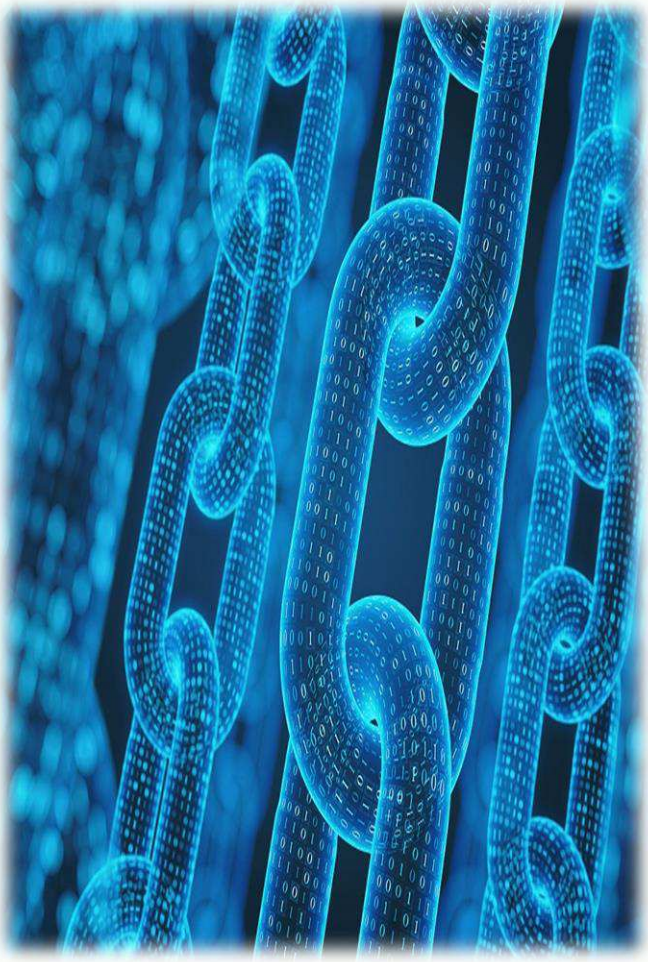


Maliyyə Monitorinqi Xidməti

METODİK VƏSAİT

Virtual aktivlər və Virtual aktivlər üzrə xidmət təminatçıları

Virtual aktivlərin istifadəsi və Virtual aktivlər üzrə xidmət təminatçılarının fəaliyyəti ilə əlaqəli meydana çıxan PL/TM risklərinə dair

DEKABR 2021

STRATEJİ TƏHLİLLƏR

MÜNDƏRİCAT

Giriş

Təqdim olunan metodik sənəddə virtual aktivlərin (o cümlədən onun əsas hissəsi olan virtual valyutaların və virtual birjaların) genezisinin və konsepsiyasının başa düşülməsi üçün qısa tarixi retrospektiv verilməklə yanaşı, virtual aktivlər üzrə əsas terminlərin şərhi, məlum nümunələr əsasında onların təsvir olunması, təsnifləşdirilməsi və sistemləşdirilməsinə cəhd olunmuşdur.

Müvafiq sahədə anlayışların aydın şəkildə ifadə olunması virtual aktivlər üzrə araşdırmanın sərhədlərini düzgün müəyyən etməyə, eləcə də anlaşmazlıqların və qarışıqlıqların qarşısını almağa yardım edir.

Son on il ərzində yeni texnologiyaların, məhsulların və onlarla əlaqədar xidmətlərin meydana gəlməsi dünya maliyyə sistemində əsas dəyişikliklərdən biri olmuşdur. Qeyd olunan yeni texnologiyalar, məhsullar və onlarla əlaqədar xidmətlər maliyyə yeniliklərini və səmərəliliyini stimullaşdırmaq, eləcə də maliyyə əlçatanlığını yaxşılaşdırmaqla yanaşı, cinayətkarlara və terrorçulara öz gəlirlərini leqallaşdırmaq və ya qeyri-qanuni fəaliyyətlərini maliyyələşdirmək üçün yeni imkanlar da yaradır.

Maliyyə sektorunun iştirakçıları yeni rəqəmsal texnologiyaların yaranması və sürətli inkişafına uyğun olaraq özlərinin biznes davranışlarını davamlı olaraq transformasiya etmək məcburiyyətində qalırlar. Texnoloji inkişaf sayəsində mobil cihazların geniş tətbiqi, məlumatların elektron formada saxlanması üzrə yaranmış yeni imkanlar, açıq məlumatlara çıxış imkanı verən yeni texnologiyalar və bu zərurətlə bağlı bank sektoru ilə digər sektorlar arasında məlumat mübadiləsinin təşkili üzrə qarşılıqlı biznes maraqlarının olması maliyyə sektorunda rəqəmsal texnologiyaların tətbiqinə müstəsna imkanlar yaradır. Öz növbəsində texnoloji tərəqqi təklif etdiyi məhsul və xidmələr baxımından çevik struktura malik kiçik şirkətlərin bazara daxil olmasına şərait yaratmaqla, ənənəvi maliyyə institutları qarşısında yeni bir çağırışa çevrilir. Bu səbəbdən, yeni rəqabət çağırışına cavab olaraq ənənəvi maliyyə institutları daha çevik və rəqabətqabiliyyətli rəqəmsal texnologiyalara əsaslanan biznes modellər, xidmətlər və strukturlar təklif edən strategiyalar əsasında fəaliyyət göstərmək məcburiyyətində qalırlar.

Rəqəmsal dəyişikliyə keçid nəticəsində bir sıra yeni anlayışlar və münasibətlər sistemi formalaşmışdır ki, bu da milli və beynəlxalq qanunvericilikdə və tənzimləmədə zəifliklərin və boşluqların yaranmasına, nəticə etibarilə onlardan sui-istifadəyə səbəb olmuşdur. Elektron pul, elekton pul kisəsi, kriptovalyuta, blokçeyn, virtual aktiv kimi anlayışlar son illər ərzində yaranan yeni anlayışların bir hissəsidir. Qeyd olunan və digər bu kimi yeni yaranmış məhsullardan sui-istifadə imkanlarını istisna etmək məqsədilə müvafiq anlayışlara hüquqi status və vahid (standart) tərif verilməsinə, bu sahədə formalaşmış münasibətlərin milli və beynəlxalq qanunverilicilik və standartlar üzrə tənzimlənməsinə, həmçinin belə xidmətlər təklif edən şəxslərə lisenziyaların verilməsi mexanizminə müvafiq tənzimləyici qurumlar tərəfindən vahid yanaşmaların formalaşdırılmasına və tətbiqinə böyük zərurət yaranmışdır.

Virtual aktivlərin bir sıra potensial faydaları mövcuddur. Virtual aktivlər və onlarla əlaqəli xidmətlər maliyyə yeniliklərini stimullaşdırır və maliyyə məhsullarına əlçatanlığı yüksəldir. Belə ki, onların vasitəsilə ödənişlər daha sadə və nisbətən ucuz (bəzi istisnaları çıxmaqla) olmaqla, adi maliyyə

məhsullarına çıxışı olmayan şəxslərə alternativ yollar təqdim edir. Virtual aktivlər biznes və maliyyə sferasının inkişafı üçün təklif etdiyi yeni imkanlar ilə yanaşı, özünün başlanğıc inkişaf mərhələsində bir sıra boşluqlara və zəifliklərə malik olması nəticə etibarilə PL, TM və digər cinayətləri törədən şəxslər üçün yeni imkanlar açması ilə xarakterizə olunur. Müvafiq texnoloji alətlərdən istifadə etməklə şəxslərin ölkələrarası köçürmələri daha sürətli edə bilməsi, belə köçürmələrdə vəsaiti göndərən və ya qəbul edən şəxsin müəyyən edilmə imkanlarının hazırkı şəraitdə olmaması (faktiki olaraq şəxsin anonim qalması), yaxud bunun üçün əlavə texniki vasitələrin istifadəsində, rəqəmsal aktiv formasında saxlanılması səbəbindən vəsaitlərin aşkar edilməsi və zərurət olduqda müsadirə olunması, eləcə də şübhəli əməliyyatların araşdırılmasında çətinliklər yaradır. Bu səbəbdən, müvafiq tənzimləmə olmadan onlar cinayətkarların və terrorçuların maliyyə əməliyyatları üçün virtual sığınacağa çevrilmə riskinə malikdir.

Sürətli transsərhəd əməliyyatlarının həyata keçirilməsi imkanı cinayətkarlara rəqəmsal aktivləri əldə etmək, yerləşdirmək və saxlamaq (çox vaxt da tənzimlənən maliyyə sistemindən kənarda) imkanı verməklə yanaşı, vəsaitləri göndərən və alan şəxsləri də gizlədir ki, bu da monitorinq subyektləri tərəfindən şübhəli fəaliyyətin vaxtında aşkar edilməsini çətinləşdirir. Qeyd edilən amillər səlahiyyətli orqanlar tərəfindən cənayət fəaliyyətinin aşkar edilməsi və istintaqın aparılması üçün əlavə maneələr yaradır.

Təqdim olunan sənəd həmçinin VA ilə əlaqəli fəaliyyət və ya əməliyyatlar həyata keçirmək istəyən özəl sektor subyektlərinə özlərinin PL/TMM öhdəliklərinin başa düşülməsinə və FATF tələblərinin effektiv şəkildə necə icra edilməsinə yardım üçün nəzərdə tutulmuşdur.

Metodik vəsaitdə rəqəmsal və virtual aktivlərin məzmunu və meydana gəlmə tarixi, virtual aktivlərin təminatçıları, sahə ilə əlaqəli olan blokçeyn və digər texnoloqiyalar, iştirakçılar, istifadəçilər barədə ilkin anlayışlar, müvafiq xidmətlər, xidmət göstərən iştirakçı və vasitəçilər, xidmətin istifadəçiləri ilə bağlı beynəlxalq qurum və müxtəlif ölkələrin yanaşmaları, virtual valyutanın ən məşhur nümunələri, virtual valyuta mübadiləsi, onların spesifik texnologiyası və işləmə mexanizmi, sahə üzrə çirkli pulların yuyulması və terrorçuluğun maliyyələşməsinin (PL/TM) potensial riskləri barədə məlumatlar verilir.

Təqdim olunan metodik vəsaitin məqsədi virtual aktiv anlayışının təbiətinin, əhatə dairəsinin, əsasında duran dəyərlərin ötürülməsi mexanizminin və belə aktivlər ilə əlaqəli PL/TM risklərinin və zəifliklərin başa düşülməsidir. Metodik sənədin son məqsədi virtual aktivlərin və onlar ilə əlaqəli risklərin idarə olunması və aşağı salınması üçün maliyyə sektoruna, nəzarət orqanlarına, hüquq mühafizə orqanlarına və digər maraqlı tərəflərə zəruri tədbirlərin müəyyən edilməsində məlumat mənbəyi olaraq yardım etməkdir. Qeyd edək ki, müvafiq sənəd virtual aktivlərin və onlarla əlaqəli fəaliyyətlərin hüquqi təhlili və sintezi məsələlərini əhatə etmir.

