RĪGAS VALSTS 3. ĢIMNĀZIJA

Pētnieciskais darbs
Programmēšanā

Kriptonaudas darbības principi un tās nākotne

12.a un 12.e1 klases skolnieki
Krists Mīlenbergs, Ričards Puķudārzs un Svens Gotvonī

RĪGĀ, 2023. GADS

Saturs

Ievads

Tēmas aktualitāte - Pēdējos gados kriptonauda ir ļoti populārs sarunas temats, šobrīd jau ir pirmā valsts, kas kā valsts valūtu izmanto kriptonaudu - El Salvadora, kas kā valūtu izmanto bitcoin. Jo vairāk cilvēki sāk pievērst kriptonaudām uzmanību, jo svarīgāk saprast, kā tad tās strādā un kādas ir barjeras to efektīvam ikdienas lietojumam.

Darba mērķis - Izprast kriptonaudas darbības pamatprincipus, cik gatavas tās ir pielietošanai ikdienā un nākotnē, kādas ir lielākās barjeras to plašākam pielietojumam pasaulē.

Darba mērķa sasniegšanai veicamo uzdevumu formulējums - teorijas izpēte, analīze, esošo pētījumu izpēte, līdz šim sastapto problēmu izpēte.

Izmantoto darba metožu uzskaitījums - Essošo pētijumu analīze, video resursi.

Teorija

Kriptonaudas darbības pamatprincipi

Pirmo reizi dzirdot par kriptonaudu var likties, ka tā ir digitāli pārvaldīta nauda, tomēr digitāli uzglabātu naudu savā bankas kontā par kriptonaudu nesauc. Pēc tezaurs.lv minētas kriptonaudas definīcijas, kriptonauda ir “Elektronisks maiņas vai maksāšanas līdzeklis, kas izmanto kriptogrāfiju, lai aizsargātu darījumus un kontrolētu jaunu vienību emisiju, darījumi tiek fiksēti publiskā žurnālā izmantojot blokķēdes tehnoloģiju.”. Tomēr darba autori vēlas piebilst, ka eksistē arī kriptonaudas, kas neizmanto blokķēdes tehnoloģiju, kā piemēram IOTA, kas izmanto pašu radītu, blokķēdei līdzīgu tehnoloģiju, ko sauc par “tangle”. Šī pētijuma nolūks ir aprakstīt kriptonaudas darbības pamatprincipus, lai jebkurš lasītājs spētu izprast, kā tās strādā.

Kriptonaudas ir decentralizētas, kas nozīmē, ka tās nav saistītas ar nevienu valsts vai institūciju, kas varētu kontrolēt tās cirkulāciju, piegādi un lietojumu, pamatojoties uz ko dažādas slavenības ir izteikuši viedokļus, ka kriptonauda ir nākotne, jo tā spēj risināt kādu svarīgu problēmu - tā atņem valstij kontroli pār naudu, jo lielāko daļu kriptonaudu kontrolēt ir praktiski neiespējami. Lai kriptonaudas būtu efektīvas ikdienas lietojumā, tām jābūt viegli izmantojamām un drošām. Šobrīd to plašam lietojumam vēl ir daudz barjeru, kas jāpārvar, lai tās kļūtu plašāk pieejamas.

Viens no svarīgākajiem jautājumiem par jebkuru valūtu ir “cik droša un stabila tā ir?”, tomēr lai šo jautājumu spētu atbildēt, ir svarīgi saprast, kā strādā kriptovalūta. Kā jau noskaidrots iepriekš, kriptonauda izmanto kriptogrāfiju un visi darījumi tiek fiksēti izmantojot blokķēdes tehnoloģiju. Kas tad ir blokķēde?

Blokķēde

Blokķēde (“blockchain”) ir tehnoloģija, ko izmanto, lai nodrošinātu informācijas drošību un neizmaināmību. Blokķēdes darbojas, veidojot savstarpēji saistītus datu blokus ļoti daudz, dažādos, nesaistītos serveros vai datoros. Bloķēdes informācija tiek apstrādāta un pārvaldīta kopienās. Katrs datu bloks satur informāciju par iepriekšējiem blokiem, kā arī jaunu informāciju, šī iebūvētā sasaiste padara blokķēdes tehnoloģiju izturīgu pret pārrakstīšanu un nodrošina informācijas integritāti un to saglabāšanu.

