ESMINIŲ 100 KLAUSIMŲ

ISMAEL SANTIAGO MORENO

KRIPTOVALIUTOS:

LENGVAS BŪDAS PRATURTĖTI –

VISI ESMINIAI KLAUSIMAI IR ATSAKYMAI

„Popieriniai pinigai išnyks, o juos pakeis kriptovaliutos" - Elon Musk

OBUOLYS

ISMAEL SANTIAGO MORENO

KRIPTOVALIUTOS:
LENGVAS BŪDAS PRATURTĖTI

Iš ispanų kalbos vertė
IEVA BARANAUSKAITĖ,
UAB „METROPOLIO VERTIMAI“

OBUOLYS

TURINYS

III. Bitkoinas. Naujasis virtualusis auksas

IV. „Ethereum“. Išmaniųjų kontraktų galia

IX. Decentralizuotų finansų („DeFi“) revoliucija

X. Decentralizuoto finansavimo („DeFi“) sėkmingų projektų verslo modeliai

I

Konceptai ir technologijos, kurių pagrindu kuriamos blokų grandinės ir kriptografinės valiutos

1

Kas sieja lygiarangių tinklą ir blokų grandinę?

Lygiarangių tinklai (angl. *peer-to-peer network*, P2P) – tai tinklai, jungiantys tūkstančius ar net milijonus kompiuterių (kitaip – mazgų, angl. *nodes*), esančių bet kurioje planetos vietoje, kur nėra centrinio susijungimo taško, kadangi šie tinklai decentralizuoti, veikia pagal tą patį ryšių protokolą, kad sukurtų vieną didelį tinklą bet kokio tipo informacijai dalytis. Tokiu būdu šio tipo tinklų dalyviai gali keistis informacija tiesiogiai, be tarpininkų, tam tereikia atsisiųsti programinę įrangą (angl. *software*), kuri jūsų kompiuterį sujungtų su kitais žmonėmis, esančiais tinkle P2P, ir tokiu būdu su jais susisiekti.

Kas yra mazgai ir protokolai?

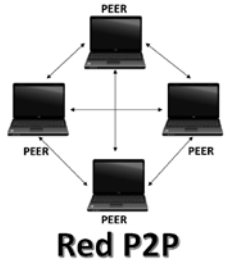
Mazgas gali būti superkompiuteris arba paprasčiausias asmeninis kompiuteris. Neatsižvelgiant į kompiuterinę galią visi mazgai turi turėti tą pačią programinę įrangą ar protokolą, kad galėtų bendrauti tarpusavyje. Šie mazgai yra sujungti P2P tinkle ir tokiu būdu galima atlikti ryšio ir duomenų perdavimo procedūras tarp dviejų ar daugiau kompiuterių, tai yra tame tinkle apdoroti ir perduoti kompiuteryje esančius duomenis, keistis ir dalytis informacija.

Pagal blokų grandinės (angl. *blockchain*) technologiją, mazgus sudaro visi į šį tinklą sujungti kompiuteriai, valdantys programinę įrangą, kad visi kartu galėtų dirbti.

Inžinerijoje kalbant apie ryšių protokolus turime galvoje taisyklių ir susitarimų rinkinį, apibrėžiantį ryšio ir duomenų perdavimo formatus bei procedūras tarp kompiuterių, ir visumą programų, naudojamų kompiuterių tinklui (mazgams) bendrauti tarpusavyje perduodant informaciją. Pvz., blokų grandinės protokolas suteikia galimybę apibrėžti bendrą dalyvaujančių tinkle kompiuterių bendravimo standartą.

P2P – tai tinklas, kuriame nėra jokios hierarchijos, kadangi mazgai pakeičia klientų ir serverių funkciją. Tokio tipo tinkle visi kompiuteriai yra vienodo lygio ir leidžia horizontalaus tipo komunikaciją. Susidomėjimą P2P labiausiai nulėmė jų panaudojimas skaitmeniniam turiniui perduoti.

