Kriptovalyuta verilənlərinin intelektual analizi məsələləri

Yadigar İmamverdiyev[1], Firəngiz Sadiyeva[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]yadigar@iit.science.az, [2]sadiyeva.firengiz@gmail.com

***Xülasə*— Kriptovalyutalar son bir neçə ildə meydana çıxmış və maliyyə sektorunda inqilabi dəyişikliklər vəd edən fenomendir. Əksər kriptovalyutaların əsaslandığı blokçeyn texnologiyası digər fəaliyyət sahələrində də diqqətəlayiq dəyişikliklərə yol açа bilər. Məqalədə kriptovalyuta texnologiyalarının qısa xülasəsi verilir, bu sahədə tətbiqi gündəmdə olan bəzi texnoloji həllər diqqətə çatdırılır və kriptovalyuta verilənlərinin intellektual analizi metodları təhlil olunur.**

Açar sözlər*— *kriptovalyuta; Bitkoin, blokçeyn, hardfork, softfork, altkoin, steyblkoin, Ethereum, intellektual analiz

I. GİRİŞ

Kriptovalyuta infrastrukturunun vacib komponentlərindən biri informasiya-analitika xidmətləridir. Bu xidmətlər kriptovalyutaların bazar qiymətləri, kapitallaşması, tranzaksiyaların həcm dinamikası, şəbəkədə komissiyaların orta miqdarı, volatillik və s. haqqında faydalı məlumatlar təqdim edirlər. Belə xidmətlər günbəgün artır. Onlar kriptovalyuta həvəskarları, treyderlər, investorlar, tədqiqatçılar və tətbiqi proqram işləyənlər üçün əvəzedilməz köməkçilərdir.

Əlbəttə, belə xidmətlər yalnız informasiyanın toplanmasını, vizuallaşdırılmasını və təqdim olunmasını yerinə yetirmirlər. Bu xidmətlərin ən əsas xidməti, adından da göründüyü kimi, analitikadır və burada intellektual analiz metodları öz potensial və güclərini göstərməyə, təxminən 10 illik coşqun inkişaf ərzində toplanmış böyük həcmli verilənlərdə gizli qanunauyğunluqları aşkarlamağa hazırdırlar. Təqdim olunan iş bu sahədə tədqiqat məsələlərini dəqiqləşdirmək məqsədilə kriptovalyutaların və onlara aid verilənlərin intellektual analizi metodlarının icmalına həsr olunmuşdur.

II. BİTKOİN: QISA İCMAL

Bitkoin blokçeyn texnologiyası ilə işləyən ilk kriptovalyutadır və hazırda kriptovalyuta bazarının təxminən yarısını tutur [1]. Onun tarixi 31 oktyabr 2008-ci il Mərkəzi Avropa vaxtı ilə 8.10-da Satoşi Nakamoto adı ilə göndərilmiş aşağıdakı cümlə ilə başlayan bir qısa məlumatla başlayıb: “Mən tamamilə birranqlı olan və etibarlı üçüncü tərəflərin iştirakını nəzərdə tutmayan elektron pul sistemi yaratmışam.” Məlumatda Bitkoinin texniki təsviri olan doqquz səhifəlik “Peer to peer electronic cash system” adlı “ağ məqalə”yə link yerləşdirilmişdi.

“Ağ məqalə” çıxdıqdan üç ay sonra Bitkoin proqram-kliyentinin ilk versiyası işə salınmışdı. 3 yanvar 2009-cu ildə ilk 50 bitkoin “generasiya” edildi, üç gün sonra isə ilk bitkoin tranzaksiyası həyata keçirildi – Satoşi Nakamoto kriptovalyuta aktivisti Hel Finniyə 10 bitkoin göndərdi. Həmin ilin oktyabrında bitkoin ilk dəfə milli pula dəyişdirildi. 1 dolları 1309 bitkoinə dəyişdirmişdilər. Qiyməti sərf olunan elektrik enerjisinin dəyəri əsasında müəyyən etmişdilər. 2010-cu ilin mayında ilk dəfə bitkoinlə mal alınmışdı – 10 min bitkoinə 2 pizza sifariş edilmişdi (çatdırılmaqla). Bitkoin tədricən populyarlaşmağa başladı və 2011-ci ildə ilk kriptovalyuta birjası yaradıldı [2].

Bitkoin blokçeyn şəbəkəsinin əsas xüsusiyyətlərindən biri tamamilə demərkəzləşmiş olmasıdır – hər hansı bir mərkəzi idarəetmə orqanı yoxdur. Bu ödəniş sisteminin əsas elementi açıq kodlu proqram kliyentdir. Proqram-kliyentlərin işlədiyi kompüterlər öz aralarında pirinq (Peer to peer, P2P) şəbəkəsində birləşirlər, burada bütün qovşaqlar bərabər hüquqludurlar. Iki tərəf arasında elektron ödəniş vasitəçilər olmadan həyata keçirilir və geriyə dönülməzdir, yəni təsdiqlənmiş əməliyyatı ləğv etmək mexanizmi yoxdur.

Bitkoin sisteminin ilkin kodu elə proqramlaşdırılıb ki, sistemdə olacaq bitkoinlərin maksimal sayı əvvəlcədən məlumdur (21 milyon bitkoin). Təkcə bitkoinlərin maksimal sayı deyil, emissiya dinamikası da (yeni bitkoinlərin buraxılışı) da proqramlaşdırılıb. Bu bitkoinləri öz kompüter avadanlığını Bitkoin şəbəkəsində hesablamalar üçün istifadə edənlər əldə edirlər (“çıxarırlar”).