Atšķirībā no tā kā darbojas banku pārskaitījumi, blokķēdes darbīas principu dēļ, pārskaitījumu nevar atcelt: kad kāda pārskaitījums tiek apstiprināts blokķēdē, tas tur arī neatgriezeniski un neatsaucami paliks. Tas nozīmē, ka vienreiz nosūtītās kriptonaudu nevar atgriezt atpakaļ, tādējādi ir svarīgi, lai lietotāji rūpīgi pārdomātu, kādām personām un uz kādām adresēm tiešām vēlas nosūtīt savu kriptonaudu. Blokķēde arī nodrošina privātuma aizsardzību un daļēju anonimitāti, jo līdzīgi kā uz maka un cilvēku lietotām banknotēm nav rakstīts lietotāja vārds, tā kripto makam nav piesaistītas identitātes, izņemot retos gadījumos, kuros lietotājs var pielietot banku pakalpojumu starpniekus lai nopirktu vai pārdotu kriptonaudu, un šo pakalpojumu sniedzējiem pēc likuma ir jāidentificē savus lietotājus.

Kā tad īst strādā šie kriptomaki, kur cilvēki var uzglabāt savu kriptonaudu? Zināms, ka jebkuru profilu internetā lielākoties sargā parole, un iespējams, divu pakāpju autentifikācija, kas garantē ka pat uzzinot paroli, nespēj iekļūt kāda profilā. Tomēr, ja visa informācija par naudu ir publiski pieejama blokķēdē, kur tiktu uzglabātas paroles, tā lai tās spētu salīdzināt un tomēr neviens neizmantotu kāda paroli lai nozagtu viņa naudu?

Lielākā daļa blokķēžu tehnoloģiju izmanto asimetrisko šifrēšanu. Asimetriskā šifrēšana nodrošina drošu un pārbaudāmu transakciju pārraidi starp lietotājiem, jo katram lietotājam ir sava unikāla publiskā atslēga, ar kuras palīdzību viņš var saņemt maksājumus, bet privātā atslēga, kas ļauj veikt maksājumus un rīkoties ar savu kriptovalūtu. Tas ļauj nodrošināt lietotāju privātumu un drošību, neizmantojot vienotu centralizētu iestādi.

Hash

Noskaidrosim kas ir kriptogrāfisks pārskats (“hash”). Tas ir matemātiska algoritma veids, kas ņem ievaddatus (piemēram, tekstu, failu vai citu informāciju) un pārveido to par fiksēta garuma skaitlisko vērtību, ko sauc par "hash value" jeb “jaucējvērtību”, vai vienkārši "hash".

Šim algoritmam ir šādas īpašības:

- Vienādiem ievaddatiem vienmēr jāpārveidojas par vienu un to pašu vērtību.
- Jaucējvērtības ir ātri aprēķināmas no ievaddatiem.
- Nelielas izmaiņas ievaddatos rada pilnīgi atšķirīgu jaucēcjvērtību.
- Ir praktiski neiespējami no jaucēcjvērtības atgūt sākotnējos ievaddatus.
- Ir gandrīz neiespējami atrast divus atšķirīgus ievaddatus, kas rada vienādas vērtības.

SHA-256 (Secure Hash Algorithm 256-bit) ir viena no populārākajām un drošākajām hash funkcijām, ko izstrādāja ASV Nacionālās drošības aģentūras (NSA) pētnieki.

Šī hash funkcija ģenerē 256 bitu (32 baitu) garu hash vērtību, kas ir pietiekami liela, lai nodrošinātu unikālas hash vērtības dažādiem ievaddatiem. SHA-256 tiek plaši izmantota kriptogrāfijā un ir galvenā hash funkcija, ko izmanto Bitcoin un citu kriptovalūtu blokķēdēs.

Šifrēšana

Viens no populārākajiem kriptonaudu piemēriem ir Bitcoin, kas izmanto "elliptic curve digital signature algorithm" (ECDSA) - asimetriskās šifrēšanas algoritmu, kas balstīts uz eliptiskām līknēm. Šāds šifrēšanas veids nodrošina nepieciešamo drošības līmeni, lai aizsargātu kriptovalūtu transakcijas no nevēlamas iejaukšanās un uzbrukumiem.

