņēmuma vērtība ir 400 miljoni ASV dolāru[20] (KL 177. p.). Visbeidzot, līdzīgi kā par krāpšanu, var runāt arī par piesavināšanos, piemēram, no šifrēšanas atslēgu pakalpojumu sniedzēju puses (KL 179. p.).[21]

3.3. Noziedzīgi nodarījumi finanšu un kredīta sfērā

Lai arī attiecībā uz kriptovalūtu likumdevējs ir nepārprotami noteicis, ka tā nav uzskatāma par likumīgu maksāšanas līdzekli, bet ir vērtības noteikts atspoguļojums, KL izpratnē varētu izvērst diskusiju par blokķēdē glabātās kriptovalūtas kā par KL 193. panta sastāva priekšmetu, jo, kā zināms, ar kriptovalūtu, tāpat kā ar legāli definēto maksāšanas līdzekli, var norēķināties par precēm un pakalpojumiem. Turklāt šeit apspriešanas vērts būtu jautājums arī par darbībām ar blokķēdē esošajiem datiem kā tādiem, un pamatoti būtu uzdot jautājumu: vai tāpat kā zādzība, arī maksāšanas līdzekļa nolaupīšana no blokķēdes būtu reāli iespējama vai tai būtu atšķirīga objektīvā izpausme. Tāpat būtu pamatoti uzdot jautājumu par KL 193.[1] pantu – attiecībā uz datu, programmatūras un iekārtu iegūšanu, izgatavošanu, izplatīšanu, izmantošanu un glabāšanu nelikumīgām darbībām ar finanšu instrumentiem un maksāšanas līdzekļiem, ievērojot jautājumu par piekļuves datu ieguvi ne tikai attiecībā uz kriptovalūtas maciņu ar šifrēšanas atslēgām, bet arī uz programmatūru, kas vērsta uz blokķēdes sistēmas graušanu, radīšanu un šajā gadījumā attiecīgu normu konkurenci ar KL 244. pantā paredzēto noziedzīgā nodarījuma sastāvu.

3.4. Noziedzīgi nodarījumi informācijas sistēmu drošības jomā

Visbeidzot, tā kā apdraudējuma objekts ir informācijas sistēmu drošība, analizējot blokķēdes darbības apdraudējumus, ir pamatoti runāt par KL 241. pantā paredzēto patvaļīgo piekļūšanu automatizētai datu apstrādes sistēmai, KL

[20] Bitcoin company made by Rigans valued at $400m. Pieejams: https://eng.lsm.lv/article/economy/economy/bitcoin-company-made-by-rigans-valued-at-400m.a261722/ [aplūkots 24.03.2019.].

[21] Janums J. 2018, 417. lpp.

243. pantā paredzēto automatizētas datu apstrādes sistēmas darbības traucēšanu un nelikumīgu rīcību ar šajā sistēmā iekļauto informāciju, KL 244. pantā paredzētajām nelikumīgām darbībām ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm, KL 244.[1] pantā paredzēto datu, programmatūras un iekārtu iegūšanu, izgatavošanu, izmainīšanu, glabāšanu un izplatīšanu, nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām, kā arī KL 245. pantā paredzēto informācijas sistēmas drošības noteikumu pārkāpšanu. It īpaši jāņem vērā, kādai informācijas tehnoloģiju arhitektūrai un nozares noteikumiem attiecīgās normas tika izstrādātas un vai tās būs iespējams attiecināt uz blokķēdi, kas ir izkliedēta, vienādranga datoru tīklā esoša sistēma, kamēr KL attiecīgo normu izstrādes laikā pamatā varējām runāt par centralizētu (pretēju izkliedētai) sistēmu vai pat par atsevišķu datoru aizsardzību.

Kopsavilkums

1. Blokķēdes jēdziena atšķirīgie skaidrojumi dažādos terminoloģijas avotos ir vien šķietami neviennozīmīgi, jo pēc būtības atbilst blokķēdes autoru darbā aprakstītajai vienādranga datoru tīklu elektroniskās naudas sistēmai *Bitcoin*.
2. Blokķēdi kā automatizētu datu apstrādes sistēmu ļauj identificēt šādas pazīmes:
   1) strukturēta datu sistēmas uzbūve (reģistrs vai virsgrāmata);
   2) satur ziņas par divpusējiem vai daudzpusējiem darījumiem (tai skaitā *bitcoin*, kriptovalūtu u. c. darījumiem);
   3) glabājas vienādranga izkliedētā datoru tīklā (*Peer-to-peer*).
3. Apdraudot tīkla (iekārtu) darbību un tajā esošo datoru darbību, it sevišķi gan to pieejamību datoru tīklam, gan tehnisko darbību, tiek apdraudēta arī pati blokķēde.
4. Saistībā ar blokķēdes lietojumu pastāv draudi, ka blokķēdē tiek ierakstīts nelikumīgs (neatļauts) darījums, kā arī nav skaidrs, vai un kādus datus un cik plašā datoru tīklā pieļaujams glabāt saskaņā ar attiecīgo jurisdikciju regulējumu.
5. Blokķēdēs pie darījumu ierakstīšanas nav paredzēts vērtēt, vai tie ir labticīgi un vai šo darījumu priekšmets ir likumīgs, taču *vieddarījumu* gadījumā to būtu iespējams veikt automatizēti.
6. Atsevišķi Krimināllikumā paredzētie noziedzīgā nodarījuma sastāvi, kuros paredzēta ar blokķēdes darbību saistītu interešu aizsardzība, nav piemērojami, jo tajos ietvertās objektīvās puses pazīmes nav piemērojamas attiecībā uz blokķēdes tehnoloģiju (normas ir novecojušas).
7. Blokķēdē ierakstītā vērtība būtu atzīstama par maksāšanas līdzekli Krimināllikuma 193. panta izpratnē.