

LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

**KRIPTOVALŪTU RAKŠANA, TĀS RISINĀJUMI UN
REALIZĀCIJA MĀJAS APSTĀKĻOS**

BAKALAURA DARBS

Autors: Rinalds Rihards Putrālis

Studenta apliecības Nr.: rp15015

Darba vadītāja: M.pol. Sintija Lejniece

Rīga 2019

ANOTĀCIJA

Bakalaura darba mērķis ir pilnveidot zināšanas par kriptovalūtu rakšanu, to veidiem, saistītajām izmaksām, iesaistītajiem dalībniekiem, ietekmi uz vidi, viedokļus par tām. Lai noteiktu efektīvākās rakšanas iespējas, darba autors portatīvajā datorā ieviesa kriptovalūtu rakšanu un veica pētījumu par iegūtajiem datiem.

Darbā tiek apskatīta kriptovalūtu rakšanas iespējas ar videokaršu, centrālā procesora, ASIC un FPGA iekārtu palīdzību. Tiek izvērtētas to priekšrocības un trūkumi, kurus izmanto reālos apstākļos, kurus vairs nē, kā arī iedalījums pēc iesaistīto dalībnieku skaita. Uzskaitīti galvenie izdevumi ar kuriem ir jāreķinās apsverot domu nodarboties ar rakšanu.

Darba rezultātā tika izvērtēts, kurš no šiem veidiem būtu vispiemērotākais, lai efektīvi nodarbotos ar rakšanu.

Atslēgas vārdi: kriptovalūtu rakšana, kriptovalūta, GPU, CPU, ASIC, FPGA.

Darba pamattekstā ir 39 lappuses, 12 attēli, 19 informācijas avoti.

ABSTRACT

Cryptocurrency mining, its solutions and realization at home

The main goal of the thesis is to improve knowledge of cryptocurrency mining, its types, associated costs, participants involved, impact on environment, opinions about them. The author has implemented cryptocurrency mining on his laptop and did researches about received data.

In the thesis were reviewed mining possibilities with the help of video cards, central processor, ASIC and FPGA devices. Were evaluated mining advantages and disadvantages, which types are used in real-life conditions and which are no longer used in real-life conditions, as well was reviewed by the number of participants involved. In the course work, the author calculates the expenses related to mining.

The result of the thesis was to evaluate which type of mining would be most effective to do mining currently.

Key words: mining, cryptocurrency, GPU, CPU, ASIC, FPGA.

The thesis work contains 39 pages, 12 images, 19 information sources.

SATURA RĀDĪTĀJS

APZĪMĒJUMU SARAKSTS	6
1. IEVADS	8
2. KRIPTOVALŪTA.....	10
2.1. Kas ir kriptovalūta?	10
2.2. Kriptovalūtas rakšanas aizsākumi	11
2.3. Kriptovalūtas rakšanas darbības principi	12
3. KRIPTOVALŪTAS RAKŠANAS VEIDI	14
3.1. CPU rakšana	14
3.2. GPU rakšana	15
3.3. FPGA rakšana	17
3.4. ASIC rakšana	18
3.5. Kā mūsdienās nodarbojas ar rakšanu	19
4. KRIPTOVALŪTU RAKŠANAS PROCESS PĒC DALĪBNIEKU SKAITA	21
4.1. Solo rakšana	21
4.2. Komandas rakšana	21
4.3. Mākoņa rakšana	22
5. KRIPTOVALŪTAS RAKŠANAS IZDEVUMI	24
5.1. Elektrības izmaksas	24
5.2. Iekārtas izmaksas	24
5.3. Telpu izvēle	24
5.4. Mainīgi ienākumi	25
6. ATTIEKSME PRET KRIPTOVALŪTĀM.....	26
6.1. Bankas attieksme pret kriptovalūtām	26
6.2. Valdības attieksme pret kriptovalūtām	26
6.3. Sabiedrības attieksme pret kriptovalūtām	27
7. KRIPTOVALŪTAS RAKŠANAS IETEKME UZ VIDU.....	28
7.1. Kriptovalūtas rakšanas negatīvā ietekme	28
8. PRAKTISKAIS DARBS	29
8.1. Apraksts par ierīci	29
8.2. Electroneum kriptovalūtas rakšana ar CPU	29
8.3. Monero kriptovalūtas rakšana ar CPU	30
REZULTĀTI.....	32
SECINĀJUMI.....	33

IZMANTOTĀ LITERATŪRA UN AVOTI	35
1. Pielikums. Ekrānuzņēmumi no kriptovalūtas rakšanas ar Electroneum	37
2. Pielikums. Ekrānuzņēmumi no kriptovalūtas rakšanas ar Monero	38

APZĪMĒJUMU SARAKSTS

AMD (<i>Advanced Micro Devices</i>)	Otrais lielākais personālo datoru mikroprocesoru ražotājs pēc Intel.
ASIC (<i>Application Specific Integrated Circuit</i>)	Kriptoalūtas rakšanas iekārta ir paredzēta tikai vienam uzdevumam, kuram tie projektēti, speciāli konfigurēti tikai noteiktas kriptoalūtas iegūšanai un, piemēram, <i>Bitcoin</i> iegūšanai paredzētie čipi neder citām vajadzībām.
Bloka ķēde	Izklaidēta datubāze, kas ir pastāvīgi augošs sakārtotu ierakstu, kurus dēvē par blokiem, saraksts. Katrs bloks satur laika zīmogu un norādi uz iepriekšējo bloku.
CPU (<i>Central Processor Unit</i>)	Centrālais procesors ir datora mezgls, kas pēc norādītās programmas, realizē datu matemātisko un loģisko apstrādi un attiecīgajos momentos ierosina pārējo mezglu darbību.
GPU (<i>Graphic Processing Unit</i>)	Videokarte ir datora ierīce, kas ģenerē tekstu vai attēlus attēlošanai datora ekrānā. Videokarte var būt vai nu speciāla paplašināšanas plate, vai arī tās funkcionalitāte var būt iebūvēta pamatplatē.
FPGA (<i>Field Programming Gate Array</i>)	Integrēta shēma, ko pēc izgatavošanas ir paredzēts konfigurēt klientam. FPGA konfigurāciju parasti nosaka, izmantojot aparatūras apraksta valodu, kas ir līdzīga lietojumprogrammas specifiskajai integrētajai shēmai (ASIC).
Hash / hash rate	Ātrums, cik daudz aprēķinus veic kriptoalūtas rakšanas kodā. Jo augstāks <i>hash rate</i> jo lielāka jauda, kas palielina iespēju atrast nākamo bloku un saņemt atlīdzību.
Nonce	Nejaušs skaitlis, kas izveidots autentifikācijas protokola laikā, lai pārliecinātos, ka vecos sakarus nevar atkārtoti izmantot atkārtotajos uzbrukumos.
Racējs	Lietotājs, kurš ir atbildīgs par sistēmas darbību. Vai arī kriptoalūtas rakšanas iekārta, kas ir atkarīga no konteksta.

Rakšana	Operāciju pārbaudes un reģistrācijas process bloka ķēde (digitāls un decentralizēts visu transakciju reģistrs).
Transakcija	Starpniecības pakalpojumi un konsultācijas finanšu darījumu jomā.

1. IEVADS

Kriptoalūtu rakšana ir vairāk nekā 10 gadus pazīstams process daļai sabiedrības. Šobrīd šādu sistēmu darbības pieprasījums un atpazīstamība ir manāmi pieaugusi, kas aktīvi tiek izmantota, lai nodrošinātu transakciju procesus starp kriptoalūtu kontiem jeb elektroniskajiem makiem.

Kriptoalūtu rakšana ir veids kā veidojas bloku ķēde un sūtīta kriptoalūta. Galvenais uzdevums ir gādāt viena bloka izlaidi noteiktā laika periodā un iekļaut transakcijas šajos blokos. Pēc bloka izveidošanas tiek dota ziņa visam tīklam, ka jaunais bloks ir jāpievieno bloka ķēdei, par ko arī racējs tiek atalgots. Jebkurš var nodarboties ar kriptoalūtu rakšanu, kam ir dators, bet ne visi spēs ar to pelnīt.

Bakalaura darbā kriptoalūtu rakšana tiek aprakstīta no dažādiem skatu punktiem. Par kriptoalūtu aizsākumu, rakšanas nepieciešamību, kādi riski pastāv saistībā ar kriptoalūtu rakšanu, tā veidiem, attieksmi pret kriptoalūtiem un to rakšanu no dažādiem skatupunktiem, to negatīvā ietekme uz vidi un kurš no piedāvātajiem risinājumiem, pēc autora domām, būtu visefektīvākais. Rezultātā tika noskaidrots, vai ir vērts nodarboties ar kriptoalūtu rakšanu.

Praktiskajā daļā autors veica kriptoalūtu rakšanu uz sava portatīvā datora ar divām dažādām kriptoalūtiem, veica analīzi ar iegūtajiem datiem un sniedza secinājumus par to efektivitāti un nepieciešamību nodarboties ar kriptoalūtu rakšanu šādā veidā.

Darbā izvirzītā hipotēze:

Dators (*Intel(R) Core(TM) i7-2670QM CPU @ 2.2 GHZ* un *Nvidia GeForce 630M*) ir spējīgs ar procesora un video kartes jaudu iegūt kriptoalūtu rakšanas procesā bez peļņas gūšanas.

Pētījuma mērķis:

Pilnveidot zināšanas par kriptoalūtu rakšanu un to veidiem, kā arī noskaidrot, kurš no tiem būtu efektīvākais kriptoalūtas rakšanas procesā pēc visiem tā aspektiem. Kā arī pašam autoram izmēģināt un izvērtēt kriptoalūtu rakšanu portatīvajā datorā.

Pētījuma uzdevumi:

1. Pētīt un analizēt literatūru par kriptoalūtu un to rakšanu;
2. Izpētīt un aprakstīt iespējamās rakšanas veidus, to izmaksas, kā arī pēc iesaistīto dalībnieku skaita un izvērtēt, kurš no tiem būtu visefektīvākais;
3. Pētīt sabiedrības un banku viedokli par kriptoalūtiem un to rakšanu;
4. Instalēt un konfigurēt kriptoalūtas rakšanas programmu datorā (*Intel(R) Core(TM) i7-2670QM CPU @ 2.2 GHZ* un *Nvidia GeForce 630M*);

5. Apkopot visu iegūto informāciju un veikt secinājumus un priekšlikumus par darba tēmu.

Pētījuma metodes:

Darba izstrādes procesā iekļautās metodes ir vēsturiskā, salīdzinošā, aprakstošā, kvantitatīvā, interneta resursu izmantošana.

Darba struktūra:

Darbs sastāv no ievada, teorētiskās daļa, kas sastāv no 6 nodaļām un 19 apakšnodaļām, kurās ir aprakstīta kriptovalūta, galvenās iezīmes par to rakšanu, viedokļi par tām un ietekmi uz vidi. Pēc teorētiskās daļas seko praktiskā daļa ar 1 nodaļu un 3 apakšnodaļām, kur tiek aprakstīta rakšanas ieviešana un rezultāti un secinājumu sadaļas. Pielikumu sadaļā ir iespējams novērot praktiskā darba – kriptovalūtas rakšanas gaitu.

2. KRIPTOVALŪTA

2.1. Kas ir kriptovalūta?

Pārsvarā kriptovalūta tiek asociēta ar *Bitcoin* jeb ar populārāko un visvērtīgāko kriptovalūtu, bet to patiesais skaits mērāms tūkstošos. Lai valūtu varētu nosaukt par kriptovalūtu, tai jāatbilst kritērijiem, kas pieminēti šajā nodalā.