Eliptiskās līknes ir balstīts uz kvadrātvienādojumu y^2 = x^3 + ax + b. Eliptiskās līknes aritmētika ir viena no galvenajām metodēm, kas izmantota kriptogrāfijā, jo tās ļauj veikt sarežģītus aprēķinus, kas ir grūti atgriezeniski. Bitcoin gadījumā eliptiskās līknes vienādojums ir y^2=x^3+7 (a=0 un b=7), jeb tā sauktā "Secp256k1", kas ir kļuvusi par vienu no visvairāk pētītajiem un izmantotajiem standartiem kriptogrāfijas jomā.

Lai ilustrētu kriptonaudu īpašuma pierādīšanas mehānismus, pieņemsim, ka mums ir jāparaksta un jāpārbauda Bitcoin transakcija, izmantojot eliptiskās līknes digitālo parakstu algoritmu (ECDSA) un eliptisko līkni secp256k1.

Privātā atslēga ir nejauši izvēlēts skaitlis d, kas ir mazāks par eliptiskās līknes noteikto skaitli n.

Eliptiskās līknes kriptogrāfijā skaitlis "n" ir līknes punktu skaita dalītājs un saucas par eliptiskās līknes skaitli. Skaitlis "n" ir liels pirmskaitlis un ir saistīts ar eliptiskās līknes bāzes punktu G. Bāzes punkts G ir tāds eliptiskās līknes punkts, ka ja to reizina ar skaitli n, rezultāts ir bezgalības punkts (neitralitātes elements eliptiskajā līknē).

Secp256k1 eliptiskajai līknei, ko izmanto Bitcoin skaitlis n = 115792089237316195423570985008687907852837564279074904382605163141518161494337

Tā kā skaitlis "n" ir liels pirmskaitlis, tas nodrošina drošību un sarežģītību eliptiskās līknes kriptogrāfijā, padarot šifrēšanas procesu grūti uzminamu vai jāatgriež.

Secp256k1 bāzes punkts G ir fiksēts un doti tā koordinātes: G = (Gx, Gy) = (55066263022277343669578718895168534326250603453777594175500187360389116729240,
32670510020758816978083085130507043184471273380659243275938904335757337482424)

Vienkāršai ilustrācijai pieņemsim, ka d=5. Publisko atslēgu Q iegūst privāto atslēgu d reizinot ar eliptiskās līknes bāzes punktu G, tātad publiskā atslēga Q ir punkts eliptiskajā līknē, ko apzīmē kā Q = d * G.

Q = d * G

Q = 5 * G = (28695624394210879124592488137516110653201860286576779384203804385410272791182,
84953501459853153369780256380685339286903451097573767075853751810885009971519)

Ziņojumu parakstīšana

Pieņemsim, ka vēlamies parakstīt ziņojumu "Hello, Bitcoin!". Izmantojam SHA-256, lai iegūtu tā kriptogrāfisko pārskatu (hash). hash = SHA-256("Hello, Bitcoin!") = 21345211001865623319131818167932239143

Tiek izvēlēts nejaušs skaitlis k, kas ir mazāks par eliptiskās līknes noteikto skaitli n.

Pieņemsim, ka n=3, bet patiesībā šīs vērtības būtu daudz lielākas.

Ar k reizinām bāzes punktu G, lai iegūtu jaunu punktu eliptiskajā līknē, ko apzīmē kā R (x1, y1) = k * G. Paraksta pirmais komponents ir x1 koordināte, kas apzīmēta ar r.

Aprēķina otro paraksta komponentu s pēc šādas formulas: s = k^(-1) * (hash + d * r) mod n, kur k^(-1) ir k modulārais inverss attiecībā pret n.

Paraksts ir pāris (r, s).

R = k * G = 3 * G = (21341003438865831675451468612002131777877597026633049990800022704084233428949, 78868048133412874972438856352738201693687824842887171226083338059494836496664)

Paraksta pirmais komponents ir x1 koordināte: r = 2134100343886583167545146861200213177787759702663304999080002270408423342894 9.

