**Informatīvais ziņojums**

**“****Par** **blokķēdes tehnoloģijas izmantošanas piemēriem, perspektīvām un tālāko rīcību jomas attīstības veicināšanai”**

Lai izpildītu Ministru kabineta (turpmāk - MK) 2018. gada 14. augusta sēdes protokola Nr. 38 48. § 5. punktu, Ekonomikas ministrija (turpmāk – EM) ir izstrādājusi informatīvo ziņojumu “Par blokķēdes tehnoloģijas izmantošanas piemēriem, perspektīvām un tālāko rīcību jomas attīstības veicināšanai” (turpmāk – informatīvais ziņojums). Tā mērķis ir padziļināti izvērtēt blokķēdes (ang. *blockchain*) tehnoloģijas izmantošanas perspektīvas publiskajā sektorā, identificēt turpmāko rīcību tās attīstības veicināšanai Latvijā, kā arī izvērtēt ar blokķēdes tehnoloģiju saistītos juridiskos un tehnoloģiskos aspektus un līdz 2019. gada 1.janvārim iesniegt izskatīšanai MK. Lai izpildītu iepriekš minēto un apkopotu priekšlikumus blokķēdes tehnoloģijas izmantošanai publiskajā sektorā, izveidota darba grupa (EM 12.10.2018. rīkojums Nr. 3.7-1\_2018\_24), kurā pārstāvēti eksperti no EM, Finanšu ministrijas (turpmāk – FM), Latvijas Bankas (turpmāk – LB), Latvijas Investīciju un attīstības aģentūras (turpmāk – LIAA), Valsts ieņēmumu dienesta (turpmāk – VID), Vides aizsardzības un reģionālās attīstības ministrijas (turpmāk – VARAM), nepieciešamības gadījumā piesaistot citu atbildīgo ministriju, kā arī nozaru asociāciju un uzņēmumu pārstāvjus. Darba grupas ietvaros sagatavotie priekšlikumi turpmākai rīcībai saistībā ar blokķēdes tehnoloģijas plašākām izmantošanas iespējām valsts pārvaldes pakalpojumu efektivitātes un drošības uzlabošanā, aktivitātēm, kas veicinātu tehnoloģijas izmantošanu privātajā sektorā, kā arī identificētās barjeras un sagatavotie priekšlikumi pasākumiem tehnoloģijas atbalstam apkopoti informatīvajā ziņojumā.

2018.gada 10. aprīlī Eiropas Komisija (turpmāk – EK) Digitalizācijas dienas ietvaros[[1]](#footnote-1) parakstīja Blokķēdes partnerības deklarāciju, kas paredz sabiedrības informēšanu un sapratnes veicināšanu par blokķēdes tehnoloģiskajām iespējām, lai veicinātu Eiropas Savienības (turpmāk – ES) kā reģiona konkurētspēju. Atbilstoši šīs deklarācijas 3. nodaļas 7. punktam gan EM, gan VARAM ir nominējusi pārstāvjus, kas ir aktīvi piedalījušies pie Eiropas Blokķēdes Pakalpojumu Infrastruktūras (turpmāk - EBPI) pamatprincipu un tehniskās specifikācijas izstrādes, lai atbalstītu blokķēdes tehnoloģijas risinājumu ieviešanu ES dalībvalstīs.

Informatīvajam ziņojumam pastāv sekojoši ierobežojumi: ņemot vērā blokķēdes tehnoloģijas straujo un neprognozējamo attīstību, šobrīd nav iespējams sniegt visaptverošu analīzi par tās izmantošanas perspektīvām un to ietekmi uz sabiedrību, tādēļ informatīvajā ziņojumā sniegts vērtējums par būtiskākajām aktivitātēm un tendencēm kontekstā ar Latvijas normatīvajos aktos jau iekļauto tiesisko regulējumu un pastāvošo blokķēdes ekosistēmas stāvokli, vienlaikus paredzot tālāko rīcību blokķēdes jomas attīstības veicināšanai Latvijā.

1. ***Blokķēdes tehnoloģijas apraksts un izcelsme***

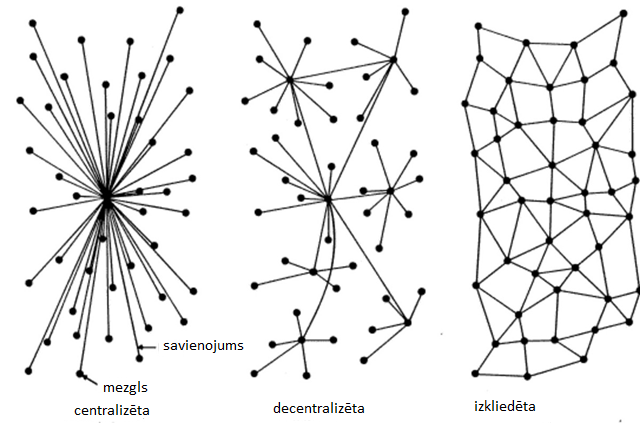
*Blockchain* jeb blokķēde ir vienots termins tehnoloģijām, kas ir radītas, lai sinhronizētu datus, kas tiek glabāti dažādos datoros vai serveros, jebkurā pasaules vietā, izmantojot tīklu tādā veidā, kas ļauj šiem datiem palikt nemainīgiem. Tehnoloģijas nosaukums definē tās darbības pamatprincipu, sadalot datus blokos, kur katrs bloks ir atkarīgs no iepriekšējiem un secīgiem blokiem, radot caurspīdīgu un pareizu informāciju, ko gandrīz nav iespējams koriģēt nemanīti. Šī izkliedētā datu bāze tiek sinhronizēta vienotā ķēdē, kur katrs datu ieraksts jeb bloks tiek glabāts vairākos datoros vai serveros, saglabājot aktuālās un vēsturiski veiktās izmaiņas katrā blokā. Lai nodrošinātu satura integritāti datos, tiek izmantots vienots protokols, kur liela nozīme ir kriptogrāfijai.

Blokķēdes tehnoloģijas būtība ir tāda, ka sinhronizācija notiek vienādranga jeb koplietošanas veidā, proti, tīklā nav viens vienīgs dators, kas kontrolē visu sistēmu. Atsevišķi uzdevumi, kas ir tā dēvēto uzticamo trešo pušu (ang. *trusted third parties*) pārziņā (piemēram, zemes kadastra reģistrs), var tikt izstrādāti atšķirīgi vai pat kļūt lieki. Tas galvenokārt attiecināms uz neapgāžamu, konkrētu datu reģistrēšanu un standarta pārbaužu veikšanu.