Kriptovalūta ir digitāls maiņas līdzeklis, kas darbojas tikai datoros, un tā tiek būvēta uz bloka ķēdes tehnoloģijām. Ņemot vērā to, ka tā nav reāla nauda un tā darbojas tūkstošiem datoru tīklā, tā ir droša pret valsts iejaukšanos vai manipulāciju. Šīs valūtas arī nav piesaistītas citas valsts valūtai vai norēķinu līdzekļiem, kā tas ir jebkurai citai valūtai. [11]

Kriptovalūta tiek nodota no vienas personas citai tiešsaistē. Iekārtas nesadarbojas savā starpā izmantojot bankas, *PayPal* vai *Facebook* jeb trešās personas. Tās savā starpā apmainās ar informāciju bez starpniekiem. Šāds maiņas līdzeklis ir drošs, jo nav jānorāda savi personas dati, lai identificētu lietotāju. Tādejādi tiek nodrošināta anonimitāte par attiecīgo lietotāju. Lietotājiem ir segvārdi, kriptovalūtas makiem ir unikālas ģenerētas adreses. Lietotāji, to segvārdi un monētu daudzums makā ir publiski pieejama informācija, taču lietotāju identitāte netiek norādīta. [4]

Šī sistēma ir uzticama, visa informācija tiek šifrēta, netiek iesaistītas trešās puses, netiek nodota papildus informācija. Arī valsts nav informēta par šādu nodarbošanos, līdz tiek mēģināts kriptovalūtu mainīt pret kādu no globāli atzītām valūtām, un notiek mēģinājumi ieskaitīt savā bankas kontā iegūtos līdzekļus. Šādus līdzekļus nepieciešams norādīt gada ienākumu deklarācijā, kā arī jāveic nodokļu samaksa. [2]

Visas notikušās transakcijas tiek identificētas, bet, lai veiktu kāda veida krāpšanos, ir jāzina attiecīgā lietotāja segvārds vai adrese un parole, ko ir gandrīz neiespējami iegūt no šifrējuma. Lai kādā transakcijā veiktu izmaiņas, ir jābūt kontrolei pār tīklu vairāk nekā pusei no ierīču jaudas, jo jauna bloka pievienošana notiek ar apstiprinājumu no pārējām ierīcēm. [3]

Kriptovalūtām nav robežu, tās darbojas jebkur, kur pieejams internets. Lai gan kriptovalūtai tiek prognozēta attīstība, šobrīd ar to pārsvarā nav iespējams norēķināties, it īpaši Latvijā. Pāris uzņēmumi Latvijā "*AirBaltic*", "*Rīgas fasādes*" un citi uzņēmumi piedāvā iespēju norēķināties tikai ar *Bitcoin*, pārējās kriptovalūtas nav iecienītas. [15] Tiek arī runāts, ka tās aktīvi tiek izmantotas "melnajā tirgū", lai norēķinātos par nelegāliem darījumiem, piemēram, narkotisko vielu, viltotas naudas vai ieroču attālinātā iegāde, jo neviena institūcija nekontrolē kriptovalūtas. [3]

Lai arī Latvijā nav specifiska regulējuma kriptovalūtām, Juridiskām vai fiziskām personām veicot darījumus, tajā skaitā ar kriptovalūtām, jāievēro nodokļu un grāmatvedības normatīvais regulējums. Latvijā tas tiek uzskatīts par likumisku maksāšanas līdzekli. [14]

2.2. Kriptovalūtas rakšanas aizsākumi

Šajā nodaļā tiks pētīti šīs kustības aizsākumi un pirmās kriptovalūtas *Bitcoin* veidošanās.

Tās aizsākumi ir meklējami diez gan nesen, jeb 2008. gada 31. oktobrī, kad kāda cilvēku grupa ar pseidonīmu *Satoshi Nakamoto* (vēljojoprojām neskaidrs grupējums) publicēja Lielbritānijas laikrakstā “*The Times*” rakstu ar nosaukumu “*Bitcoin: no lietotāja uz lietotāju elektroniskā naudas sistēma*”. [3]

Rakstā tika minēts, ka ASV un Lielbritānijas bankas ir vainojamas šo valstu finanšu krīzes veicināšanā 2008.gadā. Raksta nosaukums simbolizē plaši pieņemto *Bitcoin* koncepciju -nemainīga, nekompensējama un decentralizēta līdzekļu apmaiņa, kas nenotiek tradicionālajās finanšu sistēmās un valdībās. [4]

Šī kustība aizsākās no tā, ka noteiktai sabiedrības grupai bija priekšstats, ka sabiedrība būtu labāka vai nu bez valdības, vai ļoti minimālas valdības ietekmes. Veidojās ideja par spēcīgu kriptogrāfiju un īpašu publisko kontu kriptogrāfiju, kas sākās 1970. gadu beigās. Cilvēki jau labu laiku iepriekš bija plānojuši, kā samazināt valdības ietekmi, ko spēja paveikt 21. gadsimtā ar datoru un serveru palīdzību. Šādā veidā radās iespēja aizsargāt sevi un savas intereses no valdības, vai vismaz mazināt to. [4]

Galvenais izaicinājums bija tikt galā ar naudas maiņas izaicinājumiem, tādēļ cilvēki sadarbojās tiešsaistē, izmantojot spēcīgus tehniskus un kriptogrāfiskus risinājumus. Turpmāk tika veikti pētījumi par digitālo skaidro naudu, jaunām vērtībām, kas darbojas kā nauda un būtu anonīmas un viegli apmaināmas. Aizsākās doma un mēģinājumi izveidot spēcīgu valūtu, kas būtu decentralizēta, tiešsaistē un tajā pašā laikā privāta. Šādai filozofijai bija daudz atbalstītāju. [2]

Satoshi Nakamoto gandrīz noteikti ir pseidonīms, ko kāda persona vai cilvēku grupa pieņēma ar *Bitcoin* saistītām vajadzībām. *Satoshi Nakamoto* publicēja rakstus tikai par *Bitcoin*. *Satoshi* identitāte ir saistīta ar noteiktiem publiskiem kontiem un dažādiem kontiem dažādās tīmekļa vietnēs. [3]

Satoshi Nakamoto bija kāda cilvēku grupa, kura slēpās zem šī segvārda un lika pamatus *Bitcoin*. Tiklīdz tika nodota *Bitcoin* koda kontrole tā izstrādātājiem, šis grupējums ir pazudis bez turpmākām darbībām un daudzi uzskata, ka vairs arī neatgriezīsies. [3]

Tāpat rodas daudzi jautājumi par to, no kurienes nāk šī persona vai grupējums un kas viņš tāds ir. Pēc šī pseidonīma vārda un uzvārda var nojaust, ka saknes varētu būt no Āzijas valstīm, tāpēc tiek uzskatīts, ka šī persona visticamāk ir no Japānas.

2.3. Kriptoalūtas rakšanas darbības principi

Diezgan daudz ir par to dzirdēts, kā aptuveni darbojas kriptoalūtas rakšana, bet ir nepieciešams par to iedziļināties, lai saprastu kā tiek glabāti bloki, kā tie tiek iekļauti un verificēti. Tā kā kriptoalūtu ir daudz un dažādu, tad šajā nodaļā tiks pētīts, kā darbojas vispopulārākā kriptoalūta jeb *Bitcoin*.

Lai varētu darboties kā *Bitcoin* racējs, nepieciešams interneta savienojums, datora iekārta, jāpievienojas *Bitcoin* tīklam un jāizveido savienojums ar citām iekārtām iegūstot jau esošo bloku ķēdi. Kad iepriekš minētais ir izpildīts, tad iekārtas galvenie veicamie uzdevumi būs šādi:

1. ierīce uztver transakcijas. Jebkura ierīce uztver notiekošās transakcijas tīklā, pārbaudot un apstiprinot, vai līdzekļi, kas tiek sūtīti, jau iepriekš nav iztērēti, un vai ir pareizi norādīts saņēmējs. [2]

2. Iesaistās bloka ķēdes uzturēšanā un uztver jaunus blokus. Galvenais uzdevums ir uzturēt bloka ķēdi. Jāiegūst iepriekšējā informācija no pārējām ierīcēm, lai zinātu visus veiktos darījumus, kas jau ir daļa no bloka ķēdes. Pēc tam ierīce iegūst informāciju par jauniem blokiem, kas tiek pārraidīti tīklā. Nepieciešams apstiprināt katru saņemto bloku, apstiprinot katru darījumu blokā un pārbaudot to. [2]

3. Kad ir atjaunināta bloka ķēdes kopija, kura ir katram racējam, tad var sākt meklēt risinājumus, lai pievienotu savus blokus esošai bloka ķēdes kopijai. Lai to izdarītu, ierīce grupē darījumus par jaunākajiem blokiem, kuri ir pievienoti un paplašina bloka ķēdi ar jaunu bloku. Ir jāpārlicinās, ka katrs blokā iekļautais darījums ir derīgs. [2]

4. Nepieciešams atrast *nonce*, kas padara bloku derīgu. Šis solis prasa visietilpīgāko darbu un šī skaitļa izveidošanā iesaistās visi racēji. Arī daļēja uzdevuma izpilde tiek pieņemta, ja ierīce ir iesaistījies tīklā kā viens no komandas. [2]

5. Šis bloks ir jāpieņem visām pārējām iekārtām jeb vismaz lielākajai daļai racēju tāpat kā demokrātijā. Pastāv neliela iespēja, ka tiks pieņemts bloks un citi jauni bloki nāks klāt, nevis tiks iekļauts kāda cita konkurenta bloks. [2]

6. Ja bloks tiek atzīts par legītimu starp visiem pārējiem racējiem, tad tiek saņemts atalgojums par paveikto darbu. Atlīdzība sastāda ap 1% no darījuma summas, bet, ņemot vērā, ka *Bitcoin* ir ļoti vērtīga monēta, šī atlīdzība ir diez gan iespaidīga. Visdrīzāk, šis procents tiks

sadalīts starp vairākiem racējiem, jo *Bitcoin* blokus realizēt vienam pašam ir diezgan grūti un nāksies noteikti iesaistīties kādā komandā. [2]

Varam secināt to, ka racēju darbs iedalās divās kategorijās: apstiprināt transakcijas jeb blokus tos iekļaujot bloku saraksta kopijā un mēģinot būt pirmajam, kurš piesaka jauna, derīga bloka pievienošanu.

3. KRIPTOVALŪTAS RAKŠANAS VEIDI

Autors ir minējis, ka aprēķini, kas jāveic racējiem, ir ļoti sarežģīti. Šajā sadaļā tiks apskatīts, kāpēc tas ir tik grūti, kā arī tiks apskatīta aparatūru, ko izmanto racēji, lai veiktu šo aprēķinu.

