UOT 004.056:351

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@iit.science.az

BLOKÇEYN TEXNOLOGİYALARI: KOMPONENTLƏRİ, TƏTBİQLƏRİ VƏ PROBLEMLƏRİ

Daxil olmuşdur: 24.05.2019. Düzəliş olunmuşdur: 17.06.2019. Qəbul olunmuşdur: 01.07.2019.

Bitkoin kriptovalyutasını dəstəkləmək üçün yaradılmış blokçeyn texnologiyasının potensialı daha böyükdür və digər tətbiq sahələrində də geniş imkanlar təqdim edir. Blokçeyn texnologiyası rəqəmsal tranzaksiyaların paylanmış, təhlükəsiz və etibarlı emalını təmin edir. Son dövrlər blokçeyn texnologiyası geniş tədqiq olunmağa başlayır, lakin həm tədqiqatçılar, həm də texnologiyalar sahəsində əksər qərar qəbul edənlər arasında bu texnologiyanın əsl potensialı haqqında düzgün təsəvvür yoxdur. Bu işdə blokçeyn texnologiyasının komponentləri analiz edilir, müxtəlif sahələrdə tətbiqi təcrübələri təhlil edilir və bu texnologiyanın inkişafı üçün həll edilməsi vacib problemlər müəyyən edilir, gələcək tədqiqat istiqamətləri göstərilir.

Açar sözlər: *Bitkoin, blokçeyn, paylanmış reyestr texnologiyası, blokçeyn platforması, konsensus protokolu, Bizans imtinalarına qarşı dayanıqlılıq, Ethereum, Hyperledger-Fabric, IOTA.*

Giriş

Bitkoin kriptovalyutası 2008-ci ildə meydana çıxdıqdan sonra qısa müddətdə məşhurlaşdı, yüzlərlə alternativ kriptovalyutalar yaradıldı və bu maliyyə dünyasına böyük dəyişikliklər gətirdi [1].

Lakin Bitkoin "aysberqin yalnız görünən tərəfi"dir, onun əsasında daha incə texnologiya – blokçeyn dayanır. Bu texnologiyanın inqilabi potensialı yalnız 2015-ci ilin ikinci yarısında kəşf edilməyə başlanmışdır [2]. Hazırda blokçeyn maliyyə dünyasında ən populyar açar sözlərdən biridir, lakin blokçeynin potensialı maliyyə və bank sektoru ilə məhdudlaşmır, digər sahələr də bu innovativ texnologiyadan faydalanmaq istəyirlər. Təsadüfi deyil ki, mütəxəssislər artıq "Blockchain 1.0" (kriptovalyutalar), "Blockchain 2.0" (ağıllı müqavilələr) və "Blockchain 3.0" (dövlət idarəçiliyi, təhsil, elm, mədəniyyət və s. sahələrdə tətbiqlər) kimi inkişaf mərhələlərini ayırırlar [2]. Blokçeynə belə marağın səbəbi onun təhlükəsizliyi, şəffaflığı, anonimliyi və verilənlərin tamlığını heç bir üçüncü tərəf olmadan təmin etməsi və bu özəllikləri Bitkoinin timsalında bir neçə il müddətində praktiki olaraq fasiləsiz işləməsi ilə sübuta yetirməsidir.

Son dövrlər blokçeyn texnologiyasının bir çox sahədə tətbiqi üzrə pilot layihələr həyata keçirilir, lakin belə layihələrin texniki reallaşdırılması haqqında detallı informasiya əlyetər deyil [2,3]. Bundan başqa, blokçeyn texnologiyası Bitkoin ilə sıx bağlıdır, bu səbəbdən infrastrukturu (blokçeyn) bu infrastrukturdan istifadə edən məhsuldan (Bitkoin) fərqləndirmək də müəyyən çətinliklər yaradır. Hazırda qərar qəbul edən şəxslər konkret sahələrdə blokçeyn texnologiyasının dəqiq necə tətbiq ediləcəyini başa düşməkdə çətinlik çəkirlər [4]. Texnologiyanı daha yaxşı başa düşmək, yeni ideyalar və innovasiyalar generasiya etmək üçün blokçeyn sahəsində həyata keçirilmiş elmi-praktiki tədqiqatların və praktiki işlərin analizinə, qiymətləndirilməsinə və ümumiləşdirilməsinə ciddi ehtiyac vardır.

Bu məqalənin ideyası həmin tələbdən yaranmışdır və məqsədi blokçeyn texnologiyasının əsas komponentlərini təhlil etmək, müxtəlif sahələrdə bu texnologiyanın tətbiqi təcrübələrini analiz etmək və gələcək tədqiqat istiqamətlərini müəyyən etməkdir.

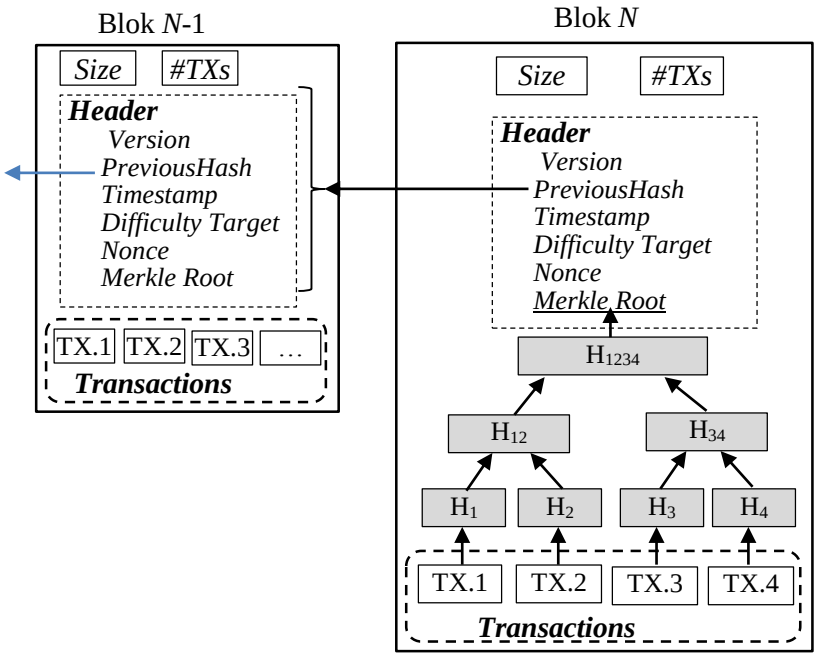
Bitkoin texnologiyasının bəzi xüsusiyyətləri

Blokçeyn texnologiyası daha çox Bitkoin ilə əlaqədar tanınır. Bitkoin ilk kriptovalyutadır, onun konsepsiyası kimliyi hələ də anonim qalan Satoshi Nakamoto tərəfindən 31 oktyabr 2009-cu ildə açıqlanmışdı [5]. Bitkoin rəqəmsal pul mübadilələri üçün mərkəzləşməmiş, hər hansı aralıq

vasitəçi olmayan mühit təqdim edir. Tranzaksiyalar maynerlər tərəfindən yoxlanılır və blok şəklində blokçeyn adlanan hamıya açıq reyestrə yazılır. Hər bir blokun başlığına özündən əvvəlki blokun başlığının SHA256 kriptoqrafik heş funksiyası ilə iki dəfə hesablanmış heşi yazılır. Bununla da Bitkoin şəbəkəsində nə vaxtsa yerinə yetirilmiş bütün tranzaksiyalar bir zəncirlə əlaqələndirilmiş olur. Bu zəncirdə hər hansı tranzaksiyanı dəyişmək mümkün deyil, bunun üçün zəncirdəki bütün blokları dəyişmək lazımdır ki, bu da praktiki olaraq mümkün deyil.

Texniki baxımdan, adından da göründüyü kimi, blokçeyn ("block" – blok + "chain" – zəncir) informasiya bloklarının zənciridir. Şəkil 1-də Bitkoin blokçeyninin strukturu təsvir olunur. Şəkil 1-də göstərildiyi kimi, hər bir Bitkoin bloku dörd komponentdən ibarətdir: blokun ölçüsü (*Size*), tranzaksiya sayğaçı (*#TXs*), blokun başlığı (*Header*) və tranzaksiyalar (*Tranzactions*). Blokun ölçüsü və tranzaksiya sayğacı, uyğun olaraq, blokdakı baytların və tranzaksiyaların saylarını göstərir. Tranzaksiyalar – bloka daxil olan tranzaksiyaların siyahısıdır. Blok başlığına altı sahə daxildir:

- *Version* – versiya nömrəsi (konsensus protokolunun yenilənməsini izləmək üçün istifadə edilir);
- *PreviousHash* – zəncirdə bilavasitə əvvəl gələn blokun heşi;
- *Timestamp* – blokun yaradılması tarixi;
- *Target* – hədəf qiyməti, mayninq prosesində bu qiymətdən kiçik olan heş axtarılır;
- *Nonce* – mayninq alqoritmində istifadə edilən sayğac;
- *Merkle Root* – bloka daxil olan bütün tranzaksiyaların heşləri əsasında yaradılan binar ağacdır.