P2P administruoja ir optimizuoja visų tinklo vartotojų juostos pločio naudojimą, pasitelkdamas tarp pačių vartotojų esantį užmegztą ryšį, tokiu būdu dėl didesnio jungčių skaičiaus gaunant efektyvesnį ryšį nei naudojant įprastas centralizuotas sistemas, kur visą juostos plotį teikia ir paskirsto išteklius paslaugai ar sistemai sąlyginai nedidelis serverių skaičius.



P2P veikimas paremtas ryšių protokolu, kuris leidžia šią programinę įrangą naudojantiesiems bendrauti tiesiogiai, be jokių tarpininkų. Šaltinis: Ismaelis Santiagas (Ismael Santiago).

Kokie didžiausi P2P pranašumai?

P2P tinklo didžiausi pranašumai:

- *Decentralizuotumas.* Šiuose tinkluose visi mazgai yra vienodi, dėl to vieno ar kito mazgo nebuvimas tokio tinklo veikimui įtakos neturi.
- *Patikimumas.* P2P tinklo paskirstytoji struktūra leidžia gauti informaciją nesiunčiant užklausų jokiems centralizuotiems serveriams.
- *Plėtimo galimybė*. Teigiama savybė – kuo daugiau mazgų bus įjungti į P2P tinklą, tuo geresnis bus jo veikimas, nes dalydamiesi savo resursais mazgai plečia viso P2P tinklo resursus. Kitaip yra serverio-kliento tinklo architektūroje, kuri turi stabilią serverių sistemą, tačiau duomenų perdavimas per juos gali sulėtėti visiems vartotojams, jei daugiau vartotojų įsijungs į tinklą.
- *Išlaidų paskirstymas vartotojams.* Resursai papildomi arba dalijami mainais už kitus išteklius, pvz., failus, pralaidumą, disko saugyklą ir kt. Žinoma, P2P tinklas turi ir trūkumų, didžiausia problema yra saugumas. P2P tinkle du ar daugiau vartotojų informacija keičiasi ir dalijasi tiesiogiai, todėl dalis vartotojų keičiasi autorinių teisių saugomais failais, dėl to tarp tokių tinklų gynėjų ir priešininkų kilo aršių ginčų.

1999 m. Jungtinėse Valstijose du verslūs jaunuoliai Šonas Faningas (Shawn Fanning) ir Synas Parkeris (Sean Parker) sukūrė projektą „Napster“ ir išpopuliarino tarp vartotojų masiškai paskirstyto tinklo konceptą įdiegę programą, skirtą dalytis muzika ir failais. „Napster“ laikoma tokio P2P tinklo, kokį naudojame šiandien, pradžia.

Projekto tikslas buvo keistis ir dalytis muzika. Vartotojams tereikėjo atsisiųsti „Napster“ programinę įrangą ir prisijungti prie tinklo, kurį jau buvo aplankę 26 mln. vartotojų, kai tuo metu interneto vartotojų iš viso buvo 248 mln. „Napster“ vartotojai galėjo keistis savo muzikos failais be jokių tarpininkų. Kadangi per „Napster“ muzika buvo dalijamasi nemokant už autorines teises, po ilgų ginčų ši platforma 2011 m. uždaryta. Tačiau jos

veikimo principas paskatino nepakankamai centralizuotų sistemų plėtrą visame pasaulyje. Būtent šios sistemos paklojo pamatus kitiems P2P tinklams, pvz., tinklui „Bitcoin“, sukūrusiam pirmąją kriptografinę valiutą tuo pačiu pavadinimu. Prie „Bitcoin“ sistemos tinklo gali laisvai prisijungti bet kuris pageidaujantis asmuo, atsisiuntęs ir savo kompiuteryje įdiegęs specialią programinę įrangą.

2

Ar atvirojo kodo programinė įranga palengvina kriptografinių valiutų vystymąsi?