Sarežģīto skaitļošanas racēju iekārtas strādā ar SHA-256 *hash* funkciju. SHA-256 (Drošs *Hash* algoritms) ir vispārējas nozīmes kriptogrāfijas *hash* funkcija, kas tika standartizēta 2001. gadā. SHA-256 bija saprātīga izvēle, jo tā bija spēcīgākā kriptogrāfiskā *hash* funkcija, kas pieejama laikā, kad tika izstrādāts *Bitcoin*. Iespējams, ka tā kļūs mazāk droša *Bitcoin* attīstības laikā, bet pašlaik tā ir pietiekami droša. Tā nākusi no ASV Nacionālās drošības aģentūras, kas ir novedusi pie dažādām sazvērētības teorijām par tās drošību un piekļuvi, bet tik un tā tiek uzskatīta par ļoti spēcīgu *hash* funkciju. [2]

SHA-256 glabā 256 bitus. Paziņojums ir sadalīts astoņos 32-bitu vārdos, kas padara to ļoti augsti optimizētu priekš 32 bitu aparatūras. Kriptoalūtu racēju uzdevums ir aprēķināt šo funkciju pēc iespējas ātrāk. Racējiem notiek individuāla sacensība vienam ar otru, jo no tā ir atkarīgs, vai tiks saņemts atalgojums, bet ja viņi ir komandā, tad sacensība tāpat pastāv. Tas, kurš iesniegs visvairāk pierādījumus, lai realizētu bloku, saņems lielāku atalgojumu. Lai to izdarītu, ir jāspēj manipulēt ar 32 bitu vārdiem, veicot 32 bitu moduļu pievienošanu un arī veicot bitu loģiku. [2]

Bitcoin pieprasa, lai SHA-256 tiktu piemērots divreiz uz bloku, lai tiktu iegūts *hash*, ko izmanto mezglos. Divkārsšās aprēķināšanas iemesli nav pilnībā precizēti, bet šajā brīdī tas ir tas, ko kriptoalūtas racējiem ir jārisina. [2]

3.1. CPU rakšana

CPU ir datora centrālais procesors, kas būtībā ir datora smadzenes. Lielāko daļu no tiem ražo firmas Intel un AMD. Tas izpilda visus uzdevumus, ko parasti saista ar skaitļošanu, piemēram, saglabājot dokumentu, ierakstot to cietajā diskā. Lielākā daļa komponentu ir veidotas, lai atbalstītu CPU darbību. Kad *Bitcoin* tika izlaists, bija iespējams izrakt 100 monētas dienā, izmantojot tikai CPU. Diemžēl šodien *Bitcoin* ar centrālo procesoru nav iespējams pateicoties ASIC. [1]

Centrālais procesors ir veidots, lai ātri pārslēgtos starp dažādiem uzdevumiem. Ja ir pieejams dators, ir pieejams arī CPU. Tas nozīmē to, ja kriptoalūtu ir atļauts rakt ar CPU, tad to var iegūt ar jebkuru datoru, taču tas ievērojami samazinās datora veiktspēju, kā arī šis nebūs efektīvākais veids kā veikt rakšanu. [1]

Racēji tiek atalgoti par pareiza rezultāta iegūvi, kas sevī ietver sarežģītus matemātiskus aprēķinus. Centrālajiem procesoriem ir maz aritmētisko loģisko vienību, ķēdes, kas veic aritmētiskas darbības, un tādējādi tās ir samērā lēnas, veicot lielu aprēķinu apjomu. [3]

CPU rakšana ir pirmsākums kriptovalūtas rakšanā jeb pirmā paaudze. 2008.gadā bloka ķēdes papildināšanas risinājumi bija pietiekami vienkārši, jo pirmsākumos tiem nebija jāveic tik sarežģīti aprēķini, kādi tie ir jāveic šobrīd. Tas vairs nav efektīvi, nenodrošina lielu aritmētiskos risinājumus, tāpēc visi lielie kriptovalūtas uzturētāji ir atteikušies no šāda rakšanas veida un dod priekšroku citiem veidiem, no kuriem ir iespējams gūt kādu atalgojumu. [3]

Autors uzskata, ka šo rakšanas veidu var pielietot tikai pie nesen izlaistām kriptovalūtām, jo nav jāveic iespaidīgi aprēķini un šī datora komponente būs spējīga veikt nepieciešamos uzdevumus un iegūt savā makā pāris monētas. Protams būs jācer arī uz to, ka attiecīgajai kriptovalūtai kādreiz celsies cena un varēs realizēt par lielām summām. Pastāv risks, kad nekad neatpelnīsies šie ieguldījumi, jo kriptovalūtas cena var nepalielināties.

3.2. GPU rakšana

GPU ir grafikas procesors jeb videokarte. Lai gan tās nav tik spēcīgas kā ASIC, taču ir daudz elastīgākas pielietojumā. Videokartes mikroshēma veic atkārtotus aprēķinus, bieži vien grafikas apstrādei. Lai gan tas ir diskutabli par GPU izmantošanu kriptovalūtu rakšanā, tos bieži izmanto spēļu datoros, lai nodrošinātu animāciju un video netraucētu attēla veidošanu. [1]

Uzņēmumi, piemēram, AMD un *Nvidia* sākotnēji izstrādāja GPU, lai iegūtu labāku grafiku. Tomēr videokaršu kompānijas pamanījušas strauju pieprasījuma pieaugumu no cilvēkiem, kas vēlas izmantot šīs mikroshēmas, lai raktu kriptovalūtas. Augstas klases videokaršu cenas ir strauji palielinājušās, un šobrīd ir milzīgs grafikas karšu trūkums. Lai pasargātu videospēļu piekritējus, daži mazumtirgotāji pašlaik ierobežo vienību skaitu, cik ir atļauts iegādāties, un dod atlaides tiem, kuri pērk citas datora komponentes faktiskajam videospēļu datoram, nevis kriptovalūtu rakšanas jaudas palielināšanai. [1]

Atšķirībā no ASIC, GPU spēj iegūt dažādas monētas. Savā īpašumā varētu iegūt dažāda veida kriptovalūtu, kā piemēram: *Ethereum*, *Ripple coin*, *Bitcoin Gold*, *Zencash* un daudzus citus ar vienu un to pašu GPU. [1]

Rakšana ar GPU tiek uzskatīta par otrās paaudzes rakšanu, kas bija alternatīvais risinājums CPU un kā arī nodrošināja daudz lielākus aritmētiskos risinājumus nekā ar CPU, tāpēc lēnām cilvēki pārgāja uz video karšu rakšanu, kas acīmredzami mazināja CPU racēju skaitu. [3]

2010. gadā tika izlaista valoda ar nosaukumu *OpenCL*. *OpenCL* ir vispārēja valoda ar mērķi veikt citas darbības, izņemot grafiku GPU. Tā ir augsta līmeņa valoda un laika gaitā

cilvēki ir izmantojuši, lai grafikas kartēs darbotos daudzu veidu aprēķini. Tas bija veids, kā iegūt *Bitcoin* ar GPU. [3]

Videokartes ātri vien tika izpirktas un radīja iztrūkumu tirgū, tāpēc krasi tika celtas cenas šīm grafikas kartēm. Sabiedrības daļa, kuri vēlējās iegādāties videokartes ar mērķi tās izmantot datorspēlēm bija neapmierināti ar šo situāciju, ko centās risināt arī ražotāji, ierobežojot to iegādes skaitu un datoriem ar spēcīgām videokartēm necēla cenas. Šīs komponentes ir pieejamas sabiedrībai, tāpēc radās šāda situācija. [16]

Grafikas procesori ir tik pievilcīgi, jo tie nav paredzēti tikai vienam uzdevumam. Ja tie ir iegādāti kriptovalūtas rakšanai un ir vēlme pārtraukt ar to nodarboties, tad var par diezgan izdevīgām summām pārdot tās kādam citam, vai ievietot savā datorā, piemēram, datorspēlēm. Daudzi ražotāji izmanto šādu iespēju pārdod videokartes, kad tās derīguma termiņš tuvojas beigām. [16]

GPU piemīt augstāka veiktspēja, jo tās spēj strādāt paralēli, kas ar nodrošina daudz vairāk aritmētisko vienību, kuras var izmantot SHA-256 aprēķinam. Lielu daļu grafikas karšu var uzstādīt darboties ātrāk, nekā tas ir paredzēts, ja ir velme uzņemties risku, ka tās var pārkarst vai darboties nepareizi. Tādejādi tiek nodrošināta lielāka peļņa, bet arī tiek paredzēts kļūdu skaita pieaugums. Ar *Bitcoin* iegūvi varētu būt izdevīgi palaist mikroshēmu ātrāk, nekā tas tiek paredzēts, pat ja tiks pieļautas dažas kļūdas. [3]

Liela priekšrocība videokartēm ir tāda, ka uz vienas mātesplates var savietot vairākas grafikas kartes, kas nozīmē to, ka nav nepieciešams katrai grafikas kartei atsevišķa mātesplate un barošanas bloks. Tādejādi tiek ietaupīti papildu līdzekļi, kā arī tiek nodrošinātas daudz vairāk aritmētiskās vienības un atrasti pareizie risinājumi. 3.2.1 attēlā attēlota GPU iekārta, kur ir sešas videokartes uz vienas mātesplates. [17]

Šādas rakšanas iekārtas ir izveidotas, lai varētu savietot vairākas kartes, kā arī nodrošinātu pietiekamu vēsumu un tās nepārkarstu, jo to galvenais ienaidnieks visā šajā procesā ir karstums un tā novadīšana, kas ir kā blakus produkts kriptovalūtas rakšanā. Daudzi šo karstumu vienkārši novada prom ar ventilatoru vai kondicionieru palīdzību ārā no telpām, bet citi to izmanto daudz efektīvāk, kā enerģiju, ko var izmantot lietderīgi, piemēram, ar šo karstumu apsildot māju. [17]

Katram risinājumam ir arī savi trūkumi, kādi piemīt šim risinājumam. Pašā nosaukumā ir teikts, ka tās ir paredzētas grafikas apstrādei, kas nozīmē to, ka visa veiktspēja netiek izmantota kriptovalūtas rakšanai. Videokartēm nav paredzēts strādāt ar citām videokartēm. Tās ir domātas vienam datoram, kura ir viena pati ar nevienu citu nesadarbojoties. [2]

Elektrības patēriņš šīm kartēm ir daudz lielāks, bet tās attaisno ar savu *hash rate*, kas ir ievērojami lielāks nekā tas būtu CPU. [2]

Videokartes ir daudzkārt efektīvākas par CPU, bet pat šodien tās netiek vairs izmantotas *Bitcoin* rakšanā, tāpēc cilvēki meklēja vēl citus risinājumus, lai varētu rakt *Bitcoin*, jo aizņemtu pārlietu ilgu laiku, lai pievienotu jaunu bloku. Toties vēl joprojām tiek izmantotas citām kriptovalūtām.