Svarīgi ir nošķirt divus atšķirīgus terminus– *blokķēde* un *kriptovalūta*. Lai gan abi ir savstarpēji saistīti, galvenā atšķirība starp šiem jēdzieniem ir saistīta tehnoloģijas darbības pamatprincipu. Blokķēdes tehnoloģijas pamatā ir izkliedēta (ang. *distributed*) datubāze (nevis centralizēta vai decentralizēta), kas ir pastāvīgi augošs sakārtotu ierakstu kopums, kurus dēvē par blokiem. Izkliedētās virsgrāmatas tehnoloģija (ang. *Distributed ledger technology* (DLT)) ir blokķēdes tehnoloģijas pamats. Tā piedāvā konsensa validācijas mehānismu (ang. *Consensus validation mechanism*), kas tiek izmantots datora un blokķēdes sistēmās, izmantojot datoru tīklu, lai panāktu vajadzīgo vienošanos par vienotu datu vērtību vai tīkla stāvokli starp izkliedētiem darījumiem bez starpnieka un centralizētas iestādes nepieciešamības atjaunināt un uzturēt šo informāciju, kas iegūta no darījumiem. 1. attēls vizualizē datubāžu shēmas un to atšķirības.

1. attēls

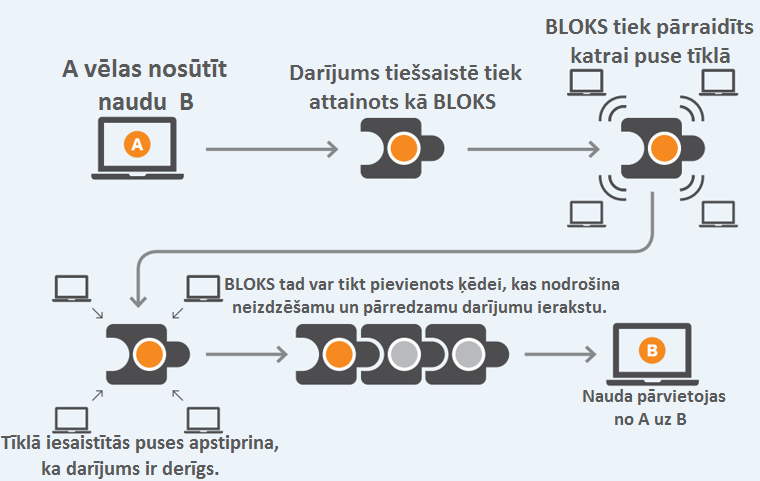
*Blokķēdes tehnoloģijas datubāzes shēmas*



Viena no lietām, kas bieži vien tiek jaukta, ir pati blokķēde un blokķēdes lietošanas gadījumi. Virtuālās valūtas - Bitcoin un Ethereum - ir tehnoloģijas izmantošanas piemēri, kas ir kļuvuši iespējami pateicoties blokķēdes koncepta attīstībai. Blokķēdi būtu jāuztver kā operētājsistēmu, piemēram, MacOS vai Windows, tādejādi Bitcoin pēc būtības ir tikai lietojumprogramma, kas darbojas šajā operētājsistēmā. Bitcoin gadījumā blokķēde ir līdzeklis Bitcoin darījumu saglabāšanai un reģistrēšanai. Katrs darījums ir apstiprināts un kopā ar apstiprinātu darījumu grupu tiek pievienots kā jauns "bloks" jau esošai darījumu ķēdei, tādējādi izveidojot nosaukumu blokķēde (ang. *blockchain*). Kad ķēdei ir pievienots darījums, tas parasti nevar tikt mainīts vai dzēsts[[2]](#footnote-2). 2. attēls vizualizē naudas pārveduma darījumu pēc blokķēdes tehnoloģijas darbības principiem.

2. attēls

*Blokķēdes darījuma vizuāla reprezentācija*



* 1. *Blokķēdi raksturojošās īpašības un sniegtās iespējas*

Blokķēdei kā tehnoloģijai ir vairākas priekšrocības, ņemot vērā ka tā vienlaicīgi var tikt klasificēta gan kā pakāpeniskā (ang. *incremental*), gan kā radikālā inovācija – t.i. atkarībā no izvēlētā pielietojuma veida, tā var gan uzlabot esošus procesus un pakalpojumus, papildinot jau eksistējošus biznesa modeļus, gan arī radīt jaunus biznesa modeļus un struktūras, pārveidojot ne vien pašu organizāciju, bet arī visu attiecīgo nozari. Kā pakāpeniska inovācija blokķēde var tikt izmantota ražošanas, loģistikas, finanšu vai citu procesu optimizēšanā, šādi paaugstinot konkrētā biznesa vai nozares efektivitāti. Analizējot blokķēdes piedāvātas iespējas starpnieku izslēgšanai plašākā nozaru griezumā, tehnoloģija var tikt izmantota kā radikāla jeb revolucionāra inovācija, kas ļauj veidot jaunas organizāciju formas – sākot ar DAO jeb decentralizētās autonomās organizācijas konceptu, kuras pārvalde notiek saskaņā ar blokķēdē ierakstītajiem noteikumiem viedo līgumu veidā, beidzot ar decentralizēto valsts pārvalžu izveidi. Saskaņā ar 2017. gadā veikto Deloitte aptauju starp dažādu jomu lielāko uzņēmumu vadītājiem[[3]](#footnote-3), 42% no respondentiem apstiprināja, ka, pēc viņu domām, blokķēde izraisīs krasas pārmaiņas viņu attiecīgajā nozarē.