Norint suprasti blokų grandinės technologijų rinkos dinamiką, labai svarbu suvokti atvirojo kodo konceptą, žinoti, kad ne viskas, kas vadinama atvirojo kodo programine įranga, yra laisvoji programinė įranga, leidžianti vartotojams ją taikyti, analizuoti jos veiklą ir (ar) laisvai platinti jos kopijas originaliu formatu ar su pakeitimais. Visa tai atlikti būtinai reikalingas šios programinės įrangos išeitinis kodas.

Atvirojo kodo programinė įranga ir laisvoji programinė įranga skiriasi. Laisvajai, akivaizdu, reikalingas atvirasis kodas, kad būtų užkirstas kelias ją naudoti komerciniais ar kariniais tikslais, priešingu atveju nuo to nebus įmanoma apsisaugoti.

Kai leidžiamas priėjimas prie išeitinio kodo ir leidžiama jį pakeisti, programuotojai gali pagerinti programą bendruoju lygiu, palengvindami jos naudojimą ir pašalindami galimus trikdžius, taip pagerindami programinės įrangos kokybę. Šis procesas decentralizuotas, priešingai nei tokie patys procesai, vykdomi su nuosavybiniu kodu, nes jį valdo konkreti vystytojų grupė, dirbanti pagal konkrečios organizacijos nurodymus.

Programinė įranga yra laisvoji, jei suteikia vartotojams keturias laisvės rūšis: ją paleisti bet kokiu tikslu, ja naudotis ir pritaikyti savo reikmėms, analizuoti jos veikimą ir platinti programos kopijas. Kitu atveju programinę įrangą pavadinti laisvąja negalima.

O dabar pasidairysime po laisvosios programinės įrangos ir atvirojo kodo istoriją. 1960–1970 m. programinė įranga buvo laikoma ne atskiru produktu, o to laikmečio didžiulių kompiuterių dalimi, pardavėjai savo klientams ją pristatydavo tam, kad šie galėtų naudotis kompiuteriais. Anuomet programuotojai ir programinės įrangos vystytojai laisvai keisdavosi kompiuterinėmis programomis. Universitetuose ir įmonėse buvo kuriama programinė įranga ir ja dalijamasi be apribojimų.

Padėtis pasikeitė XX a. devintajame dešimtmetyje, kai naujausiuose kompiuteriuose pradėtos diegti privačios operacinės sistemos, o vartotojai turėjo sutikti su jų naudojimosi sąlygomis, kurios draudė dalytis, keistis ar keisti šią įrangą. Net jei programuotojas galėjo išspręsti problemą ar pašalinti įrangoje aptiktą klaidą be savanaudiškų tikslų, sutartis draudė modifikuoti konkrečią kompiuterinę programą.

1983 m. rugsėjo 27 d. Stalmanas (Stallman) pranešė pradedąs projektą GNU, kurio tikslas buvo sukurti visiškai laisvą operacinę sistemą. 1985 m. Stalmanas įsteigė Laisvosios programinės įrangos fondą (angl. *Free software foundation*, FSF) ir paskelbė GNU Manifestą, siekdamas supažindinti publiką su projekto tikslu ir paaiškinti laisvosios programinės įrangos svarbą. 1986 m. pateikė laisvosios programinės įrangos apibūdinimą ir *copyleft* sąvoką bei išvystė tai, kad suteiktų laisvę vartotojams ir užkirstų kelią programinės įrangos pasisavinimui. 1989 m. paskelbė pirmąją GNU bendrosios licencijos versiją (angl. *general public license*, GPL), oficialiame dokumente užkoduodamas laisvosios programinės įrangos kūrimo idėjas.

Ričardas Stalmanas inicijavo GNU projektą, siekdamas sukurti pilną operacinę sistemą be išeitinio kodo naudojimo apribojimų. Šaltinis: Génesis Gabriella, Pixabay.

Kitas nepaprastai reikšmingas įvykis – „Linux“ sukūrimas. Tai laisvai platinama operacinių sistemų šeima, turinti „Linux“ tipo branduolį. Išrado Linusas Torvaldsas (Linus Torvalds) ir 1991 m. pateikė kaip modifikuojamą išeitinį kodą.