Şəkil 1. Bitkoin blokçeyninin strukturu

Mayninq sxemində T hədəf qiyməti istifadə edilir, onun cari qiyməti periodik olaraq yenidən hesablanır. Maynerlərin məqsədi elə *Nonce* qiyməti tapmaqdır ki,

$$H(B.N) < T \tag{1}$$

olsun, burada B – blokdakı tranzaksiyaları təsvir edən sətirdir, N – *Nonce* qiymətidir, '.' – konkatenasiya operatoru və H – Bitkoində istifadə edilən heş funksiyadır, yəni

$$H(S) \coloneqq SHA256\big(SHA256(S)\big). \tag{2}$$

Bitkoində H heş funksiyası elə seçilib ki, 0 ilə $2^{256}-1$ arasında müntəzəm paylanmış təsadüfi qiymətlər versin. (1) şərtinin ödənməsinə nail olmaq üçün mayner $Nonce$ qiymətini təsadüfi və ya sistematik şəkildə (məsələn, 0-dan başlayıb ardıcıl artırmaqla) seçir, həmin qiyməti blok başlığına yazır və onun heşini hesablayır. Əgər heş qiymət T-dən kiçik deyilsə, onda N-in qiymətini dəyişir, blok başlığına yazır və heşi yenidən hesablayır. Bu proses hədəf qiymətdən kiçik heş tapılana kimi təkrarlanır. Müvafiq N tapıldıqda blok Bitkoin şəbəkəsinə göndərilir və blokçeynə əlavə edilir. Blokun tapılmasına görə onu tapan mayner mükafat olaraq hazırda 12,5 bitkoin əldə edir ("mədəndən çıxarır"). Buna görə N-in uyğun qiymətinin tapılması prosesinə "Bitkoin mayninqi" deyilir. Blokun yaradılması, blokçeynə yazılması və qovşaqlara göndərilməsi protokolu isə "görülmüş işin isbatı" (Proof of Work, PoW) protokolu adlanır.

Bitkoinlərin mayninqi sürətini, yəni yeni blokların yaradılmasına sərf edilən zaman müddətini (1)-dəki T hədəf qiymətini seçməklə tənzimləmək olar. Hədəf qiymətləri böyük ədədlərdir (təxminən 67 onluq rəqəmli), buna görə Bitkoin mayninqi barəsində danışarkən, *çətinlik* terminindən istifadə etmək daha rahatdır. Çətinlik D ilə T hədəf qiyməti arasındakı münasibət

$$D = \frac{T_{max}}{T} \tag{3}$$

düsturu ilə təyin edilir, burada, $T_{max} = (2^{16}-1)\cdot 2^{208} \approx 2^{224}$ maksimal mümkün hədəf qiymətidir. Bu "ən asan" qiyməti S. Nakamoto ilk Bitkoin blokunu – Genezis blokunu yaradarkən istifadə etmişdi.

Aydındır ki, çətinliyin qiyməti bir həqiqi blokun axtarışı üçün hesablanmış heşlərin orta sayı ilə əlaqəlidir. D çətinliyinin qiyməti hər 2016 blokdan (təxminən 2 həftədən) sonra yenidən hesablanır ki, orta heş sürəti saxlandıqda növbəti 2016 blok 2 həftə müddətində yaradılsın, yəni bloklar arasındakı 10 dəqiqəlik interval təmin olunsun. Əgər çətinliyin qiyməti sabit saxlansaydı, Bitkoin şəbəkəsinə qoşulan yeni mayninq gücləri hesabına yeni blokların yaradılması müddəti qısalardı. Yeni çətinliyi (və uyğun olaraq, hədəf qiymətini) hesablamaq üçün cari çətinlik qiyməti son 2016 bloku yaratmaq üçün gözlənilən zaman müddətinin (2016×10 dəq) sərf edilən faktiki zaman müddətinə (dəqiqələrlə) nisbətinə vurulur:

$$D_{new} = D \times \frac{20160}{\text{Actual time to produce the last 2016 blocks}} \tag{4}$$

Blokçeyn arxitekturasının əsas komponentləri

Blokçeyn arxitekturasının əsas komponentləri aşağıda qısa təsvir olunur:

Tranzaksiya (TX). Blokçeynin vəziyyətinin dəyişməsi ilə nəticələnən prosesdir. Blokçeyn platformasından asılı olaraq, tranzaksiya maliyyə dəyərinin transferi və ya smart-kontraktlar kimi ixtiyari kodun yerinə yetirilməsi ola bilər [1].

Blok. Yaxın keçmişdə baş vermiş və hələlik təsdiqlənməmiş tranzaksiyaların çoxluğudur. Ənənəvi blokun strukturu barədə əvvəlki bölmədə məlumat verilmişdir.

Blokçeyn. Bütün tranzaksiyaların/blokların saxlandığı paylanmış reyestrdir [5].

Mayninq. Validasiya edilmiş tranzaksiyaların bloka əlavə edilməsi və sonra həmin blokun blokçeyn şəbəkəsinin bütün qovşaqlarına göndərilməsidir. Mayninqi xüsusi mayninq qovşaqları yerinə yetirirlər, yeni bloku mayninq edəcək qovşaq müəyyən lotereya sxeminin əsasında seçilir. Məsələn, Bitkoin-də maynerlər kriptoqrafik heş tapmacasını həll etməkdə yarışırlar və həlli birinci tapan yeni bloku formalaşdırmaq hüququ qazanır (PoW kimi tanınır). Blok mayninq edilib blokçeynə əlavə edildikdən sonra həmin blokdakı tranzaksiyalar təsdiqlənmiş hesab olunurlar [1].

Sadə/Normal qovşaq. Blokçeyn şəbəkəsində qovşaqların hesablama gücü və yaddaşın həcmi kimi resurslardan və imkanlarından asılı olaraq müxtəlif növləri ola bilər. Sadə qovşaq tranzaksiyaları yalnız göndərə və ala bilir, blokçeynin tam surətini saxlamır. Məsələn, SPV (Simplified Payment Verification) – ödənişin sadələşdirilmiş yoxlanması protokolu Bitkoin-pulqabıların smartfonlarda bütün blokçeyni saxlamadan işləməsinə imkan verir. Belə kliyentlər

tam qovşaqlardan bütün blokçeyni deyil, blok başlıqlarını alır və saxlayırlar. İkiqat xərcləməni aşkarlayacaq yoxlamanı aparmaq üçün blok başlıqları kifayətdir.

Tam qovşaq. Bu qovşaqlar blokçeynin tam surətini saxlayırlar, lakin bloku mayninq etmirlər. Tam qovşaqlar tranzaksiyaları müvafiq blokçeynin konsensus qaydalarına görə validasiya edirlər, blokun qəbul və ya fork edilməsinə kömək edirlər [6]. Bu, tam qovşaqların tranzaksiya və blok yaymaq imkanlarının olduğunu nəzərdə tutur. Buna görə də, tam qovşaqlar blokçeynin təhlükəsizliyi üçün çox vacibdirlər.

Mayner/Validator qovşaqlari. Bunlar yeni bloku mayninq və ya validasiya etmək imkanı olan tam qovşaqlardır, bununla blokçeyn genişlənir [6]. Bundan başqa, mayninq qovşaqları blokçeyndə istifadə edilən konsensus protokolunun növünə əsasən konkret kriteriyalara görə seçilir.

Konsensus protokolu. Tam qovşaqların tranzaksiyaların sırası barədə razılığa nail olmalarını təmin edən mexanizm və ya qaydalar çoxluğudur. Konsensus protokollarının müxtəlif blokçeyn tətbiqlərində istifadə edilən bir çox növü vardır. Bəzi məşhur konsensus protokolları növbəti bölmələrdə müzakirə olunur.

TX/Blok-un yekun təsdiqi müvafiq blokçeynin konsensus protokolu tərəfindən konkret tranzaksiya və ya blokun yekun təsdiqlənməsi ilə əlaqəlidir. Bu çox vacib aspektdir, çünki o, tranzaksiyanın təsdiqlənməsində gecikməni müəyyən edir və son nəticədə, blokçeynin tranzaksiya məhsuldarlığına təsir edir. Məsələn, Bitkoin-də tranzaksiya 10 dəqiqədən sonra, yəni həmin tranzaksiyanın olduğu blok mayninq edildikdən sonra ilk təsdiqlənməsini alır. Lakin son (yekun) təsdiqlənməni almaq üçün həmin tranzaksiya daha beş blokun mayninq edilib baxılan tranzaksiyanın olduğu blokçeynə əlavə edilməsini gözləməlidir. Deməli, Bitkoin blokçeynində bir tranzaksiyanın yekun təsdiqlənməsi 60 dəqiqə çəkir. HyperLedger [6, 7] və Tendermint [8] kimi blokçeynlərdə isə tranzaksiyalar anında təsdiqlənirlər.

Blokçeynin növləri

Blokçeynin digər sahələrdə tətbiqi cəhdləri onun yeni növlərinin meydana çıxmasına gətirib çıxardı. Blokçeynləri verilənlərin əlyetərliyinə görə və tranzaksiya bloklarının yaradılmasına görə siniflərə bölürlər.