3.2.1. att. GPU iekārta [17]

3.3. FPGA rakšana

FPGA iekārtām ir ļoti daudzi un dažādi pielietojumi, tās ir īpaši viegli pielāgojamas klienta vajadzībām, kas tās ar padara par vēl pievilcīgākām nekā GPU. [8]

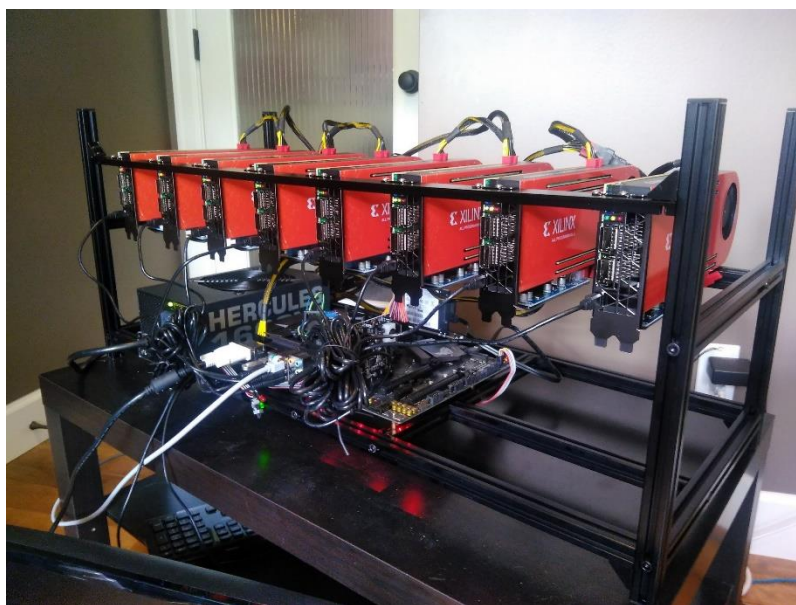
FPGA ir līdzīgas Lego blokiem. Atsevišķs Lego ļauj veidot daudzas dažādas lietas, izmantojot tos pašus, pārkonfigurējamus gabalus. Vienu gabalu var izmantot, lai izgatavotu mājas jumtu, un to pašu gabalu vēlāk var modernizēt, lai padarītu automašīnas šasiju. Līdzīgi, FPGA var izmantot, lai izveidotu gandrīz jebkuru digitālo ķēdi, un tās var darbināt dažādas programmatūras un darboties, izmantojot dažādus algoritmus - kas ir ļoti svarīgs kriptovalūtas ieguves pasaulē, jo dažādi šifrēšanas aktīvi izmanto dažādus algoritmus, lai iegūtu konkrētu *hash*, lai palaistu un uzturētu savus tīklus. [8]

Šeit jau ir nepieciešami speciāli čipi, kurus jau pielāgo pats ražotājs, toties gandrīz visa tā veikspēja tiek novadīta, lai veiktu paredzēto uzdevumu un tādā veidā ir pat efektīvāka nekā GPU. Šī komponente ir pietiekami elastīga, jo var rakt jebkuru kriptovalūtu, kas nav iespējams ar ASIC racēju. Tas ir diezgan svarīgi kriptovalūtu pasaulē, jo kriptovalūtu cena var mainīties jebkurā laikā un patērēt tik pat elektroenerģijas, cik aptuveni GPU, toties strādā daudz efektīvāk par tām, sākot ar 3 reizēm labāk. Jaudas ziņā ir tik pat efektīvs vai nedaudz mazāk efektīvs par ASIC, kurš ir dominējošais tirgū. Lai gan varētu domāt, šis ir vispopulārākais veids kā nodarboties ar rakšanu, tā nav. [8]

Pateicoties elastīgumam un arhitektūrai, FPGA nav viegli uzstādāmas. Tās var ieprogrammēt, lai tās varētu rakt jebko. Taču, lai izmantotu FPGA, ir jāzina, kā to programmēt augstā līmenī. Ar citiem rakšanas veidiem ir daudz vienkāršāk, tām jau ir sagatavotas rakšanas programmatūras un ir nepieciešamas tikai mazas izmaiņas, bet FPGA iekārtas ir jāprogrammē pašam no paša sākuma. Kā arī kods jāraksta *Verilog* vai *VHDL* valodās, kas padara visu vēl sarežģītāku priekš lietotāja. Tāpēc priekšroka tiek dota GPU un ASIC rakšanai, jo tie neprasa programmēšanu, tikai nepieciešams pieslēgt un darbināt savu komponenti. [9]

FPGA ieguva popularitāti tikai uz gadu pateicoties savai sarežģītai uzstādīšanai. Daudzi nav dzirdējuši par FPGA, jo tās nav diez ko izplatītas. Lai gan viedokļi dalās un tiek ar uzskatīts, ka tiem jauns uzplaukuma laiks gaidāms priekšā. [9]

3.3.1 attēlā redzama FPGA rakšanas iekārta aprīkota ar 8 komponentēm.



4.3.1. att. FPGA iekārta [18]

3.4. ASIC rakšana

ASIC ir specifiska integrēta shēma. Kriptvalūtu kontekstā tā ir mikroshēma, kas īpaši izveidota, lai iespējami ātri izpildītu matemātiskos aprēķinus. *Bitcoin* ASIC var aprēķināt *hash* 100 000 reizes ātrāk nekā pats labākais CPU. [1]

ASIC ir pielāgots, lai tas ļoti efektīvi raktu tikai vienu specifisku kriptovalūtu. Tas nozīmē, ka būs jāiegādājas dažādas ASIC iekārtas, ja ir vēlme iegūt dažādas monētas. Šobrīd ir vairāki uzņēmumi, piemēram, *Bitmain* un *Canaan*, kas izstrādā ASIC. Pateicoties to īpašībām un pielietojumam, spēcīgs ASIC nav lēts. [1]

Lielā jauda rezultējas ar pamatīgu elektrības patēriņu. ASIC izmaksas izmaksās ievērojamu naudas summu elektrības rēķinos. Lielākā daļa ieguves notiek valstīs ar lētu

elektroenerģiju. Dažās valstīs kriptovalūtas racēji saņem pat īpašus rūpniecības tarifus šim nolūkam. [1]

Mūsdienās kriptovalūtas rakšanā dominē BITCOIN ASIC vai lietojumprogrammu specifiskās integrālās shēmas. Tās ir mikroshēmas, kas tika izstrādātas, būvētas un optimizētas tikai *Bitcoin* ieguves nolūkā. Principā tās tiek ar vien izmantotas, lai raktu vienu izvēlētu kriptovalūtu, jo nav nevienas alternatīvas, kuras būtu pietiekami efektīvas un saņemtu kādu atalgojumu par savu paveikto darbu. Bet tā pat, lietotāji ar šīm iekārtām cenšas iesaistīties komandā, lai varētu saņemt pastāvīgu atalgojumu, nekā gaidīt to īpašo dienu, kad iekārta būs tā, kura pirmā uzģenerēs pareizo skaitli. [3]

Ja kāda no kriptovalūtām pazūd un ir iegādāta ASIC iekārta, kas veica rakšanu attiecīgajai kriptovalūtai, tad šāda iekārta vairs nav paredzēta neviena cita uzdevuma pildīšanai, kas ir diezgan liels mīnuss, tā nav elastīga. [3]

Zemāk redzamajā attēlā (3.4.1 attēls) ir attēlots *Bitmain AntMiner T9 ASIC Miner*.



3.4.1 att. ASIC Miner [19]

3.5. Kā mūsdienās nodarbojas ar rakšanu

Kā jau iepriekšējās nodaļās tika aprakstīts, ka tiek izmantoti, galvenokārt, ASIC rakšanas iekārtas, kuras nebūt nav lētas un to uzturēšana ir ļoti dārga, tās patērē ļoti daudz elektroenerģijas. Mūsdienās ar kriptovalūtu rakšanu nodarbojas jau uzņēmumi, kuri veido datu centrus. Tas nozīmē to, ka cilvēki individuāli vairs necenšas iesaistīties kriptovalūtas rakšanas procesos, vai iet kāda veida komandā, kur ieguldījumi kāda bloka pievienošanā tiks izdalīti

iesaistītajiem. Kā darbojas kriptovalūtas rakšanas centri nav zināms, jo uzņēmumi vēlas saglabāt konfidencialitāti un savas konkurences priekšrocības. [3]

Nosakot, kur izveidot kriptovalūtas rakšanas centru, ir trīs lielākie apsvērumi: klimats, elektroenerģijas izmaksas un tīkla ātrums. Vēlams ir auksts klimats, lai saglabātu zemas dzesēšanas izmaksas. [3]

Galvenie aspekti, par labu kāda kriptovalūtas centra būvēšanai, ir saglabāt pēc iespējas mazākas izmaksas. Elektrība ir viens no galvenajiem elementiem, jo sastāda vislielākos uzturēšanas izdevumus, jo jāuztur pašas iekārtas un dzesēšana. Protams arī tīkla ātrums, lai spētu saņemt vislabāko reakcijas laiku un komunikāciju starp ierīcēm. Klimats arī ir noteicošs saistībā ar dzesēšanu, bet iepriekšējiem diviem nosacījumiem ir lielāka ietekme. Populārākas vietas, kur ierīko šādus kriptovalūtas centrus ir Gruzija un Islande. [3]

4. KRIPTOVALŪTU RAKŠANAS PROCESS PĒC DALĪBNIEKU SKAITA

4.1. Solo rakšana

Solo rakšana ir kriptovalūtas rakšanas process, kurā ir iesaistītas viena īpašnieka rakšanas iekārtas. Izvēloties solo karjeru, jāpieslēdz savas iekārtas savam *Bitcoin* klientam. Tas ir domāts, lai iegūtu labākos rezultātus un atrastu blokus pats. [1]

Šajā digitālajā pasaulē solo rakšana nebūs labākais veids, kā veikt rakšanu, tādiem racējiem, kuriem aparatūras nav jaudīgas. Tāpēc vairums izvēlas tieši komandas rakšanu. [1]

Pašreizējā tehnoloģija, kas tiek izmantota solo ieguves procesā, var sniegt pieredzi, kas vairāk līdzinās dalībai loterijā. Darot to prasmīgi, pastāv iespēja uz labu atalgojumu. [1]

Ja nodarbojas ar vērtīgas kriptovalūtas solo rakšanu, piemēram, *Bitcoin* ar vienu vai pāris iekārtām, tad ienākumi būs nenosakāmi. Darba autors iesaka pievienoties komandai jeb baseinam, jo gaidīšanas laiks ir nenosakāms. [2]

Šāda veida kriptovalūtas rakšana ir iespējama, ja pieder patiešām daudz iekārtu un nav nepieciešami nekādi līdzdalībnieki, ar kuriem vēl nāktos dalīt savus ienākumus, turklāt var izvairīties no nodevām un nav jārēķinās ar citiem. [2]

4.2. Komandas rakšana

Kriptovalūtas ieguves kontekstā, komandas rakšana ir līdzekļu apvienošana, ko veic racēji, kuri dalās ar savu apstrādes jaudu tīklā un sadala atlīdzību vienlīdzīgi, atkarībā no darba apjoma, ko iesaistītās iekārtas veic, lai atrastu nākošo bloku. Atlīdzība tiek piešķirta dalībniekiem, kuri iesniedz daļēji derīgu pierādījumu. Komandas kriptovalūtas rakšana sākās, kad solo rakšanas grūtības palielinās līdz tam, kad racējiem ar vājām jaudām aizņemtu vairāki gadsimti, lai radītu bloku. Šīs problēmas risinājums ir tāds, ka racēji apvieno resursus, lai varētu ātrāk pievienot blokus, un katrs racējs saņemtu daļu no atlīdzības regulāri, nevis nejauši vienreiz pāris gados vai pat vēl retāk. [13]

Ieguvumi no komandas rakšanas ir tādi, ka visas komandas ierīces iesaista spēkus, lai atrastu pareizo risinājumu un šī jauda parasti ir tik liela, ka izskauž visus solo racējus, atstājot tiem ļoti mazu iespēju būt pirmajiem, kuri iesniedz pareizu risinājumu. [13]

Skatoties uz mīnusiem, stabila ienākumu plūsma paliks maza. Kriptovalūtas rakšanas baseins ir gluži kā loterijas baseins: grupa iegūst milzīgu balvu, bet indivīdi saņem tikai nelielu daļu. Protams, ja komanda ir tā, kura iesniedz pareizo risinājumu pirmā un tas tiek pieņemts, kā patiess, tad komanda tiek atalgota, bet šis atalgojums tad jāsadala uz tiem, kuri ir kaut kādu pienesumu devuši, lai realizētu bloku. No sākuma visu atalgojumu saņem komandas menedžeris un tas vēlāk sadala ieņēmumus par ieguldīto darbu. Kā arī, pastāv iespējas

menedžeriem krāpties, bet tas visticamāk agrāk vai vēlāk būs pamanīts un nekur nevarēs izvairīties no tā. [13]