Blokçeyn. Hər bir elektron ödəniş sistemi tranzaksiyaları haradasa saxlamalıdır. Bitkoində bütün informasiya blokların zəncirində - blokçeyndə (ing. blockchain) saxlanır. Bloklar JSON formatında ötürülür. Hər bir blokda başlıq və tranzaksiyaların siyahısı olur. Başlıqda bir neçə məlumat, o cümlədən blokun sıra nömrəsi, başlığın heşi və əvvəlki blokun heşi olur. Beləliklə, blokçeyndə Bitkoinin mövcudluğu müddətində həyata keçirilmiş bütün tranzaksiyalar saxlanır.

Bloku yaratmaq üçün mayner bloka yazılmağa növbə gözləyən tranzaksiyalar siyahısından tranzaksiyaları seçir (əlbəttə, üstünlüyü tranzaksiya haqqı yüksək olanlara verir). Sonra blok başlığının heşi hesablanır, heşin qiyməti başlıqda verilmiş hədəf qiymətindən kiçik olmalıdır (“çətinlik” parametri). Başlıqdakı nonce sahəsindəki ədəd 0-dan başlayaraq hər iterasiyada o vaxtadək artırılır ki, başlığın heşi hədəf qiymətdən kiçik olsun. Adətən, bu xassəni ödəyən heşin tapılması böyük hesablamalar tələb edir. Hədəf qiymət nə

DOI: 10.25045/NCInfoSec.2018.08

qədər kiçikdirsə, şərtin ödənməsi ehtimalı da bir o qədər kiçikdir.

Çətinlik dedikdə, bir həqiqi blokun axtarışı üçün hesablanmış heşlərin orta sayı nəzərdə tutulur. Bu qiymət hər 2016 blokdan sonra (təxminən 2 həftə) yenidən hesablanır ki, bloklar arasındakı interval 10 dəqiqə təmin olunsun.

Mayninq yeni sikkələrin mədəndən çıxarılmasıdır, blokçeynə yazılacaq yeni bloku tapan mayner mükafat olaraq nəzərdə tutulmuş sayda bitkoin alır.

Bir blokun mayninqinə təxminən 10 dəqiqə gedir. Hər 10 dəqiqədən bir 12,5 yeni bitkoin buraxılır, onu bu bloku tapan, yəni son 10 dəqiqədə olan tranzaksiyaların blokunu yaradan alır. Bu emissiya bitkoin protokolunda nəzərdə tutulub və hər 4 ildən sonra 2 dəfə azalır.

2016-cı ilin iyununa kimi hər 10 dəqiqədən sonra 25 bitkoin buraxılırdı, hazırda 12,5 bitkoin buraxılır və 2020-ci ilə kimi belə davam edəcək. Sonra 2024-cü ilə kimi 6,25 bitkoin buraxılacaq və s. Hazırda dövriyyədə 16-17 milyon bitkoin var. İlkin hesablamalara görə, 2140-cı ilə kimi 21 milyon bitkoin buraxılacaq.

Qeyd edək ki, Bitkoində mayninqin çətinliyi tədricən artırılır və bloka görə mükafat azalır. İlk dövrlər mayninq üçün fərdi kompüterlərin mərkəzi prosessorları kifayət edirdi. Sonra GPU əsasında, FPGA əsasında və nəhayət, ASIC əsasında mayninq fermaları meydana çıxdı. ASIC (Application-Spesific Integrated Circuit) – konkret məsələnin həlli üçün xüsusi inteqral sxemdir. Hazırda istehsalçılar tərəfindən mayninq üçün müxtəlif ASIC həlləri təqdim olunur. Güman olunur ki, ən böyük mayninq fermaları, Çin, İslandiya, Gürcüstan və Amerikadadır. Ən böyük 6 mayninq hovuzu Çində yerləşir və dünyada bitkoinlərin yarıdan çoxu da orada çıxarılır.

Konsensus alqoritmi. Kriptovalyuta şəbəkəsinin bütün qovşaqları eyni hüquqludursa, onda eyni anda iki blok tapıldıqda hansı blokun düzgün hesab edilməsi və şəbəkəyə əlavə edilməsi zamanı qeyri-müəyyənlik yaranır. Bundan qaçmaq üçün qərar qəbuletmə mexanizmləri təklif olunub. Bitkoin və digər şəbəkələrdə PoW (Proof-of-work, işin isbatı) alqoritmi istifadə edilir, burada ən böyük hesablama gücünə malik qovşağın düzgün bloku tapmaq şansı ən yüksəkdir; PoS (Proof-of-stake, hissənin isbatı) alqoritmində hesabında daha çox kriptovalyutaya olan qovşağın “çəkisi” daha böyükdür; dPoS (delegated PoS) alqoritmində səlahiyyət şəbəkənin bütün iştirakçıları tərəfindən ümumi səsvermə ilə seçilən müəyyən sayda qovşağa verilir.

Kriptobirjalar. Kriptovalyutaya tələbin artması ilə paralel olaraq 2011-ci ildən onların mübadiləsi üçün onlayn birjalar yaranmağa başladı. Bu birjalar xüsusiyyətinə görə əsasən 2 yerə bölünür: 1) Kriptovalyutanın real valyutaya mübadilə edildiyi birjalar; 2) Bitkoinlərin digər kriptavalyutalara mübadilə edildiyi birjalar.

İlk bitkoin birjası MtGox 2011-ci ilin martında işə salınmışdı. İlk dövrlər 1 bitkoin 5-6 sent idi, yarımildən sonra 10 dəfə artmışdı. Birja fəaliyyəti dövründə bir neçə dəfə hakerlər tərəfindən sındırılmışdı. 2014-cü ildə siyasi və iqtisadi səbəblərdən birja öz varlığını sonlandırmışdır.

Hazırda kriptovalyutaların alqı-satqısı ilə məşğul olan onlarla böyük birja vardır: Binance, Bitfinex, Livecoin, Poloniex, Btc-e, Bittrex, BtcChina və s.

III. KRİPTOVALYUTALARDA HARDFORK VƏ SOFTFORK

Bitkoinin ilkin kodu açıqdır və istənilən şəxs onun zəif yerlərini tapa və təkmilləşdirə, yəni fork yarada bilər.