Aprēķinām otro paraksta komponentu s: s = k^(-1) * (hash + d * r) mod n s = 3^(-1) * (21345211001865623319131818167932239143 + 5 * 2134100343886583167545146861200213177787759702663304999080002270408423342894 49) mod n s = 84155132950406785520842900641864 2

Tātad, paraksts ir pāris (r, s) = (21341003438865831675451468612002131777877597026633049990800022704084233428949, 84155132950406785520842900641864 2).

Parakstu pārbaudīšana

Lai pārbaudītu parakstu, mums ir nepieciešams ziņojums, publiskā atslēga un paraksts. Mēs izmantojam šādus aprēķinus:

No ziņojuma tiek iegūts kriptogrāfisks pārskats (hash) tādā pašā veidā kā parakstīšanas laikā.

hash = SHA-256("Hello, Bitcoin!") = 21345211001865623319131818167932239143

Aprēķina divus koeficientus u1 un u2 pēc šādām formulām: u1 = hash * w mod n un u2 = r * w mod n, kur w ir modulārais inverss attiecībā pret skaitli n, kas nozīmē, ka w * s ≡ 1 (mod n). Tādējādi, w = s^(-1) mod n.

Iegūstam modulāro inversu w:

s = 84155132950406785520842900641864 2

w = s^(-1) mod n = 60302338491139961096959693555 1538

Aprēķinām koeficientus u1 un u2:

hash = 21345211001865623319131818167932239143

r =

213410034388658316754514686120021317778775970266330499908000227040842334289
49
u1 = hash * w mod n = 445954855946825299972704944816827862 40
u2 = r * w mod n = 102183790519424467812864584205191537661
Tātad, mums ir w = 603023384911399610969596935551538
u1 = 445954855946825299972704944816827862 40
u2 = 102183790519424467812864584205191537661

Tālāk aprēķina punktu P (x, y) eliptiskajā līknē, izmantojot šo formulu: P = u1 * G + u2 * Q. Šeit G ir bāzes punkts, un Q ir publiskā atslēga. Iesaistot iepriekš iegūtos rezultātus, sanāk ka P =
(213410034388658316754514686120021317778775970266330499908000227040842334289
49,
740765687877731078203157799510764186546068463306024639491822878667615299331
0)

Paraksts tiek uzskatīts par derīgu, ja x koordināte punktam P ir vienāda ar paraksta pirmo komponentu r. Citos vārdos, ja x mod n = r, tad paraksts ir derīgs.

Pārbaudām, vai P(x) koordināte ir vienāda ar r:

P(x) =
213410034388658316754514686120021317778775970266330499908000227040842334289
49

r =
213410034388658316754514686120021317778775970266330499908000227040842334289
49

Tā kā P(x) = r, paraksts ir derīgs. Tas apliecina, ka ziņojums "Hello, Bitcoin!" ir parakstīts ar privāto atslēgu, kas atbilst norādītajai publiskajai atslēgai.

Kā bitcoin izmanto šo šifrēšanu, un kas pārbauda maksājumus

Kā jau iepriekš minēts, katram Bitcoin lietotājam ir divas atslēgas: privātā un publiskā, kuru pielietojums jau tika paskaidrtos - ar privāto paraksta transakcijas, ar publisko pārbauda to likumību. Kad lietotājs vēlas veikt transakciju, kriptonaudas maks izveido ziņojumu un paraksta to ar savu privāto atslēgu, izmantojot ECDSA paraksta veidošanas procesu. Parakstītā transakcija satur informāciju par darījumu, piemēram, sūtītāja un saņēmēja adreses, pārskaitāmo summu un parakstu.

Šāda veida asimetriskās šifrēšanas metode ir laikietilpīga, jo tā ietver sarežģītus matemātiskus aprēķinus, lai šifrētu un pārbaudītu informāciju. Lai apstiprinātu un pievienotu jaunu bloku blokķēdē, nepieciešams atrisināt šo kriptogrāfiski sarežģītu problēmu, un to dara tā saucamie "Maineri". Šie "Maineri" ir spēcīgi datori, kas strādā, lai izveidotu jaunus blokus un nodrošinātu drošību blokķēdē, un tiem ir jāveic sarežģīti aprēķini, kas var patērēt daudz laika un resursu, tāpēc tie tiek atalgoti kā noteikts katrā kriptovalūtā - ar emisijām, un lai veiktu maksājumu ar kriptonaudu ir jāmaksā nodevas, kas arī iet kā atalgojums maineriem.