Rakšanas baseini atalgojumu aprēķina izmantojot aprēķināšanas sniegšanas konceptu. Atlīdzība ir saistīta ar skaitļošanas jaudu, ko iesniedz baseinam. Tā ir sistēma, kas darbojas labi, bet ir atšķirīgas starp baseiniem. Tas nozīmē, jo vairāk tiek iesniegti pienesumi jauna bloka pievienošanai baseinā, jo lielāka atlīdzība pienākas. Šo principu var uzskatīt par godīgu, bet nosacījumi, protams, var atšķirties starp baseiniem. Tāpēc, pirms pievienošanās kādam baseinam, jānoskaidro, kā tiek izsniegti ieņēmumi, cik liela ir to nodeva un citus interesējošos jautājumus. [13]

Ja ir jāizvēlas starp esošajiem rakšanas veidiem – solo, komandas, mākoņu –, tad autors dod priekšroku komandas kriptovalūtas rakšanai, jo reti kurš būs spējīgs nodarboties ar solo rakšanu zemās jaudas dēļ. Mākoņa rakšanā pastāv lielas krāpnieciskas darbības risks, vai reālas mākoņa rakšanas serviss, bet ieņēmumi būs pielīdzināmi nullei vai pat ar zaudējumiem. Tas neizslēdz, ka komandas rakšana būs pelnoša, jo viss ir atkarīgs no komandas, tās jaudas, iesaistīto dalībnieku skaita un citiem faktoriem. Tiek uzskatīts, ka šī būs vispareizākā izvēle, lai efektīvi nodarbotos ar kriptovalūtas rakšanu un gūtu pastāvīgus ienākumus, jo pastāv daudz lielākas iespējas pievienot jaunu bloku. [13]

4.3. Mākoņa rakšana

Mākoņa rakšana ir *Bitcoin* ieguves process, izmantojot attālo datu centru ar kopīgu apstrādes jaudu. Šis rakšanas veids ļauj racējiem rakt *Bitcoin* vai alternatīvas kriptovalūtas bez aparatūras pārvaldīšanas. Rakšanas fermas izvieto un uztur kompānija, un klientam vienkārši jāreģistrējas un jāiegādājas akcijas vai jānoslēdz līgums. Tā kā mākoņa rakšana tiek sniegta kā pakalpojums, kompānija iekasē naudu par iekārtu uzturēšanu, kas var radīt mazāku peļņu. [12]

Ņemot vērā iepriekš minēto mākoņu kriptovalūtas rakšana ir ideāls risinājums: jauda tiek iznomāta no iekārtām, kas atrodas, iespējams, attālā, vēsā vietā. Mākoņu kriptovalūtas rakšanas uzņēmums rūpējas par racēju uzturēšanu un operācijas ieņēmumi tiek dalīti. [12]

Nav jāveic nekādi ieguldījumi iekārtu iegādē un visu izdara pats uzņēmums, klients tikai iegādājas jaudu un cer, ka šī kompānija ir pietiekami jaudīga un pieņem pareizos lēmumus, lai varētu pievienot bloku. [12]

Taču nepieciešams pieminēt arī shēmu risku. Kad *Bitcoin* sāka gūt panākumus, uzdarbojās daudz shēmu, un slavenākās no tām bija *Bitcoin Savings and Trust*, *Bitconnect and OneCoin*. Šie uzņēmumi sludināja, ka tiem pieder kriptovalūtas rakšanas iekārtas, sniedza diezgan ticamus pierādījumus un liela sabiedrības daļa paļāvās uz šiem krāpniekiem un veica paskaitījumus un ticēja, ka gūs kādu peļņu. Izrādījās, ka krāpniekiem nav iekārtu, un cilvēki

tiek apmānīti un ir atdevuši naudu ne par ko. Šādi neliela sabiedrības daļa tika apmānīta un cilvēki nevēlējās sniegt sūdzības par pāris simtiem dolāru, ko ieguldījuši. [12]

Neskatoties uz cilvēku negatīvo pieredzi, ir arī dažas “reālas” mākoņu kriptovalūtas rakšanas kompānijas, kam pieder aparatūra un raktuves. Zināmākās trīs kompānijas ir: *Genesis Mining*, *Bitclub Network* un *Hashflare*. Ir uzņēmumi, kuriem patiešām pieder daudz kriptovalūtu rakšanas iekārtu un klienti var vērot kā viņiem veicas, skatīties kāda peļņa vai zaudējumi pēc kriptovalūtas cenas svārstībām. Kompānijas cenšas, lai tās būtu ieguvējas neatkarīgi no tā, vai cena ceļas, vai krītas. Ja, piemēram, *Bitcoin* cena krasi aug, tad tas nozīmē, ka klients saņems mazāk, nekā vienkārši iegādājoties *Bitcoin* un turot savā makā. Toties, ja tā krasi krītas cenā, klients neko nenopelnīs un cietīs zaudējumus. [12]

Galvenais ir neaizrauties ar lielu līdzekļu ieguldīšanu šajos pakalpojumos un kriptovalūtās kopumā, jo visu laiku pastāv risks, ka attiecīgā kriptovalūta var bankrotēt un nekādas atmaksas netiks veiktas. Autora prāt nepieciešams ieguldīt tik, cik ir gatavība zaudēt. [12]

Visus aspektus izvērtējot, vieglākais ceļš saņemt ienākumus ir iegādājoties *Bitcoin*, vai kādu citu vērtīgu kriptovalūtu, kad kriptovalūtas cena ir zema un cerēt, ka tā kādu dienu krasi celsies augšā. Tādā veidā neapgrūtinot sevi un vēlāk pārdodot savu kriptovalūtu iegūstot diezgan labus ienākumus. Labāk izvairīties no kriptovalūtas mākoņa rakšanas, vai arī detalizēti izpētīt visu un ja apmierina, tad var mēģināt piedalīties šādā darbībā.

5. KRIPTOVALŪTAS RAKŠANAS IZDEVUMI

Uzsākot kriptovalūtu rakšanu ir jāreķinās ar tādiem aspektiem kā elektrības un iekārtu izmaksas, atbilstošu telpu izvēli rakšanas iekārtām, kā arī ar mainīgo ienesīgumu. Pēc šīs nodaļas autors sniegs galvenos secinājumus, vai kriptovalūtu rakšana ir laba investīcija.

5.1. Elektrības izmaksas

Iepriekš tika minēts, ka šīs fermas ievērojami patērē elektrību. Lielākā daļa ASIC racēja iekārtas patērē 1'500Wh un darbojas visu cauru diennakti jeb 24 stundas dienā un patērē $1,500 \times 24 = 36,000\text{Wh}$ jeb 36kWh. Mēnesī šāda viena ferma patērēs 1,080 kWh, kas būtu ap 205 EUR rēķins, lai nodrošinātu elektrību (ja vidējā cena, ko piedāvā elektrības sniedzēji ir ~0.19 EUR/kWh). Citās valstīs elektrības izmaksas ir zemākas nekā Latvijā. [1]

Kriptovalūtas procesā arī izdalās karstums tāpēc nepieciešams rast risinājumus iekārtu dzesēšanai, lai tās nepārkarstu un pēc iespējas efektīvāk veiktu rakšanu. Būs jāiegādājas dzesēšanas iekārtas, vai jānovada siltums, kā enerģija, kas sildītu māju vai ūdeni. [1]

5.2. Iekārtas izmaksas

Racēju aktivitātes ir radījušas deficītu tirgū visām komponentēm un iekārtām, kas ir saistītas ar kriptovalūtas rakšanu -videokartes, ASIC racēja iekārtas, barošanas blokus, mātes plates. Pieaugošā pieprasījuma dēļ pieaug arī komponentu cenas. [1]

Pašlaik cenas ir augstas un tie, kuri vēlas uzsākt kriptovalūtas rakšanu, iekārtu atpelnīšanas periods būs ilgāks nekā tiem, kas šīs iekārtas iegādājās pirms šo komponentu deficīta sākuma. Pirms iegādāties kriptovalūtas rakšanas iekārtu vai videokartes ir jāaplūko tās veiktspēja un elektrības patēriņš, lai varētu izreķināt kāds būs šīs iekārtas ienesīgums un vai tas spēs pārsniegt tā izmaksas. [1]

Vidusmēra videokartēm veiktspēja ir vien nedaudz zemāka par 20-30% zemāka nekā augsta līmeņa videokartēm un to cena ir uz pusi mazāka.. Toties augsta līmeņa GPU elektrības patēriņš ir ievērojami zemāks, kas ilgākā laika posmā atpelnītos labāk. [1]

5.3. Telpu izvēle

Iekārtām nepieciešamas drošas, tīras, sausas un labi ventilējamas telpas. Visticamāk šīs iekārtas arī netiks turētas dzīvoklī, jo tās ir pietiekoši skaļas. Ja šādas telpas nav pieejamas, tad tās arī būs liekas izmaksas. [1]

Telpai jābūt:

- drošai, lai izskaustu nesankcionētu piekļuvi un netiktu fiziski bojātas iekārtas;
- tīrai, lai ventilatoriem nebūtu jādzenā putekļus un to kalpošanas ilgums būtu pēc iespējas garāks, kā arī pašas iekārtas nepārkarstu;
- sausai, lai pasargātu no kondensāta un ūdens nokļūšanas uz fermām, kas var radīt bojājumus un īssavienojumus;
- labi ventilējamai, lai novadītu karstumu, ko rada iekārtas un nebūtu jādzesē jau ar sakarsušu gaisu;
- nodrošinātai ar interneta piekļuvi un elektrību. [1]

5.4. Mainīgi ienākumi

Ienākumi var būt ļoti mainīgi. Vienu dienu kriptovalūtas vērtība strauji pieaug, citu dienu vērtība dramatiski krītas. Lielās svārstības, ko piedzīvo kriptovalūtas parasti balstās uz kādu sistēmas ievainojamību vai nelabvēlīgu lielvalstu regulāciju attiecībā pret kriptovalūtām, vai kāda cita iemesla dēļ. [1]

Viens no lielākajiem riskiem ir, ka valūtas vērtības samazinās, vairs nenes peļņu, nepiedzīvo kāpumus, kas tirgū rada ik pa laikam pieplūdumu ar iekārtām, kuras pārdod bijušie racēji, mēģinot mazināt savu zaudējumu apmēru. [1]

6. ATTIEKSME PRET KRIPTOVALŪTĀM

6.1. Bankas attieksme pret kriptovalūtām

Daudz ir dzirdēts, ka bankas nosoda kriptovalūtas un šo kustību, jo tās netiek kontrolētas un neviens neaizstāvēs tos lietotājus, ja kaut kas atgadīsies ar tām un pastāv liels risks zaudēt visus ieguldījumus šajās valūtās.