Būtiska blokķēdes īpašība, kas atšķir to no citām izkliedētām datubāzēm ir tā, ka katrs bloks satur laika zīmogu un norādi uz iepriekšējo bloku. Šī funkcija blokķēdi padara īpaši drošu arī pret ierakstu izmainīšanu — lai izmainītu kādu no senākiem blokiem, ir jāveic izmaiņas arī visos tam sekojošajos blokos. Papildus iepriekšminētajām raksturojošajām īpašībām un iespējām, blokķēdes tehnoloģijas plaša mēroga pielietojumam ir vēl vairākas priekšrocības, kas padara to par nesabojājamu digitālu datu ierakstu virsgrāmatu:

* Konsensa mehānismi: Lai darījums tiktu pieņemts un reģistrēts blokķēdē, visiem dalībniekiem ir jāpiekrīt ievērot tos pašus noteikumus. Tas ir konsenss (ang. *consensus*). Ja darījums pārkāpj kādu no noteikumiem, par kuriem tīkls ir vienojies, darījums tiks uzskatīts par nederīgu. Konsess ļauj katram dalībniekam uzticēties tīklam, jo viņi zina, ka katrs darījums izpildīs noteikumus, ko tie apstiprināja, kad tīkls tika palaists.
* Pārredzamība: dati par jebkura sistēmā uzskaitīta līdzekļa jeb aktīva pirmavotu, to kustību un ar to saistītiem darījumiem ir pārskatāmi un jebkurā laikā pieejami visiem autorizētajiem lietotājiem;
* Pastāvība: vienreiz ievadītu informāciju nevar izdzēst vai mainīt. Ja notikušais darījums jeb transakcija bija kļūdaina, tā tiek atcelta ar jauno darījumu un informācija par abiem no šiem darījumiem paliek redzama un pieejama[[4]](#footnote-4);
* Drošība: drošības mērķos tiek izmantota kriptogrāfija un *proof-of-work, proof-of-stake* u.c. algoritmu mehānismi. Turklāt katrs blokķēdes bloks ir šifrēts - to veido nejaušs ciparu virknējums, ko nav iespējams atšifrēt bez atslēgas. Šo atslēgu blokķēdes īpašnieks var nodot blokķēdes saņēmējam. Tādejādi tiek minimizēti riski nesankcionētai piekļuvei sensitīviem datiem un palielināta tehnoloģijas drošība;
* Uzticēšanas (ang. *trust*) faktora izslēgšana: darījumus var veikt starp nepazīstamiem dalībniekiem bez starpnieku iesaistīšanos. Blokķēde var nodrošināt uzticamību starp daudziem lietotājiem, kuri savā starpā nav pazīstami. To var ilustrēt ar pūli, kur katram no pūļa dalībniekiem ir vienāds dokuments. Katrs pūļa dalībnieks var patvaļīgi veikt izmaiņas dokumentā, bet viņa darbība būs pamanāma uz pārējā pūļa fona.

1. ***Blokķēde un tās riski***

Šī informatīvā ziņojuma pamatā ir blokķēdes risinājumi, kas spētu tikt pielietoti valsts pārvaldē, tāpēc tā ietvaros netiek apskatīti riski, kas ir raksturīgi privātajiem blokķēdes risinājumiem.

* 1. *Tehnoloģiskie riski*

Saskaņā ar Nīderlandes daudzpusīgo pieredzi blokķēdes tehnoloģisko risinājumu ieviešanā loģistikas, agrikultūras un riteņbraukšanas jomās, lai tehnoloģija būtu droša, katram risinājumam ir nepieciešami vismaz astoņi mezgli (ang. *nodes*). Līdz ar to valsts pārvaldē ir nepieciešams nodrošināt atbalstu blokķēdes risinājumiem atbilstoši to pielietojuma būtībai. Turpmāk šis aspekts detalizēti ir izvērtējams, pilnveidojot valsts vienoto IKT arhitektūru. Veicināma arī privāto un NVO uzturēto mezglu darbība, kas palielinās sistēmas uzticamību. Pamatā tehnoloģija būtu potenciāli izmantojama nozarēs, kur šie uzņēmumi darbojas, piemēram, bankas varētu uzturēt mezglu ar kadastra ierakstiem un darījumu apliecinošiem dokumentiem.

Atkarībā no izvēlētā risinājuma, vienošanās par kādas darbības apstiprināšanu var tikt panākts, ja tām piekrīt vismaz puse no mezgliem. Ja tīklā ir pietiekami daudz privāto mezglu, tad teorētiski pastāv iespēja veikt kaitnieciskās darbības. Lai izvairītos no šī riska, būtu jānosaka, ka privāto mezglu funkcijas ir tikai uzraugošas un informatīvas, nevis lēmumu pieņemošas, vai arī iespējams piešķirt tiesības apstiprināt izmaiņas tikai publiskajiem mezgliem.

Blokķēdes tehnoloģijas viens no produktiem ir Viedais līgums (ang. *smart contract*), kas ir programmas kods, ko pēc publicēšanas var vai nevar mainīt, atkarībā no iestatījumiem. Viedais līgums izpildās vismaz daļēji automatizēti, iestājoties noteiktam notikumam. Piemēram, līdz ar naudas ieskaitīšanu no personas A uz personas B kontu, dzīvokļa īpašumtiesības pāriet no personas B uz personu A. To var izmantot īpašumiem, kuru īpašuma tiesības ir nostiprinātas publiskajos reģistros, piemēram auto vai nekustamā īpašuma reģistros.

Lai viedo līgumu infrastruktūra spētu strādāt ar viedajiem līgumiem, ir nepieciešami pielāgojumi konkrētajā datu bāzē. Iepriekš minētajā piemērā ar dzīvokļa iegādi ir nepieciešams pielāgot Valsts vienoto datorizēto zemesgrāmatu, lai tā veiktu īpašnieka izmaiņas un banku programmatūrā, lai tā automātiski informētu par naudas par darījuma veikšanu.

Šobrīd viedo līgumu tehnoloģija attīstās un tajā ir virkne drošības nepilnību. Tā kā viedais līgums pēc būtības ir programma, tad tajā var tikt iestrādāts kaitīgs kods, kas nav pamanāms, lietotājam, kurš nav jomas speciālists. Kaitīgs kods var veikt vērtību īpašnieka maiņu, nesankcionētās izmaiņas reģistros utt, tādēļ sākotnēji valsts pārvaldē izmantotajos risinājumos būtu atļaujami tikai iepriekš auditētie līgumi, kur parastie lietotāji var aizpildīt tikai datus, nevis rediģēt līguma kodu.

Tāpat kā citi pirmskvantu ēras risinājumi, arī blokķēdes šobrīd nav noturīgas pret kvantu skaitļošanas risinājumiem, līdz ar to nepieciešams strādāt pie kvantu skaitļošanas noturīgajiem risinājumiem gan vietējā, gan globālā mērogā.