Bölmə

Bir

1

RƏQƏMSAL VƏ VİRTUAL AKTİV ANLAYIŞLARI

- rəqəmsal aktiv
- virtual aktiv
- kriptovalyuta
- e-pul
- fiat valyuta
- VAXT

Rəqəmsal aktiv anlayışı

Keçən əsrin 90-cı illərinin ortalarında *rəqəmsal aktiv* dedikdə, paylanan reyestrdə unikal identifikator formasında dövriyyədə olan, istifadəsi mümkün, "ikili say sistemi" üzərindən qurulan və dəyər üzərində mülkiyyət hüququndan irəli gələn istənilən informasiya resursu və ya qeyri-maddi aktiv başa düşülürdü. Həmin dövrdə rəqəmsal aktivlər video, şəkil, səs və sənəd kimi informasiya resursları ilə ifadə olunurdu. Lakin daha sonralar texnoloji inkişaf səviyyəsi yüksəldikcə, bu terminin əhatə dairəsinə daha geniş və daha mürəkkəb alətlər də daxil edilmişdir. Rəqəmsallaşmanın ilk nümunəsi kimi elektron sənəd dövriyyəsinə keçidi göstərmək olar.

Rəqəmsallaşma sisteminin əsasında "İkili say sistemi" durur. Kompüterlər istənilən bir məlumatı (hər hansı bir mətn, rəqəm, səs, qrafik və s.) yalnız iki simvoldan ibarət uzun bir kod şəklində saxlayaraq emal edirlər. Müvafiq prosesi rahatlaşdırmaq üçün bütün məlumatlar ikili (binar) hesablama sistemi formasına salınmışdır. Kompüterlərin yaddaşında olan binar kodların sonradan insanlara anlaşılan formada təqdim edilməsi isə dekodlaşdırma adlanır.

Müvafiq rəqəmsal texnologiyaların yaratdığı üstünlüklər sayəsində banklar və digər maliyyə institutları öz müştərilərinə ənənəvi xidmətləri distant formada təklif etməyə başladılar. Rəqəmsallaşmanın şirkətlərə verdiyi digər üstünlüklərdən biri də əməliyyat xərclərinin aşağı salınmasıdır. Bunun nəticəsində İT şirkətlərinin maliyyə bazarına ("techfin"), maliyyə şirkətlərinin isə İT sektoruna ("fintech") daxil olmasına imkanlar yaranmışdır.

Rəqəmsal aktiv bütün digər aktivlər (qeyri-rəqəmsal) kimi mütləq olaraq tələb və təklif ilə müəyyən olunan maliyyə dəyərinə malik olmalıdır.

Rəqəmsal mülkiyyət anlayışını informasiya texnologiyasından istifadə edərək elektron formada yaradılmış rəqəmsal obyektlər olan kompüter animasiyası, elektron musiqi, rəqəmsal rəsm daha yaxşı təsvir edir. Elektron formada mövcud olan bu obyektlər də əqli mülkiyyət sahəsinə aid edilir.

Rəqəmsal aktivləri iki hissəyə bölünür: maddi formada təcəssüm oluna bilən aktivlər (məsələn, elektron pullar) və iqtisadi dəyəri olan qeyri-maddi formaya malik aktivlər (məsələn, kriptovalyuta). Rəqəmsal aktivlərin sonuncu forması daha çox "virtual aktiv" və ya "virtual mülkiyyət" kimi adlandırılır.

Virtual aktiv və virtual aktivlər üzrə xidmət təminatçıları anlayışları

Bütün dünya üzrə dəyəri sürətlə ötürməyə imkan verən yeni texnologiyalar kimi blokçeyn, bitkoynlar, kriptoaktivlər, virtual aktivlər və s. tamamilə yeni terminlər olmaqla son zamanlar qlobal leksikonda daha fəal istifadə olunmaqdadır. Sürətlə inkişaf etməkdə olan blokçeyn və ya paylanan reyestr *("distributed ledger technologies")* texnologiyaları maliyyə mənzərəsini kökündən dəyişmək potensialına malik olduğunu göstərdi. Lakin bu texnologiyaların sürəti, qlobal əhatə dairəsi və hər şeydən əvvəl anonimlik imkanları səlahiyyətli dövlət orqanları tərəfindən həyata keçirilən nəzarətdən yayınmaq istəyən şəxsləri də özünə cəlb edir. Blokçeyn texnologiyasının uğurlu tətbiqi virtual aktivlərin geniş yayılması üçün əsaslar yaratmışdır. Bununla yanaşı, maliyyə sektorunu qeyd olunan yeni texnologiyaların doğurduğu yeni risklərdən qorumaq və sui-istifadə imkanlarını məhdudlaşdırmaq məqsədilə müvafiq sahədə adekvat nəzarət və tənzimləmə sisteminin qurulması məsələsi öz aktuallığını saxlayır.

2018-ci ildə FATF standartlarına edilmiş dəyişikliklər nəticəsində FATF-ın lüğətinə iki yeni anlayış (termin) daxil olunmuşdur: **virtual aktivlər (VA) və virtual aktivlər üzrə xidmət təminatçıları (VAXT).** FATF-a əsasən, ***virtual aktiv*** – rəqəmsal formada ticarəti aparıla (dövriyyədə olan) və ya köçürülə bilən (ötürülə bilən), ödəniş və ya investisiya məqsədləri üçün istifadə oluna bilən **dəyərlərin rəqəmsal ifadəsi formasıdır**. Virtual aktivlər özündə **fiat valyutaların, qiymətli kağızların və FATF-ın Tövsiyələri ilə əhatə olunmuş digər maliyyə aktivlərinin rəqəmsal ifadəsini ehtiva etmir.** Virtual aktiv mübadilə vasitəsi, hesablaşma vahidi və yığım vasitəsi kimi **üç funksiyanı** yerinə yetirə bilər, lakin hazırda əksər yurisdiksiyalarda qanuni ödəniş vasitəsi (legal tender) statusuna malik deyildir. Virtual aktivlər hər hansı səlahiyyətli qurumlar tərəfindən buraxılmır və onlara zəmanət verilmir, qeyd olunan funksiyalar yalnız virtual aktivlərin istifadəçilərinin birliyi daxilində olan razılaşma əsasında yerinə yetirilir.

Təbiəti etibarilə virtual aktivlərin ənənəvi aktivlər ilə oxşar və fərqli cəhətləri mövcuddur. Məsələn, ənənəvi aktivlər kimi virtual aktivlər də təminatlı və təminatsız ola bilər. Təminatlı virtual aktivlərin təminatı qismində maddi və qeyri-maddi aktivlər çıxış edə bilər. Virtual aktivlərin qeyd olunan və digər xüsusiyyətləri barədə ətraflı məlumat növbəti bölmələrin birində əhatə olunacaqdır. FATF terminologiyasında virtual aktivlər termini virtual valyuta termininin xələfi olaraq istifadə edilmişdir. Virtual aktivlər sahəsində elektron pullar, virtual valyutalar, kriptovalyutalar kimi məna cəhətdən bir-birinə yaxın çoxsaylı terminlərdən istifadə edilsə də, onların ifadə etdiyi mənalar bəzən qismən üst-üstə düşə, bəzən isə bir-birinə ziddiyyət təşkil edə, yaxud məzmun və predmetə görə bir-birindən fərqlənə bilərlər. Əslində, virtual valyuta və elektron valyuta terminlərinin tərifinin valyutanın tərifinə uyğun olub-olmaması və ya onların da əmtəə olaraq nəzərdən keçirilməsinin zəruri olub-olmaması məsələləri hələ də diskusiya mövzusudur.

Virtual aktivlər üzrə xidmət təminatçıları (VAXT) - FATF-ın hər hansı digər Tövsiyələri ilə əhatə olunmayan və digər fiziki və ya hüquqi şəxs üçün və ya onların adından aşağıdakı növ fəaliyyət və ya əməliyyatların birini və ya bir neçəsini sahibkarlıq fəaliyyəti qismində həyata keçirən istənilən fiziki və ya hüquqi şəxs kimi müəyyən olunur:

a. virtual aktivlər ilə fiat valyutalar arasında mübadilə;
b. virtual aktivlərin öz aralarında (bir və ya daha çox formaları arasında) mübadilə;
c. virtual aktivlərin köçürülməsi (müvafiq konteksdə köçürmə - virtual aktivləri bir ünvandan və ya virtual aktiv hesablarından digərinə keçirən digər fiziki və ya hüquqi şəxs adından əməliyyatların həyata keçirilməsi deməkdir);

d. virtual aktivlər üzərində nəzarəti həyata keçirməyə imkan verən virtual aktivlərin və ya alətlərin saxlanılması və (və ya) idarə olunması;
e. virtual aktivlərin emitentinin təklifi və (və ya) belə aktivlərin satışı ilə əlaqəli maliyyə xidmətlərinin təmin edilməsində iştirak.

Beləliklə, ümumi mənada VAXT-lar – müştərinin adından virtual valyutanın fiat valyuta ilə mübadiləsini aparan, öz aralarında virtual aktivləri mübadilə edən, onu üçüncü tərəfə (şəxslərə) ötürən, sahibləri adından belə aktivləri saxlayan, yaxud emitentin təklifi və ya virtual aktivlərin satışı ilə əlaqəli olan maliyyə xidmətlərinin göstərilməsində iştirak edən təşkilatlar və ya fərdi şəxslərdir.

VAXT-ların müvafiq tərifi FATF-ın 2019-cu ildə qəbul etdiyi "VA və VAXT-lar üzrə risk əsaslı yanaşma" adlı rəhbərliyində yer almışdır. Lakin 2021-ci ilin oktyabrında FATF-ın yenilənmiş rəhbərliyi VAXT-lara istifadə etdikləri texnologiyalardan asılı olmayaraq, yalnız VA-lar ilə əməliyyatlarda (ötürülmə, mübadilə) iştirak edib-etməmə meyarı üzrə kriptovalyuta xarakterli təşkilatların aid edilməsini təklif etmişdir (ətraflı məlumat 8-ci bölmədə verilmişdir).

Virtual aktivlər, fiat valyutalar, e-pullar və kriptovalyutaların fərqləndirici xüsusiyyətləri. Virtual aktivlər və onlarla əlaqəli anlayışların fərqləndirilməsi məqsədilə bu anlayışların beynəlxalq aləmdə qəbul olunmuş (lakin hazırda standartlaşdırılmamış) tərifl ərinin nəzərdən keçirilməsi zəruridir.

Rəqəmsal aktivlər – müstəqil, birmənalı identifikasiya edilə bilən, istifadəsi mümkün və dəyəri olan, "ikili say sistemi" üzərindən qurulan istənilən dəyərdir.

Rəqəmsal valyutalar – rəqəmsal aktivlərin tərkib hissəsi olmaqla virtual valyutanın (fiat olmayan valyutanın), eləcə də elektron pulların (fiat valyutanın) rəqəmsal ifadə vasitəsi kimi çıxış edir.

Elektron pullar (e-pullar) – fiat valyutanın rəqəmsal ifadə vasitəsi olmaqla, fiat valyutada ifadə olunan dəyərin elektron köçürülməsi üçün istifadə olunur. Elektron pullar fiat valyutanın rəqəmsal köçürülməsi mexanizmini özündə təmsil edir, yəni onlar valyutanın elektron köçürülməsi üçün istifadə olunur və qanuni ödəniş vasitəsi statusuna malik olur.