Galvenā priekšrocība cilvēkiem vairs nav jāiet, jāpieprasa tradicionālajām bankām, ja viņiem ir nepieciešams finansējums. No lietotāja uz lietotāju tīklos, tostarp tie, kas balstās uz kriptovalūtām, kļūst arvien izplatītāki un tiem, kurus tradicionālās bankas varētu atteikt, tagad ir vēl viens veids, kā finansēt. [5]

Var teikt, ka cilvēki meklē citus veidus, kā tikt pie līdzekļiem. Cilvēki ir gatavi riskēt un mēģināt, ko citu, cerot uz to, ka gūs kādus panākumus izvairoties no darbībām ar bankām. Šis baida bankas un tās iestājas pret kriptovalūtām kā tādām, jo tās ir gandrīz vai neiespējami kontrolēt, nav zināms kādiem mērķiem tiek veikti darījumi, kā arī nav zināmi dati, kuram pieder konts. [5]

Tradicionālajām bankām ir jārīkojas tādās jomās kā klientu apkalpošana, digitālie piedāvājumi. Ja bankas nedomās par digitālajiem risinājumiem, kas pārsniedz standarta mobilās bankas lietotnes, pastāv risks, ka bankas paliks novārtā. [5]

Lai centrālās bankas nezaudētu savas pozīcijas, tām noteikti būtu jānāk pretī ar piedāvājumiem, kādus piedāvā kriptovalūtas, vai jāiesaistās pašiem šajos tīklos izsniedzot, piemēram, aizdevums *Bitcoin*. Kriptovalūtas, iespējams, varētu pilnībā izskaust bankas, ja lielākā daļa sabiedrības un uzņēmumi pārietu uz norēķiniem ar kriptovalūtu apmaksu, ko noteikti bankas nepieļautu, visādos veidos ar iesaistot valdību. [5]

6.2. Valdības attieksme pret kriptovalūtām

Valdības iet laukumā līdz un cenšas ieviest dažādus likumus, lai kontrolētu notikumus valstī. Ir valdības, kuras ir atzinušas kriptovalūtas un atbalsta tās, ir arī tādas, kuras boikotē to darbību, kā arī kurām ir diezgan neitrāla attieksme pret tām.

Runājot par jaunām zinātnēm un tehnoloģijām, nav iespējams nerunāt par Amerikas Savienotajām Valstīm. Saskaņā ar *Outlier Ventures* statistiku, gandrīz ceturta daļa pasaules bloku ķēdes kompāniju ir no Amerikas Savienotajām Valstīm, un ASV var uzskatīt par bloka ķēdes tehnoloģijas attīstības centru. Tomēr, no otras puses, atšķirībā no ASV bloku ķēdes tehnoloģijas straujas attīstības ASV ir konservatīvs priekšstats par bloka ķēdes tehnoloģijas akciju cenu strauju pieaugumu. [6]

Amerikas Savienotajām Valstīm ir pozitīva attieksme pret kriptovalūtām un varētu teikt, ka ir vienas no lielākajām bloka ķēdes turētājām, toties neatbalsta krasus cenas kāpumus šīm kriptovalūtām. ASV uzmana un strikti pārvalda kriptovalūtas. Valdība uzskata, ka šī sistēma patērē diez gan daudz enerģijas un joslas platums, kas tiek izmantots bloka ķēdēs nodrošināšanā ir problemātisks. Pastāv ar liels risks ar kontu pārvaldīšanu, ja lietotājs kaut kādā veidā pazaudē pieeju savam privātajam kontam, tad šim kontam ir principā neiespējami tikt klāt. Savukārt, ja lietotājs nozaudē savu paroli bankā, to ir iespējams viegli atjaunot. [6]

6.3. Sabiedrības attieksme pret kriptovalūtām

Cilvēku attieksme pret tām ir visai dažāda, daži pieturās pie pārbaudītām vērtībām un garantijām par saviem līdzekļiem, tāpēc paliek uzticīgi bankām. Kā arī ir daļa sabiedrības, kas vēlas uzņemties risku un iegādājas kriptovalūtas, vai pat paši iegulda līdzekļus un piedalās kriptovalūtu rakšanā.

The Irish Times iegūtie jaunie pētījumi liecina, ka aptuveni 120 000 cilvēku Īrijā pieder kriptovalūtas, kas ir par 300% vairāk nekā pēdējos četros gados. [7]

Acīmredzami, ka kriptovalūtu popularitāte pieaug un to turētāju skaits aug ar katru gadu. Protams, ka populārākā no tām ir *Bitcoin*. Autors uzskata, ka cilvēki cenšas uz *Bitcoin* cenas kritumiem to iegādāties un uz to lieliem kāpumiem – pārdot. [7]

Valdību un sabiedrības attieksme pret kriptovalūtām ir vienāda – gan tādi, kas atzīst un atbalsta, gan tādi, kuri ir pilnībā ir pret to un asi kritizē, kā arī tādi, kuriem nav viedokļa, vai vispār nav dzirdējuši par tām.

7. KRIPTOVALŪTAS RAKŠANAS IETEKME UZ VIDĪ

7.1. Kriptoalūtas rakšanas negatīvā ietekme

Visi zina to, ka jebkura elektrotehnikas ierīce patērē elektrību un tas nav nekāds jaunums, ka šīs ierīces darbojas uz elektrības patēriņu.

Jebkurai sistēmai, kas izmanto elektroenerģiju, ir negatīva ietekme uz vidi, piemēram, elektroenerģijas izmantošana veicina siltumnīcefekta gāzu emisijas (elektrība veido aptuveni 25% no emisijām, un *Bitcoin* uzturēšana aptuveni 0,01% no elektroenerģijas patēriņa). *Bitcoin* ar saviem lielajiem elektrības patēriņiem veido tikai 0,01% emisijas uz kopējā fona, tas nav sevišķi liels faktors. Iespējams visas kriptoalūtu uzturēšanas kopā varētu radīt 0,03%, jo pārējām kriptoalūtām ir daudz mazāk iekārtu nekā tās, kuras tiek izmantotas *Bitcoin* rakšanā. Ir arī daudzi raksti, kur tiek vainota kriptoalūtu rakšana, kā iemesls globālajai sasilšanai, bet netiek vainotas, piemēram, bankas, kuru ietekme uz vidi noteikti ir daudz lielāka. [10]

Kriptoalūtu rakšanā tiek patērētas izejvielas, kā metāls, varš un citas, lai saražotu komponentes, ko izmanto, lai ražotu jebkādu citus produktus. Pētījumi liecina, ka elektrības patēriņš un izejvielas būtiski neietekmē apkārtējo vidi, taču šī darbība rada siltumu, kas varētu veicināt globālo sasilšanu. [11]

Elektroenerģijas ražošanā tiek izmantoti dažādi veidi. Viens no video postošākajiem veidiem kā iegūt elektrību ir dedzinot fosilos kurināmos, ko galvenokārt piekļūst Ķīna, kas ar ir lielākā ogļu patērētāja elektroenerģijas ražošanā. Ķīna ir viena no lielākajām kriptoalūtu rakšanas valstīm un elektrības saražošana šādā veidā piesārņo gaisu, ūdeni, kā arī augsni. [11]

Lauka izveidošana kriptoalūtu ieguves veikšanai, kā arī jebkura datu centra izveide rada ainavas izmaiņas. Iemesls tam ir ne tikai ēku būvniecība, bet arī lineāro sakaru ierīkošana, ar nosacījumu, ka tiek izveidotas nosacītas platības. Elektrības līnijas, elektriskais tīkls (iekšējais un ārējais), optisko šķiedru kanāli liela apjoma informācijas pārraidei, ceļi (apmales, grāvji, notekas u.c.), santehnika, ugunsdzēsības infrastruktūra (betonēšana, teritorijas apgrīšana, zaļo zonu sastāva maiņa), drošības infrastruktūra (žogi, apsardze), sanitārās aizsardzības zonas. [11]

Šie visi faktori ir pieskaitāmi, ja tiek ieviesti lieli kriptoalūtu rakšanas centri, vai jebkādi lieli datu centri, kas izmaina visu apkārtējo vidi.

Ne tikai vide tiek ietekmēta, bet arī cilvēku veselība. Pasliktinās gaisa, ūdens un augsnes kvalitāte. Lai gan darba autors neatrada pētījumus par kriptoalūtas rakšanas ietekmi un veselību, arī tam ir negatīvie aspekti, kas ietekmē cilvēka veselību.

8. PRAKTISKAIS DARBS

8.1. Apraksts par ierīci

Autors savā darbā veicat kriptovalūtas rakšanu mājas apstākļos kā praktisko daļu. Autora mērķis ir noskaidrot sava datora spējas šāda veida uzdevumu izpildē. Pirmā problēma ar ko saskarās darba autors ir nespēja veikt kriptovalūtas rakšanu ar grafisko karti. Tika meklēti dažādi risinājumi, bet iznākums bija neveiksmīgs. Autors uzskata, ka grafiskās kartes nodrošina daudz lielākas jaudas nekā procesori, tāpēc šīs problēmas risinājumi tiks meklēti arī turpmāk.

Rezultātā autors veica šo uzdevumu tikai ar centrālā procesora palīdzību jeb CPU, ar kuru izdevās pievienoties kopējam kriptovalūtas rakšanas tīklam un mēģināt veikt attiecīgos uzdevumus ar sava procesora jaudu. Dators ir aprīkots ar *Intel(R) Core(TM) i7-2670QM CPU @ 2.2 GHZ*.

8.2. Electroneum kriptovalūtas rakšana ar CPU

Pirmā kriptovalūta, ar ko autors vēlējās veikt rakšanu ir *Electroneum*. *Electroneum* tika izvēlēts atverot saiti www.youtube.com un ierakstot angļiski kriptovalūtas rakšana ar CPU/GPU. Tā tika nonākts pie viena no populārākajiem video materiāliem, kura norādēm tika sekots.

Pirmais uzdevums, ko nācās veikt, bija atvērt digitālo maku, un veikt reģistrāciju ar *Facebook* kontu. Nākamajā solī, tika instalēta kriptovalūtas rakšanas programma un ievadīta nepieciešamā informācija, kā piemēram, izvēlētais tīkls ar portu, digitālā maka adrese un cita informāciju. Tika noskaidrots, ka GPU nepiedalās šī uzdevuma veikšanā, jo saņemts brīdinājums par to, ko var aplūkot pielikumos zem attēla (10.5. att. GPU brīdinājumi). Papildus tika saņemti apstiprinājumi, ka tiek veikta rakšana ar procesora palīdzību.

Par veiksmīgu darbību liecina visi saņemtie paziņojumi, par jaunas transakcijas pievienošanu, ko var aplūkot 1.pielikumā zem attēla (10.1. att. Informācija par jauna bloka pievienošanu), kas liecina par to, ka notiek komunikācija kriptovalūtas rakšanas tīklā.

Tika saņemta informācija par to, cik daudz *hash rate* spēj procesors sniegt sekundes laikā, kas ir aplūkojams 1.pielikumā zem attēla (10.2. att. *Hash rate* paziņojums). Jaudas ir mazas salīdzinot ar to, ko GPU varētu sniegt

Tika saņemti paziņojumi par neveiksmīgiem mēģinājumiem veikt transakciju, bet pienesums bija tik mazs, ka netika saņemts atalgojums- redzams 1. pielikumā zem attēla (10.3. att. Paziņojums par saņemtajām neveiksmēm), kā arī tika piefiksēts, ka ir pazudis tīkla savienojums.

Autora mērķis bija noskaidrot, cik procentuāli tiek izmantots centrālais procesors pie standarta konfigurācijām, kas aptuveni vidēji aizņēma 50% un pārējo procesora jaudu aizņēma citus uzdevumus veicot, kas aplūkojams pielikumā 1. zem attēla (10.4. att. Datora procesora jaudas noslogotība).