Kriptonaudas maku drošība ir svarīga, jo tie glabā visu lietotāja kriptonaudu ar privātu un publisku atslēgu. Ja maka pieejas frāze tiek nozaudēta vai kādam cits ir piekļuves pie tās, lietotājs var zaudēt savu kriptonaudu neatgriezeniski.

Drošības problēmas galvenokārt rodas ar uzlauztām vai nozagtām privātajām atslēgām, jo ar šī brīža pieejamām tehnoloģijām uzlauzt šifrēšanu šobrīd ir tuvu neiespējami. Tas varētu kļūt par realitāti ar tālāku kvantu datoru attīstību, jo tie šos aprēķinus var veikt daudz ātrāk. Tā kā visa līdzekļu piederība saistās ar šo atslēgu turēšanu un glabāšanu, lai identificētu kam pieder blokķēdē, tās zaudējot vai atdodot, līdzekļus neatgriezeniski pazaudē. Tā kā šī blokķēde nepieder nevienai centralizētai iestādei, bet to uztur tūkstošiem serveru visā pasaulē - nav iestādes kas risinās tavas problēmas vai spēs tavu naudu tev atņemt, ja pietiekami gudri to glabāsi.

"Maineri"

"Maineri" patērē ļoti daudz enerģijas, kas ir bijis viens no lielākajiem kritikas punktiem par kriptonaudu, un to ir centušies risināt ar citiem vienprātības risinājumiem, kas atvieglotu mineru darbu, lai patērētu mazāk enerģijas.

Maineri lejupielādē un sinhronizē blokķēdi, lai viņiem būtu jaunākā informācija par transakcijām un blokiem, saņem jaunas, vēl neapstiprinātas transakcijas no tīkla un pārbauda to derīgumu, tostarp parakstu un dubultmaksājumu pārbaudi.

Tālāk maineri izvēlas kopu derīgu transakciju, kas tiks iekļautas nākamajā blokā. Parasti tiek izvēlētas transakcijas ar augstākām nodevām, lai maksimizētu mineru peļņu. Maineri veido bloka galveni (header), kas satur metainformāciju, piemēram, bloka versiju, saiti uz iepriekšējo bloku, transakciju pārskata hash un laikzīmogu.

Maineri sāk skaitlisko procesu, ko sauc par "darba pierādījumu" (proof-of-work) aprēķināšanu. Bitcoin šis process ir balstīts uz SHA-256 hash funkciju.

Maineri izmanto nejauši izvēlētu skaitli, ko sauc par "nonsu" (nonce), un izveido hash no bloka galvenes un nonses. Mērķis ir atrast tādu nonsi, kas ļauj iegūt hash, kas ir zemāks par noteiktu mērķa vērtību. Šī vērtība tiek pielāgota laika gaitā, lai uzturētu konsekventu bloku izveides ātrumu.

Maineri pārbauda daudzus nonses, mainot tos un atkārtoti aprēķinot hash, līdz tiek atrasts derīgs risinājums.

Ja bloks ir derīgs, citi Maineri apstiprina to, izmantojot vienprātības mehānismu, un turpina strādāt pie nākamā bloka, ņemot vērā jaunāko pievienoto bloku.

Jauni bloki tiek pievienoti blokķēdei vienmēr virs iepriekšējā bloka, veidojot blokķēdes struktūru. Šī struktūra nodrošina, ka visas transakcijas ir hronoloģiskā secībā un ka tikai derīgas transakcijas tiek iekļautas blokķēdē.

Tīkla dalībnieki izplata jauno bloku visā tīklā, lai nodrošinātu, ka visiem dalībniekiem ir vienāda un sinhronizēta blokķēdes versija.