Branduolio atsiradimas GNU projekte reiškė, jog pilnų operacinių sistemų vis dėlto neegzistavo, nors jau buvo išvystyta nemažai komponentų. Torvaldsas užpildė spragą ir sudarė sąlygas daugybei programinės įrangos kūrėjų iš viso pasaulio prisidėti prie jų plėtros.

„Linux“ branduolio pavertimas GNU projekto programinės įrangos komponentu leido įgyvendinti visiškai laisvos operacinės sistemos idėją.

Nuo XX a. dešimtojo dešimtmečio vidurio ėmė steigtis daug naujųjų technologijų bendrovių, siūlančių žiniatinklio (angl. *web*) paslaugas. Daugiausiai buvo naudojama „GNU/Linux“ operacinė sistema, žiniatinklio paslaugas teikė „Apache“ serveris, duomenų bazes valdė „Mysql“ sistema, o kurti dinaminius serverio tinklalapius buvo naudojama PHP programavimo kalba.

1997 m. Erikas Retmondas (Eric Ratmond) paskelbė programišių (angl. *hacker*) bendruomenės ir laisvosios programinės įrangos atsiradimo pradžios reflektyviąją analizę. Šis dokumentas paragino „Netscape“ komunikacijų korporaciją (angl. *Netscape communications corporation*)* pritaikyti laisvosios programinės įrangos visuotinės plėtros modelį. Šis kodas tapo „Mozilla Firefox“ naršyklės pagrindu.

Retmondas su bendraminčiais priėjo prie išvados, jog FSF agitavimas socialiniu lygmeniu nepatrauklus tokioms kompanijoms kaip „Netscape“, ir ėmė ieškoti būdų, kaip pritaikyti laisvąją programinę įrangą verslui. Tada pasiūlyta vartoti „atvirojo kodo“ sąvoką, tokiu būdu išvengiant ideologinių sąsajų ir supriešinimo su terminu „laisvoji programinė įranga“. Pažvelgę į kriptografines valiutas ir jų aiškią bloko grandinių technologiją pamatysime, jog „Bitcoin“ protokolas ir jo programinė įranga skelbiami atvirai tam, kad bet kuris programuotojas bet kurioje pasaulio vietoje galėtų su ja susipažinti arba susikurti asmeninę,

* „Netscape Communications Corporation“ buvo nepriklausoma amerikiečių kompiuterių paslaugų įmonė JAV. – Vert.

modifikuotą jos versiją. „Bitcoin“ vienintelių savininkų neturi – juos valdo vartotojai, dalyvaujantys šioje ekosistemoje.

„Bitcoin“ gali teisingai funkcionuoti tik tuo atveju, kai visos procese dalyvaujančios šalys laikosi susitarimų, iš čia kyla didžioji dalis valiutos stiprybių ir kartu silpnybių. Todėl visi vartotojai, kriptografinės valiutos kasėjai (toliau – kasėjai), investuotojai ir programuotojai veikia vedami tų pačių paskatų – apsaugoti tokius susitarimus.

Išeitinis „Bitcoin“ kodas naudojamas kaip pagrindas daugelyje programinės įrangos projektų. Iš jo kilusi ir labiausiai paplitusi programinės įrangos forma yra kitos kriptografinės valiutos ar žetonai (angl. *tokens*). MIT licencija buvo programinės įrangos licencija, kurią savo laiku Satošis Nakamoto (Satoshi Nakamoto) parinko „Bitcoin“. Ši licencija įprastai taikoma, kai programinės įrangos kūrėjas pageidauja, jog kodas būtų prieinamas kuo didesniam vystytojų kiekiui. Techniškai ši licencija – trumpa, paprasta ir lengvai suprantama.

3

Svarbiausias vaidmuo tenka protokolams?