Fork (ing. «çəngəl») – proqram təminatında məhsulun hər biri müstəqil inkişaf etdirilən bir neçə paralel budağa ayrılmasıdır və ya çoxdan mövcud olanın əsasında yeni məhsulun buraxılmasıdır. Məsələn, Xiaomi-nin MIUI sistemi forkdur, Android ƏS-nə əsaslanır, lakin ondan asılı olmadan inkişaf etdirilir.

Kriptovalyuta sahəsində fork – blok-zəncir sisteminin proqram koduna dəyişikliklərin edilməsidir, nəticədə sistemin iş qaydaları dəyişir. Bu hadisəni iki tipə ayırmaq olar: hardfork və softfork. Terminlərin kökü aparat və proqram təminatı mənasını verən sözlərdən deyil, «hard» və «soft» ingilis sözlərinin ilkin mənasından yaranıb.

Softfork – kriptovalyutanın proqram kodunun «yumşaq» dəyişdirilməsi prosesidir, onun gedişində blokçeyn şəbəkəsində işləyən maşınların proqram təminatının tam dəyişməsi tələb edilmir. Softfork zamanı edilən dəyişikliklər ona qədər yaradılmış verilənlərlə uyarlığı saxlayır, lakin yeni verilənlərin yaranması prosesi dəyişir. Zəruriyyət yarandıqda softforku asanlıqla ləğv etmək olar.

Kriptovalyutada softforkun aparılmasının səbəbi, adətən, onun əsaslarına toxunmadan təkmilləşdirilməsi, aşkarlanmış hansısa nöqsanların aradan qaldırılması ehtiyacı olur. Bitcoin-də belə ehtiyac blokun həcminin artan tranzaksiyaları sürətlə emal etməyə imkan verməməsi səbəbindən yaranmışdı. Problemin həlli kimi Bitcoin Core komandası verilənlərin həcmini optimallaşdıran SegWit protokolunun tətbiqini seçmişdi.

Hardfork proqram koduna «sərt» dəyişiklik edilməsidir, bundan sonra köhnə proqram təminatı ilə uyarlıq itir. Faktiki olaraq, hardfork gedişində əvvəlkindən fərqli, tamamilə yeni prinsip ilə işləyən yeni kriptovalyuta yaradılır. Softfork zamanı şəbəkənin proqram təminatı yenilənmiş qovşaqları köhnə proqram təminatı ilə işləyən qovşaqlarla qarşılıqlı əlaqə saxlaya bilirlərsə, hardfork zamanı köhnə şəbəkə ilə qarşılıqlı əlaqə tamamilə itir.

Hardforkun səbəbləri də softforkun səbəbləri ilə oxşardır, yaradıcıları kriptovalyutanın iş qaydalarına müvafiq dəyişikliklər etmək istəyirlər. Fərq ondadır ki, hardfork zamanı onlar mövcud sistemi yeniləmək yox, «blokçeyni və maynerləri ilə öz Bitcoin»ləriuni yaratmaq istəyirlər. Bitcoin üçün ən məşhur hardfork Bitcoin Cash hesab olunur. Yeni valyuta köhnədən blokun ölçüsünün 1 MB-dan 8 MB-a artırılması ilə fərqlənir. Bu tranzaksiyaları daha sürətlə yerinə yetirməyə imkan verir, lakin köhnə sistemlə uyarlıq itir.

Aydın məsələdir ki, kriptovalyutalar sahəsində işlərin miqyası xeyli böyüyüb və forkların həyata keçirilməsi investisiyalar tələb edir.

ICO (Initial Coin Offering) – kriptovalyuta layihələri üçün investisiyaların cəlb edilməsi formasıdır. ICO təşəbbüskarı

investorlara tokenlər satır. Tokenlərin real dəyəri layihə birjaya çıxana qədər qeyri-müəyyən olur. Tokeni alan tərəf, yəni investorlar bu startap tokenini gələcəkdə ICO-da nəzərdə tutulmuş servisləri, xidmətləri və malları əldə etmək üçün istifadə edə bilərlər. Yaxud layihə birjaya çıxdıqdan və dəyəri artdıqdan sonra, dividendlər əldə edə və ya tokeni sata bilərlər.

İlk ICO 2013-cü ildə həyata keçirilmiş Mastercoin (hazırda Omni) olmuşdur. Təşəbbüskarlar 5 milyon dollar toplamağa nail olmuşdular. Sayca ikinci ICO ən uğurlarından biri oldu (NXT), 1 milyard token buraxılmışdı. 2017-ci ilin payızında isə kapitallaşma 70 milyon dollar təşkil edirdi. Ethereum üçün başladılan ICO layihəsində 18 milyon dollar investisiya toplanmışdı.

IV. BİTKOİNİN FORKLARI – ALTKOİNLƏR

Litecoin – uğurlu Bitcoin forklarından biridir. Bitkoinin nöqsanları əməliyyatların yavaş emalı və tranzaksiya haqlarının yüksək olmasıdır. 2011-ci ilin oktyabrında Charlie Lee bu nöqsanları aradan qaldırmaq üçün Litecoin təklif etdi. Litecoin - Scrypt heş alqoritmindən istifadə edir (Bitkoində SHA-256). Emissiya 84 milyon sikkə ilə məhdudlanıb, bu Bitkoindən 4 dəfə çoxdur. Bitkoinə analoji olaraq, rəqəmsal “gümüş” adlanır. Segwit və Lightning Network mexanizmlərinə ilk keçənlərdən biridir, bu blokda tranzaksiyaların sayını əhəmiyyətli dərəcədə artırmağa və tranzaksiyanın təsdiqlənməsi vaxtını azaltmağa imkan vermişdir.