Papildus ir jāatzīmē, ka tehnoloģija ir samēra jauna, tāpēc daudz kas nav standartizēts. Blokķēdes risinājumi šobrīd attīstās diezgan fragmentēti – uz blokķēdi balstītos risinājumus visērtāk ir būvēt, izmantojot jau kādu standartizētu ietvaru (analoģiski programmēšanas valodai programmas koda rakstīšanai), tomēr šobrīd ir vairākas ievērojamas platformas, piemēram IBM HyperLedger, Ethereum, R3 Corda un Microsoft Azure Blockchain, kuras savā starpā ir gandrīz nesaderīgas un vienas noteiktās platformas izmantošana veido lielu atkarību no tās sniegtām funkcionālajām iespējām. Lai arī blokķēdes attīstībā piedalās daudzi uzņēmumi ar ilgu vēsturi un reputāciju, virkne jauno uzņēmumu var nebūt ilgtspējīgi un pārvērtēt savas spējas ieviest risinājumus. Arī lielajiem uzņēmumiem trūkst attiecīgās jomas speciālistu.

Blokķēdes tehnoloģijai šobrīd ir problēma ar lielu datu apjoma apstrādi jeb mēroga problēma. Kā zināms, datu bāzēs bieži uztur liela apjoma datus, piemēram, attēlus, dokumentus, u.c. failus. Taču blokķēdes tehnoloģija spēj apstrādāt tikai nelielus datu apjomus. Lielākiem datu apjomiem tehnoloģija nav piemērota, vai arī jāmeklē kāds hibrīdrisinājums. Viens no piemēriem šai mēroga problēmai ir Bitcoin bloķēdes bloka izmērs, kurš ir tikai 1MB liels. Tas nozīmē, ka sekundē Bitcoin spēj veikt tikai 3-4 transakcijas, taču ja Bitcoin popularitāte būtu augusi, tad tehnoloģijai vajadzētu spēt apstrādāt tūkstošiem transakciju sekundē.

* 1. *Informācijas drošības riski*

Lai arī blokķēdē esošo informāciju ir ievērojami grūtāk nesankcionēti un neiespējami nepamanīti izmainīt, tai ir vieglāk piekļūt, jo tā glabājās vairākās vietās. Līdz ar to pilotprojektus blokķēdes jomā labāk nerealizēt sistēmās, kas paredz sensitīvo datu glabāšanu izkliedēti starp mezgliem. Jāatzīmē, ka blokķēdei, papildus pēc būtības visiem tradicionālajiem informācijas sistēmu riskiem, piemīt arī būtisks risks saistībā ar privātās atslēgas drošību, kas var novest pie uzticamas, bet nesankcionētas informācijas iekļaušanu.

* 1. *Citi riski*

Papildus iepriekšminētajiem riskiem jāņem vērā arī normatīvā regulējuma un sabiedrības izpratnes riski. Regulējošo normu neesamība, tehnoloģijas izmantošanas kompetence un sabiedrības neizpratne par tehnoloģiju, tehnoloģijas asociēšana vienīgi ar kriptovalūtām (piemēram, bitcoin, Ethereum un Ripple) rada juridiskos un uzticēšanas riskus, kas jāņem vērā veidojot blokķēdes tehnoloģijas pilotprojektus publiskajā sektorā.

1. ***Tehnoloģijas pielietojums***

Blokķēdes tehnoloģija spēj pavērt jaunas biznesa iespējas, radīt efektīvākus risinājumus un nākotnē varētu samazināt starpnieku nozīmi un biznesa apjomus. Šī specifiskā sistēma finanšu un grāmatvedības uzskaites sektorā ļautu novērst iespēju veikt datos jebkāda veida viltojumus, tos mainīt ar atpakaļejošu datumu un pārdot vienu un to pašu aktīvu divas reizes dažādiem pircējiem. Ar blokķēdes palīdzību jebkura transakcija tiek iekodēta noteiktā sistēmā, ko jebkurā laikā ir viegli pārbaudīt un izanalizēt[[5]](#footnote-5)

Blokķēdes risinājumus primāri iespējams izmantot jomās, kur ir nepieciešamība pēc paaugstinātas drošības reģistriem (zemes, uzņēmumu, licenču, izglītības dokumentu) vai darbību auditēšanas reģistriem (dokumentu aprite, naudas transakcijas, u.c). Blokķēde izslēdz iespēju, ka kādas izmaiņas sistēmā netiks pamanītas, ņemot vērā, ka praktiski izslēgta iespēja veikt nesankcionēto darbību vai iznīcināt datu bāzi, jo uzlauzt var vienu vai dažus mezglus, bet praktiski neiespējami ir uzlauzt visus vai lielāko daļu mezglu. Blokķēde neaizsargā pret autorizēto lietotāju kļūdainām vai kaitnieciskām darbībām, tā tikai palīdz šādas darbības pamanīt, t.i.,. blokķēde nodrošina nemainīgumu nevis patiesumu.

Blokķēde var tikt izmantota kā inovatīvs instruments jebkuras uz vērtīgās informācijas koordinēšanas balstītas centralizētas sistēmas pārveidošanā[[6]](#footnote-6). Blokķēdes tehnoloģija šīs sistēmas decentralizē, izslēdzot nepieciešamību pēc uzticamiem starpniekiem (tādiem, kā bankas, valdība u.c.), to vietā nodrošinot pārbaudi un autorizāciju sistēmā īstenotajām darbībām – šiem mērķiem tiek izmantoti efektīvie un augsto drošības pakāpi nodrošinošie konsensa mehānismi. Centralizētajās sistēmās dalībnieki sazinās viens ar otru, izmantojot vienu centrālo datu serveri, kurā tiek uzglabāta visa informācija ( piemēram, uzņēmums, kura visi biroja datori ir savienoti ar centrālo serveri). Šī pieeja nodrošina vieglu datu pārvaldi, bet padara sistēmu atkarīgu no šī viena centrālā elementa. Decentralizētas sistēmas ir sarežģītākas un nodrošina saziņu starp vairākiem serveriem (P2P jeb *peer-to-peer* komunikācija). Kā piemēru var minēt uzņēmumu, kuram ir vairāki biroji dažādās valstīs, katram no tiem ir savs serveris un tie ir savienoti savā starpā. Izkliedētajās sistēmās saites starp serveriem nepastāv un visi dalībnieki (jeb “mezgli”, no angļu valodas “nodes”) ir neatkarīgas vienības, kas saņem, glabā un rada datus, ka arī tiešajā veidā apmainās ar tiem[[7]](#footnote-7).