Mütəxəssislər blokçeyn verilənlərinə girişlə əlaqədar olaraq blokçeynləri açıq (ing. public) və özəl (ing. private) olmaqla iki sinfə bölməyi tövsiyə edirlər [9].

Blokçeynlər tranzaksiyaları emal etməyə, yəni tranzaksiyaların yeni bloklarını yaratmağa qoyulan məhdudiyyətdən asılı olaraq inklüziv (ing. permissionless) və ekskluziv (ing. permissioned) blokçeynlərə bölünürlər. İnkluziv blokçeyndə istənilən qovşaq tranzaksiyaların yeni blokunu yarada bilər. Ekskluziv blokçeyndə isə tranzaksiyaların emalını yalnız seçilmiş qovşaqlar həyata keçirə bilərlər.

Ethereum platformasının sahibi Vitalik Buterin 2015-ci ildə şirkət bloqunda nəşr etdiyi məqalədə blokçeynləri 3 sinfə təsnif edir [9]:

- *açıq blokçeyn* (ing. *public blockchain*) – tamamilə açıq blokçeyndir, tranzaksiyalar azad şəkildə həyata keçirilir və onlara heç kim nəzarət etmir, hər bir kəs konsensus prosedurunda iştirak edə bilər;
- *konsorsium blokçeyni* (ing. *consortium blockchains*) – konsensus proseduruna seçilmiş qovşaqlar nəzarət edir;
- *özəl blokçeyn* (ing. *fully private blockchain*) – mərkəzi orqan bütün tranzaksiyaları izləyir və nəzarət edir.

Böyük Britaniya hökumətinin baş elmi məsləhətçisi ser Mark Valport da oxşar təsnifat təklif edir [10]. O, paylanmış reyestrlər və onların dövlət idarəetməsində potensialı mövzusundakı məruzəsində blokçeynləri aşağıdakı 3 sinfə bölür:

- *inklüziv reyestrlər* (ing. *permissionless public ledgers*) – burada tranzaksiyaları təsdiqləyən mərkəzi orqan yoxdur. Bitkoin və Ethereum belə reyestrlərə misaldır;

- *eksklüziv açıq reyestrlər* (ing. *permissioned public ledgers*) – burada tranzaksiyaları müəyyən subyektlər təsdiqləyir. Bunlar idarəedici orqan, səlahiyyətli əməkdaş, müəssisə və s. ola bilər. İstifadəçilər verilənlərə baxa bilərlər (xüsusilə, vacib informasiya gizli saxlana bilər);
- *eksklüziv özəl reyestrlər* (ing. *permissioned private ledgers*) – əvvəlki növə oxşayır, fərq ondadır ki, verilənlər hamıya açıq deyil.

Hibrid blokçeyn. Açıq və özəl blokçeynlər arasında bir balansdır, onu "qismən mərkəzsizləşmiş" və ya "konsorsium blokçeyni" də adlandırırlar. Məsələn, on sənaye təşkilatının konsorsiumunda hər bir təşkilat blokçeyn şəbəkəsində özünün mayninq/yoxlama qovşağını dəstəkləyir. Bu halda blok ən azı yeddi qovşaq tərəfindən imzalandıqda həqiqi ola bilər. Bütün qovşaqların blokçeyndən oxumaq üçün açıq girişi ola bilər və ya bu yalnız konkret qovşaqlara məhdudlaşdırıla bilər [9]. Lakin demərkəzləşmənin azalması səbəbindən blokçeyn yazılarının saxtalaşdırılması ehtimalı var [3].

Blokçeyn budaqlanmaları. Açıq blokçeynlərin çoxu budaqlanmaya meyllidirlər. Budaqlanma (ing. fork) – blokçeyn şəbəkəsinə müəyyən dəyişiklik edilməsi, təkmilləşdirilməsi, aşkarlanmış hansısa nöqsanların aradan qaldırılması, məsələn, blokun uzunluğunun, mayninq alqoritminin, konsensus protokolunun modifikasiyası nəticəsində yaranır [1, 11]. Budaqlanmanın iki növü var:

Soft fork – blokçeynin proqram kodunun "yumşaq" dəyişdirilməsi prosesidir, onun gedişində blokçeyn şəbəkəsində işləyən qovşaqların proqram təminatının tam dəyişməsi tələb edilmir. Soft fork zamanı edilən dəyişikliklər ona qədər yaradılmış verilənlərlə uyarlığı saxlayır, lakin yeni verilənlərin yaranması prosesi dəyişir.

Hard fork – proqram koduna «sərt» dəyişiklik edilməsidir, bundan sonra köhnə proqram təminatı ilə qarşılıqlı əlaqə tamamilə itir. Faktiki olaraq, hard fork gedişində əvvəlkindən fərqli, tamalilə yeni prinsip ilə işləyən yeni blokçeyn yaradılır.

Konsensus protokolları

Bu bölmədə konsensus mexanizmlərinin əsas növləri, onların işləmə prinsipləri analiz edilir. Konsensus qrup tərəfindən qərar qəbulu prosesidir, qrupun bütün üzvləri qrupun maraqları baxımından qrup qərarını dəstəkləməyə razılaşırlar [12]. Blokçeyn üçün də konsensus protokolları olduqca vacibdir, çünki blokçeyn demərkəzləşmiş bərabərhüquqlu qovşaqların sistemidir və onda mərkəzi hakimiyyət orqanı yoxdur. Belə sistemlərdə ciddi problemlərdən biri mərkəzi hakimiyyət orqanı olmadan qərar qəbul edilməsidir.

Blokçeyndə mərkəzi orqan olmadan bütün qovşaqlarda blokçeynlərin eyni olmasını təmin etmək lazımdır. Konsensus protokolları blokçeyndə bu problemin həlli üçün istifadə edilir, həqiqiliyin yoxlanması şəbəkənin bir çox iştirakçısı arasında paylanır və izafilik hesabına sistemin imtinalara dayanıqlılığı təmin edilir [13].

PoW protokolu yuxarıda təsvir olunmuşdur, onun ən böyük üstünlüyü Bitkoində bir neçə il ərzində real istismarla yoxlanmış etibarlılığıdır, bunu bir çox digər konsensus protokolu barəsində demək mümkün deyil. *PoW*-un nöqsanlarına gəlincə, gecikmələr böyükdür, hesablama həcmi olduqca çoxdur, bunun nəticəsində elektrik enerjisi xərcləri də olduqca yüksək olur.

Proof of Stake (PoS) konsensus protokolunda mayninq prosesi virtualdır və maynerləri validatorlar əvəz edirlər. PoS protokolu Peercoin və NXT-də istifadə edilir. Validatorlar bloku bağlamaq hüququnu əldə etmək məqsədilə püşkatmada iştirak üçün malik olduqları sikkələrin bir hissəsini mərcə (depozitə) qoyurlar. Bloku bağlayacaq validator qovşaqları onların malik olduğu sikkələrin sayından və bu sikkələrə malik olması müddətindən asılı olan ehtimalla təsadüfi seçilir [14]. Bundan başqa, mayninqin çətinliyi də sikkələrin sayına tərs mütənasib olur. Əgər blok əlavə olunursa, validatorlar mərc paylarına mütənasib mükafat alırlar və bundan sonra onların balansları (sikkələrin sayı) yenidən müəyyən edilir. Bundan başqa, blokçeynin saxta tranzaksiyalar olan versiyasına pul qoyan iştirakçılar qoyduqları pulu itirirlər.

Lakin PoS sxemində "Nothing at Stake" problemi vardır – validatorlar bir neçə rəqib bloka səs verməklə təhlükəsizliyi poza bilərlər. Bunun sayəsində, sistemdə forkların tez-tez olması ehtimalı yüksəlir, bu kriptovalyutanı dəyərsizləşdirir və sistemi nüfuzdan salır.

Delegated Proof-of-Stake (DPoS) protokolu 2014-cü ildə Graphene layihəsi çərçivəsində işlənib və ilk dəfə BitShares, sonra isə Steem və EOS blokçeyn-layihələrində işə salınıb. DPoS-un işinin əsas prinsipi iştirakçıların səs verənlərə və validasiya edənlərə bölünməsidir. Sistemdə səsvermə hüququna malik olan iştirakçılar (kriptovalyuta sahibləri) tranzaksiya validatorları ola bilməzlər. Validatorlar öz kimliklərini açıqlayırlar və tam şəbəkə qovşağının işini fasiləsiz dəstəkləyəcəklərini, tranzaksiyaların verifikasiyasını vaxtında yerinə yetirəcəklərini və yeni blokları formalaşdıracaqlarını bəyan edirlər.

DPoS protokolunda hər bir istifadəçi validator qovşağı olmağa öz namizədliyini irəli sürə bilər, Sonra bütün istifadəçilər arasında namizədlərə səsvermə keçirilir, hər bir səsin çəkisi səs verənin aktivlərinin miqdarı ilə müəyyən edilir. Səsvermə nəticəsində N namizəd seçilir (N-i icma müəyyən edir, adətən, 20-50 namizəd) və onlar yeni blok formalaşdırmaq hüququ qazanırlar. Əgər səsvermədə iştirak edən aktivlərin böyük hissəsinə düzgün istifadəçilər nəzarət edirsə, protokolun qaydaları düzgün qərar qəbul edilməsini təmin edir.