Litecoin-in mayninqi Bitkoindən daha mürəkkəbdir. Vacib və əsas fərq odur ki, Scrypt operativ yaddaşdan intensiv istifadə edir. Bu halda Litecoin üçün ASIC-maynerlərin yaradılması məqsədəuyğun deyil və məhz buna görə də Litecoin mayninqi üçün ənənəvi videokartlar geniş istifadə edilir.

Ethereum (Efirium, efir) – əsas protokolu 2013-cü ildə rus əsilli kanadalı proqramçı Vitalik Buterin tərəfindən işlənmişdi, şəbəkə isə 30 iyul 2015-ci ildə işə salınmışdı. Ethereum-un əsas ideyası blokçeynin funksional imkanlarının genişləndirilməsi idi.

İlk baxışda Ethereum da Bitkoinə oxşayır, onun kimi paylanmış açıq şəbəkədir, burada da tranzaksiyalar edilir və bloka yazılır, onları da dəyişmək mümkün deyil. Lakin onların arasında bəzi əhəmiyyətli texniki fərqlər var, daha vacib fərq onların təyinat və imkanlarında olan fərqlərdir.

Bitkoin – blokçeyn texnologiyasının konkret bir tətbiqidir, elektron ödəniş sisteminin reallaşdırılmasıdır. Lakin blokçeyn texnologiyasının imkanları daha genişdir və Bitkoin-də bu imkanların kiçik bir hissəsi reallaşdırılıb. Etherum-un yaradılmasının əsas hərəkətverici ideyası tranzaksiyanın – kriptovalyuta protokolunun əsas vahidinin smart-kontraktla əvəz edilməsidir. Smart-kontrakt daxilində təkcə pul vahidinin bir hesabdan digərinə keçirilməsini deyil, istifadəçilər arasında qarşılıqlı əlaqənin daha geniş məntiqini və şərtlərini təsvir etmək olar.

Smart-kontrakt elektron alqoritm və yaşərtdir, onun yerinə yetirilməsi zamanı tərəflər pul, aksiya, daşınmaz əmsal və ya digər aktivləri mübadiləedə bilərlər. Maliyyə aləti kimi kriptovalyuta istifadə edilir. Blokçeyn texnologiyasının hesabına smart-kontraktlar paylanmış reyestrdə saxlanır və tərəflərdən heç birinin onu dəyişmək imkanı yoxdur.

Smart-kontraktlar banklar, notariuslar, hüquqşünaslar və s. kimi vasitəçilərdən yan keçməyə imkan verir, çünki onlar alqı-satqının şərtlərini özləri müstəqil yoxlayırlar və təsdiqləyirlər. Ethereum yaradıcısı smart-kontraktların işini belə izah edir. Əvvəlcə aktiv və ya valyuta proqrama köçürülür. Bundan sonra proqram kontraktın yerinə yetirilməsini izləməyə başlayır. Şərtlər yerinə yetirilən kimi tərəflər aktivləri mübadilə edirlər. Satıcı müəyyən edilmiş məbləği, alıcı isə malı alır.

Ethereum həmçinin demərkəzləşmiş avtonom təşkilatların (Decentralized Autonomous Organization, DAO) yaradılması üçün də istifadə edilə bilər. DAO – Ethereum blokçeynində yazılmış smart-kontraktların köməyi ilə idarə edilən, vahid lideri olmayan, tam avtonom demərkəzləşmiş təşkilatdır. Burada proqram kodu ənənəvi təşkilatın strukturunu və qaydalarını əvəz edir, mərkəzləşdirilmiş insan nəzarətinin zəruriliyini aradan qaldırır. DAO tokenləri alanların hamısına məxsusdur, lakin burada token aksiyaların hissə və ya paketi deyi, səs hüququ üçün ödənişdir.

Ripple – öz xarakteristikalarına görə kriptovalyuta tərifinə tam uyğun gəlmir – onda blokçeyn yoxdur. Emissiya 100 milyard sikkə olmaqla bir dəfəyə edilmişdi, onun 55 milyardı dərhal dövriyyəyə daxil edilmişdi, qalanı isə hər ay 1 milyard sikkə olmaqla smart-kontraktlar vasitəsilə çıxarılırdı. Yaradıcılarının məqsədi komissiya haqları minimal və tranzaksiya sürəti dəfələrlə böyük olmaqla SWIFT sisteminə rəqib yaratmaq idi. Buna müəyyən dərəcədə nail olmalarını Bank of America, Unicredit, BNP Paribas və s. kimi məşhur bankların Ripple infrastrukturuna qoşulması təsdiqləyir.

Bitcoin Cash – Bitkoin şəbəkəsinin ən məşhur və uğurlu hardforklarından biridir, 1 avqust 2017-ci ildə meydana çıxıb. Hardforkun məqsədi şəbəkənin miqyaslanması, buraxma qabiliyyətinin artırılması və tranzaksiya haqqının azaldılması problemlərinin həlli idi. Blokun həcmini 32 Mbayta kimi artırmaq imkanı olmaqla əvvəlcə 2 Mbayt olması barədə qərar qəbul edilmişdi.

Zcash – Bitkoin-dən daha təhlükəsiz olmağı iddia edən başqa virtual valyutadır. Zcash saytında deyilir ki, "Bitkoin valyuta üçün http istifadə edir, Zcash isə https - təhlükəsiz nəqliyyat qatını". Bu kriptovalyuta sıfır məlumat adlanan şifrələmədən istifadə edir. Yəni şifrələnmiş informasiya açıq informasiya haqqında heç bir məlumat vermir.

Dash – Bitkoinin forklarından biridir, 2014-cü ildə bazara çıxıb. Digər altkoinlər kimi, dash da bitkoini təkmilləşdirmək ideyası ilə yaradılıb (Evan Daffild). Təşəkkül prosesində üç ad dəyişib: əvvəlcə Xcoin, sonra DarkCoin adlanırdı, 2015-ci ildən indiki adını alıb.