* 1. *Blokķēdes tehnoloģijas potenciālā pielietojuma piemēri un iniciatīvas*

EK virzītās iniciatīvas digitālajos jautājumos paver jaunas iespējas blokķēdes tehnoloģijas risinājumu plaša mēroga ieviešanai publiskajā sektorā ES dalībvalstu starpā. Kopš 2018. gada februārī izveidotā ES Blokķēžu novērošanas centra un foruma, kā arī pēc iepriekšminētās ES dalībvalstu atbalstītās Blokķēdes partnerības deklarācijas ir uzsākti pilotprojekti un plānotas darbības valdības līmenī ES mērogā. Šīs darbības mērķtiecīgi tiek veiktas, lai pārredzamā nākotnē tiktu izmantotas daudzās blokķēžu piedāvātās iespējas un lai izvairītos no sadrumstalotas pieejas, veicinot savstarpēji savietojamu infrastruktūru, kas sekmēs uzticamu digitālo pakalpojumu pieejamību. 2018.gada laikā jau ir veikts nozīmīgs darbs identificējot izmantošanas piemērus pārrobežu publiskā sektora digitālo pakalpojumu jomā, kurus varētu uzlabot ar blokķēdes tehnoloģijas sniegtajām iespējām.

* + 1. *Eiropas pašpārvaldes identitātes sistēma*

Kā viena no iniciatīvām, kas ir guvusi atzinīgu novērtējumu EK blokķēdes deklarācijas partnerības ietvaros, ir priekšlikums izveidot Eiropas mēroga publisku blokķēdes infrastruktūru, kurā būtu publiski pieejama juridiski saistoša digitālā identitāte. Eiropas pašpārvaldes identitātes sistēma (ang. *European Self-Sovereign Identity Framework*) paredzētu esošajiem elektroniskajiem parakstiem būt savstarpēji savietojamiem ar pašpārvaldes identitātes modeli, izmantojot decentralizētus identifikatorus (ang. *Decentralized Identifiers*).

Šī pašpārvaldes identitātes blokķēdes platformas ieviešana tiek plānota kā daļa no kopējas pašpārvaldes identitātes ekosistēmas, kuras pamatā ir sadarboties spējīgi standarti un patiesa konkurence starp risinājumu nodrošinātājiem (piemēram, Uport, Civic un daudzi citi). Identitātes infrastruktūra, kas tiks radīta, ir visprecīzāk skaidrojama kā decentralizēta reģistra infrastruktūra, ko kopīgi ekspluatē visas 28 Eiropas Savienības dalībvalstis.

* + 1. *Pārrobežu blokķēdes izmantošana izglītību apliecinošu dokumentu datiem Eiropas Savienībā*

Vairākas ES dalībvalstis un EEZ valstis, tai skaitā Nīderlande, Beļģija, Itālija, Malta, Francija, Norvēģija un Horvātija, ir iesniegušas vienotu pieprasījumu strādāt pie pārrobežu izglītību apliecinošu dokumentu datu apmaiņas platformas izstrādes, kas tiktu īstenota izmantojot blokķēdes tehnoloģiju Izglītības diplomu gadījumā tiek ierosināts izstrādāt sistēmu, kas var pārbaudīt akadēmiskā nosaukuma/iegūtā grāda autentiskumu, saglabājot privātumu.

Pašlaik tiek analizētas dažādas iespējas, tostarp Grieķijas priekšlikums –“Diplomata”. Lai diplomu ieguvēji varētu apliecināt, ka viņiem ir konkrētas augstākās izglītības iestādes piešķirts grāds, “Diplomata” ietver kriptogrāfijas protokolu un pieteikumu, kas pastiprina tā ticamību.

Šī projekta mērķis ir izveidot labu sadarbību ar citām iestādēm un izstrādāt pārliecinošu blokķēdes lietošanas gadījumu valdības iniciatīvai vai sistēmai, kas nodrošina pievienoto vērtību visiem studentiem vai pilsoņiem un iestādēm ES. Students vai pilsonis, kas vēlas turpināt studijas ārvalstu iestādē vai pieteikties uz sev interesējošu darbu ārvalstīs, bieži saskaras ar izaicinājumu - dalīties ar iegūto vai nepieciešamo izglītības dokumentu un tā pieņemšanu kā autentisku dokumentu. Šī līdz šim uz papīra dokumentu sagatavošanu balstītā procedūra rada papildus darbu un neērtības studentiem, darba meklētājiem un iesaistītajai administrācijai, turklāt tā nesniedz uzticību iesniegtajam dokumentam un neierobežo krāpniecisku darbību iespējamību. Šis mērķis tika formulēts Vienotā pētniecības centra (ang. *Joint Research Center*) ziņojumā par blokķēdi izglītībā ar vairākiem izmantošanas scenārijiem:

* izmantojot blokķēdi pastāvīgi drošiem sertifikātiem;
* izmantojot blokķēdi, lai pārbaudītu daudzpakāpju akreditāciju;
* izmantojot blokķēdi kā mūžīgu iegūtās izglītības uzskaites pasi.[[8]](#footnote-8)
  + 1. *E-komercijas PVN piemērošana*

EK muitu politikas izstrādātājs un īstenotājs DG TAXUD ierosina pārskatāmā nākotnē ieviest IOSS (ang. *Import One-Stop-Shop (IOSS) VAT identification*) PVN identifikācijas numuru izplatīto reģistru, potenciāli, izmantojot ES mēroga blokķēdes infrastruktūru kā vienu no iespējamajiem risinājumiem. Šis projekts ļautu tirgotājiem, kas reģistrēti ārpus ES, iecelt starpnieku vienā dalībvalstī, ar kuru viņi izpildītu savus PVN nomaksas pienākumus. Papildus IOSS PVN identifikācijas numura validācijai, tas ļautu izvairīties no dubultās PVN iekasēšanas importa darījumos. Tirgotāji, izmantojot savu starpnieku, nodokļu administrācijai piešķirtu IOSS PVN identifikācijas numuru. Lai pareizi tiktu piemērots PVN, importa dalībvalstu muitas iestādēm būtu jāpārbauda IOSS PVN numuru derīgums. Lai to nodrošinātu, dalībvalstu muitas iestādēm būtu jābūt pieejamai datu bāzei ar derīgiem IOSS PVN numuriem, kurus visu dalībvalstu nodokļu iestādes piešķirtu ārvalstu tirgotājiem. Dalībvalstu IOSS PVN identifikācijas numuru pārbaudes biežums ir aptuveni 6 pārbaudes sekundē, ņemot vērā 180 miljonu importa deklarāciju gadā, kas pakļaujas importa shēmai. Ņemot vērā reģistra pieejamību, uzticamību un veiktspējas prasības, šāda shēma varētu tikt izmantota lielākajā daļā dalībvalstu.