Fiat valyutaya ("real valyuta", "real pullar" və ya "milli valyuta") ölkənin qanuni ödəniş vasitəsi olan, emitent ölkədə dövriyyədə olan, bütün sahələrdə istifadə olunan və mübadilə vasitəsi kimi qəbul olunan kağız və dəmir pullar aid edilir. Fiat valyutanın fərqləndirici xüsusiyyətlərinə aşağıdakıları aid etmək olar:

- fiat valyuta onu emissiya edən hökumətin zəmanəti ilə dəstəklənir;
- özünün daxili dəyərinə malik olmasa da, səlahiyyətli orqan tərəfindən belə dəyərin təminatına dair cəmiyyətdə yaxşı inam mövcud olur;
- fiat valyuta ehtiyat valyuta funksiyasını daşıya bilər.

Kriptovalyuta – fiziki və hüquqi şəxslər tərəfindən mübadilə vasitəsi olaraq qəbul edilən və elektron şəkildə ötürülə, saxlanıla və satıla bilən rəqəmsal valyuta sinfidir. Kriptovalyuta – adətən, birbaşa olaraq onu hazırlayanlar tərəfindən, yaxud onun protokolları (məsələn, iş sübutlu mayninq – "proof-of-work mining") ilə müəyyən olunan alqoritmik qaydalar ilə buraxılan və zəmanət verilən dəyərin rəqəmsal təcəssümüdür. Bir sıra hallarda kriptovalyutalar mal və xidmətlərin ödənişi üçün istifadə oluna və nəticə etibarilə də pula alternativ kimi nəzərdən keçirilə bilər. Kriptovalyutalar adətən, əks mərkəzləşmiş olur, yəni onlar mərkəzi banklar, dövlət orqanları, kredit institutları və ya elektron pul təsisatları tərəfindən buraxılmır və ya zəmanət verilmir ki, nəticə etibarilə də buraxılan kriptovalyutaların sayı hazırda tənzimlənmir. Kriptovalyuta - *paylanan reyestr (blokçeyn) texnologiyasına (*kriptoqrafiya, eyniranqlı şəbəkə ("peer-to-peer"), konsensus mexanizmi) *əsaslanan* virtual aktiv növüdür.

Bölmə
İki

2

BLOKÇEYN TEXNOLOGİYASI

- verilənlər bazası
- bloklar, zəncirlər
- paylanan reyestr
- qovşaqlar
- əksmərkəzləşmə
- smart müqavilələr
- konsensus alqoritmi
- kriptoqrafiya
- uçot modelləri
- merkl ağacı

Blokçeynin mənşəyi və aktuallığı

20-ci əsrdə internetin meydana gəlməsi, beynəlxalq ticarətin inkişafı ilə bağlı transsərhəd köçürmələrinin həcminin artması, nağdsız ödəniş sisteminin inkişafı bank sisteminin maliyyə münasibətlərinin aparıcı həlqəsinə çevrilməsi üçün zəmin hazırlamışdır. Bu inkişaf rəqəmsal tarixin ilk dönüş nöqtələrindən biri hesab olunur.

İnternet şəbəkəsinin meydana gəlməsi ilə yanaşı, ilk rəqəmsal ödəniş valyutasının yaranması 1989-cu ilə təsadüf edir. 1993-cü ildə Devid Çaum adlı görkəmli riyaziyyatçı rəqəmsal ödəniş sistemi olan "eCash" adlı sistem təklif etdi. Bu sistem internet vasitəsilə mal və xidmətlər üçün təhlükəsiz və anonim şəkildə ödəniş etməyə imkan verən texniki cəhətdən təkmil bir məhsul olmaqla, şəbəkə üzrə xırda elektron sikkələri köçürmək üçün ideal idi. Bu səbəbdən, "Microsoft" və digər şirkətlər "eCash"i özlərinin proqram təminatlarına yerləşdirmək istəyirdilər. Həmin dövrdə "onlayn" alış-veriş edənləri məlumatların və əməliyyatların təhlükəsizliyi məsələləri narahat etmirdi.

Sistemin işləmə prinsipi elektron ödənişlərin icrası ilə yanaşı, köçürmələrdə anonimliyin və təhlükəsizliyin təmin edilməsi və valyutanın ilk qeyri-dövlət emissiyası ilə əlaqələndirilirdi. "Digicash" valyutasının ("Cyberbucks" kimi də tanınır) emissiyasına şirkətin özü cavabdehlik daşıyırdı. Başlanğıcda test məqsədi ilə emissiya edilən 1 milyon şərti vahid ilkin sərmayə yatırımı olaraq həyata keçirilmiş və həvəskar şəxslər arasında bölüşdürülmüşdür. Əməliyyatlar birbaşa bank sistemi ilə əlaqəli işləyirdi və əsasən internet üzərindən xırda ödənişlərin həyata keçirilməsində istifadə olunurdu. Bu sistemdə Devid Çaum məxfilik və kriptoqrafik elementlərdən istifadə etməklə bank vasitəsi ilə vəsaitlərin bir şəxsdən digərinə köçürülməsini tətbiq etmək istəmişdir. Lakin şirkətin inkişafı ona mümkün qədər çox insanın cəlb edilməsi ilə bağlı olduğundan, müvafiq kütləni yığa bilməyən şirkət 1998-ci ildə özünü müflis elan etmişdir.

Ümumiyyətlə, 20-ci əsrin ikinci yarısından 21-ci əsrin əvvəllərinədək olan ilkin dövrdə anonim elektron ödəniş vasitələrinin yaradılmasına aşağıdakı cəhdlər olmuşdur:

İl	Kriptolayihənin adı	Müəllif
1977	"RSA"	Ron Rivest
1989	"DigiCash" rəqəmsal valyutası	Devid Çaum
1993	"Ecash" anonim internet ödəniş sistemi	Devid Çaum
1996	"E-gold" rəqəmsal ödəniş şəbəkəsi	Duqlas Cekson
1997	"Hashcash" ("PoW" əsasında)	Adam Blek
1998	"B-Money" və "Bit-Gold"	Vey Day və Nik Zabo
1999	"Napster" faylları ilə mübadilənin eyniranqlı şəbəkəsi	Şon Fanninq
2002	"Tor" anonim ödəniş şəbəkəsi	Rocer Dinqledayn
2003	"Second life" virtual iqtisadiyyat və valyuta layihəsi	Filip Rozdeyl
2004	"RPoW" ilk rəqəmsal sikkə ("PoW" əsasında)	Hal Finni

Elektron valyutaların yaranmasında əsas töhfə həmçinin amerikalı Hal Finni (Harold Thomas Finney II) ilə əlaqələndirilir. 2004-cü ildə Finni ilk dəfə "RPoW" ("Reusable Proof Of Work" texnologiyası) çoxtətbiqli iş sübutu protokolu əsasında işləyən elektron valyuta yaratdı. O, "hashcash" alqoritminə əsaslanan və istənilən veb-saytda xidmətlərə görə ödəniş etmək üçün istifadə oluna bilən tokenlər yaratmağa xidmət edirdi. Finninin təklif

etdiyi “RPoW” protokolu tokenin yaradılması üçün müəyyən bir hesablamalar etmək və eyni işin təkrar görülməsinin qarşısını almaqla ikili xərcin aradan qaldırılmasına imkan verirdi. Bundan əvvəl Adam Blekin təklif etdiyi işin sübutu (“PoW”) protokolunda tokenləri təkrar istifadə etmək mümkün deyildi. Finni isə üçüncü tərəfə proqram təminatının “RpoW” serverində işlədiyini yoxlamağa imkan verən “etibarlı hesablama” adlı xüsusi təhlükəsizlik funksiyaları vasitəsilə “PoW” tokenlərini təkrar istifadə oluna bilən hala gətirdi.

Beləliklə, “RpoW” ikiqat xərcləmə problemini həll etdi. Bununla yanaşı, Finni şəxsiyyətlərini açıqlamadan iki nəfərin e-poçt vasitəsilə ünsiyyət yaratma modelini də hazırlamışdır. Lakin müvafiq layihələrin reallaşması uğursuz olmuşdur. Bunun əsas səbəbi valyutanın yaradıcıları tərəfindən emissiya olunması və ona nəzarətin həyata keçirilməsi olmuşdur. Başqa sözlə, bu halda dövlət və mərkəzi bankların müvafiq funksiyası şirkətlərə həvalə olunması düşünülürdü, lakin bu, avtomatik olaraq müvafiq valyutalara etibar məsələsini təmin etmirdi.

Qlobal maliyyə böhranının baş verdiyi 2008-ci ilin sonunda Satoshi Nakamoto təxəllüslü bir şəxs “bitkoin” (“bitcoin”) adlı kriptovalyutadan istifadə edərək birbaşa elektron hesablaşmalar sistemi üçün ***yeni bir protokol*** olan mərkəzləşdirilməmiş eyniranqlı “P2P” (yaxud “bərabərdən bərabərə” - “peer-to-peer”) protokolunu təsvir etdi. Bu protokol etibarlı bir üçüncü tərəfə müraciət etmədən, milyardlarla cihaz arasında birbaşa ötürülən məlumatların bütövlüyünü (tamlığını) təmin edən paylanan hesablamalar şəklində bir sıra qaydalar müəyyən etdi. İlk baxışda əhəmiyyətsiz görünən bu yenilik bütün informasiya texnologiyaları dünyasını həyəcanlandıran və onun təsəvvürünü fəth edən bir qığılcım oldu.

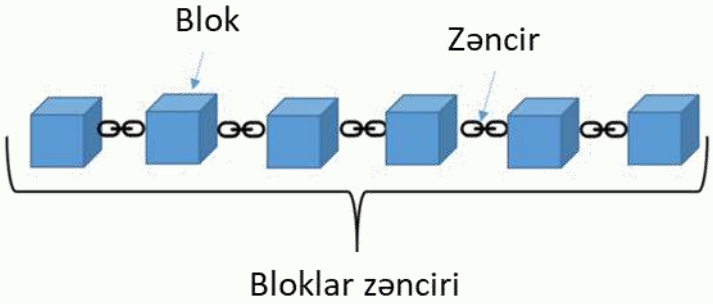
Yaranan yeni virtual valyutaların əsasında **blokçeyn** (“blockchain”) texnologiyası dayanırdı. Blokçeyn texnologiyası ideyası hələ 1991-ci ildə tədqiqatçı alimlər Stuart Haber və Scott Stornett tərəfindən verilmişdir. Onlar “Rəqəmsal sənədə zaman qeydini necə yerləşdirmək olar” (“How to Time-Stamp a Digital Document”) adlı əsərində müasir blokçeynin qurulmasının əsasını təşkil edən sxemi təsvir etmişlər. 1994-cü ildə Stuart və Scott rəqəmsal sənədlərə zaman qeydinin daxil edilməsi xidmətini göstərən “Surety” (zəmanət) xidmətini yaratdılar. Müvafiq xidmət sənədin heş (“hash”) funksiyasını hesablamaq üçün “Surety AbsoluteProof” protokolunu təklif edir.

“Surety” serverindəki heş (“hash”) funksiyası ilə “zaman qeydi” identifikatorunu yaratmaq üçün “zaman qeydi” daxil edildikdən sonra sənəd identifikatoru saxlanc üçün müştəriyə və “Absolute Proof” reyestrinin verilənlər bazasına göndərilir. Bu verilənlər bazası “Surety” servisinin identifikatorlarını saxlayır və onun arxitekturası bir-biri ilə əlaqəli heş zəncirdən ibarət olur. Bununla da, Haber və Stornett dəyişməz, ardıcıl məlumatların saxlanması ideyasının reallaşdırılmasına nail olmuşlar. Digər bir məsələ isə məlumatlara əminliyin təmin edilməsi idi. Bu problemin həlli üçün Haber və Stornett 1995-ci ildən etibarən “New York Times” jurnalını ictimai protokol kimi istifadə etməyə başladılar. Onlar bunu “Surety”yə həftə ərzində əlavə edilmiş bütün identifikatorların heş kodunu çap edərək, nəticələri qəzetin “Bildirişlər: həm itirilmiş, həm də tapılmış” adlı gözə çarpmayan bölməsində çap etməyə başladılar.