Seçilmiş validatorlar psevdotəsadüfi şəkildə qarışdırılır və növbə yaradılır. Qarışdırma xüsusi alqoritmlə yerinə yetirilir və növbəni əvvəlcədən söyləmək mümkün deyil. Sonra zaman periodu ayrılır ki, bu müddətdə validatorlardan hər biri növbəyə uyğun olaraq bir blok formalaşdıra bilər. Bu zaman periodunda hər bir validatora dəqiq zaman intervalı ayrılır (adətən 1 san). Bu interval ərzində ya validator yeni tranzaksiyaları yoxlamağa və yeni blok formalaşdırmağa müvəffəq olur, ya da bu işi növbədəkı, sonrakı validatora buraxmalı olur. Zaman periodu qurtardıqdan sonra validatorlar yenidən qarışdırılır və yeni növbə yaranır.

Qeyd etmək vacibdir ki, DPoS-da səs verənlər yeni səsverməni istənilən zaman keçirə bilərlər. Deməli, validatorların cari qrupu dəyişə və növbələr yeni tərkibdə formalaşa bilər. Bundan başqa, bir səs verən birdən çox namizədə səs verə bilər, yəni öz aktivlərinin çəkisini bir neçə namizəd arasında bölə bilər.

PoW və PoS-dan fərqli olaraq, DPoS-da maynerlər blok yaratmaq üçün rəqabət yox, əməkdaşlıq edə bilərlər. Blokların yaradılmasını qismən mərkəzləşdirməklə DPoS digər alqoritmlərin əksəriyyətindən dəfələrlə sürətlə işləyir. DPoS protokolundan istifadə edən EOS blokun blokçeynə yazılmasına 2 saniyədən az vaxt sərf edilən ilk blokçeyn olmuşdur. Bu, Bitkoin-dəki 10 dəqiqədən dəfələrlə sürətlidir. Cədvəl 1-də PoW, PoS və DPoS konsensus protokollarının bir neçə parametr üzrə müqayisəsi verilir.

Cədvəl 1.

PoW, PoS və DPoS konsensus protokollarının müqayisəsi

	PoW	**PoS**	**DPoS**
Layihəyə misal	Bitkoin, Ethereum	Peercoin	NEO
Blokun yaradılması müddəti	Bitkoin: ~7-10 dəq Ethereum: ~12-15 san	~9 dəq	15 san
Məhsuldarlıq (1 saniyədə tranzaksiyaların sayı)	Bitkoin: 7-10 Ethereum: 15-30	7	1000
Tranzaksiya xərci	Bitkoin: $0.168 Ethereum: $0.066	~0,006	Seçməklə
Blokda tranzaksiyaların sayı	Bitkoin: 4424-ə qədər Ethereum: 30-200	2-10	500-ə qədər
Elektrik enerjisi xərcləri	Bitkoin: 69 974 983 Ethereum: 51 765 837	18630	50,4
Tam qovşaqların sayı	Bitkoin: 10102 Ethereum: 12754	12	7 konsensus qovşağı
Əsas xarakteristikası	Demərkəzləşmə, təhlükəsizlik	Miqyaslanma, az enerji sərfi	Miqyaslanma, kiçik tranzaksiya haqqı

PoW və PoS konsensus protokollarından başqa PoA (Proof-of-Audit), PoB (Proof-of-Burn), PoC (Proof-of-Capacity), RoE (Proof of Existence), PoI (Proof of Importance), PoP (Proof of Process), PoR (Proof of Resource) və s. kimi konsensus mexanizmləri təklif edilmişdir. Proof-of-X mexanizmlərinin ətraflı təsviri və qiymətləndirilməsi [14]-də verilir.

Bir neçə blokçeyndə *BFT* (**Byzantine Fault Tolerance – Bizans imtinalarına qarşı dayanıqlılıq**) konsensus alqoritmlərinin müxtəlif versiyaları istifadə edilir. BFT – kifayət qədər mürəkkəb konsepsiyadır, paylanmış sistemlərin "Bizans generalları problemi"nə dayanıqlılığını göstərən xarakteristikasıdır – bədniyyətli və sıradan çıxmış elementlər olduqda sistemin etibarlı qalması imkanını göstərir. BFT-əsaslı konsensus protokollarının əksəriyyətində yeni bloku təqdim edəcək validator dairəvi yanaşma ilə seçilir. Kvorumun digər iştirakçı-qovşaqları blokun və ondakı tranzaksiyaların həqiqiliyinə səs verirlər. Əksər hallarda səslərin 2/3-i qazanıldıqdan sonra blokçeynə daxil edilir [14].

BFT-nin üstünlüklərinə aid miqyaslanma və ucuz tranzaksiyaları, nöqsanlarına aid isə müəyyən qədər mərkəzləşməni misal göstərmək olar. *BFT* alqoritmlərinin müxtəlif variantları *Hyperledger, Ripple, Stellar* və *Tendermint* blokçeynlərində konsensus alqoritmlərinin əsasında dayanır.

PBFT (Practical BFT) alqoritmi *Hyperledger Fabric*-də istifadə edilir, burada əvvəlcədən seçilmiş bir neçə (20-dən çox olmayaraq) *PBFT* validatoru olur. *PBFT* konsensus qovşaqlarının ən çoxu 1/3-i bədniyyətli olmasına dayanıqlıdır. *PBFT*-in bir məhdudiyyəti vardır – sistem gecikmələrlə olsa də, bütün tranzaksiyalar çatdırıldıqda işləyir.

Hyperledger Fabric-də tranzaksiyaların təsdiqlənməsini həyata keçirən konsensus şəbəkəsi bir neçə yoxlama qovşağından ibarət altşəbəkədir, tranzaksiyalar yerinə yetirilərkən konsensusun saxlanması və şəbəkə iştirakçıları arasında verilənlərin düzgün sinxronlaşdırılmasının təmin edilməsi üçün cavabdehdir. Hyperledger-də tranzaksiya yoxlama qovşaqlarının ən azı 60 %-i onu bəyəndikdə təsdiqlənmiş sayılır.

Federated Byzantine Agreement (FBA) protokolu *Stellar* və *Ripple*-də istifadə edilən *BFT* variantlarından biridir. Ümumi ideya ondan ibarətdir ki, öz məxsusi zəncirinə cavabdeh olan hər bir general (validator) həqiqiliyi müəyyən etmək üçün məlumatları sıralayır. *Ripple*-də validatorlar əvvəlcədən seçilir. Stellar-da istənilən qovşaq validator ola bilər, hansı validatora etibar etməyi istifadəçi özü seçir.

DBFT (Delegated Byzantine Fault Tolerance) protokolu *NEO* açıq kodlu blokçeyn layihəsində reallaşdırılıb. DBFT konsensus protokolu proksi səsverməsinə əsaslanır. *NEO* holderlərinin çoxu sadə qovşaqlardır, onlar sikkələri ötürə/mübadilə edə bilərlər, blokların yoxlanmasında isə iştirak etmirlər. Holderlər blokçeynə xidmət edən nümayəndələri – xüsusi uçot qovşaqlarını seçirlər. Bu qovşaqlar blokçeynə yazılan hər bir bloku yoxlayır. Uçot qovşaqları isə öz aralarından təsadüfi qaydada bir spiker seçirlər. Spiker blokçeynə yazılacaq növbəti bloku hər bir uçot qovşağına təqdim edir. Əgər nümayəndələrin 66 %-i razılaşırsa, blok təsdiqlənmiş sayılır. Uçot qovşağı olmaq üçün müəyyən tələblər gözlənilməlidir: xüsusi avadanlıq, ayrılmış İnternet-bağlantı və *NEO* platformasında buraxılmış müəyyən sayda kriptovalyuta tokeni (GAS) olmalıdır.

2014-cü ildə Cey Kvon *PoS*-blokçeyni kontekstində *BFT* yanaşmasını tətbiq edərək Tendermint konsensus alqoritmini kəşf etdi [8]. C.Kvonun əsas yeniliyi blokların, heşlər arasında əlaqənin, dinamik validatorlar çoxluğunun və liderin rotasiya ilə seçilməsi qaydasının köməyi ilə *BFT* tədqiqatlarını blokçeynə adaptasiya edə bilməsidir. *Tendermint*-dən sonra özündə *BFT* elementlərini və digər blokçeynlərin müxtəlif cəhətlərini birləşdirən çox sayda konsensus alqoritmi meydana çıxdı (*Honeybadger, Ouroboros, Tezos, Casper* və s.) [14].

Yeni perspektivli konsensus alqoritmlərindən istiqamətlənmiş atsiklik qrafları (*ing. Directed Acyclic Graph, DAG*) və onların *Hashgraph, Tangle* və *Block*-lattice kimi reallaşdırmalarını misal göstərmək olar [14].