Kad miners ir veiksmīgi pievienojis bloku blokķēdei, tas saņem atlīdzību kriptovalūtā. Bitcoin gadījumā šī atlīdzība ir kombinācija no fiksēta bloka atlīdzības (kas samazinās ar laiku) un visu blokā iekļauto transakciju maksām.

Šī atlīdzība tiek izmaksāta mineram, veidojot īpašu transakciju, kas saucas par "maksājuma transakciju" (coinbase transaction), kas tiek iekļauta jaunajā blokā. Maksājuma transakcija rada jaunas kriptovalūtas monētas un nosūta tās uz mineru norādīto adresi. Mineru atlīdzība ir ļoti svarīgs mehānisms kriptovalūtu tīklos, jo tas nodrošina mineru motivāciju turpināt darbu un uzturēt sistēmu, kā arī palīdz regulēt jaunu kriptovalūtas monētu radīšanu.

Maineri turpina šo procesu, veicot transakciju apstiprināšanu, bloku veidošanu un darbības pierādījuma aprēķināšanu, nodrošinot kriptovalūtu tīkla drošību un integritāti.

Vienprātības mehānismi

Vienprātības mehānisms ir sakaru protokols, kas nosaka, vai blokķēdes tīkls izskatīs konkrētu darījumu. Ir vairāki dažādi vienprātības mehānismi - Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Importance (PoI), Proof of Capacity (PoC), Proof of Elapsed Time (PoET), Proof of Activity (PoA), Proof of Authority (PoA). Lielākoties tiek izmantoti šie trīs mehānismi:

1. Proof of work (PoW). Maineri risina sarežģīt kriptogrāfiskās problēmas, lai izveidotu bloku. Tie Maineri, kuri pabeidz bloku izveides procesu, tiek atlīdzināti ar kriptonaudu. Tas ir izplatīts vienprātības mehanisms, ko lieto populārākie kriptonaudu tīkli, piemēram, Bitcoin un Litecoin. Vairāki Maineri strādā kopīgi lai atšifrētu vienu tā saucamo “bloku”, un Maineris kurš veiksmīgi pirmais atšifrē to, tiek apbalvots. Proof of Work ir ļoti atkarīgs no veiksmes, jo apbalvojumu saņem tikai viens cilvēks, taču var palielināt savas iespējas, iegādājoties vairāk minerus, vai arī iegādājoties stiprākus minerus. Proof of Work mehānisms prasa lielu enerģijas patēriņu un ilgu apstrādes laiku.
2. Proof of Stake (PoS). Katrs Maineris uzliek likmi jeb “Stake” ar zināmu kriptovalūtas summu, jo lielāka likme, jo lielāka ir iespēja, ka tas Maineris tiks izvēlēts kā pārbaudītājs jeb “Validator”. Pārbaudītājs ir Maineris, kas apstiprina darījumus un saņem par to atlīdzību. Šis vienprātības mehānisms attīstījās kā zemu izmaksu, zemu enerģiju patērējoša alternatīva Proof of Work (PoW) algoritmam, par piemēriem var nosaukt Ethereum un BNB kriptonaudas. Tomēr tam ir trūkums, ka tas stimulē uzkrāšanu, nevis tērēšanu.
3. Delegated Proof of Stake (DPoS). Šis mehānisms ir līdzīgs proof of stake, bet pēc kriptonaudas ieguldīšanas Maineri balso par noteiktiem lietotājiem, kuri izveido blokus un saņem atlīdzību. DPoS ir izmantots tīklos, piemēram, Steemit un BitShares. Tas tiek uzskatīts par efektīvu un energoefektīvu alternatīvu Proof of Work (PoW) un Proof of Stake (PoS) mehānismiem, jo tas neprasa lielu enerģijas patēriņu, lai apstiprinātu blokus.

Kriptonaudas barjeras

Lai kriptonaudu varētu sākt lietot plašāks loks populācijas ikdienā, tai ir jābūt pietiekami ērti un viegi izmantojamai un nāktos pārvarēt dažādas līdz šim nepārvarētas barjeras.