Bir çox qəzet oxucuları rəqəmlər və hərflər toplusunun arxasında nəyin gizləndiyini bilmirdilər. Həllin dahiliyi həm də ondadır ki, qəzetin populyarlığı heş kodların saxtalaşdırılmamasının qarantına çevrilmişdir. Heşlərin bir-biri ilə və qəzetin tirajları ilə əlaqəliliyi hər hansı maraqlı şəxsin məlumatları dəyişdirmək istəyinə mane olurdu, belə ki, bu halda qəzetin bütün tirajlarında dəyişiklik etmək lazım gəlirdi. Müvafiq texnologiya dünyanın ilk blokçeyn texnologiyası hesab edilir. Bu blokçeynin müasir blokçeynlərdən yalnız bir fərqi varki, oda internet üzrəindən deyil çap mediasının autentifikasiyasında istifadə etməsidir.

Blokçeynin məzmunu, mərkəzləşdirilmiş və əksmərkəzləşdirilmiş sistemlər

Blokçeyn - müxtəlif məlumatların saxlanıla biləcəyi çox sayda blokdan ibarət bir zəncirdir.



Blokçeyn texnologiyası şəxslər arasında əməliyyatların birbaşa icrasına imkan verməklə, bir sıra ənənəvi iri şirkətlərin göstərdiyi vasitəçi xidmətləri əvəz etmə (üçüncü tərəf olan vasitəçilərin, etibarlı tərəflərin iştirakı olmadan) imkanına sahibdir. Qısa formada ifadə etsək, blokçeyn texnologiyasının işləmə prinsipi həyata keçirilmiş əməliyyatların bloklarda saxlanılması və hər sonrakı blokun əvvəlki blokdakı məlumatları xüsusi alqoritmin köməyilə şifrəli formada əlaqələndirməsindən ibarətdir.

İlk baxışdan müvafiq texnologiya mürəkkəb görünsə də (bu həqiqətən də belə ola bilər) onun əsas konsepsiyası kifayət qədər sadədir.

Blokçeyn ilk əvvəl **verilənlər bazasının xüsusi bir növüdür**. Blokçeyni başa düşmək üçün əvvəlcə verilənlər bazasının (məlumat bazasının) nə olduğuna qısaca aydınlıq gətirək və onların müqayisəsini aparaq.

Verilənlər bazası kompüter sistemində elektron şəkildə saxlanılan informasiya toplusudur. Verilənlər bazasında olan informasiya və ya məlumatlar, adətən, konkret bir informasiyanın daha asan axtarışını və filtrini asanlaşdırıldığı qaydada istifadə olunur. Böyük həcmli verilənlər bazası güclü kompüterlərdən ibarət olan serverlərdə saxlanılır.

Ənənəvi maliyyə sahələrində verilənlər bazası vahid serverdə yerləşdiyi halda, blokçeyndə isə verilənlər bazası eyni anda dünya üzrə yüzlərlə və ya minlərlə bir-biri ilə əlaqəli olmayan ayrı-ayrı kompüterlərdə (serverlərdə) saxlanıla bilər. Bu baxımdan, blokçeyni həmçinin **Paylanan reyestr texnologiyası** *(Distributed Ledger Technology)* da adlandırırlar. Blokçeyndə verilənlər bazası şəbəkə iştirakçılarının hər birində olur və iştirakçılar məlumatları müvafiq bazaya öncədən xüsusi olaraq razılaşdırılmış protokola əsasən əlavə edə, eləcə də istədikləri an əməliyyatlara baxa və auditini həyata keçirə bilərlər. Paylanan əksmərkəzləşdirilmiş serverdən istifadənin əsas müsbət tərəflərindən biri serverlərdən birinin zədələndiyi və ya yararsız hala düşdüyü halda, digər serverlərdə məlumatların qorunub saxlanılması imkanlarının olmasıdır.

Ənənəvi vahid serverdə olan verilənlər bazasına mərkəzləşdirilmiş sistem, bir çox kompüterlərdə mövcüd olan paylanan verilənlər bazasına isə əksmərkəzləşdirilmiş sistem deyilir.

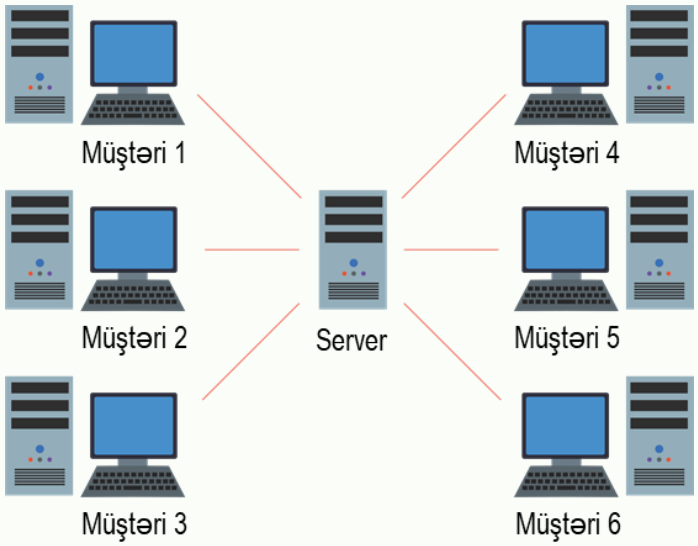
Blokçeynin əsas yaradılma ideyası *əksmərkəzləşmə* olduğundan, mərkəzləşmiş yanaşmanı rədd edir. Lakin praktikada mərkəzləşmiş və ya əksmərkəzləşmiş sistemlər xalis şəkildə mövcud deyildir. Müvafiq sistemlər *paylanılan və paylanılmayan* ola bilər. Mərkəzləşmiş və ya əksmərkəzləşmiş olmasından asılı olmayaraq, istənilən halda sistemin paylanması imkanları mümkündür.

Mərkəzləşmiş (paylanan) sistem – tapşırıqların və ya məlumatların bölgüsünə, eləcə də qovşaqlar arasında iş yükünün bölgüsünə məsul olan əsas qovşağın (“node”) olduğu sistemdir.

Adından göründüyü kimi, mərkəzləşmiş sistem bütün inzibati səlahiyyətləri ilə birlikdə mərkəzləşmiş idarəetməyə malikdir. Belə sistemləri hazırlamaq, dəstəkləmək, onlara inam yaratmaq və onları idarə etmək asandır, lakin onlar bir sıra aşağıdakı məhdidiyyətlərə malikdir:

- mərkəzi imtina nöqtəsi (mərkəzi serverdən asılılıq) mövcud olduğundan, onlar daha az sabitliyə malikdir;
- hücuma qarşı daha zəifdirlər, nəticə etibarilə də daha az mühafizə olunur;
- idarəetmənin mərkəzləşməsi qeyri-etik fəaliyyətlərə gətirib çıxara bilər;
- onların ölçüsünün artırılması əksər hallarda çətindir.

Tipik mərkəzləşmiş sistem aşağıdakı kimi təsvir oluna bilər:



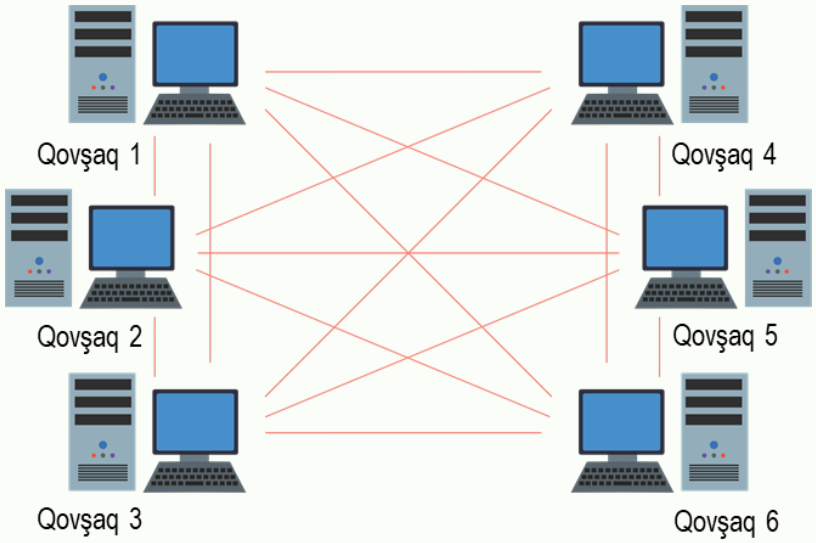
Əksmərkəzləşmiş (paylanan) sistem – əksinə, özü-özlüyündə əsas qovşağın olmadığı, lakin hesablamaların paylana bilən olduğu sistemdir. Blokçeyn də belə nümunələrdən biridir.

Adından göründüyü kimi, əksmərkəzləşmiş sistem mərkəzi idarəetmə orqanına malik deyil və onun hər bir qovşağı bərabər səlahiyyətlərə malikdir. Belə sistemləri hazırlamaq, dəstəkləmək, idarə etmək və ya ona etibar yaratmaq çətindir. Bu sistemlərin nümunəsi kimi blokçeyni göstərmək olar. Lakin mərkəzləşmiş sistemlərdən fərqli olaraq, blokçeyndə vəzifələr (tapşırıqlar) bölünmür və qovşaqlara paylanmır, belə ki, blokçeyndə bunu edə biləcək rəhbər (mərkəz) mövcud olmur və işin təşkili bütün şəbəkə iştirakçıları və ya öncədən seçilmiş iştirakçılar tərəfindən icra edilir.

Əksmərkəzləşmiş sistemlər aşağıdakı üstünlüklərə malikdir:

- mərkəzi imtina nöqtəsi (mərkəzi serverdən asılılıq) mövcud deyildir, bu səbəbdən, onlar daha sabit və imtinaya qarşı davamlıdır;
- hücumlara qarşı davamlıdır, belə ki, onlar asan hücum üçün əlçatan olan mərkəzi nöqtəyə malik deyil və nəticə etibarilə daha da mühafizə olunurlar;
- hamı üçün bərabər səlahiyyətləri olan simmetrik sistemi təmsil edir, bu səbəbdən onda qeyri-etik əməliyyatların həcmi aşağıdır və o, öz təbiətinə görə demokratikdir.

Əksmərkəzləşmiş sistemin nümunələrindən biri (pirinq sistemi – hamı hamı ilə) aşağıdakı kimi təsvir oluna bilər:



Qeyd etmək vacibdir ki, sistemin mərkəzləşməsi və ya əksmərkəzləşməsi yalnız texniki arxitektura ilə müəyyən olunmur. Daha doğrusu, texniki baxımdan sistem mərkəzləşmiş və ya əksmərkəzləşmiş ola bilər, lakin məntiqi və ya siyasi cəhətdən tamamilə başqa quruluşa malik ola bilər.