Dash da Bitkoinin müəyyən problemlərini həll edir, əgər Bitkoin bərabər hüquqlu qovşaqların birranqlı şəbəkəsidirsə, Dash ikiranqlı arxitekturaya malikdir. Birinci səviyyə Bitkoinə oxşayır, burada mayninq vasitəsilə sikkələr buraxılır və yeni bloklar blokçeynə yazılır. Ikinci səviyyədə Masternodlar (əsas qovşaqlar) işləyir.

Masternodlar – kriptovalyutanın bütün blokçeyninin saxlandığı qovşaqlardır, şəbəkənin iş qabiliyyətinin dəstəklənməsi üçün bir sıra vacib funksiyalar, o cümlədən , İnstantSend, PrivateSend və DAO servislərini yerinə yetirirlər.

PrivateSend – bu mexanizm ödənişlərin anonimliyini təmin etmək üçün yaradılıb (Daffildin fikrincə, Bitkoin anonimliyi təmin etmir). Ödəniş bərabər hissslərə bölünür, masternodlar vasitəsilə qarışdırırlır və alan tərəfə göndərilir. Beləliklə, “izlər itirilir” və zamanla ödənişin mənbəyini müəyyən etmək mümkün olmur. Bu mexanizmi yalnız Dash Core pulqabıları dəstəkləyir.

InstantSend – ani tranzaksiyalar üçün nəzərdə tutulmuş xidmətdir. Tranzaksiya bir neçə saniyədə emal edilir. Bu belə işləyir: müştəri ödəniş edir, tranzaksiya 7-10 təsadüfi masternoda göndərilir. Masternodlar təkrar istifadəsinin qarşısını almaq üçün tranzaksiya girişlərini təxminən bir saatlığa bağlayırlar. Tranzaksiyanın təsdiqlənməsi 1-3 saniyə çəkir.

V. STABİL KRİPTOVALYUTALAR – STEYBLKOİNLƏR

Kriptovalyutaların volabilliyi çox yüksəkdir, bu onları spekylyantlar üçün cəlbedici və geniş istifadə üçün yararsız edir. İdeal kriptovalyuta öz alıcılıq qabiliyyəti baxımından stabilliyini saxlamalı, yaxud kiçik inflyasiyaya məruz qalmalıdır. Belə ideal kriptovalyuta steyblkoin adlanır. Ən sadə formada steyblkoin fiat valyutasında stabil dəyəri olan adi kriptovalyutadır.

İlk dəfə “stabil kirptovalyuta” ideyasını 2012-ci ildə Mastercoin komandası irəli sürmüşdü. Bundan sonra yevro və ya yuan əsasında steyblkoin yaratmağa bir neçə cəhd edilmişdi. Lakin steyblkoin ideyasını yalnız üç il sonra uğurla reallaşdırmaq mümkün oldu. Həmin vaxt bazara dollara bağlanmış məşhur Tether çıxdı.

Steyblkoinlərin stabilliyinə təminat ilə nail olurlar. Onların əksəriyyətinə valyutalar və qiymətli metallar, kriptovalyutalar, neft, brilyant kimi aktivlərlə təminat verilir.

Hazırda bazarda steyblkoinlərin üç növü təmsil olur:

1. “Fiat”la təmin olunmuş (ing. fiat-collateralized);
2. Kriptovalyuta ilə təmin olunmuş (ing. crypto-collateralized);
3. Təmin olunmamış (ing. non-collateralized).

Fiat valyuta ilə təmin olunma – steyblkoinlərin yaradılmasının ən sadə üsuludur. Mahiyyətcə bu girov öhdəliyidir. Müəyyən miqdarda fiat valyuta təminat kimi qoyulur və bu valyutaya 1:1 nisbətində steyblkoin buraxılır. Bu metod sadə və etibarlıdır, lakin steyblkoinlərin buraxılması və geriyə mübadilə edilməsi üçün üçüncü tərəfin iştirakını tələb edir. Üçüncü tərəfin fəaliyyətinə nəzarət etmək və müntəzəm auditlər aparmaq lazım gəlir. Aydındır ki, fiat valyutası əvəzinə digər aktivlər də, məsələn, qızıl, gümüş və ya neft də istifadə edilə bilər

İkinci metod – kriptovalyutalarla təminat da əvvəlki metoda oxşayır, lakin bu halda steyblkoin ənənəvi aktivlərlə deyil, kriptoaktivlərlə təmin edilir. Kriptovalyutaların volatilliyi nəzərə alınaraq, bu steyblkoinlər çox zaman ehtiyat ilə təmin olunurlar. Yəni 100 $ məbləğində steyblkoin buraxmaq üçün təminat vermək lazımdır – məsələn, ETH ilə 200 $ məbləğində təminat yaratmaq lazımdır. Beləliklə, əgər hətta baza aktivinin qiyməti 20 % düşsə də, steyblkoin öz dəyərini saxlayacaq. Lakin təminatçı aktivi dəyərsizləşdirən görünməmiş hadisə «qara qu quşu» hadisəsi baş versə, steyblkoin də dəyərini itirəcək və təminatçı daha böyük zərərə düşəcək, çünki steyblkoinlər izafi ehtiyatla təmin olunublar. Məhz buna görə bəzi ekspertlər belə yanaşmanəın əleyhinə çıxış edirlər.

Təmin olunmamış steyblkoinlərin stabilliyi senyoraj hesabına təmin olunur. ***Senyoraj*** – pul emissiyası hesabına yaranan gəlirdir və emitent tərəfindən mənimsənilir. Pul kütləsinin artımından gəlir götürən dövlətlər senyorajdan geniş istifadə edirlər.

Steyblkoin kursunu bir səviyyədə saxlamaq üçün emitentlər onun təklif olunan həcmini smart-kontraktların köməyi ilə nəzarət edirlər. Bu zaman kriptovalyuta sahibləri gələcək senyorajda pay aksiyaları əldə edirlər. Bu konsepsiya “seigniorage shares” adını almışdır. Onu 2014-cü ildə Robert Sems təklif etmişdir və Basecoin və Havven kimi layihələr ona əsaslanır.