Blokçeyn platformaları

Blokçeyn-şəbəkənin arxitekturasını işləyərkən, xüsusilə də korporativ tətbiqlər üçün, blokçeyn platformasının seçilməsi həlledicidir. Hazırda Bitkoin, *Ethereum* (*Quorum* və budaqlanmaları), *HyperLedger Fabric*, *R3 Corda* ilə yanaşı, digər həllər də (məsələn, IOTA) əlyetərdir.

Ethereum – əsas protokolu 2013-cü ildə rus əsilli kanadalı proqramçı Vitalik Buterin tərəfindən işlənmişdi, şəbəkə isə 2015-ci ildə işə salınmışdı [15]. Ethereum-un əsas ideyası blokçeynin funksional imkanlarının genişləndirilməsi idi, Bitkoin-də bu imkanların kiçik bir hissəsi reallaşdırılıb.

Etherum-un yaradılmasının əsas hərəkətverici ideyası tranzaksiyanın – kriptovalyuta protokolunun əsas vahidinin smart-kontrakt ilə əvəz edilməsidir. Smart kontraktların istifadəsi ideyasını 1994-cü ildə Nick Szabo təklif etmişdi [1, 2]. Ethereum smart-kontraktları praktikada geniş istifadə edən ilk platformadır.

Smart-kontrakt vasitəçi olmadan, avtomatik yerinə yetirilən kontraktlardır. Kontrakt şərtlərinin və ödənişin yerinə yetirilməsinə xüsusi proqram nəzarət edir. İstifadəçilər smart-kontrakt daxilində təkcə pul vahidinin bir hesabdan digərinə keçirilməsini deyil, aksiya, daşınmaz əmlak və ya digər aktivləri mübadilə edə bilərlər. Blokçeyn texnologiyasının hesabına smart-kontraktlar paylanmış reyestrdə saxlanılır və tərəflərdən heç birinin onu dəyişmək imkanı yoxdur. Kriptovalyuta isə maliyyə aləti kimi istifadə edilir.

Ethereum-da istənilən demərkəzləşmiş tətbiqin (*Decentralized application, Dapp*) proqram kodunu yerinə yetirmək mümkündür. Ethereum həmçinin demərkəzləşmiş avtonom təşkilatların – *DAO* (*Decentralized Autonomous Organization*) və *DAC* (Decentralized Autonomous Corporations) yaradılması üçün də istifadə edilə bilər [16]. DAO – Ethereum blokçeynində 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 deyil, səs hüququ üçün ödənişdir.

HyperLedger-Fabric – blokçeyn əsaslı xidmətlərin qurulması üçün ən yetkin universal platformadır [17], *Linux Foundation* tərəfindən idarə olunur (*Fabric* ilə yanaşı *HyperLedger*-də blokçeyn texnologiyası ilə əlaqəli *Sawtooth*, *Indy*, *Iroha* və *Burrow* kimi layihələr də yer alır). Bu platforma mövcud proqram komponentlərindən və *PKI* şəbəkəsindən istifadə etməyə imkan verir. Lakin universallığın nəticəsi olaraq, ixtisaslaşmış blokçeyn platformalarından, məsələn, maliyyə sektorunda tətbiq edilən *Corda*-dan daha mürəkkəbdir.

Hyperledger-Fabric tranzaksiyaları təsdiqləmək üçün *PBFT* protokolundan və variantlarından (*SIEVE*) istifadə edir. Bunun sayəsində *Hyperledger-Fabric* çox kiçik enerji və hesablama resursları tələb edir və icazəli reyestrlər üçün olduqca əlverişli texnologiyadır. Lakin icazəli reyestrlərin bir sıra məhdudiyyətləri mövcuddur. Qismən demərkəzləşmiş olduğuna görə, etimad müəyyən mayner/validator qovşaqlarında yerləşdirilib. Uğurlu zərərli kod hücumunda bu qovşaqların yoluxması tranzaksiyaların təsdiqlənməsinə böyük miqyasda təsir edə bilər.

Həmçinin, *BFT* əsaslı konsensus protokollarının kommunikasiya mürəkkəbliyi yüksəkdir və əlverişsiz şəbəkə şəraitində çox pis işləyirlər. Həmin protokollar həm də pis miqyaslanırlar, yəni validator qovşaqlarının sayı artdıqda tranzaksiyaların emal məhsuldarlığı əhəmiyyətli dərəcədə azalır. Məsələn, *HyperLedger-Fabric*-də təsdiqləyən qovşaqların sayı 1-dən 14-ə artırılsa, məhsuldarlıq 1500 *TPS*-dan çox azalır [18]. Lakin *BFT* əsaslı protokollar icazəsiz blokçeynlərlə müqayisədə kiçik gecikmə və xeyli yüksək məhsuldarlıq göstərirlər.

R3 Corda – Məhdud girişli paylanmış reyestr platformasıdır, *JVM* (*Java Virtual Machine*) əsasında smart-kontraktları yerinə yetirir. *Corda* dünyanın 70-dən çox aparıcı bankı və maliyyə təşkilatının daxil olduğu *R3* konsorsiumu tərəfindən yaradılmışdır. *Ethereum* və *Lisk* kimi digər smart-kontrakt platformalarından fərqli olaraq, Corda yalnız xüsusi maliyyə tətbiqləri üçün nəzərdə tutulub.

Corda-nın əsas xüsusiyyəti ənənəvi mənada vahid blokçeyn istifadə etməməsidir. Bunun əvəzində, tranzaksiyaların yoxlanması və imzalanması (yəni konsensusa nail olunması) üçün xüsusi "notarial" qovşaqlar istifadə edilir. Eyni bir şəbəkə daxilində müxtəlif konsensus alqoritmləri istifadə edilə bilər. Xüsusilə qeyd etmək lazımdır ki, *Corda*-da *PoW* istifadə edilmir və mayninq yoxdur. *Corda*-da edilən tranzaksiyalar bütün iştirakçılara ötürülmü, verilənlər bazasındakı tranzaksiyalar yalnız onlara baxmaq və idarə etmək icazəsi olan iştirakçılara verilir [19]. Bunun üçün *Corda*-da xüsusi identifikasiya servisləri istifadə edilir.

IOTA – xüsusi olaraq Əşyaların İnterneti üçün yaradılmış kriptovalyuta və platformadır [20]. *IOTA* bir şəbəkədə birləşdirilmiş smart maşınların iştirakı ilə smart müəssisələrin reallaşdırılmasını təmin edə biləcək tranzaksiya "yanacağı"dır.

IOTA Bitkoinə və *Etheriuma* oxşamır, çünki faktiki olaraq blokçeyndən istifadə etmir. Bu platforma istiqamətlənmiş atsiklik qrafın əsasında işləyən xüsusi *Tangle* verilənlər strukturundan istifadə edir. Tangle-da bloklar yoxdur, tranzaksiyalar isə xüsusi sxem üzrə əlaqələndirilir: meydana çıxan hər bir yeni tranzaksiya iki köhnə tranzaksiyanı təsdiqləyir. Ən böyük imkanı tranzaksiyaların emal sürətini praktiki olaraq qeyri-məhdud artırmaq potensialıdır.

Belə sistem verifikasiyaların tam bir "hörümçəyini" formalaşdırır, bu şəbəkəni iki dəfə xərcləmə təhlükəsindən qoruyur və daha yüksək effektivliklə işləməyə məcbur edir. Yəni şəbəkədə tranzaksiyalar nə qədər çoxdursa, onlar bir o qədər sürətlə emal olunacaqlar.

Qeyd edək ki, *IOTA*-da mayninq mümkün deyil, bütün sikkələr bir dəfə də buraxılıb və onların sayı təxminən 2,8 trilyondur.

Cədvəl 2-də bir sıra blokçeyn platformalarının müqayisəsi təqdim olunur.

Cədvəl 2.

Bəzi blokçeyn platformalarının əsas xarakteristikaları

	Bitkoin	**Ethereum**	**HyperLedger-Fabric**	**Corda**	**IOTA**
Idarəçilik	Yaradıcılar heyəti	Yaradıcılar heyəti (*DAO*)	*Linux Foundation*	*R3 Company*	*IOTA Foundation*
Əməliyyat rejimi	Açıq blokçeyn	Açıq blokçeyn	Ekskluziv özəl reyestr	Ekskluziv özəl reyestr	Açıq blokçeyn
Kriptovalyuta	Bitkoin (*BTC*)	*Ether (ETH)*	–	–	*MIOTA*
Konsensus protokolu	*PoW*	*PoW*	*PBFT*	Yalnız tranzaksiyaya cəlb olunmuş tərəflər iştirak edir	*Tangle*

Blokçeyn texnologiyalarında yeni istiqamətlərdən biri də blokçeyn bulud xidmətlərinin (*Blockchain as a Service, BaaS*) təşkil olunmasıdır. *BaaS*, əsasən, *SaaS (Software As A Service)* modelinə əsaslansa da, blokçeynin müxtəlif bulud modelləri ilə bir sıra variantlarda bir çox inteqrasiya senariləri mövcuddur (mayninq, proqram təminatının işlənməsi, müxtəlif blokçeyn xidmətləri və s.). Bir sıra böyük şirkətlər artıq öz *BaaS* həllərini təqdim etmişdir (*Microsoft, Oracle, Amazon, IBM*). *Microsoft* öz *Azure* bulud platformasında eksperimental *BaaS* sistemini 2015-ci ildə işə salmışdı. Hazırda *Azure BaaS* platforması müəssisələrdə blokçeyn texnologiyasının sürətli tətbiqi üçün *Ethereum, Quorum, HyperLedger-Fabric, Corda* və digər populyar paylanmış reyestrlər üçün hazır şablonlar təqdim edir.