Informatikoje ir telekomunikacijose ryšių protokolas yra taisyklių visuma, kuri leidžia dviem ar daugiau ryšių sistemos priemonėms (kompiuteriai, išmanieji telefonai ir pan.) susisieti tarpusavyje ir perduoti informaciją.

Apsikeisti pranešimams komunikacijos sistemos naudoja aiškiai apibrėžtus protokolus. Visi pranešimai turi tikslią reikšmę, kuriai yra priskirtas atsakymas iš numatytų įmanomų kiekvienam konkrečiam atvejui atsakymų skalės. Įprastai apsikeitimas pranešimais nepriklauso nuo to, kaip bus įgyvendintas. Sąveikaujančių šalių ryšių protokolai turi būti suderinti tarpusavyje.

Vadovaudamiesi šiais aiškinimais ir apibrėžimais, pradedame suprasti ryšių protokolo konceptą. Tai yra gairių rinkinys, kuris leidžia skirtingiems sistemos elementams tarpusavyje užmegzti ryšį apsikeičiant informacija. Interneto protokolas (angl. *internet*

protocol, IP) yra taisyklės, pagal kurias veikiantys kompiuteriai susisiekia tarpusavyje internete.

Svarbiausi interneto ryšių protokolai yra TCP (perdavimo valdymo protokolas, angl. *transmission control protocol*) ir interneto protokolas. Jų bendras veikimas (TCP/IP) leidžia susieti visus tinkle esančius įrenginius.

IP svarbus tuo, kad jo funkcija yra užtikrinti ryšį dviem kryptimis – gavėjo arba siuntėjo, kad būtų galima perduoti duomenis.

Kiti interneto protokolų pavyzdžiai yra protokolas HTTP (angl. *hypertext transfer protocol*), kuris yra taisyklių rinkinys kurti tinklalapius ir jais dalytis. HTTP sukūrimas sąlygojo pasaulio saityno (angl. *world wide web*), kurį vadiname internetu, sukūrimą.

Protokolas SMTP (angl. *simple mail transfer protocol*) – taisyklių rinkinys, skirtas internetu siųsti pranešimus. SMTP įgalino elektroninių laiškų siuntimą. Tačiau kam priklauso visi šie interneto protokolai?

Protokolai nepriklauso niekam. Interneto protokolai yra įrankiai, kurie gali būti naudojami įvairiais būdais ir yra sukurti kaip naudingi standartai. TCP/IP, HTTP ar SMTP protokolai padėjo sukurti „informacijos internetą“, tapo „Twitter“, „Google“, „Facebook“ ir kitų daugybės bendrovių sėkmingos veiklos pagrindu. Jei neegzistuotų šie pradiniai, pagrindiniai protokolai ar būtų naudojami neteisingai, nė viena iš šių bendrovių nebūtų galėjusi išplėtoti savo verslo modelio.

Perdavimo valdymo protokolas TCP – vienas svarbiausių interneto sudėtinių elementų.
Šaltinis: techeek, Pixabay.

Vienas iš plačiajai visuomenei geriausiai žinomų technologinių protokolų yra „BitTorrent“, kuris naudojamas turiniu, pvz., muzika, knygomis ar filmais, dalytis decentralizuotai.

„BitTorrent“ yra sukonfigūruotas decentralizuotoje sistemoje tarp lygiaverčių tinklo modelių P2P, leidžiantis tiesiogiai keistis turiniu tarp kompiuterių, nereikalaujant patikimo tarpininko, kurį, priešingai, turi, pvz., „Netflix“ platforma – naudoja centrinį serverį.