Kriptonaudas tirgus ir pārāk mazs. Tas nozīmē, ka ar trigu var viegli manipulēt, mainīt kriptonaudas cenu. Pašlaik tas izpaužaš tā ka cilvēks ar pietiekamu kapitālu var samazināt vai paaugstināt kriptonaudas vērtību pietiekami pērkot vai pārdodot to. Mazais tirgus vēl nozīmē to, ka tas paļaujas uz citiem tirgiem, piemēram, bankām. Bankai bankrotējot, caur kuru tiek izmainīta kriptonauda ar naudu, pašas kriptonaudas vērtība krītas, kā tas piemēram notika ar USDC (USD coin), kad bankrotēja Silicon Valey Bank, vai gandrīz visām kriptonaudām pēc FTX maksātnespējas.

Vēl viena barjiera ir datoru ieguve. Kopš kriptonaudas atklāšanas un popularizēšanas ir palielinājies pieprasijums prieks datoru detaļam, ar to pieauga detaļu cenas un samazinājās pieejamo skaits detaļu [1]. Ražojot daudz detaļu sāk samazināties resursu skaits, piemēram, silikons priekš micročipu izstrādes [2].

Kriptonaudu maksājumi aizņem pietiekami ilgu laiku - atkarībā no kriptonaudas, bet piemēram bitcoin maksājumi aizņem ap 15-30 minūtēm, reizēm pat vairākām stundām, lai apstiprinātos. Tas gan atkarīgs no nodevas lieluma, ko iestati, tomēr neviens nevēlas maksāt 1 eiro nodevu papildus produkta cenai un PVN. Tas nozīmē, ka tādās situācijās, kā iepērkoties veikalā var nākties gaidīt līdz maksājums tiek pastiprināts.

Pāšreizējā Kriptonaudas aina

Pašlaik, kriptonaudas ir atkarīgas no citiem tirgiem. Padarot to cenas viegli manipulējamas, ko var redzēt pēc kriptonaudu nestabilējām vērtībām. Vērtība var mainīties, jo tika iesaldēta nauda ar kuru tiktu apmainīta kriptovalūtas maiņa, vai kāds, kuram pieder liela daļa no kriptonaudas kopuma, nolēma to masveidā pārdot vai arī kāds, kādi nopirka to masveidā paugstinot tās vērtību. Pašlaik to var pielīdzināt akciju tirgum ar mazāk regulācijām.

Kriptonauda patērē daudz enerģijas. Pašlaik vispopulārākā kriptonauda ir Bitcoin, kas patērē apmēram 127 TWh gadā. [3]. Kontekstam - Latvija 2018. gadā patērēja 7.2 TWh [4]. Gadā visas kriptonaudas rada starp 25 milijonu līdz 50 milijonu tonnu CO2 emisiju. Lielākā daļa kriptonaudu izmanto proof of work mehānismu, kas patērē vairāk elektrības, bet Ethereum kriptonauda patērē 99.9% mazāk elektrību izmantojot proof of stake mehānismu. Izmantojot Ethereum tiek patērēts tik pat daudz CO2 cik noreiķinoties ar karti.

Valstis, kur tiek iegūta kriptonauda, nav sagatavojušas savas infrastruktūras. Kriptonaudas iegūšana var uzlikt lielāku spriedzi uz elektrotīkla, piemēram, Teksas ECORT. Pietam ne visa elektrība ir iegūta no atjaunojamamiem enerģijas avotiem, bet no ogļu dedzināšanas, gazēs dedzināšanas, kas tiek izmantota iegūstot kriptonaudu. Vēl resursu trūkums priekš mineru detaļām traucē citiem tirgiem un padara resursus dārgākus, piemēram, pašreizējā micročipu krīze [2].