Tətbiq sahəsi üçün blokçeynin uyğunluğu meyarları

Jason Bloomberg "Eight reasons to be skeptical about blockchain" adlı məqaləsində blokçeyni müxtəlif sahələrdə tətbiq üçün olduqca mürəkkəb hesab edir [21]. O qeyd edir ki, blokçeyn vəziyyəti sadələşdirmək deyil, əksinə, mürəkkəbləşdirə bilər.

Blokçeynin ən çox rast gəlinən tənqidlərindən biri odur ki, blokçeyn əsaslı tətbiqlərin bir çoxunu mərkəzləşdirilmiş verilənlər bazaları kimi mövcud texnologiyalardan istifadə etməklə reallaşdırmaq olar. Sistemə irəli sürülən tələblər hazırkı relyasiya verilənlər bazaları ilə qarşılanırsa, blokçeyndən istifadə etmək mənasızdır. *Oracle* və *MySQL* kimi sistemlər onilliklər boyu inkişaf etmişdir. Bu texnologiyalar trilyonlarca sorğu yerinə yetirən minlərlə serverdə işləyir. Onlar ən əhatəli, test edilmiş, səhvləri düzəldilmiş və kodları optimallaşdırılmış olduğundan, saniyədə minlərlə əməliyyat yerinə yetirməyə qadirdirlər.

Ekspertlər blokçeyn texnologiyasının tətbiq edilib-edilməməsi barədə düzgün qərar qəbul etmək üçün aşağıdakı əsas suallara cavab verilməsinin zəruri olduğunu irəli sürürlər [3, 22].

- Paylaşılan verilənlər bazasının olması zəruridirmi?
- Verilənləri bir neçə tərəfin daxil etməsi zəruridirmi?
- Verilənləri daxil edən potensial tərəflər etibarsızdırmı? (Onların digərlərinin əvvəlki məlumatlarını dəyişdirməsinin qarşısı alınmalıdırmı)?
- Vasitəçilərdən imtina etməyə ehtiyac varmı (tranzaksiyaları təsdiqləyən və ya həqiqiliyini yoxlayan etibarlı vasitəçilərdən imtina etmək zəruridirmi)?
- Tranzaksiyaların bir-biri ilə necə bağlı olduğunu görmək lazımdırmı (bir istifadəçi ilə bağlı tranzaksiyaları müxtəlif aktorlar müstəqil olaraq qeydə almalıdırmı)?

Bu suallardan bir və ya bir neçəsinə mənfi cavab verilsə, blokçeyn texnologiyasının tətbiqi real fayda gətirməyə və əlavə xərclərə səbəb ola bilər.

Blokçeynin tətbiqinə aid misallar

Blokçeyn dövlət sektorunda. Dövlətlər blokçeyn texnologiyasının tətbiqi üzrə ilk addımlarını atırlar [23, 24]. Məsələn, Estoniya dövlət sektorunda bütün verilənlərin qorunması üçün "*Keyless Signature Infrastructure* (*KSI*)" adlı texnologiyanı tətbiq edir [25]. Baza faylı hər dəfə dəyişdikdə zəncirə yeni yazı əlavə edilir və bu informasiya sonradan dəyişilə bilməz. Hər bir yazının tarixçəsi tam şəffafdır, sistemin daxilindən və xaricindən icazəsiz müdaxilə aşkarlana və qarşısı alına bilər. *KSI* müxtəlif verilənlər bazalarında edilən dəyişiklikləri izləməyə imkan verir, yazını kim dəyişir, hansı dəyişikliklər edilir və nə vaxt edilir.

İsveç hökuməti blokçeyn texnologiyasını daşınmaz əmlakın alqı-satqısı sahəsində tətbiq edir [26]. Ölkədəki daşınmaz əmlakın ümumi həcmi İsveçin ümumi daxili məhsulunun dəyərindən üç dəfə çoxdur. Lakin daşınmaz əmlakın qeydiyyatı və alqı-satqısı çətin prosedurlar tələb edir. Blokçeyn texnologiyasının tətbiqindən sonra alqı-satqının tamamlanması üçün tələb edilən müddətin 3-6 aydan bir neçə günə, bəzi hallarda isə bir neçə saata düşəcəyi gözlənilir. Mülkiyyət hüququnun izlənməsi üçün blokçeynin istifadəsinin əlavə üstünlüyü ondadır ki, insayderləri də yoxlamaq mümkündür, dövlət qulluqçularının informasiyanı icazəsiz manipulyasiya etmələri daha çətin olacaq.

Dubayda blokçeyn strategiyası çərçivəsində nəzərdə tutulur ki, blokçeyn texnologiyasını istifadə edən bütün hökumət strukturları 2020-ci ilə kimi *Smart Dubai* layihəsinə daxil olacaq [27]. Bütün sənədləşmə, məsələn, vizanın alınması, hesabların ödənilməsi, lisenziyaların müddətinin uzadılması rəqəmsal formada aparılacaq. Blokçeyn texnologiyası sənədlərin emalı proseslərini optimallaşdıracaq, kağız sənədlərin emalına sərf edilən 25,1 milyon iş saatına qənaət edəcək, avtomobillə sənəd dalınca gedişləri azaltmaqla karbon qazı ilə çirklənməni əhəmiyyətli dərəcədə aşağı salacaq.

Səsvermə prosesinin təşkili – blokçeynin dövlət sektorunda tətbiqi senarilərindən biridir [28, 29]. Məsələn, 2018-ci ilin yayında İsveçrənin *Zug* kantonunda bələdiyyə seçkiləri blokçeyndən istifadə edilməklə keçirilmişdi. Blokçeynə səsvermənin nəticələri və yerli sakinlərin məlumatları daxil edilirdi.

Dövlət xidmətləri sistemində blokçeyn təhlükəsizlik, sənədlərin razılaşdırılması və verilənlərin yoxlanması problemlərini həll etməyə, inzibati maneələri azaltmağa qadirdir [30-32].

Bundan başqa, öz xüsusiyyətlərinə görə, blokçeyn büdcə prosesinin şəffaflığını artırmağın və korrupsiya faktorlarını azaltmağın unikal alətlərindən biri kimi çıxış edə bilər.

Blokçeyn təhsildə. Blokçeyn texnologiyası Avropada və ondan kənarda bir çox universitetlər üçün maraq doğurur – bu barədə Avropa Komissiyasının 2017-ci ildəki "Blokçeyn təhsildə" hesabatında deyilir. Yeni texnologiya təhsil müəssisələrində verilənlərin idarə edilməsinə çəkilən xərcləri azaltmağa, təhsil prosesinə bütün mərhələlərdə nəzarət etməyə, uçot yazılarının təhsil müəssisələri tərəfindən yoxlanması zəruriliyini aradan qaldırmağa imkan verir.

Blokçeyn texnologiyasının təhsil sahəsində tətbiqinin hələ başlanğıc səviyyəsində olmasına baxmayaraq, getdikcə daha çox sayda təhsil müəssisəsi ona maraq göstərir. Massaçusets Texnologiya İnstitutu da onların arasındadır, burada blokçeyn üzrə pilot layihə çərçivəsində 100-dən çox məzuna rəqəmsal diplom təqdim olunub [33].

2017-ci ilin oktyabrında Melburn Universiteti təhsil və alimlik dərəcələrinə dair sənədlər haqqında informasiyanın qeydə alınması və saxlanması üçün blokçeyn əsasında mobil sistemi test etməyə başlamışdı. Bu sistem saxta diplomlarla mübarizəni təmin edəcək, işəgötürənlərin yoxlanmış məlumatlara sürətli çıxışını təmin edəcək.

Blokçeyn səhiyyədə. Blokçeyn texnologiyasının səhiyyə sahəsində tətbiq üçün də böyük potensialı var, pasiyentlərə, tibbi xidmət provayderlərinə və səhiyyə təşkilatlarına rəqəmsal verilənləri təhlükəsiz şəkildə mübadilə etməyə imkan verir [34-36]. Məsələn, Estoniya vətəndaşlarının elektron tibb kartları blokçeyn texnologiyasından istifadə etməklə idarə edilir [25]. Onun istifadəsinin üstünlüyü əhalinin fərdi məlumatlarının konfidensiallığının və məxfiliyinin yüksəldilməsi, pasiyentlər haqqında informasiyanın istənilən tibb müəssisəsi üçün sürətli və fasiləsiz əlyetər olmasıdır.

Lisenziyaları, vəsiqə və sertifikatları, diplomları, müqavilələri, arayışları, hesabat və çıxarışları, incəsənət məhsullarını, intellektual mülkiyyət obyektlərini autentifikasiya etmək üçün blokçeyn ən əlverişli texnologiyadır [33,37].