İstifadəçilərin tələbatlarından çıxış edərək, sistemi düzgün layihələndirmək imkanına malik olmaq üçün arxitekturanın müvafiq aspektlərini nəzərdən keçirək.

Texniki aspekt. Qeyd olunduğu kimi, texniki arxitektura baxımından sistem mərkəzləşmiş və əksmərkəzləşmiş ola bilər. Burada sistemin yaradılması üçün nə qədər fiziki kompüterlərin (və ya qovşaqların) istifadə olunduğu, bütün sistemin çökməsinə qədər onun saxlaya biləcəyi qovşaq imtinalarının sayı və s. təhlil olunur.

Siyasi aspekt. Burada insan, insan qrupları və təşkilatın ümumilikdə sistem üzərində malik olduğu nəzarət təhlil edilir. Əgər sistemin bütün kompüterlərinə konkret bir şəxs və ya şəxslərin kiçik dairəsi tərəfindən nəzarət olunursa, bu halda sistem aydın şəkildə mərkəzləşmiş sistemdir. Lakin əgər hər hansı konkret şəxs və ya qrup sistemə nəzarət etmirsə və bütün istifadəçilərin sistem üzərində bərabər hüquqları vardırsa, bu halda siyasi mənada bu əksmərkəzləşmiş sistem hesab olunur.

Məntiqi aspekt. Quruluşundan asılı olaraq, sistem mərkəzləşmiş və ya əksmərkəzləşmiş ola bilər (onun texniki olaraq mərkəzləşmiş və ya əksmərkəzləşmiş olmasından asılı olmayaraq). Bunu aşağıdakı nümunə ilə izah etmək olar: təsəvvür edin ki, sistemi şaquli olaraq bölürük, üstəlik də onun hər bir yarısının da özünün xidmət təchizatrçıları və istifadəçiləri vardır. Əgər sistemin hər iki yarısı müstəqil vahidlər kimi işləyə bilirsə, deməli, onlar məntiqi olaraq əksmərkəzləşmişdir. Əks halda, bu məntiqi olaraq mərkəzləşmiş sistem olacaqdır.

Blokçeyn: inkişaf mərhələləri, işləmə prinsipi, tərkib hissələri, əməliyyatlar və istifadə olunduğu sahələr

Blokçeyn texnologiyasının yaranması ilə rəqəmsal aktiv anlayışının məzmunu dəyişməsə də, bu, müvafiq terminin daha geniş mövzuları əhatə etməsinə təkan verdi. Qeyd etmək vacibdir ki, rəqəmsal aktivlərin bir çoxu gələcəkdə bütün sahələri və hətta dünya bazarını köklü formada dəyişmə potensialına malikdir.

Müvafiq texnologiyanın əsas üstünlüyü vasitəçininin olmaması imkanı, bloklar zəncirinin proqramlaşdırıla bilinməsi, eləcə də şəbəkə kodu və ya simvolun özünə daxil

edilmiş qaydalardan (standartlardan) istifadə olunması xüsusiyyətləri ilə əlaqələndirilir. Həmçinin müvafiq standartlar şəbəkə istifadəçiləri tərəfindən veb üzərindən davamlı olaraq yoxlanılır.

Blokçeyn texnologiyası aşağıdakı inkişaf mərhələlərini keçmişdir:

Birinci nəsil blokçeyn. Birinci nəsil blokçeyn texnologiyası "bitcoin"in yaradılması ilə əlaqələndirlir. Müvafiq blokçeyn texnologiya eyniranqlı (pirinq) şəbəkə üzvləri tərəfindən heç bir vasitəçi (mərkəzi server) olmadan ümumi razılıq əsasında qəbul edilmiş ödəniş vasitəsinin bir şəxsdən digər şəxsə köçürülməsini nəzərdə tuturdu.

Blokçeynin birinci nəsli aşağıdakı əsas fərqləndirici xüsusiyyətlərə malikdir:

- xüsusi riyazi hesablamalar ilə ("hashing") hər növbəti blokun yaradılması;
- əməliyyatların təsdiqlənməsi üçün xüsusi "mayninq" sistemindən istifadə.

İkinci nəsil blokçeyn. Blokçeynin ikinci nəsli "Ethereum" ilə başlayır. Müvafiq texnologiya öncədən müəyyən edilmiş bir alqoritmə uyğun öz-özünə işləyə və bütün şərtləri yerinə yetirə bilən **smart müqavilələrin** yaranmasını əhatə edir. Bu yenilik, mahiyyət etibarı ilə blokçeyn texnologiyasından yalnız virtual valyutalar üçün deyil, həmçinin digər sahələrdə qurumlararası əməkdaşlıq formaları üzrə platforma qismində istifadə oluna bilməsi ilə bağlıdır.

Üçüncü nəsil blokçeyn. Blokçeynin üçüncü nəsli fərqli blokçeynləri bir-biri ilə əlaqələndirən platformalar ("interchain") və miqyaslanma problemlərini həll edən blokçeynlər ilə əlaqələndirilir. Bu sistemlərdə fərqli blokçeynlərarası əlaqələrin yaranması və mübadilə imkanları üzərindən işlərin görülməsi nəzərdə tutulur.

Müvafiq blokçeyn platformaları ödəniş vasitəsi funksiyasından əlavə, maliyyə sektorunun digər sahələrində də effektiv istifadə oluna bilər. Müxtəlif fəaliyyət sahələrində istifadə olunan blokçeynlər texniki strukturuna görə bir-birindən fərqlənə bilərlər. Aşağıdakı sahələrdə blokçeyn texnologiyasından geniş istifadə imkanları mövcuddur:

- müəlliflik və sahiblik hüququ ("Ascribe");
- əmtəə və xammal ilə əməliyyatlar ("The Real Asset company");
- verilənlərin idarə edilməsi ("Factom");
- rəqəmsal şəxsiyyətin həqiqiliyinin yoxlanılması və giriş hüquqlarının təsdiqi ("2WAY.IO", "ShoCard", "Guardtime", "BlockVerify", "HYPR", "Onename");
- energetika ("Energy Blokchain Labs");
- elektron səsvermə vasitələri ("Follow My Vote");
- kazino və onlayn oyunlar ("First blood", "Etheria");
- əşyaların interneti ("Chronicled");
- müxtəlif dövlət orqanları və sahibkarlıq sahələri.

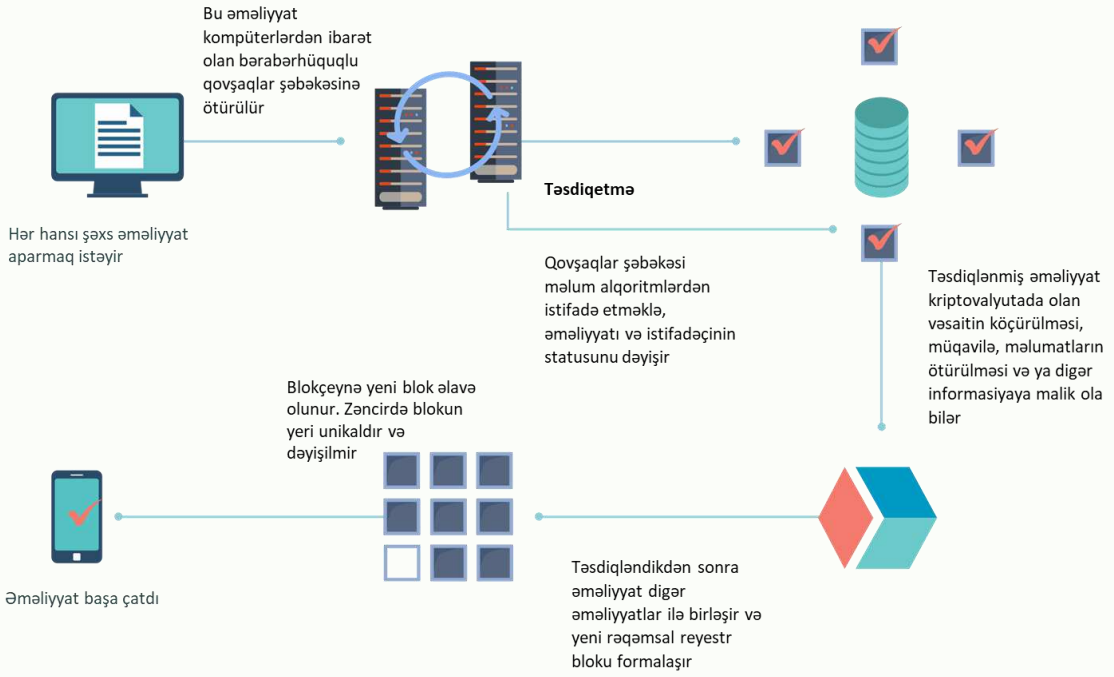
Texniki baxımdan blokçeyn aşağıdakı xarakterik xüsusiyyətlərə malikdir:

- etibar edilən üçüncü tərəfin, yəni vasitəçinin iştirakı olmadan dəyərlərin ötürülməsi imkanı (bərabərhüquqlu imkanlar vermə);
- əməliyyatların (dəyərlərlə mübadilənin) ümumi, əksmərkəzləşmiş və açıq reyestri olması (reyestrin verilənlər bazasının çoxsaylı qovşaqların hər birində təkrarlanması);
- reyestrin verilənlər bazasına düzəlişlərin (dəyişikliklərin) oluna bilinməməsi, hər bir yazının sabit və dəyişməz olması (istənilən yeni yazının verilənlər bazasının müxtəlif qovşaqlarında yerləşmiş bütün nüsxələrində meydana gəlməsi);
- əməliyyatların yoxlanılması, təhlükəsizliyinin təmin olunması və təsdiq edilməsi üçün etibar edilmiş üçüncü tərəflərin vasitəçi kimi çıxış etməsinə zərurətin olmaması;
- internet üzərindən daha bir funksional qat olmaqla, digər internet texnologiyalar ilə birlikdə mövcud ola bilməsi;
- məlumat mübadiləsinin açıq sisteminin yaradılması imkanları ("TCP/IP" protokollarına eynilə oxşar olaraq).

Blokçeyn texnologiyasının əsasını **əməliyyatlar** və verilənlərin qrup halında bir yerə toplandığı **bloklar** təşkil edir. Hər bir blok özündə əməliyyatların məcmusunu və əvvəlki blokla əlaqəni təmsil edir ki, texnologiyanın adının mənşəyi (block – blok, chain – zəncir) də buradan yaranmışdır. Bloklararası əlaqə blokçeynin protokoluna qoyulmuş xüsusi heş-funksiyaların köməyi ilə həyata keçirilir. Blokların əlavə edilməsi isə blokçeynin protokolunda qeyd edilən formada validatorlar tərəfindən aparılır.

Ümumi ödəniş sistemlərində blokçeyn tsikli aşağıdakı kimidir. “A” şəxsi “B” şəxsinə vəsait köçürmək istədikdə, “A” şəxsi ona aid cüzdandan “B” şəxsinin cüzdanına köçürmə edir. Köçürmə edildikdən sonra əməliyyat ümumi bazada validatorlar tərəfindən təsdiqlənməsini gözləyir. Validator öncədən blokçeynin protokolunda nəzərdə tutulmuş düsturla əməliyyatın həqiqiliyini yoxladıqdan sonra onu təsdiqləyir və digər təsdiqlənmiş əməliyyatlarla birlikdə məlumatı yeni bloka əlavə edir. Validator yeni bloku əlavə etdikdə müəyyən riyazi funksiyaları yerinə yetirməli olur. Hər təsdiqlənən əməliyyata və ya blokun yaradılmasına görə validator mükafat əldə etmək imkanına malik olur. Validator müvafiq məlumatları bloka əlavə etdikdən və blokun yaradılması üçün zəruri hesablamaları başa çatdırdıqdan sonra yeni blok yaranır və blok zəncirinə əlavə olunur. Yeni blok blokçeynə əlavə olunduqdan sonra proses başa çatmış hesab olunur.