Lai gan sākotnēji DG TAXUD apsver iespēju PVN numuru identifikācijai dot priekšroku citiem risinājuma piemēriem, viņu skatījumā šis būtu lielisks projekts priekš EBPI, kas būtu saistīta ar reģistra koplietošanu valsts nodokļu vai muitas iestādēm. Piedāvātajā risinājumā, ieviešot plašu reģistru, tiek nodrošināta reģistrācijas informācijas pārsūtīšana un izslēgšana, kas paredzēta importēšanas sistēmas tiesību aktos. Šī pieeja, galvenokārt, vērsta uz dalībvalstu efektivitāti un izmaksu pieaugumu dalībvalstīm.

* 1. *Blokķēdes tehnoloģiju perspektīvas Latvijas publiskajā sektorā*

Pieņemot EK virzītās iniciatīvas un Blokķēdes partnerības deklarācijas ietvaros noteikto nodomu uzsākt pārrobežu starpvalstu sadarbību blokķēdes tehnoloģijas potenciālo publiskā sektoru pilotprojektu apskatīšanai un ieviešanai, EM ir uzsākusi sarunas ar nozares ekspertiem, darba grupas un publiskā sektora pārstāvjiem. Sarunu rezultātā šobrīd ir identificēti divi potenciālie pilotprojekti, kas varētu tikt apskatīti tuvāk un pētīti līdz 2019. gada beigām.

* + 1. *Potenciālais pilotprojekts ar Uzņēmumu reģistru*

Pateicoties veiksmīgam sarunu procesam, kas ir izveidojies starp valsts sektora blokķēdes tehnoloģijas darbības perspektīvu darba grupu, nozares ekspertiem, Tieslietu ministriju (turpmāk – TM) un Uzņēmumu reģistru (turpmāk – UR) ir izdevies identificēt nākamo attīstības posmu SIA dalībnieku reģistra vešanas kārtībā.

UR saskata iespēju un pievienoto vērtību blokķēdes tehnoloģijas sniegtajam pienesumam attiecībā uz SIA dalībnieku reģistra vešanu. Pašlaik Komerclikums paredz, ka SIA valdei ir pienākums vest dalībnieku reģistru pie katras īpašnieku vai citām izmaiņām attiecībā uz īpašniekiem, kā arī valdei ir jāiesniedz UR aktuālā dalībnieku reģistra versija. Valdei tas ir jāizdara 3 dienu laikā no izmaiņu brīža. Šajā gadījumā Komerclikums jau šobrīd paredz, ka informācija ir jāsniedz valsts institūcijai, kura to pēc tam publisko. Precīza statistika par izmaiņu biežumu un skaitu šobrīd gan nav pieejama, jo bieži vien uzņēmumi ,iesniedzot dalībnieku reģistru, vienlaikus veic vairākas izmaiņas, piemēram, jaunas SIA reģistrācija, pamatkapitāla izmaiņas (pamatkapitāls tiek palielināts vai samazināts) vai izmaiņas dalībnieku sastāvā. Saskaņā ar UR aplēsēm šādi gadījumi varētu būt aptuveni 25-30 tūkstoši/gadā. Vienlaikus, uzlabojot, pilnveidojot un attīstot līdzšinējās procedūras SIA dalībnieku reģistra vešanā, izmantojot blokķēdes tehnoloģijas sniegtās iespējas, jāņem vērā, ka jānodrošina arī patieso labuma guvēju reģistrācijas un atklāšanas nosacījumi

Šajā sakarā EM un UR ir uzsākuši sadarbības sarunas par jauna pilotprojekta risinājuma izstrādi, kas ieviesīs nākamā līmeņa drošību un pielietojumu Valdības nolūkiem, kas ne tikai kalpos Latvijas iedzīvotājiem un uzņēmējiem, bet arī ES mērogā pozicionēs Latviju kā vienu no vadošajām valstīm blokķēdes tehnoloģijas adaptēšanas ziņā valsts sniegto pakalpojumu jomā.

* + 1. *Potenciālais pilotprojekts ar Valsts ieņēmumu dienestu*

Apzinoties kases aparātu reformas nozīmību ēnu ekonomikas izskaušanas veicināšanā, kā arī nepieciešamību nodrošināt uzņēmējdarbības videi labvēlīgus apstākļus, kas ir priekšnoteikums Latvijas tautsaimniecības konkurētspējīgai attīstībai, EM uzskata, ka ir nepieciešams nodrošināt saprātīgu līdzsvaru starp nodokļu politikas veidotāju interesēm, no vienas puses, un uzņēmējdarbībai piemērotu vidi, no otras puses. Šāda samērīga risinājuma izstrāde kases aparātu reformas pirmajam posmam noslēdzoties, neapdraudētu uzņēmējdarbības attīstību, būtu vēlama, lai stiprinātu cīņu par ēnu ekonomikas mazināšanu.

Lai rastu risinājumu iepriekš minētajam izaicinājumam – īstenot kases aparātu reformu, ievērojot visu iesaistīto pušu objektīvās intereses, EM uzskata, ka nepieciešams aktualizēt diskusiju par kases aparātu reformas pielāgošanu 21.gadsimta tehnoloģisko risinājumu iespējām un IT infrastruktūrai, t.i., risinājumiem, kas stiprinātu VID uzraudzības kapacitāti un paredzētu samērīgu finanšu un administratīvo slogu komersantiem tiem noteikto prasību izpildes nodrošināšanai.

EM ieskatā viens no šādiem risinājumiem, pēc kases aparātu reformas pirmā posma noslēgšanās, būtu tehniska risinājuma izstrāde elektroniskajās ierīcēs un iekārtās, lai ieviestu tirdzniecības datu nodošanu VID tiešsaistes režīmā, izmantojot blokķēdes tehnoloģiju. Iepriekš minētais priekšlikums būtu ieviešams kā nākotnes risinājums, ko uzņēmēji pēc savas iniciatīvas varētu izmantot ērtākai un efektīvākai sadarbības veidošanai ar Valsts ieņēmumu dienestu.