Kriptonaudas nākotne

Lai kriptonauda tiktu masveidā adoptēta būtu jāparvar daudz barjeru, kā neatkarība no citiem tirgiem, resursu efektīva izmantošana un CO2 emisiju samazināšana, kā arī valstīm būtu jāvēlas kriptonaudu pieņemt kā oficiālu valūtu, jeb zaudēt kontroli pār to, pilnībā izmainot valsts monetāro politiku. Visticamāk tuvākajā laikā kriptonauda netiks pieņemta masveidā, bet kā jauna inovatīva tehnoloģija tā varētu tikt arvien plašāk adoptēta, jo tā ir parocīgāka un tajā ir redzams potenciāls. Tomēr, pasaules valstu valdības aizvien vairāk pēdējo gadu laikā cenšas to izplatību ierobežot un aktīvi strādā pie savu kriptonaudu izveides, lai turpinātu savu kontroli pār iedzīvotāju finansēm (Ķīna, drīzmā ASV). Valdību veidotai kriptonaudai tāpat kā parastai naudai būs stabilitātes priekšrocība, jo to izmantos visā valstī, kas noteikts ar likumu, līdz ar to tās ārējā ietekme, īpaši lielajām valstu valūtām, būs mazāka. Lai kāda kriptonauda būtu neatkarīga no citiem tirgiem, tai būtu jākļūst pietiekami izplatītai un pielietotai ikdienā, lai investori nespētu izmainīt tās cenu vienkārši lielos daudzumos to nopērkot vai pārdodot. Līdz ar to, lai tās varētu masveidā adaptēt, vispirms ir jāpārvar visas pārējās barjeras, un tad jācer ka cilvēki vēlēsies tās adoptēt ikdienas pielietojumam un valstis tās neaizliegs.

Kriptonaudu apskats

Darba praktiskajā daļā tika salīdzinātas trīs populāras kriptonaudas: “Bitcoin” (PoW), “Ethereum” (PoS) un “Dogecoin” (PoW). Tika salīdzināti vairāki faktori: cena, pašreizējais piedāvājums, maksas, cik grūti iegūt, hash rate, vienas dienas aktīvais piedāvājums, pašreizējais piedāvājums, piedāvājums, 100 populārākās adreses, paredzamā TWh gadā un minimālās TWh gadā. Šie faktori labi attēlo kriptonaudas pielietojumu, stabilitāti un tās ietekmi uz dabu. Dati attēloti dienās. Dati tika ievākti no [11,12,13].

Darba praktiskā daļa pieejama saitē https://kripto.svenons.xyz

Atsauces

1. Tech4Gamers. Kāpēc datoru komponentes ir tik dārgas? Pieejams: https://tech4gamers.com/why-are-pc-parts-so-expensive/ [Skatīts 2023. gada 8. maijā].
2. Yahoo Finance (2021). Šīs nozares ciestu visvairāk globālās mikroshēmu trūkuma dēļ. Pieejams: https://finance.yahoo.com/news/these-industries-are-hit-hardest-by-the-global-chip-shortage-122854251.html [Skatīts 2023. gada 8. maijā].
3. Rocky Mountain Institute. Kriptovalūtu enerģijas patēriņa problēma. Pieejams: https://rmi.org/cryptocurrencys-energy-consumption-problem/ [Skatīts 2023. gada 8. maijā].
4. Vikipēdija (2021). Enerģija Latvijā. Pieejams: https://en.wikipedia.org/wiki/Energy_in_Latvia [Skatīts 2023. gada 8. maijā].
5. Kaspersky. Kas ir kriptovalūta? Pieejams: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency [Skatīts 2023. gada 8. maijā].
6. Built In. Kā izveidot kriptovalūtu. Pieejams: https://builtin.com/blockchain/how-to-create-a-cryptocurrency [Skatīts 2023. gada 8. maijā].
7. Investopedia (2021). Kā izveidot kriptovalūtu. Pieejams: https://www.investopedia.com/how-to-make-a-cryptocurrency-5215343 [Skatīts 2023. gada 8. maijā].
8. Whiteboard Crypto (2021). Kā darbojas Bitcoin kriptogrāfija? [Video]. YouTube. Pieejams: https://www.youtube.com/watch?v=3QCykHU89To&ab_channel=WhiteboardCrypto [Skatīts 2023. gada 8. maijā].
9. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Pieejams: https://bitcoin.org/bitcoin.pdf [Skatīts 2023. gada 8. maijā].
10. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security and Privacy, 104-121. doi:10.1109/SP.2015.14
11. Coin Metrics. Pieejams: https://coinmetrics.io (Skatīts: 2023.gada 25.maijā)
12. DigiEconomist. Pieejams: https://digiconomist.net (Skatīts: 2023.gada 25.maijā)
13. Cambridge Centre for Alternative Finance. Pieejams: https://ccaf.io (Skatīts: 2023.gada 25.maijā)