Blokçeyn prosesini, onun necə işlədiyini aşağıdakı kimi təsvir etmək olar:

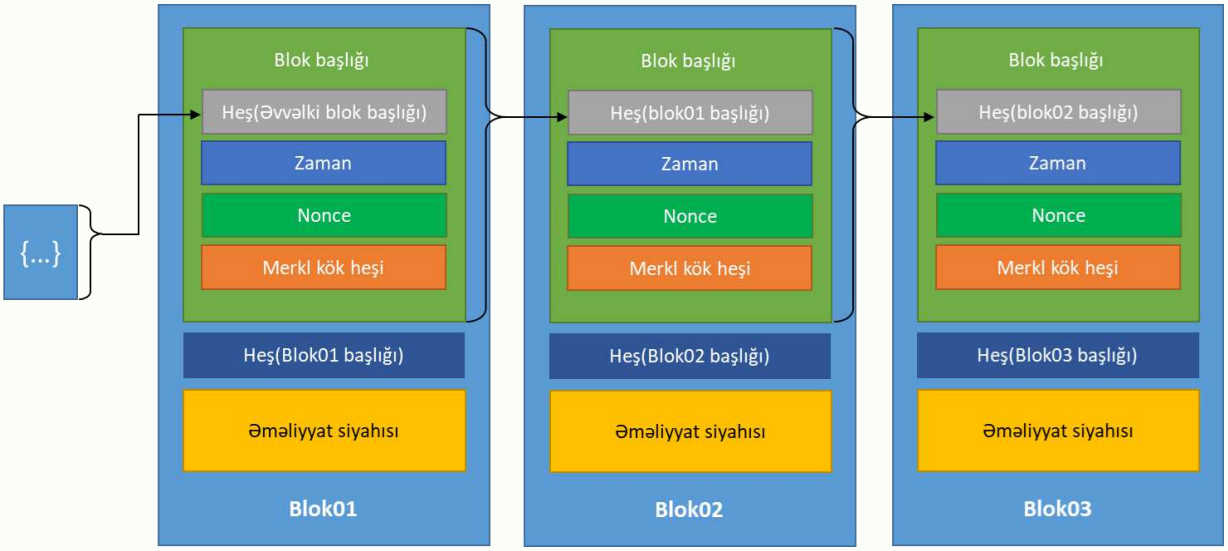


Blok - blokçeyn daxilində olan əməliyyatları özündə saxlayan və qruplaşdıran elementdir. Blok, ənənəvi mühasibatlıqda jurnalın (reyestrin) yerinə yetirdiyi funksiyanı həyata keçirir. Əməliyyatların etibarlılığını yoxladıqdan və təsdiqlədikdən sonra şəbəkə üzvləri (qovşaqlar) onlardan qruplaşdırılmış şəkildə bloklar əmələ gətirir. Blokçeyndə ilkin bloka ondan əvvəlki blokun olmaması səbəbi ilə **Geneziz (genesis) bloku** deyilir.

Blokçeyndə bloklar aşağıdakı iki hissədən ibarət olur:

- **Başlıq** (Head) hissə;
- **Əməliyyat** (Payload) hissə.

Tipik blokçeyn şəbəkəsində blokların struktur sxemi aşağıda verilmişdir:



Başlıq hissə əsasən aşağıdakı məlumat parametrlərindən ibarətdir:

- Blokun versiya adı (“ver_block”);
- Blokun yaradılma tarixi və saatı (“timestamp”);
- Əvvəlki blokun heşi (“prev_block”);
- Verilmiş blokda bütün əməliyyatların heşi (“mrkl_root”);
- Mayninqdə istifadə olunan və digər təsadüfi parametrlər: “difficulty target” (mürəkkəblik hədəfi), “nonce” və “bits” parametrləri;
- Yeni blokun heş kodu.

Müvafiq parametrlər arasında ən əhəmiyyətlisi əvvəlki blokun heş məlumatıdır. Ona əlaqələndirici heş də deyilir. Bu heş kod vasitəsi ilə hər yeni yaradılan blokun daha öncə yaradılmış bloklar ilə əlaqəsini müəyyən etmək mümkündür. Blokçeyndən asılı olaraq, heşlər müxtəlif alqoritmlər ilə hesablana bilər. Hazırda məsələn, “Bitcoin” praktikasında daha çox istifadə olunan alqoritmlərdən biri “SHA-256” alqoritmidir. Bu alqoritm assimetrik formada işləyir (daha ətraflı növbəti bölmələrin birində).

Yeni yaradılacaq blokun heş nəticəsinin hesablanması üçün əməliyyatların vahid heş nəticəsi olan vahid “Merkl” heş nəticəsindən və əlaqələndirici heşdən istifadə olunur.

Blokçeyn texnologiyasında hər bir heş-kodun hesablanması əvvəlcədən nəzərdə tutulmuş mürəkkəb bir funksiyanın hesablanmasını nəzərdə tutur (lakin bu blokçeyn protokolundan aslı olaraq fərqli fəaliyyət də ola bilər).

Başlıq şəbəkənin sabitliyinə və dəyişməzliyinə (“immutability”) cavab verən informasiyanı əks etdirir. Başlıq zəncirdə olan özündən əvvəlki bloka istinad edir. Hər bir blok başlığı əvvəlki blokun heşinə malikdir, bu səbəbdən də hər hansı istifadəçi əvvəlki blokun əməliyyatını hissolunmaz şəkildə dəyişə bilməz.

Əməliyyat hissəsi blok daxilində əməliyyatların qeydə alındığı hissədir. Əməliyyat hissəsi verilmiş bloka daxil olan əməliyyatların sayğacından və siyahısından ibarətdir. Burada blokda saxlanılmalı olan və blokçeyn şəbəkəsinə daxil edilməli olan bütün əməliyyatların siyahısı, onların məbləğləri, tərəflərin ünvanları və bir sıra digər təfərrüatlar qeyd edilir.

Bitkoynin nümunəsində blokçeyn şəbəkəsindəki blokların strukturu aşağıda verilmişdir:

Blok 632276	
Heş	00000000000000007beef62d08dd723c4342bdf89dcf1fe77ba
Təsdiq	75 553
Zaman qeydi (timestamp)	2021-12-18 10:45
Hündürlük	632276
Mayner	F2Pool
Əməliyyatların sayı	2 917
Mürəkəbblik	15 138 043 247 082,88
Merkl ağacı	3437b44e1dfe1dbe50e45975ee0df3b60d97a5864a925b90a2fc
Versiya	0×20000000
Bitlər (bits)	387 094 518
Çəki	3 998 764 WU
Ölçü	1 293 790 bayt
Nonce (birdəfəlik kod)	3 719 213 695
Əməliyyatların həcmi	5519.61929761 BTC
Bloka görə mükafat	6.25000000 BTC
Komissiya mükafatı	0.61968993 BTC

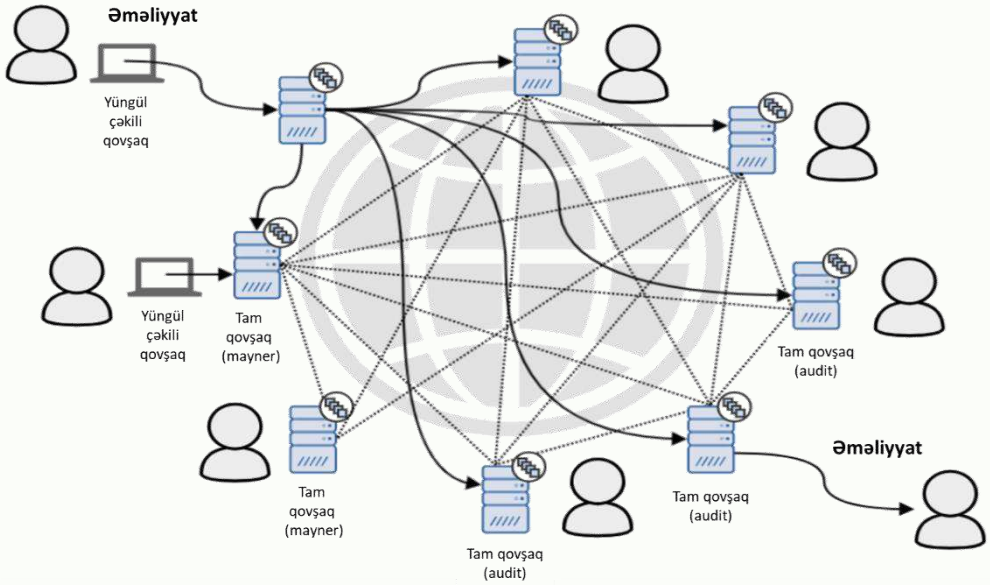
Blokçeynin protokolundan asılı olaraq hər blokda əməliyyatların maksimal saxlanılma sayı mövcuddur. Bu rəqəm əsasən əməliyyatların ölçüsündən asılıdır.

Əməliyyatlar blokun tərkib hissəsidir. Blokun başlıq hissəsinə analoji olaraq əməliyyatların da öz heş nəticələri olur. Bütün əməliyyatlar blokun baş hissəsində “Merkl kök”ün heş nəticəsi ilə bir-birinə bağlı olur. İlk öncə “Merkl ağacı” prinsipinə uyğun olaraq bütün əməliyyatların vahid heş nəticəsi əldə olunur. Alınmış vahid heş nəticəsinə (“Merkl kök”ünün heşi) özündən əvvəlki blokun heşi və blok yaradılması üçün istifadə edilən parametrlər (nonce, bits və s.) əlavə olunaraq yeni blokun heş nəticəsi formalaşır. Yaradılmış blok bütün şəbəkə iştirakçılarının məlumat bazasına yerləşdirilir. Bloklarda hər hansısa manipulyasiya xarakterli dəyişikliyin edilməsi üçün bütün əvvəlki bloklardada uyğun dəyişikliklərin edilməsi tələb olunur ki, bu da texniki baxımdan qeyri-mümkündür. Ehtiyac yarandığı halda, şəbəkə iştirakçıları bloklarda olan əməliyyatlara baxış etmək və müvafiq məlumatları əldə etməkdə maneəsiz icazə hüququna malikdirlər.

Blokçeyndə qovşaq anlayışı və onların növləri

Blokçeyndə bərabərhüquqlara malik şəbəkə iştirakçılarının (qovşaqların) müxtəlif funksiyaları və səlahiyyətləri ola bilər.

Blokçeynin şəbəkə iştirakçıları olan **qovşaqların** (“nodes”) hər biri bir və ya bir neçə iştirakçını təmsil edə bilər. Blokçeyn texnologiyasında əməliyyatların yaranması və ötürülməsi hər hansı iki iştirakçı qovşaq arasında olur və bu zaman tərəflərin hər birinin öz eyniləşdirmə məlumatlarını bilməsi kifayət edir (blokçeyn protokolundan asılı olaraq).