FM jau ir norādījusi, ka, Valdības rīcības plānā iekļauto 26.4.pasākumu “Viedkaršu ieviešana kases aparātos” sakarā, 2016.gada nogalē jau tika sagatavots redzējums kases aparātu reformas otrajam posmam. Papildus, FM vērsa uzmanību, ka kases aparātu reformas otro posmu, t.i., elektronisko kases aparātu tiešsaistes sistēmas ieviešanu, bija paredzēts realizēt, pastiprinot elektronisko kases aparātu tehniskās prasības, elektroniskajā kases aparātā integrējot kontroles moduli, kas veiktu kases čeku elektronisku parakstīšanu. Elektroniskā kases aparāta čeka elektroniska parakstīšana nodrošinātu katra kases čeka autentiskumu un kontrolētu čeka identificējošo datu pareizību un saglabāšanu. Atkarībā no izvēlētā konkrētā tehnoloģiskā risinājuma, varētu tikt paredzēta arī elektroniskajā kases aparātā reģistrētās informācijas nosūtīšana VID.

Attiecībā uz turpmāku identificētās problēmas risinājuma virzību, EM ir uzsākusi sarunas ar nozares ekspertiem, kas jau ir praktizējušies blokķēdes tehnoloģijā balstītu risinājumu izstrādē grāmatvedības uzskaites sistēmām, audita un maksājumu nolūkiem un kopumā atbalsta jaunu tehnoloģiju ieviešanu attiecībā uz kases aparātiem. EM tālākos plānos ir turpināt iesāktās sarunas, paralēli veidojot sadarbības platformu hakatona (ang. *hackathon*) formātā starp valsts sektora pārstāvjiem (VID un FM) un nozares ekspertiem, lai adresētu sociālo partneru radušās bažas un, potenciāli nonāktu līdz uz blokķēdes tehnoloģijas balstīta pilotprojekta izstrādei iepriekšminētajai problēmai. Šī sadarbības platforma nodrošinātu 21. gadsimtam atbilstošu un laikmetīgu pieeju aktīvai problēmas risināšanai, lai veicinātu ātrāku un efektīvāku kases aparātu reformas un jaunajās elektroniskajās ierīcēs un iekārtās reģistrēto ticamo datu nosūtīšanas darbību VID tiešsaistes vai citā režīmā, kas, potenciāli, pildītu reformas papildinošu funkciju.

* 1. *Blokķēdes tehnoloģijas ekosistēma Latvijas mērogā*

Saskaņā ar EM, šobrīd blokķēdes jomā Latvijā darbojas aptuveni 25 jaunuzņēmumu. Lai pārstāvētu ieinteresētās puses un informētu sabiedrību par tendencēm blokķēdes informācijas tehnoloģijas jomā, kā arī nodrošinātu sadarbību pie blokķēdes tehnoloģijas sniegto attīstības iespēju izpētes un ieviešanas, 2017. gada martā tika reģistrēta “Latvijas Blockchain asociācija”. Asociācija apvieno piecus ar blokķēdes tehnoloģiju saistītus uzņēmumus un kriptovalūtas entuziastus.

Latvijā dibinātie jaunuzņēmumi, kas izstrādā blokķēdes tehnoloģijā balstītus risinājumus jau ir guvuši panākumus globālā tirgū, darbojoties datorspēļu, autentifikācijas un kripto aktīvu jomās. Piemēram, Latvijā dibinātais uzņēmums "BitFury", kas specializējas blokķēdes infrastruktūras un transakciju nodrošināšanā, ir kļuvis par vienu no vadošajiem nozares uzņēmumiem. Jaunuzņēmums “Digipulse” ir piesaistījis investīcijas aptuveni miljona euro vērtībā ICO (ang. *Initial Coin Offering*) procesā, savukārt uzņēmums "Notakey" piedāvā identitātes un autentifikācijas risinājumus uzņēmumiem. Jaunuzņēmums “Monetizr” ir izstrādājis īpašu IT risinājumu, blokķēdes protokolu un kriptovalūtas atalgojuma sistēmu spēļu izstrādātājiem. “Globitex” ir radījis profesionālu Bitcoin tirgus vietu, lai aizpildītu nepieciešamību priekš valdības līmeņa apmaiņas platformas ar attīstītiem IT risinājumiem, saderīgiem gan priekš individuāliem, gan institucionāliem Bitcoin tirgus dalībniekiem. “AndIT Solutions” ir izstrādājis kriptovalūtu pieņemšanas un apmaiņas platformu, ko izmanto komersanti visā pasaulē, lai pieņemtu kriptovalūtas, kā alternatīvu norēķinu veidu.

Publiskajā sektorā, sākot ar 2014. gadu LB aktīvi informēja Latvijas iedzīvotājus par riskiem, kas saistīti ar Bitcoin pirkšanu un izmantošanu norēķinos, paralēli skaidrojot Latvijas iedzīvotājiem blokķēdes tehnoloģijas īpašības un potenciālu tikt izmantotai ārpus virtuālo valūtu jomas un uzlabot daudzus ekonomiskos procesus. Šobrīd LB piedalās Eiropas centrālo banku projektā, kura ietvaros testē dažādus blokķēdes tehnoloģijā izveidotos maksājumu sistēmas prototipus.

Būtisku lomu blokķēdes ekosistēmā ieņem platformas un atbalsta centri, kas izglīto attīstītājus par risinājumu izmantošanas iespējām. Piemēram, “CryptoLab” apmāca un sniedz dažāda veida konsultācijas saistībā ar investīciju iespējām kriptovalūtās un to ikdienas lietošanu. “Blockvis” ir IT blokķēdes profesionāļu grupa, kas izglīto sabiedrību un izstrādā pielietojumus blockchain tehnoloģijai viedo līgumu jomā. Vienlaikus sabiedrības un IT speciālistu un blokķēdes tehnoloģijas entuziastu izglītošanai tiek rīkotas jaunuzņēmumu nozari pārstāvošu publisku un privātu partneru (Techchill, Startin,.lv, LIAA) organizētas konferences, diskusijas un tīklošanās pasākumi, piemēram, “RIGA COMM”, kuros Baltijas un ārvalstu digitālo pakalpojumu sniedzēju un produktu izstrādātāji diskutē par blokķēdes tehnoloģijas nozīmi un pielietojumu.

Lai attīstītu blokķēdes tehnoloģijā balstītus risinājumus, uzņēmējiem pieejams atbalsts jau esošo valsts atbalsta programmu ietvaros, tai skaitā akcelerācijas un riska kapitāla fondos. Viena no fondu pārvaldniekiem “Overkill Ventures” viena no specializācijas jomām papildus mākslīgā intelekta un mašīnmācīšanās, lietu interneta, paplašinātās un virtuālās realitātes risinājumiem, ir arī blokķēdes tehnoloģija. Tāpat Latvijas Universitātes studentu Biznesa Inkubatora 2018.gada pavasarī un rudenī organizētā jaunuzņēmumu blokķēdes pirms-akcelerācijas programmā ļāva tās dalībniekiem attīstīt pamatzināšanas par blokķēdes tehnoloģiju un tās izmantošanas iespējām, kā arī attīstīt savas biznesa idejas un gūt mentoru padomus un ieteikumus.