Steyblkoinlərin yaradılması ilə bağlı bir sıra layihələr var, onlardan ən populyarlarını göstərək.

Tether – qiyməti dollar kursuna 1:1 nisbətində bağlı olan steyblkoindir – mübadilə zamanı 1 USDT 1 dollara uyğundur. Dövriyyədəki hər bir USDT 1 dollar ilə təmin olunur, o, mərkəzləşmiş idarə olunan əmanət hesabında saxlanır.

MakerDAO – demərkəzləşmiş avtonom təşkilatdır, onun valyutası ABŞ dollarına bağlıdır, lakin ETH ilə tam təmin olunur. Hər bir Dai 1 dollara uyğundur. Qiymətin stabilliyi avtonom smart-kontrakt sisteminin köməyi ilə dəstəklənir.

Basecoin – ABŞ dollarına bağlıdır, qiyməti 1 dollara uyğundur, lakin təmin olunmamış steyblkoindir. Koin buraxılışınmın artırılması və ya azaldılması haqqında qərar konsensus əsasında qəbul edilir.

TrueUSD – ABŞ dollarına bağlı, 100 % təmin olunmuş steyblkoin yaratmaq cəhdidir. Layihə Tether-ə oxşardır, lakin qanunla qorunur, şəffafdır və yoxlanılıb. TrueCoin komandası Cooley və Arnold & Porter birlikdə təmin olunmuş kriptovalyutalar üçün hüquqi sistem işləyib hazırlamışdır. Onlar həmçinin normativ-hüquqi uyğunluq və bank xidməti üzrə qəyyumlar və mütəxəssislər şəbəkəsini də inkişaf etdirirlər.

VI. KRİPTOVALYUTALARDA BƏZİ TEXNOLOJİ HƏLLƏR

Blokçeynin ən vacib göstəriciləri miqyaslama, təhlükəsizlik və demərkəzləşmədir, lakin burada bəzi problemlər var.

Blokçeynlə əlaqəli əsas problemlərdən biri informasiyanın şəbəkədə iştirak edən hər bir sistemdə kopyalanmasıdır. Hazırda bitkoin üçün fərdi kompüterə kopyalanan bloklar 200 qiqabaytdan çox yer tutur. Mərkəzləşmə olmadığından istifadəçilər böyük həcmdə informasiyanı kopyalamağa

məcburdurlar. Lakin belə yanaşma dələduzluğun və şəbəkənin sahibləri (və ya idarəçiləri) tərəfindən informasiyanın saxtalaşdırılmasının qarşısını alır.

Ethereum kriptovalyuta şəbəkəsində tranzaksiyaların təsdiqlənməsi sürətini artırmaq üçün “şardinq” texnologiyasından istifadə etməyə cəhd edir. Şardinq – blokçeyn şəbəkəsinin tranzaksiyaları paralel emal edə bilən bir neçə kiçik çəbəkə komponentlərinə (“şard”lara) bölünməsini nəzərdə tutur. Bu şəbəkənin buraxma qabiliyyətini artırmağın və Visa və Mastercard-da olduğu kimi saniyədə minlərlə tranzaksiya emal etməyin metodlarından biri ola bilər.

Bitkoin blokçeyn şəbəkəsində isə tranzaksiyaların təsdiqlənməsi sürətini artırmaq üçün Lightning Network (LN) ideyasından istifadə etməyə hazırlaşır. LN-in ideyası ondan ibarətdir ki, tranzaksiyaların hamısı blokçeynə yazılmamalıdır. Təsəvvür edin ki, biz sizinlə öz aramızda sistematik olaraq bir neçə tranzaksiya edirik. Bu halda tranzaksiyaları qeydə almaq və onlar zəncirdən çıxarmaq olar.

Sadə dillə izah olunsa, bu belə işləyir: biz öz aramızda ödəniş kanalı açırıq və onun açılmasını blokçeyndə yazırıq. Bundan sonra tranzaksiyaları bu ödəniş kanalı ilə edə və kanalı lazım olduğu müddətdə açıq saxlaya bilərik (hətta on illərlə). Biz yalnız kanalı bağladıqda blokçeynə qayıdırıq və məhz bu zaman kanal ilə yerinə yetirilmiş tranzaksiyaların son vəziyyətini blokçeynə yazırıq. İstənilən sayda ödəniş kanalları yaratmaq və blokçeyndə tranzaksiyaları minimuma qədər azaltmaq olar.

LN Bitkoin şəbəkəsi üzərində “ikinci səviyyə şəbəkəsidir”, blokçeyn şəbəkəsi yükünü artırmadan tranzaksiya axınını istənilən dəfə artırmağa imkan verir (nəzəri olaraq). Bu o deməkdir ki, bunun sayəsində Bitkoin maynerlərin elektrik enerjisini artırmadan öz buraxma qabiliyyətini artıra biləcək.

PoW tranzaksiyaların blokçeyndə təsdiq olunmasının yeganə üsulu deyil. Bir neçə digər metod da vardır, onlardan ən ümidvericisi “proof-of-stake” (POS) – “hissə ilə isbat” adlanır. Onun əsas üstünlüyü ondadır ki, o hesablamalardan imtina etməyə imkan verir.

Yanaşmanın mahiyyəti belədir. POS metodu ilə işləyən maynerlər hesablama maşınlarının gücü ilə deyil, öz pulqabılarının ölçüləri ilə yarışırlar. Bitkoinə tətbiq etdikdə bu təxminən belə olacaq. Maynerlər əvvəlki kimi sadə iştirakçılardan tranzaksiyaları toplamalı və onların düzgünlüyünü yoxlamalıdırlar. Blokçeynə yazmaq hüququ isə hər 10 dəqiqədən bir püşklə müəyyən edilir – uduş ehtimalı maynerin hesabında olan məbləğlə düz mütənasibdir. Beləliklə, bitkoin pulqabınızda nə qədər çox pul varsa, növbəti bloku blokçeynə yazmaq hüququnu sizin alacağınız ehtimalı bir o qədər böyükdür. Ümumiyyətlə, heç bir hesablama tələb edilmir, buna görə əvvəlcə hesablamalara, sonra isə soyutmaya kilovattlarla enerji xərcləmək lazım gəlmir.