Blokların formalaşması və ötürülməsi blokçeyn sisteminin daxilində əvvəlcədən qurulmuş proqram təminatları üzərindən aparılır. Blokçeyn şəbəkəsində qovşaqlar üç əsas funksiyanı yerinə yetirir:

- şəbəkədaxili konsensus qaydalarının icra edilməsi;
- məlumatın açıqlanması (əməliyyatlar və vəsaitlərin məbləği haqqında);
- təsdiqlənmiş əməliyyatların surətinin saxlanılması.

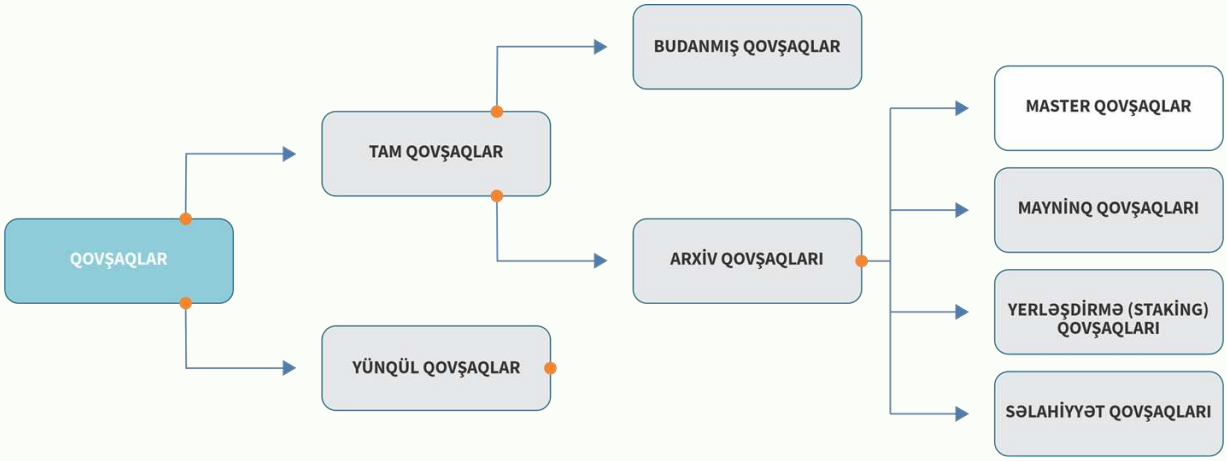
Blokçeyn texnologiyasında əsasən iki növ qovşaq (iştirakçı) mövcuddur (blokçeyn sistemindən asılı olaraq dəyişə bilər):

• **Tam qovşaqlar ("full node").** Tam qovşaqlar mərkəzləşdirilməmiş şəbəkədə server qismində çıxış edir. Onların əsas vəzifələrinə digər qovşaqlar arasında konsensusun saxlanılması (bu barədə növbəti bölmələrin birində ətraflı məlumat veriləcək) və əməliyyatların yoxlanılması daxildir. Tam qovşaqlar həmçinin blokçeynin surətini saxlayırlar ki, bu da onları daha təhlükəsiz etməklə ani göndərişlər və şəxsi əməliyyatlar kimi xüsusiyyətləri fərdiləşdirməyə imkan verir.

Tam qovşaqlar şəbəkənin gələcəyi ilə bağlı təkliflər üzrə qərarların qəbulunu səsvermə vasitəsilə həyata keçirirlər: təklifin keçməsi üçün 51%-dən çox səs toplanması tələb olunur.

• **Yüngül çəkili qovşaqlar ("lightweight nodes"**). Müvafiq qovşaqlar bütün blokların nüsxəsini deyil, yalnız özü üçün zəruri məlumatları (əsasən blok başlıqlarını) saxlayırlar. Yüngül çəkili qovşaqların əsas üstünlükləri daha az hesablama gücünə və yaddaşa ehtiyac duymaları və bu səbəbdən də mobil platformalarda işləmə imkanlarının olmasıdır. Bu şəbəkə üzvləri bütün blokçeyn şəbəkəsində baş vermiş əməliyyatları görə bilməsələr də, özlərinə məxsus balans və əməliyyatları izləmə imkanları mövcuddur.

Tam və yüngül çəkili qovşaqlar öz növbəsində daşıdıqları fərqli funksiyalara görə alt qruplara bölünürlər.



Tam qovşaqlar **budanmış ("pruned")** və **arxiv ("archival")** qovşaqlara bölünürlər.

Budanmış qovşaqlar ("pruned nodes"). Bu növ qovşaqların xarakterik xüsusiyyəti başlanğıcdan blokları yükləməyə başlaması və əvvəlcədən müəyyən edilmiş limitə çatan kimi yalnız başlıqları saxlayaraq ən köhnə blokların daxilindəki məlumatların silməsindən ibarətdir. Məsələn, ölçü limitinin 550 MB olaraq təyin edildiyi halda, belə qovşaqlar yalnız sabit disk sahəsinə sığa biləcək həcmdə son blokları saxlayacaqdır. Lakin bunun üçün əvvəlcə bütün blokçeyn sinxronizasiyasından keçilmə tələb olunur. Müvafiq prosedur blokların düzgünlüyünün yoxlanılmasını təmin edir. Budanmış qovşaqlar tam qovşaqlar hesab olunur və bu səbəbdən də əməliyyatları təsdiq etmə və konsensusda iştirak etmə səlahiyyətinə malik olurlar.

Arxiv qovşaq ("archival nodes"). Arxiv qovşaqlar blokçeynin bütün verilənlər bazasını özündə saxlamaqla, konsensus qaydalarının icra edilməsi və blokların təsdiqlənməsində iştirak edir.

Budanmış qovşaq ("node") ilə arxiv qovşağı arasındakı fərq onların serverdə və ya kompüterdə tutduğu sabit disk sahəsinin həcmi ilə bağlıdır.

Arxiv qovşaqlar blokçeynə bloklar əlavə edə bilən və edə bilməyən alt növlərə bölünür. Müvafiq alt növlərə bölgü əsasən blokçeynin növünə uyğun olaraq aparılır.

- **Mayninq qovşaqları ("mining nodes").** Bu növ qovşaqlar işin sübutu ("PoW" - "Proof of Work") konsensusu ilə işləyən blokçeynlərə (məsələn, bitkoyn) aiddir. Maynerlər blok yaratmaq üçün lazımi işi gördüklərini sübut etmək məqsədi daşıyan qovşaqlardır. Tapşırığı yerinə yetirmək üçün maynerlər ya tam arxiv qovşaqlar olmalı, yaxud blokçeynin cari vəziyyətini və növbəti blok üçün tələb olunan parametrləri öyrənmək üçün şəbəkədəki digər tam qovşaqlardan məlumat almalıdır. Proses iştirakçıları kriptoqrafik məsələni həll etmək üçün texniki alət-komponentlərdən (video kart, prosesor və ya "ASIC" – xüsusi təyinatlı inteqral sxemlər) istifadə edirlər. Məsələni ilk həll edən şəxs öz nəticələrini şəbəkəyə təqdim edir, tam qovşaqlar tərəfindən yoxlanıldıqdan və konsensusa çatdıqdan sonra mövcud blokçeynə bloku əlavə etmək hüququ verilir. Görülən işə görə maynerlər şəbəkə haqlarına əlavə olaraq əvvəlcədən müəyyən edilmiş həcmdə mükafatlar alırlar.

- **Pay qovşaqları ("Staking Nodes").** Bu növ qovşaqları ənənəvi fiat valyutada olan pul depoziti ilə müqayisə etmək olar. İştirakçı tərəfindən girov qoyulan vəsaitə görə mükafat əldə olunur. Müvafiq blokçeynlərdə əvvəlcədən müəyyən edilmiş qaydalar toplusuna və şans amilinə əsaslanaraq, kimin bloku yaratması və mükafatı alması önəmli rol oynayır. Bunun üçün fasiləsiz (daim) şəbəkədə qalmaq və blokçeynin işlək vəziyyətdə saxlamanmasını təmin etmək tələb olunur. Müvafiq qovşaqların istifadə formaları və fəaliyyəti bir qədər mürəkkəb olur və bir çox halda şəbəkənin mərkəzləşməsinə gətirib çıxarır. Lakin onların əsas müsbət tərəfləri hər hansı bahalı avadanlığa və mürəkkəb hesablamalara ehtiyacın olmamasındadır.

- **Master qoşvaqlar (“Masternodes”).** Pay qovşaqları (“staking nodes”) ilə müqayisədə master qovşaqlar blokçeyninə blokun əlavə olunması mümkün deyildir. Bu növ qovşaqların yeganə təyinatı əməliyyatları izləmək və onları yoxlamaqdır. Bundan əlavə, master qovşağın işə salınması şəbəkəni qorumaqla yanaşı, göstərilmiş xidmətə görə şəbəkədən mükafatların alınması imkanını yaradır. Master şəbəkənin qurulması məqsədilə girov qismində müəyyən həcmdə vəsaitin bloklanması və fasiləsiz rejimdə onlayn aktivliyin təmin edilməsi tələb olunur.

Blokçeynin fundamental əsasları. Kriptoqrafiya və heş funksiyalar

Blokçeynin köməyilə biznesin real problemlərini həll etməyi öyrənməkdən ötrü blokçeynin nə olduğunu və necə işlədiyini dərindən başa düşmək lazımdır. Yuxarıda qeyd edildiyi kimi blokçeyn platformaları özlərinin fəaliyyət və texniki xüsusiyyətlərinə görə bir birindən fərqlənirlər. Buna baxmayaraq, hər bir blokçeynin əsası iki əsas parametrdən ibarətdir: **kriptoqrafiya** və **konsensus alqoritmləri.** Müvafiq parametrlər bir qədər fərqli variantlarda olsa da, mahiyyət etibarilə demək olar ki, bütün blokçeynlərdə mövcüd olur.

Texniki baxımdan blokçeyn texnologiyasının nüvəsini kriptoqrafiya, oyun nəzəriyyəsi və inormatika konsepsiyalarının məcmusu təşkil edir.

Əvvəlcə ümumi səviyyədə müvafiq komponentlərin blokçeyndə hansı rol oynadığını, daha sonra isə bu komponentlərin əsaslarını daha ətraflı nəzərdən keçirək. Bundan əvvəl isə adi mərkəzləşmiş sistemlərin necə işlədiklərini xatırlayaq. Ənənəvi yanaşmaya əsasən, əməliyyatların (dəyişikliklərin) yalnız bir tarixini dəstəkləyən (saxlayan) mərkəzləşmiş sistem mövcuddur. O, bütün verilənlər bazası üzərində paralel nəzarəti həyata keçirməli və vasitəçilər üzərindən sistemə etibarı təmin etməlidir. Belə stabil sistemin əsas problemi düzgün olub-olmamasından asılı olmayaraq, mərkəzləşmiş sistemə etibar etməkdir. Bundan əlavə, vasitəçilər üçün əlavə xərclər qaçılmaz olur, əməliyyatın baş vermə müddəti isə aydın səbəblərə görə böyük olur. Bütün sistem üzərində tam nəzarətin olması mərkəzləşmiş idarəetmə orqanlarına praktiki olaraq hər bir addımı atmağa imkan verir.