Naujovė, kurią sukūrė „Bitcoin“ protokolas, yra P2P technologijos ir kriptografijos derinys. Šis technologijų derinys kartu su kriptografinių valiutų vienetu arba jų vertės vienetu – žetonais ar kriptografinėmis valiutomis (bitkoinais (angl. *bitcoin*, BTC), eteriais (angl. *ethereum,* ETH*)* ir kt.) išmokama kompensacija skatina dalyvavimą šiuose protokoluose ir jų naudojimą, verčia keisti ligšiolinį nuobodų protokolų pasaulį, sudarant galimybes pasaulinei investuotojų bendruomenei investuoti į juos bei šitaip demokratizuoti tokių atvirų protokolų finansavimą ir plėtrą. Ši aplinkybė įkvėpė daug verslininkų vystyti programas remiantis šia nauja baze ir kurti naujus, decentralizuotoje sistemoje veikiančius protokolus.

„Bitcoin“ remiasi blokų grandinės technologija, kuri savo procesuose dalijantis turiniu decentralizuota forma naudoja atvirą protokolą, sukurtą apsikeisti failais tarp vienodų P2P internete, kur kompiuterių tinklas, arba vadinamieji mazgai, sąveikauja tarpusavyje lygiavertiškai, tuo pačiu metu veikdami ir kaip klientai, ir kaip serveriai visų kitų tinklo mazgų atžvilgiu, tarp susijungusių prietaisų leidžiant tiesioginį apsikeitimą informacija bet kokiu formatu.

Norint naudoti „Bitcoino“ protokolą, reikalinga kriptografinė valiuta ir „Bitcoin“ apskaitos vienetas. Išsiaiškinkime dažnai pasitaikančią painiavą: „Bitcoin“ protokolo pavadinimas rašomas didžiąja „B“ raide, o bitkoino apskaitos vienetas, naudojamas „Bitcoin“ protokole, rašomas mažąja „b“ raide.

„Bitcoin“ apskaitos vienetas yra vadinamas kriptografine valiuta, nes „Bitcoin“ protokolo kūrėjo idėja buvo sukurti decentralizuotą mokėjimų sistemą, kurią valdytų bendruomenė ir nereikėtų subjekto, atliekančio centrinio, pagrindinio banko funkcijas.

4

Ar kriptografinių valiutų veikimas grindžiamas žaidimų teorija?

Žaidimų teorija – taikomosios matematikos ir teorinės ekonomikos šaka, nagrinėjanti sprendimus, jų optimalių baigmių egzistavimo sąlygas (kad individas patirtų sėkmę, reikia atsižvelgti į kitų situacijos dalyvių priimamus sprendimus). Ši teorija remiasi tyrinėjimais, kaip ekonominė sistema siejasi su individo elgesiu. Ypač tais atvejais, kai kaštų ir naudos neįmanoma nustatyti iš anksto, nes tai priklauso nuo trečiosios šalies. Žaidžiant nereikia klausti, ką mes darysime, reikia savęs klausti, ką darysime, atsižvelgdami į tai, ką, mūsų nuomone, darys kiti ir kaip jie elgsis galvodami apie mūsų būsimus veiksmus. Žaidimų teorijos atliekami tyrimai leidžia geriau suprasti, kaip bendradarbiavimas arba individualizmas gali paveikti ekonominę sistemą. Šie aspektai labai svarbūs vis labiau tarpusavyje susijusiame pasaulyje ir viena nuo kitos vis labiau priklausančiose ekonomikose. Tačiau tai ne viskas, nes žaidimų teorija ir jos analizė, kaip matysime toliau, apima daug platesnį veikimo lauką.

1928 m. žymus matematikas Džonas fon Noimanas (John von Neumann) paskelbė straipsnių seriją apie žaidimų teoriją. Tai tapo šios teorijos pradžia ir vienu svarbiausių mokslinių Noimano indėlių. Tačiau žaidimų teorija ėmė populiarėti, kai Našas (John Forbes Nash) sukūrė pusiausvyros koncepciją (Našo pusiausvyra).

Našo pusiausvyra pasiekiama situacijoje, kai žaidime dalyvaujant dviem ar daugiau žaidėjų, visi žino vienas kito strategijas, bet nė vienas nenori žengti individualaus žingsnio ir priimti vienašališko sprendimo, nes tai galėtų pabloginti jo padėtį. Kai visi žaidėjai priima savo sprendimus ir negali jų pakeisti, nes kitaip pablogintų savo padėtį, laikoma, kad Našo pusiausvyra pasiekta.