Latvijas jaunuzņēmumi spējuši piesaistīt investīcijas ICO procesā vairāk nekā 28 miljonu euro vērtībā. “Digipulse” (0,85 miljoni euro), “HashRush” (1,55 miljoni euro), “Aeternum” (3,05 miljoni euro)” , “ Forty Seven Bank” (10,84 miljoni euro), “Globitex” (9,7 miljoni euro), “Cryder” (29,6 tūkstoši euro).

1. ***Tālākā rīcība blokķēdes tehnoloģijas adaptēšanā un jomas attīstībā***

Ņemot vērā blokķēdes tehnoloģijas potenciālu uzlabot valsts pārvaldes pakalpojumu racionalitāti un drošību, kā arī padarīt daudzus biznesa procesus efektīvākus, tādējādi veicinot Latvijas uzņēmumu konkurētspēju, kā arī tehnoloģijas, kā jaunas IT jomas tālākās attīstības perspektīvu, kas dotu iespēju Latvijas jaunuzņēmumiem iziet globālajā tirgū, ir fundamentāli svarīgi veicināt tehnoloģijas izmantošanu valsts pārvaldē un privātajā sektorā, kā arī sagatavot priekšlikumus pasākumiem tehnoloģijas atbalstam blokķēdes tehnoloģijas darbības perspektīvu darba grupas ietvaros, iesaistot arī privātā sektora pārstāvjus.

Ņemot vērā, ka viena no EM prioritātēm izcilas uzņēmējdarbības veidošanā ir veicināt digiālo risinājumu lietojumu uzņēmējdarbībā, publisko pakalpojumu digitalizācijā, kā arī kopumā sekmēt EM un tās padotības iestāžu un citu institūciju kompetences jomā esošo Digitālās ekonomikas un sabiedrības indeksa (turpmāk – DESI) komponenšu pilnveidošanu, 2019. un 2020.gadā plānots turpināt aktivitātes, kas saistītas ar blokķēdes tehnoloģijas potenciāla apzināšanu un lietošanu, tai skaitā sarunu ciklus, sabiedrību izglītojošus pasākumus un diskusijas par blokķēdes jomas attīstību. Savukārt, atsaucoties uz šajā informatīvajā ziņojumā minētajām EK virzītajām iniciatīvām un Blokķēdes partnerības deklarācijas ietvaros noteikto nodomu uzsākt pārrobežu starpvalstu sadarbību potenciālo publiskā sektoru pilotprojektu apskatīšanai un ieviešanai EM līdz 2019. gada beigām plāno organizēt un atbalstīt hakatonu, kas būtu vērsts uz blokķēdes tehnoloģijā balstītas pilotprojekta izstrādi publiskajā sektorā, kur tas spētu sniegt papildus pievienoto vērtību konkrētai darbībai vai pakalpojumam.

Lai veicinātu plānoto pilotprojektu realizāciju, sekotu līdzi blokķēdes tehnoloģijas globālajām attīstības tendencēm un ES politikas attīstībai šajā jomā, kā arī efektīvi aizstāvētu Latvijas valsts pozīciju un intereses, nodrošinātu raitu starpinstitucionālo informācijas apmaiņu, koordinēti veicinātu sabiedrības informētības un izglītošanas pasākumus, nodrošinātu sadarbību ar privāto sektoru, kā arī identificētu barjeras tehnoloģijas attīstībai un piedāvātu risinājumus to pārvarēšanai, LB un EM ierosina turpināt izveidotās darba grupas (EM 12.10.2018. rīkojums Nr. 3.7-1\_2018\_24) darbu vismaz līdz 2019. gada beigām ar vienu no uzdevumiem sagatavot kārtējo darba grupas ziņojumu par paveikto 2019. gadā un priekšlikumus turpmākajiem pasākumiem tehnoloģijas atbalstam. Darba grupas kārtējo ziņojumu līdz 2020. gada 1. janvārim iesniegt izskatīšanai Ministru kabineta sēdē. Papildus tiek aicināts TM izvērtēt un sniegt darba grupai atzinumu par esošā juridiskā ietvara attiecināšanu uz blokķēdē reģistrētiem darījumiem un viedajiem līgumiem, un nepieciešamību veidot jaunu ietvaru Latvijā, lai tie tiktu atzīti par tiesiskiem.

Ekonomikas ministrs R.Nemiro

Vīza:

Valsts sekretārs Ē.Eglītis

E.Ozoliņš - Ozols, 67013011

e-pasts: [edgars.ozolins-ozols@em.gov.lv](mailto:edgars.ozolins-ozols@em.gov.lv)

1. Eiropas Komisija. Deklarācija blokķēžu tehnoloģiju jomā [tiešsaiste]. Pieejams: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership [↑](#footnote-ref-1)
2. STEPTOE & JOHNSON LLP “Blockchain Technology and regulatory investigations”, 2017, pieejams: <https://www.steptoe.com/images/content/1/7/v2/171967/LIT-FebMar18-Feature-Blockchain.pdf> [↑](#footnote-ref-2)
3. Deloitte “Innovation and blochchain surbey”, 2017 Pieejams: https://www2.deloitte.com/us/en/pages/about-deloitte/articles/2017-innovation-blockchain-survey.html [↑](#footnote-ref-3)
4. Karim Sultan, Umar Ruhi un Rubina Lakhani, “CONCEPTUALIZING BLOCKCHAINS: CHARACTERISTICS & APPLICATIONS”, 2018. Pieejams: https://arxiv.org/ftp/arxiv/papers/1806/1806.03693.pdf [↑](#footnote-ref-4)
5. LAFPA, 2017. pieejams: <https://lafpa.lv/content/uploads/2017/02/Fintech_viss-kop%C4%81.pdf> [↑](#footnote-ref-5)
6. Wright, De Filippi, 2015 [tiešsaiste] https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2580664) [↑](#footnote-ref-6)
7. Karibasic, 2016 <https://blogs.perficient.com/2016/12/15/how-will-internet-of-things-use-blockchain/> [↑](#footnote-ref-7)
8. European Commission’s Science for Policy report by the Joint Research Centre, 2017. Pieejams: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255\_blockchain\_in\_education(1).pdf [↑](#footnote-ref-8)