PoS sxemi nəzəri baxımından əsaslı işləsə də, Bitkoin ölçüsündə olan heç bir blokçeyn sistemində praktiki reallaşdırılmayıb. PoS sxeminin təmiz şəkildə və ya hibrid reallaşdırdığı kriptovalyutalar olsa da (Bitcoin, Dark, BitShares, Blocknet və digələri), onların heç biri yükünə və kapitallaşmasına görə Bitkoinlə müqayisə edilə bilməz.

PoS sxeminə bitkoin yox, Ethereum keçməyə hazırlaşır. Bəzi tədqiqatçılar bunu Ethereumun valideyninin (Bitkoin) kölgəsindən çıxmaq, özünün müstəqil, proqressiv imicini təsdiqləmək üçün etdiyini söyləyirlər.

VII. KRİPTOVALYUTA VERİLƏNLƏRİNİN ANALIZI

İnternetdə bir sıra açıq (pulsuz) və ödənişli kriptovalyuta verilənləri mövcuddur:

- Bitkoin şəbəkəsində tranzaksiyaların və komissiyaların dinamikası;
- Kriptoaktivlərin və birjaların statistikası və reytinqləri;
- ICO-trekerlər və Token Sale reytinqləri;
- Bazar indeksləri;
- Kriptovalyutaların bazar kapitallaşması və s.

Əlbəttə, adi istifadəçiləri ən çox maraqlandıran məsələ bitkoin və digər kriptovalyuta kurslarının proqnozu məsələsidir. Qeyd edək ki, ən məşhur kriptovalyuta kimi Bitkoin kursunun proqnozu üçün bir çox analiz və tədqiqatlar aparılmışdır. İlk əvvəl, ezaman sıralarının analizi üçün nəzərdə tutulmuş aşağıdakı modellər tətbiq edilmişdir:

- ARIMA (Autoregressive Integrated Moving Average);
- ARCH (AutoRegressive Conditional Heteroskeda-sticity);
- GARCH (generalized ARCH).

Məsələn, [3]-də bitkoinlərin dəyişkənliyinin vaxtla əhəmiyyətli dərəcədə fərqləndiyini və bu əlaqənin T-GARCH (1.1) modelinin ən yaxşı şəkildə əks etdirildiyini təsbit edir. Bitkoin ilə real iqtisadiyyat göstəriciləri arasındakı əlaqələr zamanla uyğun olmayan və əsasən əhəmiyyətsiz olduğu qənaətinə gəlinir.

Uzun müddət, makro-maliyyə göstəriciləri Altcoinin qiymətinin bitkoin-dən daha az formalaşmasını müəyyənləşdirmişdir. Virtual valyuta təchizatı ekzogen olduğu üçün qiymətlərin formalaşmasında məhdud rol oynayır [4].

Bitcoin'in artan məşhurluğu və tacirlərin tanınması sayəsində, dəyər yaranmasına təsir göstərən amilləri anlamaq üçün getdikcə daha çox əhəmiyyət kəsb edir. Ən çox istifadə edilən kriptiovalyutaların 66 hissəsini təhlil edən şifrəli empirik məlumatlardan istifadə edərək tənzimləmə modelinin kriptovalyuta dəyərinin üç əsas sürücüsünə istinad etdiyi qiymətləndirilmişdir [5]:

- istehsalçı şəbəkələrində rəqabət səviyyəsi,
- vahid istehsal nisbəti,
- kriptovalyuta üçün mayninq alqoritminin çətinliyi.

Bitkoin kimi kriptovalyutalar bir investisiya aktivi kimi qururlar və özlərini tez-tez Yeni Qızıl adlanırlar. Lakin [6]-da aparılmış araşdırma göstərir ki, bu iki aktiv bir-birindən çox

fərqlənirlər. Birincisi, bitkoin və qızılın, eləcə də digər aktivlərin şərti dəyişiklik xassələri analiz və müqayisə edilir. İkincisi, zamana görə dəyişən şərti korrelyasiyaları qiymətləndirmək üçün BEKK-GARCH modeli tətbiq edilir. Nəticələr, göstərir ki, bitkoinin davranışı qızılın davranışının tam əksinədir.

Bitkoin üçün zaman əsaslı valyuta qiymətləndirmələri keçirilmişdir. Araşdırmanın nəticəsi olaraq, 10.01.2018 və 18.01.2018 tarixləri arasında neyron şəbəkələrinin MPL (6-3-1) modeli ilə təxmin edilən qiymətlərin istiqaməti və kəmiyyəti ARIMA (1.1.6) modelindən daha yaxşı olmuşdur [7].

[8]-də GARCH modelləri istifadə edilməklə bitkoinin maliyyə aktivi imkanları araşdırılır. İlkin model qızıla və dollar müəyyən oxşarlıq göstərir, bitkoinin hedcin imkanlarını və mübadilə vasitəsi kimi üstünlüklərini nümayiş etdirir. Asimmetrik GARCH göstərir ki, bitkoin riskin idarə edilməsində faydalı ola bilər, xüsusilə riskə meyl etməyən investorlar üçün idealdır. Ümumilikdə, bitkoinin maliyyə bazarlarında və portfel idarəçiliyində yeri var, çünki mübadilə vasitəsi üstünlüyü və dəyəri saxlama üstünlüyü miqyasında qızıl və amerikan dolları arasında təsnif edilə bilər.