Našo pusiausvyros dėsnis taikomas siekiant sureguliuoti įmonių tarpusavio varžymąsi ir rengiant viešųjų pirkimų konkursus. Remiantis Našo pusiausvyra parengti teisės aktai leidžia išvengti oligopolijos, taigi, antimonopoliniai įstatymai apibrėžia būdus, kaip išvengti dalyvaujančių šalių susitarimo dėl kainų.

Džono Forbso Našo jaunesniojo biografija pasakojama 2001 m. filme „Nuostabus protas“ (angl. *A Beautiful Mind*), laimėjusiame keturis Oskaro apdovanojimus, tarp jų – geriausio metų filmo. Šaltinis: WorldSpectrum, Pixabay.

Bloko grandinių technologijos egzistavimas įmanomas dėl žaidimų teorijos. Ši teorija naudoja technologiją pasiekti, kad žaidėjai, arba kasėjai, galėtų užtikrinti nepertraukiamą tinklo saugumą. Geriausias žaidimų teorijos pritaikymo pavyzdys yra susitarimo dėl darbo įrodymo protokolas (angl. *proof of work*, PoW), kai kasėjai dalyvauja žaidime, vadinamame kriptografinės valiutos gavyba (vartosenoje paplitęs žodis „kasimas“, toliau – gavyba) ir sandorių patvirtinimas, kurio tikslas yra priimti sandorius, juos apdoroti, patikrinti ir patvirtinti, jog viskas atlikta teisingai.

Norėdami tai padaryti, kasėjai naudoja pažangiausias informacines technologijas ir sudėtingą kriptografiją tikrinti duomenis. Žaidime kiekvienas žaidėjas priima sprendimą, kurį patvirtina ir priima kiti dalyviai. Žaidimo pabaigoje pasiekiamas tikslas: užtikrinti, kad būtų įvykdyti tinklo sandoriai, jie būtų saugūs ir nepakenktų sistemai. Taip pavyko išspręsti nuolatinę decentralizuotų sistemų kompiuterinio saugumo dilemą – vadinamąją „Bizantijos generolų problemą“, iškylančią paskirstytuose tinkluose, tokiuose kaip „Bitcoin“ ir kitų kriptografinių valiutų.

„Bizantijos generolų problema“ yra mąstymo eksperimentas, sukurtas iliustruoti dilemą, iškylančią norint pasiekti subjektų grupės, kuri turi bendrą tikslą, susitarimą, turint omeny, kad joje yra kenkėjų, siekiančių pagreitinti visą procesą. Be to, manytina, jog ryšys tarp jų būna ribotas ir nesaugus.

Problema vaizduojama kaip karinė scena, kurioje Bizantijos generolų grupė su savo kariuomene apsupa ketinamą pulti miestą. Pvz., įsivaizduokime situaciją, kurioje senovės generolai atakuoja miestą skirtingose vietose ir turi tarpusavyje

susitarti, kaip koordinuotai atlikti veiksmus. Iš tų generolų tik vienas yra vadas ir gali įsakyti. Be to, šie generolai susisiekia tik su pasiuntiniais, o du galimi vado įsakymai bus arba pulti, arba trauktis. Įvertinę priešo elgesį, generolai privalo pasidalyti savo įžvalgomis ir susitarti dėl bendro kovos plano, kaip pulti miestą ir laimėti mūšį.

Be to, egzistuoja tikimybė, jog tarp generolų gali būti išdavikų, kurie siunčia melagingus pranešimus siekdami suklaidinti sąžiningus generolus. Algoritmas, turintis išspręsti šią problemą, turi užtikrinti, kad visi sąžiningi generolai priimtų bendrų veiksmų planą, dėl ko saujelė išdavikų savo tikslo pasiekti negalėtų. Vienas didžiausių „Bitcoin“ laimėjimų yra tai, kad buvo pasiūlytas pirmasis praktinis šios „Bizantijos generolų problemos“ sprendimas.