Lai noteiktu, cik elektrību patērē dators, tika iegādāts elektroniskais elektroenerģijas skaitītājs. Kas arī strādāja kā garants, ka netiks uztaisīts milzīgs elektrības rēķins. Tika uzņemts fotoattēls ar patērēto elektrību pēc sešām nostrādātām stundām, protams, kriptovalūtas rakšana tika veikta ilgāku laika posmu, bet patērētie kWh stundā lielas izmaiņas netika novērotas. Stundas laikā portatīvais dators veicot kriptovalūtas rakšanu aptuveni patērēja 0,19 kWh, kas liecina par to, ka elektroenerģijas patēriņš būtiski nav audzis, ko var aplūkot pielikumā 1. zem attēla (10.6. att. Patērētie kWh). Tika veikta *Electroneum* rakšana aptuveni diennakti, kuru laikā tika patērēti aptuveni 4,56 kWh, kas aptuveni izmaksāja 0,68 euro, pieņemot to, ka viens kWh izmaksā aptuveni piecpadsmit eiro centus.

Autors secina, ka datora procesoram ir grūti nodarboties ar kriptovalūtas rakšanu, jo *hash rates* nav no tiem lielākajiem. Dators spēja piedalīties dažu bloku realizēšanā, bet ieguldījums bija tik mazs, ka netika saņemts atalgots un tika izdoti paziņojumi par piedalīšanos. Pēc diennakts autors pieņēma lēmumu pārtraukt rakšanu, jo uzskatīja, ka nekādus panākumus nerasniegs.

8.3. Monero kriptovalūtas rakšana ar CPU

Ņemot vērā to, ka pirmās kriptovalūtas rakšana bija nesekmīga, autors veica izpēti par labāko virtuālo monētu, kas bija *Monero*. Šoreiz tika veikta padziļināta izpēte balstoties uz datora veikspēju. Autors izvēlējās atbilstošu rakšanas tīklu, kas ir speciāli domāta diezgan vājiem veikspējas rādītājiem.

Pirmie soļi, kurus veikt, lai nonāktu līdz pašai rakšanai ir diez gan līdzīgi kā iepriekšējai monētai. Vispirms jāizveido *Monero* virtuālais maks lejupielādējot programmu datorā un atverot maku.

Tam sekoja rakšanas programmas instalācija, kura ir tieši tā pati, kas ir *Electroneum*, tikai ar konfigurācijas izmaiņām, kas domātas *Monero* jeb norādot, ka nepieciešams rakt *Monero*, savu izvēlēto tīklu, kas paredzēta zemiem rādītājiem, attiecīgo portu, sava maka adresi, kā arī citu informāciju.

Pēc tam izvēlētajā tīklā bija nepieciešams norādīt, sava maka adresi un sava racēja identifikators, bet tas vēl nenozīmēja, ka tikšu saņemts atalgojums.

Līdz ko visi uzdevumi bija paveikti, tika palaista racēja programma, lai tā darbojas fonā un ik pa laikam tika pārbaudīts, vai tā veiksmīgi darbojas. Par veiksmīgu darbību liecina

programmas paziņojumi, ko var redzēt pielikumā 2. zem attēla (10.7. att. Pievieno jaunu bloku). Netiek saņemtas nekādas sistēmas kļūdas, tiek identificēti jauni bloki, kuri ir jāpievieno sarakstam jeb bloka ķēdei, kā arī dators iesaistās tajos, lai gan nesaņemtu nekādu atlīdzību, jo jaudas ir tik lielas tīklā, ka dators nespēj dot pienesumu, ko var aplūkot pielikumā 2. zem attēla (10.9. att.).

Elektroenerģijas patēriņā nebija novērojamas lielas izmaiņas, aptuveni 0,19 kWh stundā.

Par iegūtajiem rezultātiem, cik bieži jāpievieno jauns bloks un par to, ka veiksmīgi piedalos tīklā norāda visi paziņojumi, kas ir redzams pielikumā 2. zem attēla (10.8. att.).

REZULTĀTI

Svarīgākos rezultātus, kurus autors ieguva veicot savu praktisko darbu, bija atrast savam datoram piemērotu monētu, ko rakt, atbilstošu tīklu, kas paredzēts zemas veiktspējas ierīcēm.

Pēc diennakts darbības autors secina, ka *Electroneum* nav piemērots autora datoram kriptovalūtas rakšanā un uzturēšanā.

Savukārt *Monero* kriptovalūta bija piemērota autora datoram, jo tā bija piemērota autora datora centrālajam procesoram ar mazu veiktspēju. Rakšanas programmas uzstādīšana atšķīrās tikai ar citu parametru ievadīšanu, kas tika izmantota *Electroneum* monētas rakšanā. Ņemot vērā paziņojumus, ka tiek atjaunināta bloka ķēde un tiek atjaunināts saraksts, kas nebija novērojams ar iepriekšējo monētu, autors secināja, ka *Monero* kriptovalūta ir piemērota savam datoram. Darbā attēloti autora mēģinājumi rakt kriptovalūtu ar *Electroneum* un *Monero*. Praktiskajā daļā tika noskaidrots elektroenerģijas patēriņš abos variantos.

Autors guva papildu padziļinātas zināšanas par kriptovalūtām, bet galvenokārt par pašu *Bitcoin*, lai gan visas kriptovalūtas darbojas uz diezgan līdzīgiem principiem. Kā arī par rakšanas iekārtām, to iedalījumiem un iesaistītajiem dalībniekiem.

SECINĀJUMI

Bakalaura darbā „Kriptovalūtu rakšana, tā risinājumi un realizācija mājas apstākļos” autors apskatīja četrus dažādus kriptovalūtas rakšanas veidus, kā arī pēc to dalībnieku skaita un tika arī minēti izdevumi ar kuriem jāreķinās, ja ir doma iesaistīties rakšanā. Galvenais autora uzdevums bija veikt kriptovalūtas rakšanu, kas tika veiksmīgi izpildīts.

Darba rezultātā izvirzītā hipotēze daļēji tika apstiprināta, jo autora datoram nefunkcionēja video karte, netika iegūta kaut mazākā daļa kriptovalūtas to rakšanas procesā, un peļņu tas nenesa. Visi uzstādītie uzdevumi tika izpildīti un mērķis sasniegts. Autors iepazinās ar dažāda veida literatūru par kriptovalūtas rakšanu, pilnveidoja pamatzināšanas, kā arī aprakstīja katra rakšanas veida priekšrocības un trūkumus. Salīdzināja tos savā starpā pēc to veikspējām un monētu rakšanas dažādību. Darbā ir minētas galvenās izmaksas ar ko jāsaskaras uzsākot rakšanu.

Autors secina, ka nepieciešami ievērojami naudas līdzekļi, kurus var investēt, lai iegādātos un uzturētu kriptovalūtas rakšanas iekārtas. Jāveic aprēķini, vai atmaksāsies šīs iekārtas, izvērtējot pēc visām izmaksām un lielajiem riskiem, kuri pastāv saistībā ar šo procesu.

Autors iepazinās ar attieksmi pret kriptovalūtām un to rakšanu no vadības, bankām un sabiedrības. Valdībai un sabiedrībai viedokļi atšķiras, bet bankām tas noteikti ir jauns izaicinājums un konkurents, kas liek domāt pie tā, lai kriptovalūtas atbalstītāji tomēr paliktu banku paspārnē.

Praktiskajā daļā autors veica kriptovalūtas rakšanu ar savu personīgo datoru, mēģinot to darīt ar divām dažādām kriptovalūtām. Ar pirmo mēģinājumu tas neizdevās, tika saņemtas dažāda veida kļūmes un tika pieņemts lēmums neturpināt rakt *Electroneum*. Autors saskārās ar izaicinājumu nespējot veikt rakšanu ar savu grafisko karti, ko nespēja bakalaura darba rakstīšanas laikā sakārtot. Savukārt veiksmīga izrādījās rakšana ar *Monero*, pēc gudrāku lēmumu pieņemšanas, kas aprakstīts darba gaitā.

Autors secina, ka nav vērts rakt populāru monētu ar savu datora procesoru palīdzību. Nekādus ieņēmumus šī darbība nenes, noteikti būtu nepieciešams iegādāties ierīces ar lielām veikspējām un izvērtēt, kuru monētu rakt. Lai gūtu ieņēmumus, nepieciešams darboties komandā, jo pastāvniecīga iespēja būt pirmajam, kurš sniegs atrisinājumu bloka pievienošanai.

Autora izvēle būtu ASIC ferma, bet noteikti būtu nopietni jāpārdomā, kurai kriptovalūtai uzticēties, jo šīs iekārtas piedalās tikai vienas valūtas rakšanā un, ja izvēlēta kriptovalūta bankrotē, tad iegādāto iekārtu var jaukt ārā vai kā citādāk ar viņu rīkoties, jo nespēs nevienu citu uzdevumu pildīt. ASIC iekārtām ir daudz augstāka veikspēja rakšanā, nekā pārējiem veidiem un tās visvairāk tiek izmantotas lielos uzņēmumos, kas dod vēl lielāku

pārliecību par to iegādi. Kā arī noteikti iesaistītos komandas rakšanā, kas dotu lielākas izredzes pievienot jaunus blokus bloka ķēdē.

Autors tic kriptovalūtu nākotnei un uzskata, ka tās pastāvēs, kamēr būs lietotāji un to atbalstītāji, kuri turpinās ieguldīt līdzekļus.

Autors neuzsāks nopietnu darbošanos ar kriptovalūtu rakšanu, jo pastāv pārlietu liels risks, ka ieguldītie naudas resursi neatmaksāsies, vai arī tas notiks pēc ilga laika.

Gudrākais un ātrākais variants, lai saņemtu kādu peļņu, būtu iegādājoties vērtīgu kriptovalūtu, kad tās cena ir ļoti zema un cerēt, ka tā strauji pieaugs un tad meklēt iespējas to pārdot. Vēl viens variants ir rakt kā tikko parādījušos kriptovalūtu un cerēt, ka tā vienu dienu kļūs populāra un cena kāps. Autors secina, ka, visu laiku pastāv risks, un veiksmē ir atkarīga no ļoti daudziem faktoriem.

IZMANTOTĀ LITERATŪRA UN AVOTI

- [1] Rinalds Rihards Putrālis *Mainings un tā tehniskie risinājumi*, kursa darbs, 2018.
- [2] Ray King, What is Cryptocurrency? Your Complete Crypto ABC [tiešsaiste]. Pieejams: https://www.bitdegree.org/tutorials/what-is-cryptocurrency/#How_Does_Cryptocurrency_Work [aplūkots 28.04.2019.].
- [3] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder with a preface by Jeremy Clark *Bitcoin and Cryptocurrency Technologies* New Jersey, USA 131. – 139, 142-143, 201-202. [tiešsaiste]. Pieejams: https://www.lopp.net/pdf/princeton_bitcoin_book.pdf [aplūkots 12.03.2019.].
- [4] Brian Curran, Andrew Norry *The complete beginner's guide to Bitcoin*, Kooc Media Ltd. 1-4. [tiešsaiste]. Pieejams: <https://kriptoakademia.com/wp-content/uploads/2019/02/bitcoin-book.pdf> [aplūkots 12.03.2019.].
- [5] Jonathan Tarud *Is Traditional Banking Under Threat from Cryptocurrency?* [tiešsaiste]. Pieejams: <https://www.koombea.com/blog/cryptocurrency/> [aplūkots 22.05.2019.].
- [6] MyBestToken *Governments' Attitudes Towards Blockchain and Cryptocurrency* [tiešsaiste]. Pieejams: <https://medium.com/@MyBestToken/governments-attitudes-towards-blockchain-and-cryptocurrency-16ee9fcf7ed0> [aplūkots 22.05.2019.].
- [7] Mark Paul *Irish attitudes to cryptocurrencies shifting 'from suspicion to curiosity'* [tiešsaiste]. Pieejams: <https://www.irishtimes.com/business/technology/irish-attitudes-to-cryptocurrencies-shifting-from-suspicion-to-curiosity-1.3525859> [aplūkots 22.05.2019.].
- [8] BLOCKBASE GROUP *How fpga mining works: the a-b-cs of fpga mining* [tiešsaiste]. Pieejams: <https://blockbasemining.com/how-fpga-mining-works/> [aplūkots 23.05.2019.].
- [9] Ciprian V. *Your chance to jump into the fpga train is now! – fpga for dummies and experts alike* [tiešsaiste]. Pieejams: <https://1stminingrig.com/your-chance-to-jump-into-the-fpga-train-is-now-fpga-for-dummies-and-experts-alike/> [aplūkots 23.05.2019.].
- [10] Thomas DeMichele *Cryptocurrency Mining is Destroying the Environment* [tiešsaiste]. Pieejams: <http://factmyth.com/factoids/cryptocurrency-mining-is-destroying-the-environment/> [aplūkots 23.05.2019.].
- [11] Nazar Mozol *Cryptocurrencies and their impact on the environment* [tiešsaiste]. Pieejams: <https://goodanswer.space/en/cryptocurrencies-and-their-impact-on-the-environment/> [aplūkots 23.05.2019.].
- [12] Steven Hey *Bitcoin Cloud Mining Sites – Do They Actually Work?* [tiešsaiste]. Pieejams: <https://99bitcoins.com/bitcoin-mining/cloud-mining/> [aplūkots 24.05.2019.].