Geniş iştirakçı dairələri üçün blokçeyn əsasında etimad mühitinin yaradılması layihələri xüsusi maraq doğurur [38]. Məsələn, *British Petroleum* və *Shell* neft və neft məhsullarının ticarəti üçün blokçeyn platforması işə salmışdılarr [39]. *IBM* şirkəti 2018-ci ildə yeyinti sənayesi məhsullarının həyat tsiklinin izlənilməsi üçün *Food Trust* blokçeyn-platformasını qurmuşdu [40]. Onun test edilməsinə *Nestle, Dole Food, Golden State Foods, McCormick* və s. şirkətləri qoşulmuşdu.

IBM şirkəti *AIG* və *Chartered PLC* ilə birlikdə blokçeyn texnologiyalarının əsasında sığorta polisinin tətbiqi imkanını öyrənmişdir. Məqsəd şəffaflığı və etimad səviyyəsini artırmaqla sığorta sahəsində dələduzluq risklərini azaltmaqdır.

Blokçeyn texnologiyası: aktual elmi-tədqiqat problemləri

Blokçeyn texnologiyası son illərdə geniş tətbiq olunmağa başlamışdır və tədqiqatçıların qarşısına praktikanın ehtiyaclarından qaynaqlanan müxtəlif tədqiqat problemləri qoyulmuşdur [41]. Blokçeynin ən aktual problemləri arasından miqyaslanma məsələlərini [42] və təhlükəsizlik və gizliliyin təmin edilməsini [43] qeyd etmək olar.

Hazırda blokçeynin məlum olan ən fundamental təhlükəsizlik boşluğu təkrar xərcləmə (ing. double spending) və çoxluq hücumlarıdır ("51 % hücumu", Sivilla hücumu (ing. *Sybil attack*) və *DDoS* hücumu). Bu hücumların Bitkoin şəbəkəsində baş tutması ehtimalı hazırda olduqca kiçikdir. Digər blokçeyn layihələrində həmin hücumların qarşısını almaq üçün müxtəlif əlavə tədbirlər nəzərdə tutulur.

Geniş yayılmış blokçeyn texnologiyası kimi Bitkoinin əsas problemi tranzaksiyaların emal sürətinin olduqca aşağı olmasıdır (saniyədə 6-7 tranzaksiya); müqayisə üçün qeyd edək ki, bu göstərici VISA sistemində 2000-dir. Ümumiyyətlə, blokçeyn-şəbəkənin miqyaslanması məsələsi əlaqəli üç parametrin – təhlükəsizlik, demərkəzləşmə və miqyaslanmanın optimallaşdırılması arasında balanslaşdırmanı tələb edir. V.Buterinin "blokçeynin miqyaslanması trilemması"na görə,

blokçeyn bu parametrlərdən yalnız ikisi üzrə yaxşı nəticə göstərə bilər. Tranzaksiyaların emal sürətini yüksəltmək üçün blokçeyn ya təhlükəsizliyi, ya da demərkəzləşməni qurban verməlidir. Praktikada yüksək sürət nümayiş etdirən blokçeynlərdə, adətən, demərkəzləşmə güzəştə gedilir və hazırda mərkəzləşmə meylləri üstün gəlir.

Miqyaslanmanın daha bir cəhəti blokçeynin fasiləsiz böyüməsi və istifadəçilərin saxlamalı olduğu verilənlərin həcminin artması ilə bağlıdır. Təhlükəsizlik baxımından blokçeyndəki yazıların pozulmaması vacibdir, bu səbəbdən, məsələn, Bitkoin-də tam blokçeyn təxminən 200 Qbaytdır və hər gün 175 Mbayt artır.

Beləliklə, miqyaslanmanın təmin edilməsi üçün yanaşmaların işlənməsi aktiv tədqiqat istiqamətlərindəndir. Bu sahədə bəzi təşəbbüsləri xatırlatmaq olar: qlobal reyestrin qovşaqların bir qrupu tərəfindən idarə edilən daha kiçik altreyestrlərə bölünməsi, saxlanmanı optimallaşdırmaq üçün köhnə tranzaksiyaların silinməsi, blokçeynlər iyerarxiyasından istifadə edilməsi (məsələn, *Lighting Network* texnologiyası), blokçeynin seqmentlərə bölünməsi (ing. *sharding*), blokun ölçüsünün artırılması (məsələn,*SegWit*) və s.

PoW konsensus protokolunun icrası böyük xərclər tələb edir. Bitkoin şəbəkəsi mayninqə bütöv bir dövlətin istehlak etdiyi qədər elektrik enerjisi sərf edir. Xərcləri minimallaşdırmaq üçün çox sayda alternativ konsensus protokolları təklif edilmişdir, lakin əksər kriptovalyutalarda PoW protokolunun hansısa forması istifadə edilir. Konsensus protokollarının hər birinin müxtəlif situasiyalarda təmin etdiyi üstünlükləri qiymətləndirmək, onların əsaslandırılmış müqayisəsini aparmaq lazımdır.

Məlum olduğu kimi, kriptoqrafiyada ən çətin məsələ açarların idarə olunması problemidir və bu kriptovalyutalarda da öz qüvvəsində qalır. Bitkoin-in mövcudluğu illərində xeyli hallar olmuşdur ki, istifadəçilər bütün bitkoinlərini itirmişlər: sərt diski atmışdılar, parolu unutmuşdular və ya pulqabını qorumaq üçün zəruri tədbirlər görməmişdilər. Buna görə açarların itirilməsinin və ya oğurlanmasının qarşısını almağa imkan verən daha etibarlı həllər tələb edilir. Bitkoin-də istifadə edilən multi-imza metodu və ya sirrin bölgüsü metodları belə həllər ola bilər. Lakin bu həllərin təhdid modelinə uyğunluq dərəcəsi qiymətləndirilməlidir.

Anonimliyin idarə edilməsi də ciddi problemlərdən biridir. Hazırda kriptovalyuta verilənlərinin anonimliyinin təmin olunmasına yönəlmiş çoxsaylı tədqiqatlar vardır, lakin gizliliyin təmin olunmasına aid işlər azdır. *Monero* və *Zcash* kimi platformalar nəzəri olaraq daha etibarlı anonimlik zəmanəti verirlər, lakin onların praktiki analizi hələlik aparılmayıb – istisna deyil ki, onlarda özünəməxsus zəif yerlər vardır [43].

Paylanmış reyestrlər verilənlərin tamlığını təmin edirlər, lakin onların həqiqiliyinə zəmanət vermirlər. Onlarda konfidensiallıq ilə fəaliyyətin izlənilə bilməsi arasında balans yoxdur. Nəticədə blokçeyn-şəbəkənin iştirakçılarının anonimliyi müxtəlif növ qeyri-qanuni fəaliyyətlərlə ənənəvi mübarizə sistemlərini dağıdır. Buna görə hətta ən liberal yurisdiksiyalar da blokçeyndə maksimal sərt *KYC* (*Know Your Customer* – öz müştərini tanı) prosedurundan keçməyi nəzərdə tutan tənzimləyici tədbirlər həyata keçirməyə başlayıblar.

Təklif edilmiş blokçeyn həllərinin müxtəlif kriteriyalara görə qiymətləndirilməsi – gizlilik, təhlükəsizlik, enerji sərfi, məhsuldarlıq, təsdiqləmədə gecikmə, istifadənin asanlığı meyarları arasında optimal balansın axtarılması probleminin həlli aktualdır.

Nəticə

Blokçeyn kriptoqrafiya, şəbəkə, paylanmış konsensus protokolları kimi bir neçə konsepsiyanı birləşdirir. O, paylanmış verilənlər bazalarında sinxronlaşdırma problemini paylanmış konsensus mexanizmi ilə həll etməyə cəhd edir. Blokçeyn texnologiyasının əsas xarakteristikaları şəffaflıq, anonimlik, dəyişməzlik, avtonomluq, paylanmış və açıq kodlu olmasıdır.

Blokçeyn texnologiyası rəqəmsal tranzaksiyaların bir-birinə etibar etməyən qovşaqlardan ibarət olan şəbəkədə paylanmış və təhlükəsiz qeydiyyatını həyata keçirməyə imkan verir. O,

Bitkoin və digər kriptovalyutaların əsasında dayanan texnologiyadır. Bəzi ekspertlər blokçeyni dünyanı dəyişəcək texnologiyalardan biri hesab edirlər. Blokçeynin bir çox sahədə, xüsusilə də mərkəzləşmənin qeyri-təbii və gizliliyin vacib olduğu sahələrdə informasiya menecmentini kökündən dəyişəcəyi gözlənilir.

Blokçeyn texnologiyalarının yuxarıda sadalanmış bu və digər problemlərinin həlli istiqamətində bütün dünyada elmi-praktiki tədqiqatlar genişlənir. Yeni konsensus protokollarının işlənməsi, blokçeynlər əsasında təklif edilmiş həllərin müxtəlif kriteriyalar üzrə test edilməsi və qiymətləndirilməsi, blokçeynlərin təhlükəsizliyi, blokçeynin miqyaslanması üçün müxtəlif yanaşmaların işlənməsi, blokçeyn verilənlərinin intellektual analizi əsas tədqiqat istiqamətləridir.