[9]-da bitkoinin ABŞ dollarına nisbətən məzənnəsinin dəyişməsi statistik analiz edilir, maliyyədə ən məşhur 15 parametrik paylanma nəzərdən keçirilir. Ümumiləşdirilmiş hiperbolik paylanmanın daha yaxşı nəticə verdiyi göstərilir. Valyuta məzənnəsinin gələcək qiymətləri üçün proqnozlar verilir.

Tədqiqatların ikinci istiqaməti kimi maşın təlimi metodlarının, xüsusilə neyron şəbəkələrinin tətbiqini ayırmaq olar. [10]-da neyron şəbəkəsi istifadə edilərək bitkoinin bir gün əvvəlki qiyməti və həcmi əsasında meyli proqnoz edilir.

Məlumdur ki, maşın təlimi metodlarından dərin təlim arxitekturaları şəkil və mətnlərin tanınması sahəsində yüksək nəticələr göstərmişdir, lakin maliyyə sahəsində çox istifadə edilmir. [11]-da cari qiymətə görə növbəti dövrün qiymətinin istiqamətini proqnozlaşdırmaq üçün konvolyusiya neyron şəbəkələri (Convolutional Neural Network, CNN) istifadə edilir.

Bayes optimallaşdırılmış rekurrent neyron şəbəkəsi (recurrent neural network, RNN) və uzun-qısamüddətli yaddaş (Long Short Term Memory, LSTM) şəbəkəsi bitkoin qiymətinin proqnozlaşdırılmasına tətbiq edilir. Zaman sıralarının proqnozlaşdırılması üçün məşhur ARIMA modeli dərin öyrənmə modelləri ilə müqayisə edilir. Gözlənildiyi kimi, qeyri-xətti olan dərin öyrənmə metodlarının xətası ARIMA proqnozuna nisbətən çox azdır [12].

Kriptovalyutaların qiymətlərinin proqnozlaşdırılması üçün [13]-də ARIMA modeli ilə təkrarlanan dərin çoxlaylı neyron şəbəkəsi (seq2seq) müqayisə edilir.

NƏTİCƏ

Kriptovalyutalar son bir neçə ildə meydana çıxsalar da, informasiya texnologiyalarında və maliyyə texnologiyalarında ən məşhur trendə çevrilmiş, dövriyyə həcmi milyardlarla ölçülən böyük bir ekosistem formalaşdırmağa nail olmuşdur. Bu ekosistemin mahiyyətini başa düşmək, əlaqədar sahələrdə baş verən dinamik dəyişiklikləri analiz etmək, gizli qanunauyğunluqları aşkarlamaq üçün kriptovalyutalarla əlaqəli verilənlərin intellektual analizi metodlarının işlənməsi vacibdir.

ƏDƏBİYYAT

[1] N. Hətəmova, Bitcoin texnologiyasının elmi-nəzəri və praktiki problemləri, “İnformasiya təhlükəsizliyinin aktual problemləri” III respublika elmi-praktiki seminarının matertialları, s.112-115, 2017.

[2] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S.Goldfeder,” Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press” , 2016.

[3] J. Šafka, “Virtual currencies in real economy: Bitcoin”. Diploma thesis. 2014.

[4] P. Ciaian, M. Rajcaniova, “Virtual relationships: Short-and long-run evidence from BitCoin and altcoin markets”, Journal of International Financial Markets, Institutions and Money, vol. 52, pp. 173-195, 2018.

[5] A.S. Hayes “Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin” Telematics and Informatics, vol. 34(7), pp.1308-1321, 2017.

[6] T. Klein, H.P. Thu, T. Walther, “Bitcoin is not the New Gold – A comparison of volatility, correlation, and portfolio performance” International Review of Financial Analysis, vol. 59, pp.105-116, 2018.

[7] E.E. Şahini, “Kripto para bitcoin: ARIMA ve yapay sinir ağları ile fiyat tahmini” Fiscaoeconomia, vol.2 (2), pp. 74-92, 2018.

[8] A. H. Dyhrberg, ‘Bitcoin, gold and the dollar – A GARCH volatility analysis”. Finance Research Letters, vol.16, pp. 85-92, 2016.

[9] J. Chu, S. Nadarajah and S. Chan , “Statistical analysis of the exchange rate of bitcoin”, PloS one,vol. 10(7), e0133678, 2015.

[10] J. Almeida, S. Tata, A. Moser and V. Smit, “ Bitcoin prediciton using ANN”, Neural networks, vol. 7, pp. 1-12, 2015.

[11] A. Dingli and K. Fournier ,” Financial time series forecasting – A deep learning approach,” International Journal of Machine Learning and Computing, vol. 7, pp. 118-122, 2017.

[12] S. McNally, J. Roche and S. Caton,” Predicting the price of Bitcoin using Machine Learning”, 26th Euromicro International Conf. Parallel, Distributed and Network-based Processing, pp. 339-343, March 2018.

[13] J. Rebane, I. Karlsson, S. Denic and P. Papapetrou, “Seq2Seq RNNs and ARIMA models for cryptocurrency prediction: A comparative study”, 2018.

ISSUES OF MINING CRYPTOCURRENCY DATA

Yadigar İmamverdiyev, Firəngiz Sadiyeva
[1,2]Institute of Information Technology of ANAS,
Baku, Azerbaijan
[1]yadigar@iit.science.az, [2]sadiyeva.firengiz@gmail.com

Abstract – Cryptocurrencies are the phenomenon that has emerged over the last few years and promises revolutionary changes in the financial sector. Blockchain technology based on most cryptocurrencies can also cause noticeable changes in other areas of activity. The article gives a brief overview of cryptocurrency technologies, some of the technological solutions that are on the agenda in this area are highlighted and analytical methods of cryptocurrency data are analyzed.

Keywords – cryptocurrency; Bitcoin; blockchain; hardfork; softfork; altcoin; stable coin; Ethereum; data mining