- [13] Gavin Phillips *What Is a Cryptocurrency Mining Pool? Everything You Need to Know* [tiešsaiste]. Pieejams: <https://blocksdecoded.com/cryptocurrency-mining-pool-explained/> [aplūkots 24.05.2019.].
- [14] Valsts Ieņēmumu Dienests *Fiziskas personas darbības ar kriptovalūtām* [tiešsaiste]. Pieejams: <https://www.vid.gov.lv/lv/fiziskas-personas-darbibas-ar-kriptoalutam> [aplūkots 25.05.2019.].
- [15] Cred24 *10 uzņēmumi Latvijā, kuros vari norēķināties ar Bitcoin* [tiešsaiste]. Pieejams: <https://cred24.lv/10-uznemumi-latvija-kuros-vari-norekinaties-ar-bitcoin/> [aplūkots 25.05.2019.].
- [16] Pieci.lv, Valērija Kovaļeviča, speciāli Pieci.lv, LSM.lv ziņu redakcija *Kriptovalūtas «rakšanas» dēļ pieaugušas videokaršu cenas* [tiešsaiste]. Pieejams: <https://www.lsm.lv/raksts/zinas/ekonomika/kriptoalutas-rakšanas-del-pieaugusas-videokarsu-cenas.a271678/> [aplūkots 25.05.2019.].
- [17] *GPU attēls* [tiešsaiste]. Pieejams: <https://www.google.lv/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=2ahUK Ewibx7nVgriAhVWAxAIHTH8BC0QjRx6BAgBEAU&url=http%3A%2F%2Fwww.coinminingrigs.com%2Fhow-to-build-a-6-gpu-mining-rig%2F&psig=AOvVaw1Sk7fnVKNjS8dy3nN4Fnon&ust=155895403331410> [aplūkots 25.05.2019.].
- [18] *FPGA attēls* [tiešsaiste]. Pieejams: https://www.google.lv/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=2ahUK Ewj35rag7niAhXJwosKHRjhDuQQjRx6BAgBEAU&url=https%3A%2F%2F1stminingrig.com%2Fyour-chance-to-jump-into-the-fpga-train-is-now-fpga-for-dummies-and-experts-alike%2F&psig=AOvVaw2nh2l3u24s_A7o_b8kwcAS&ust=1558954362114644 [aplūkots 25.05.2019.].
- [19] *ASIC attēls* [tiešsaiste]. Pieejams: https://www.google.lv/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=2ahUK Ewie0NvehLniAhUBtIsKHeaOCv4QjRx6BAgBEAU&url=https%3A%2F%2Fwww.amazon.com%2FAntMiner-T9-11-5TH-0-126W-Bitcoin%2Fdp%2FB01NCX6ZPO&psig=AOvVaw0qhlex3PZzTDiVkJHe_Br0&ust=1558954619349643 [aplūkots 25.05.2019.].

PIELIKUMI

1. Pielikums. Ekrānuzņēmumi no kriptovalūtas rakšanas ar Electroneum

```
[2019-04-28 21:45:40] : New block detected.  
[2019-04-28 21:46:40] : New block detected.  
[2019-04-28 21:47:40] : New block detected.  
[2019-04-28 21:47:59] : New block detected.  
[2019-04-28 21:48:00] : New block detected.  
[2019-04-28 21:48:38] : New block detected.
```

10.1. att. Informācija par jauna bloka pievienošanu

```
HASHRATE REPORT - CPU  
| ID | 10s | 60s | 15m | ID | 10s | 60s | 15m |  
| 0 | 45.5 | 42.7 | 45.0 | 1 | 48.5 | 45.8 | 47.4 |  
| 2 | 48.4 | 45.5 | 47.1 |  
Totals (CPU): 142.4 134.0 139.6 H/s  
-----  
Totals (ALL): 142.4 134.0 139.6 H/s  
Highest: 151.9 H/s
```

10.2. att. Hash rate paziņojums

```
Error details:  
| Count | Error text | Last seen |  
| 7 | Low difficulty share | 2019-04-29 09:22:53 |  
| 1 | [NETWORK ERROR] | 2019-04-29 01:30:08 |
```

10.3. att. Paziņojums par saņemtajām neveiksmēm

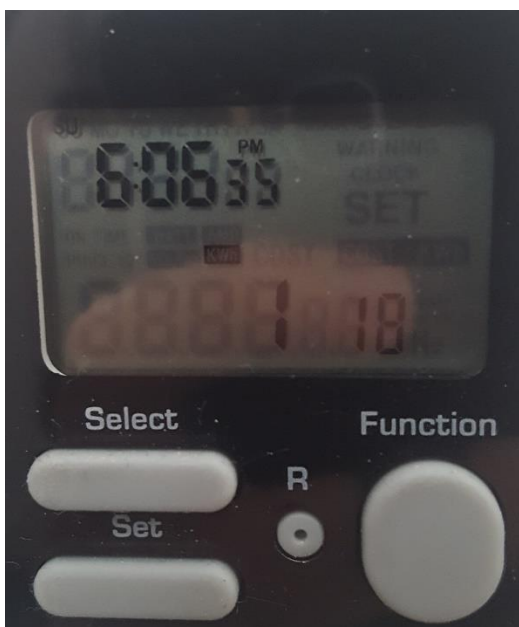


Utilization	Speed	Base speed:	2,20 GHz
62%	2,78 GHz	Sockets:	1
Processes	Threads	Cores:	4
193	3338	Logical processors:	8
Up time	Handles	Virtualization:	Enabled
11:05:44:30	113989	L1 cache:	256 KB
		L2 cache:	1,0 MB
		L3 cache:	6,0 MB

10.4. att. Datora procesora jaudas noslogotība

```
[2019-05-05 17:47:09] : NVIDIA: try to load library 'xmrstak_cuda_backend_cuda10_0'  
WARNING: NVIDIA Insufficient driver!  
WARNING: NVIDIA no device found  
[2019-05-05 17:47:09] : NVIDIA: try to load library 'xmrstak_cuda_backend_cuda9_2'  
WARNING: NVIDIA cannot load backend library: xmrstak_cuda_backend_cuda9_2.dll  
WARNING: NVIDIA Insufficient driver!  
WARNING: NVIDIA no device found  
[2019-05-05 17:47:09] : NVIDIA: try to load library 'xmrstak_cuda_backend'  
NVIDIA: found 1 potential device's  
[2019-05-05 17:47:10] : WARNING: backend NVIDIA disabled.
```

10.5. att. GPU brīdinājumi



10.6. att. Patēriete kWh

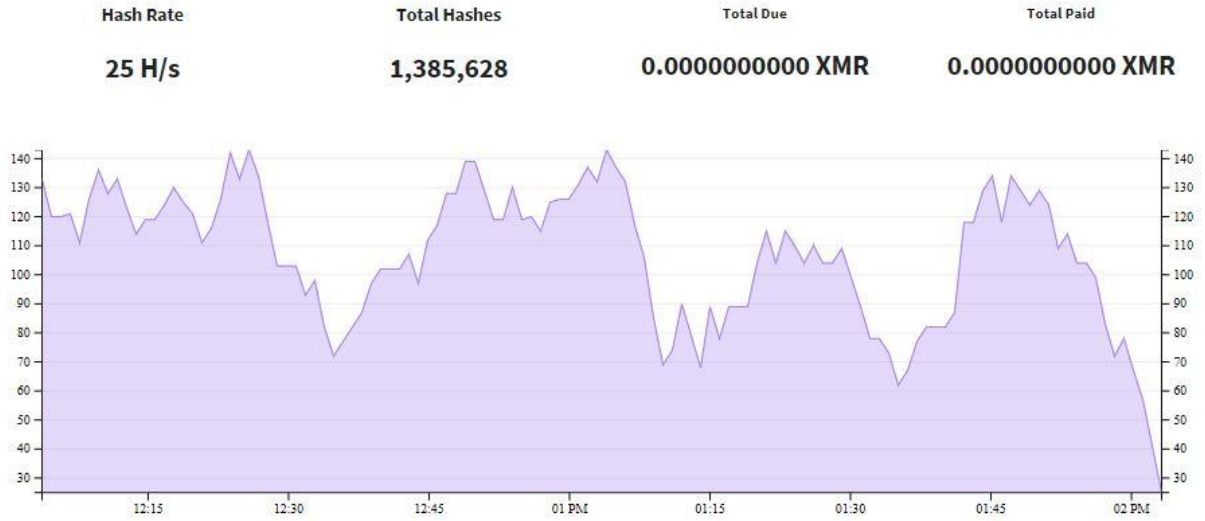
2. Pielikums. Ekrānuzņēmumi no kriptovalūtas rakšanas ar Monero

```
Error details:  
Yay! No errors.  
[2019-05-09 17:06:03] : New block detected.  
[2019-05-09 17:06:12] : New block detected.  
[2019-05-09 17:06:15] : Difficulty changed. Now: 1200.  
[2019-05-09 17:06:15] : New block detected.  
[2019-05-09 17:06:40] : Result accepted by the pool.  
[2019-05-09 17:06:44] : New block detected.
```

10.7. att. Iesaistīšanās bloka pievienošanā

```
RESULT REPORT
Currency      : monero
Difficulty    : 1320
Good results  : 65 / 65 (100.0 %)
Avg result time : 29.2 sec
Pool-side hashes : 83030
```

10.8. att. Statistika



10.9. att. Hash rate grafiks

Bakalaura darbs „Kriptoalūtu rakšana, tās risinājumi un realizācija mājas apstākļos”
izstrādāts LU Datorikas fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie
informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: Rinalds Rihards Putrālis _____

Rekomendēju/nerekomendēju darbu aizstāvēšanai (*nederīgo svītro vadītājs*)

Vadītāja: Politikas pētnieks M.pol. Sintija Lejniece _____ .05.2019.

Recenzents: profesors Dr.sc.comp. Juris Vīksna

Darbs iesniegts Datorikas fakultātē __.05.2019.

Dekāna pilnvarotā persona: vecākā metodiķe Ārija Sproģe _____

Darbs aizstāvēts bakalaura gala pārbaudījuma komisijas sēdē

03.06.2019. prot. Nr. _____

Komisijas sekretārs(-e): _____