Ədəbiyyat

1. Narayanan A., Bonneau J., Felten E., Miller A., and Goldfeder S. Bitkoin and cryptocurrency technologies: A comprehensive introduction, Princeton University Press, 2016, 336 p.
2. Swan M. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc., 2015, 150 p.
3. Zheng Z., Xie S., Dai H. N., Chen X., & Wang H. Blockchain challenges and opportunities: a survey // International Journal of Web and Grid Services, 2018, vol. 14, no. 4, pp. 352-375.
4. Wüst K., and Gervais A. Do you need blockchain? / IEEE Crypto Valley Conference on Blockchain Technology, 2018, pp. 45-54.
5. Nakamoto S. Bitkoin: A peer-to-peer electronic cash system. 2009. https://bitkoin.org/bitkoin.pdf.
6. Makhdoom I., Abolhasan M., Abbas H., & Ni W. Blockchain's adoption in IoT: The challenges, and a way forward // Journal of Network and Computer Applications, 2019, vol. 125, pp. 251-279.
7. The-Linux-Foundation, 2018. Hyperledger Business Blockchain Technologies. https://www.hyperledger.org/projects
8. Kwon J. Tendermint: Consensus without mining. Draft v. 0.6, fall. 2014? 11 p.
9. Buterin V. On public and private blockchains. 2015. https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/
10. Walport M. Distributed ledger technology: beyond blockchain. UK Government Office for Science, 2016, 88 p.
11. Yli-Huumo J., Ko D., Choi S., Park S., & Smolander K. Where is current research on blockchain technology? – A systematic review // PloS one, 2016, vol. 11(10), e0163477.
12. Zheng Z., Xie S., Dai H., Chen X., & Wang H. An overview of blockchain technology: Architecture, consensus, and future trends / IEEE International Congress on Big Data, 2017, pp. 557-564.
13. Nguyen G.-T., and Kim K. A survey about consensus algorithms used in blockchain // Journal of Information Processing Systems, 2018, vol. 14, no. 1, pp. 101-128.
14. Tschorsch F., Scheuermann B. Bitkoin and beyond: a technical survey on decentralized digital currencies // IEEE Communications Surveys & Tutorials, 2015, vol. 18, no. 3, pp. 2084–2123.
15. Buterin V. Ethereum white paper: a next generation smart contract & decentralized application platform. 2013.
16. Wang S., Yuan Y., Wang X., Li J., Qin R., & Wang F.Y. An overview of smart contract: architecture, applications, and future trends / IEEE Intelligent Vehicles Symposium, 2018, pp. 108-113.
17. Androulaki E., Barger A., Bortnikov V., Cachin C., et al. Hyperledger fabric: a distributed operating system for permissioned blockchains / Proceedings of the Thirteenth EuroSys Conference, 2018, pp. 30.
18. Scherer M. Performance and scalability of blockchain networks and smart contracts. Master's thesis. Umea University, Sweden. 2017.

19. Brown R.G., Carlyle J., Grigg I., & Hearn M. Corda: an introduction. R3 CEV. 2016, 15 p.
20. IOTA developer documentation. https://docs.iota.org/
21. Bloomberg J. Eight reasons to be skeptical about blockchain, May 31, 2017. https://www.forbes.com/sites/jasonbloomberg/2017/05/31/eight-reasons-to-be-skeptical-about-blockchain/#4a89d3be5eb1
22. Gatteschi V., Lamberti F., Demartini C., Pranteda C., and Santamaria V. To blockchain or not to blockchain: That is the question // IEEE IT Professional, 2018, vol. 20, no. 2, pp. 62-74.
23. de Meijer C. R. The UK and blockchain technology: A balanced approach // Journal of Payments Strategy & Systems, 2016, vol. 9, no. 4, pp. 220-229.
24. Kshetri N, Voas J. Blockchain in developing countries // IEEE IT Professional, 2018, vol. 20, no. 2, pp. 11-14.
25. Sullivan C., & Burger E. E-residency and blockchain // Computer Law & Security Review, 2017, vol. 33, no. 4, pp. 470-481.
26. Veuger J. Trust in a viable real estate economy with disruption and blockchain // Facilities, 2018, vol. 36, no. 1/2, pp. 103-120.
27. Nordrum A. Govern by blockchain Dubai wants one platform to rule them all, while Illinois will try anything. IEEE Spectrum, 2017, vol. 54, no. 10, pp. 54-55.
28. Khan K. M., Arshad J., & Khan M. M. Secure digital voting system based on blockchain technology // International Journal of Electronic Government Research (IJEGR), 2018, vol. 14, no. 1, pp. 53-62.
29. Kshetri N., & Voas J. Blockchain-enabled e-voting // IEEE Software, 2018, vol. 35, no. 4, pp. 95-99.
30. Alketbi A., Nasir Q., & Talib M. A. Blockchain for government services – Use cases, security benefits and challenges / Proc. of the 15th IEEE Learning and Technology Conference, 2018, pp. 112-119.
31. Wolfond G. A Blockchain ecosystem for digital identity: Improving service delivery in Canada's public and private sectors // Technology Innovation Management Review, 2017, vol. 7, no. 10, pp. 35-40.
32. Ølnes S., Ubacht J., & Janssen M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing // Government Information Quarterly, 2017, vol. 34, no. 3, pp. 355-364.
33. Arenas R., & Fernandez P. CredenceLedger: A permissioned blockchain for verifiable academic credentials / IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), 2018, pp. 1-6.
34. Mettler M. Blockchain technology in healthcare: The revolution starts here / Proc. of the 18th IEEE International Conference on e-Health Networking, Applications and Services (Healthcom), 2016, pp. 1-3.
35. Hölbl M., Kompara M., Kamišalić A., & Nemec Zlatolas L. A systematic review of the use of blockchain in healthcare // Symmetry, 2018, vol. 10, 470, 22 p. doi:10.3390/sym10100470
36. Radanović I., & Likić R. Opportunities for use of blockchain technology in medicine // Applied Health Economics and Health Policy, 2018, vol. 16, no. 5, pp. 583-590.
37. Graglia J. M., & Mellon C. Blockchain and property in 2018: At the end of the beginning // Innovations: Technology, Governance, Globalization, 2018, vol. 12, no. 1-2, pp. 90-116.
38. Yermack D. Corporate governance and blockchains // Review of Finance, 2017, vol. 21, no. 1, pp. 7-31.
39. Andoni M., Robu V., Flynn D., Abram S., Geach D., Jenkins D., McCallum P., & Peacock A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities // Renewable and Sustainable Energy Reviews, 2019, vol. 100, pp. 143-174.
40. Galvez J. F., Mejuto J. C., Simal-Gandara J. Future challenges on the use of blockchain for food traceability analysis // TrAC Trends in Analytical Chemistry, 2018, vol. 107, pp. 222-232.

41. Risius M., & Spohrer K. A blockchain research framework // Business & Information Systems Engineering, 2017, vol. 59, no. 6, pp. 385-409.
42. Lin I. C., & Liao T. C. A survey of blockchain security issues and challenges // IJ Network Security, 2017, vol. 19, no. 5, pp. 653-659.
43. Meiklejohn S., Top ten obstacles along Distributed Ledgers' path to adoption // IEEE Security & Privacy, 2018, vol. 16, no. 4, pp. 13-19.

УДК 004.056:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@iit.science.az

Технологии блокчейн: компоненты, применение и проблемы

Потенциал технологии блокчейн, созданной для поддержки криптовалюты Bitkoin, намного больше и предлагает широкие возможности для других приложений. Технология блокчейн обеспечивает распределенную, безопасную и надежную обработку цифровых транзакций. В последние годы блокчейны стали широко применяться, но нет правильного понимания потенциала этой технологии среди исследователей, а также большинства лиц, принимающих решения в области технологий. В данной работе анализируются компоненты технологии блокчейн, обобщается опыт практического применения в различных областях и определяются важные проблемы для развития этой технологии, выделяются направления будущих исследований.

Ключевые слова: *биткоин, блокчейн, технология распределенного реестра, платформа блокчейна, протокол консенсуса, византийская отказоустойчивость, Ethereum, Hyperledger-Fabric, IOTA.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@iit.science.az

Blockchain technology: components, applications and problems

The potential of the blockchain technology created to support Bitcoin cryptocurrency is high and offers many opportunities for other applications. Blockchain technology provides distributed, secure and reliable processing of digital transactions. In recent years, blockchains have become widely used, but there is no correct understanding of the potential of this technology among researchers, as well as many decision makers in the field of technology. This paper analyzes the components of the blockchain technology, summarizes the experience of practical applications in various fields and identifies important problems for the development of this technology, and highlights the future research areas.

Keywords*: Bitcoin, blockchain, distributed registry technology, blockchain platform, consensus protocol, Byzantine fault-tolerance, Ethereum, Hyperledger-Fabric, IOTA.*