PoW algoritmas – tai pirminio susitarimo blokų grandinės tinkle algoritmas. Blokų grandinėje toks algoritmas taikomas sandoriams patvirtinti ir naujiems blokams kurti. Pagal šį algoritmą žaidėjai tarpusavyje varžosi, kas greičiau užbaigs tinkle sandorius ir gaus atlygį.

5

Ar skaitmeninis apribojimas lemia kriptografinių valiutų atsiradimą?

Iš pradžių išsiaiškinkime žodžio „apribojimas“ reikšmę ekonomikos kontekste ir tuomet galėsime jį taikyti kriptografinėms monetoms ir blokų grandinėms.

Pirmiausia, terminas „apribojimas“ reiškia, jog turimų išteklių kiekis yra nepakankamas pagaminti tiek produktų ir suteikti tiek paslaugų, kad būtų patenkinti žmonių poreikiai. Tokiu atveju neįmanoma patenkinti visų jų poreikių, todėl tenka pasirinkti iš kelių variantų, kaip paskirstyti turimus išteklius.

Tai paklausos ypatybės, kurios padeda apibrėžti išteklių trūkumą, kai trūkumas nėra apibrėžiamas kiekiu, o reaguoja į situaciją, kai numatoma paklausa ateityje viršija numatomą pasiūlą, todėl susidaro išteklius.

ESMINIŲ 100 KLAUSIMŲ

Viskas, ką reikia žinoti apie KRIPTOVALIUTAS ir blokų grandinių (*blockchain*) technologiją – vienoje knygoje! Susipažinkite su pasaulio finansų ateitimi, kuri jau šiandien milijonus žmonių pavertė turtingais, o netolimoje ateityje iš esmės sukrės pasaulio pinigų dėsnius, šalių ekonomikas ir kiekvieno iš mūsų asmeninius finansus.

2021 metais pasaulyje buvo 140 milijonų kripto rinkos dalyvių, o augimas kasmet siekia 130 procentų. Tai pati sparčiausia technologinė revoliucija pasaulyje, savo greičiu lenkianti viską, kas kada nors yra įvykę žmonijos istorijoje. Toks augimas reiškia tik viena: 2024 metais kripto vartotojų jau bus milijardas! Dabar jūs galite būti didžiausios žmonijos istorijoje finansinės permainos, kuri sukurs naujus milijonierius ir milijardierius, dalimi. Skaitykite šią knygą ir sužinokite, nuo ko pradėti ir kaip veikia kripto pasaulis.

Taip pat sužinokite:

- Kaip galime pasipelnyti iš decentralizuotų finansų (*DeFi*)?
- Kas yra tokenų (žetonų) ekonomika?
- Kaip pirkti ir parduoti kriptovaliutas?
- Kaip reglamentuojamas kriptoturtas?
- Ar galime iš kriptovaliutų susikurti pelningą turto portfelį?
- Ką reikia žinoti apie kriptovaliutų rinkoje egzistuojančias kibernetines grėsmes?

Pažinkite revoliucinės kriptovaliutų ir blokų grandinių technologijos esmę ir sužinokite pagrindinius postulatus: vertės internetą, ekonominių aktyvų tokenizaciją ir decentralizuotus ateities pasaulio finansus.

VISKAS, KĄ REIKIA ŽINOTI APIE KRIPTOVALIUTAS

Jeigu norite pasinaudoti unikalia žmonijos istorijoje galimybe lengvai praturtėti, privalote perskaityti „Kriptovaliutos: lengvas būdas praturtėti".

OBUOLYS
anno 2004
#obuolys.lt

ISBN 978-609-484-441-6

9 786094 844416

www.obuolys.lt

Knygos pigiau, įdomybės ir ištraukos nemokamai

KITI FORMATAI:

Audio knyga

Elektroninė knyga

Viršelio detalės: © Shutterstock