Kriptoqrafiya, oyun nəzəriyyəsi və informatikanın köməyilə blokçeynin mərkəzləşmiş vasitəçilər problemini necə həll etməsi məsələsini nəzərdən keçirək. Təyinatlarından asılı olmayaraq, blokçeynin bütün əməliyyatları kriptoqrafik olaraq qorunur. Kriptoqrafiyanın köməyilə “A” şəxsinin heç bir şəkildə “B” şəxsinin imzasını saxtalaşdırmaqla “B” şəxsi adından əməliyyat həyata keçirməyəcəyinə zəmanət vermək olar.

Müxtəlif mürəkkəblik dərəcəsinə malik müxtəlif tətbiqi məsələlər (problemlər) və vəziyyətlər mövcuddur. Müvafiq olaraq, kriptoqrafiyanın əsas protokolları və oyun nəzəriyyəsinin konsensusu tətbiqi istifadədən asılı olaraq müxtəlif ola bilər. Buna baxmayaraq, razılaşdırılmış reyestrin və ya yoxlanılmış əməliyyatların verilənlər bazasının aparılmasının ümumi prinsipi həmişə eynidir. Kriptoqrafiya və oyun nəzəriyyəsi anlayışlarının daha əvvəllər mövcud olmasına baxmayaraq, məhz kompüter elmləri sahəsində bu fraqmentlər məlumatların təşkil olunmuş strukturu və eyniranqlı şəbəkələrin texnologiyaları vasitəsilə birləşdirilir. Rəqəmsal dünyada istənilən məntiqi və ya riyazi konsepsiyaların həyata keçirilməsi üçün əlaqəli bilik sahələrini əhatə edən "proqram təminatının ağıllı işlənməsi" lazımdır. Məhz belə yanaşma sayəsində blokçeyni hazırlayan şəxslər tətbiqlərə kriptoqrafiya və oyun nəzəriyyəsi anlayışlarını daxil edirlər ki, əksmərkəzləşmə və qovşaqlar arasında hesablamaların paylanması təmin edilsin.

Kriptoqrafiya, oyun nəzəriyyəsi və onların blokçeyndə tətbiqi məsələləri ayrıca araşdırma və elm sahələri olduğundan, müvafiq sənəddə onlar barəsində yalnız xülasə məlumatlar verməklə kifayətlənəcəyik. Daha sonra bitkoynin misalında blokçeynin tətbiqinin qısa xülasəsi təqdim olunacaqdır.

Kriptoqrafiya. Kriptoqrafiya blokçeynin daha mürəkkəb tərkib hissəsidir. Bu, qabaqcıl riyazi metodlara əsaslanan müstəqil araşdırma sahəsidir. *Kriptoqrafiya* - məlumatların identifikasiyasını, bütövlüyünü və məxfiliyini təmin etmək üsulları haqqında elmdir. Mətnin mühafizəsi texnikası kimi kriptoqrafiya yazı ilə birlikdə yaranmışdır - gizli yazı üsulları qədim Hindistan, Mesopotamiya, Misir sivilizasiyalarına da məlum idi.

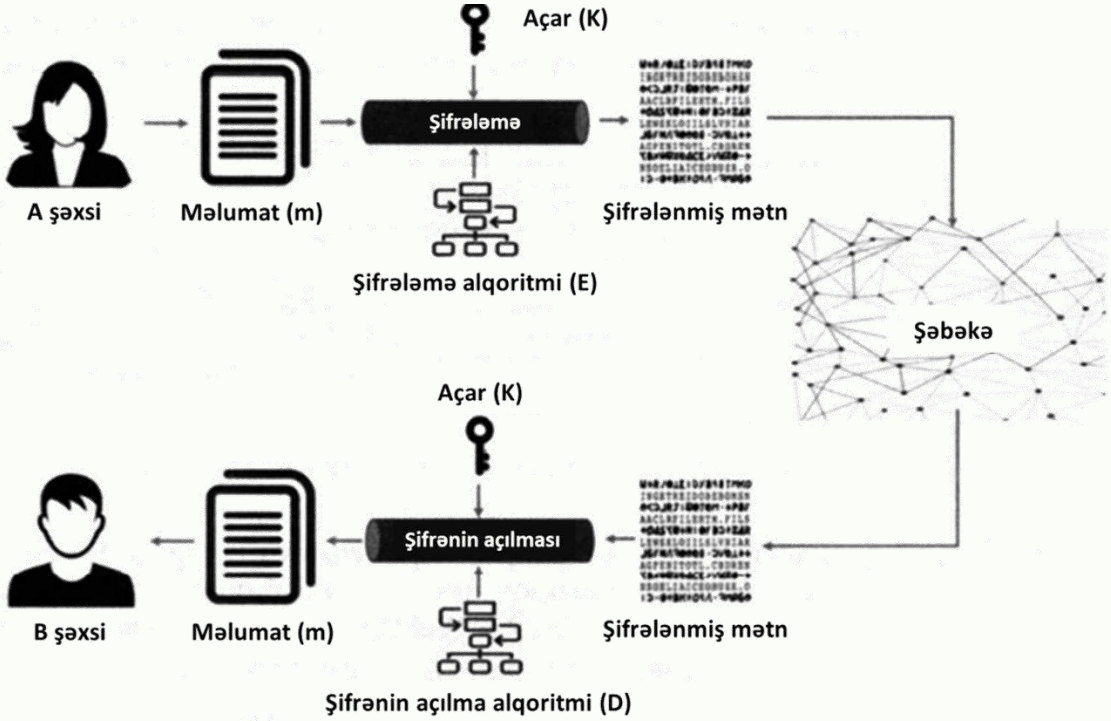
20-ci əsrdən başlayaraq kriptoqrafiyada texniki vasitələr ilə şifrələmə metodlarından istifadə olunur. Ümumilikdə iki növ kriptoqrafiya mövcuddur: **simmetrik açarlı** kriptoqrafiya və **assimetrik (açıq) açarlı** kriptoqrafiya.

Simmetrik açarlı kriptoqrafiya (və ya simmetrik şifrələmə) eyni açarın həm şifrələnmə, həm də deşifrələnmə (şifrənin açılması) üçün istifadə edildiyi məlumat şifrələməsi növüdür. Məlumatın kodlaşdırılmasının bu üsulu hökumətlə ordu arasında gizli əlaqəni asanlaşdırmaq üçün son onilliklərdə geniş yayılmışdır. Hal-hazırda simmetrik açar alqoritmləri verilənlərin təhlükəsizliyini yaxşılaşdırmaq üçün müxtəlif növ kompüter sistemlərində geniş istifadə olunur.

Simmetrik şifrələmə sxemi iki və ya daha çox istifadəçi tərəfindən istifadə edilən tək açara əsaslanır. Eyni açar mətni şifrələmək və şifrəsini açmaq üçün istifadə olunur. Şifrələmə prosesi açıq mətnin (girişin) şifrə adlanan şifrələmə alqoritmi ilə işlənməsindən ibarətdir ki, bu da öz növbəsində şifrəli mətn (çıxış) yaradır. Şifrələmə sxemi kifayət qədər güclüdürsə, insanın şifrəli mətndə olan məlumatı oxuması və ya əldə etməsinin yeganə yolu onun şifrəsini açan müvafiq açardan istifadə etməkdir. Şifrənin açılması prosesi əsasən şifrəli mətni yenidən açıq mətnə çevirir.

Qeyd olunanları konkret nümunədə nəzərdən keçirək. Fərz edək ki, "A" şəxsi "B" şəxsinə məlumat ("m") göndərmək istəyir. Əgər o, məlumatı sadəcə olduğu kimi – açıq mətn formasında göndərsə, istənilən düşmən, məsələn, "C" şəxsi məlumatı asanlıqla ələ keçirə və bununla da konfidensiallıq pozula bilər. Beləliklə, şifrələnmiş məlumat (şifrəli mətn) yaratmaq üçün "A" şəxsi şifrələmə alqoritmi ("E") və məxfi açardan ("K") istifadə etməklə məlumatı şifrələmək istəyir. Bədniyyətli şəxsin məlumatı ələ keçirməsi üçün onun həm alqoritmi ("E"), həm də açarı ("K") ələ keçirməsi tələb olunur. Alqoritm və açar nə qədər güclüdürsə, rəqibə hücum etmək də bir o qədər çətin olacaqdır.

Simmetrik açarın nümunəsində kriptoqrafiya işinin ümumi prinsipləri sxematik olaraq aşağıda verilmişdir:



Hazırda daha çox istifadə edilən iki simmetrik şifrələmə üsulu mövcuddur: blok və axın şifrələrinə əsaslanır.

Simmetrik şifrələmə alqoritmləri məlumatların təhlükəsizliyini və istifadəçilərin məxfiliyini yaxşılaşdırmaq üçün bir çox müasir kompüter sistemlərində istifadə olunur. Həm təhlükəsiz mesajlaşma proqramlarında, həm də "bulud yaddaşı"nda geniş istifadə olunan *Qabaqcıl Şifrələmə Standartı ("Advanced Encryption Standard" - "AES")* simmetrik şifrələmənin əsas nümunələrindən biridir.

Lakin blokçeyn texnologiyası vahid server üzərindən deyil, bərabərhüquqlu istifadəçilərin fəaliyyət göstərdiyi platformalar təklif etdiyindən, simmetrik şifrələmə üsulundan istifadə bir qədər problemli məsələyə çevrilir. Bu səbəbdən, blokçeyn texnologiyasında şəbəkə iştirakçıları məlumatları əsasən *assimetrik şifrləmədən* istifadə etməklə bir-birinə ötürürlər.

Açıq açarlı kriptoqrafiya *("Publik Key Cryptography" – "PKC")* kimi də məlum olan ***assimetrik açarlı kriptoqrafiya*** Diffi və Hellman tərəfindən irəli sürülmüş inqilabi konsepsiyadır. Bu texnologiyanın köməyilə onlar rəqəmsal imzalar tətbiq etməklə, simmetrik kriptoqrafik sistemdə açarların yayımlanması problemini həll etmişlər. Simmetrik kriptoqrafiyada istifadə olunan tək açardan fərqli olaraq bu növ şifrələmədə həm qapalı (şəxsi), həm də açıq açardan istifadə olunur. Açar cütlərinin istifadəsi Açıq açarlı kriptoqrafiyaya ("PKC") digər kriptoqrafik metodlara xas olan problemləri həll etmək üçün istifadə edilə bilən unikal xüsusiyyətlər və imkanlar verir. Kriptoqrafiyanın bu forması müasir kompüter təhlükəsizliyinin vacib elementi olmaqla yanaşı, inkişaf etməkdə olan kriptovalyuta ekosisteminin vacib komponentinə çevrilmişdir.

Açıq açarlı kriptoqrafiyada açıq açardan göndərən tərəfindən məlumatı şifrələmək üçün istifadə olunur, qapalı (şəxsi) açar isə məlumatın şifrəsini açmaq üçün alıcı tərəfindən istifadə olunur. İki açar bir-birindən fərqli olduğundan, açıq açar şəxsi təhlükəsizliyə xələl gətirmədən təhlükəsiz şəkildə paylaşıla bilər. Hər bir asimmetrik açar cütü unikaldır və açıq açardan istifadə etməklə şifrələnmiş məlumatın yalnız müvafiq şəxsi açara malik olan şəxs tərəfindən oxuna bilməsini təmin edir.

Asimmetrik şifrələmə alqoritmləri riyazi cəhətdən əlaqəli olan açar cütləri yaratdığından, simmetrik kriptoqrafiya ilə müqayisədə müvafiq növ açarların şifrə kodu

daha uzundur. Bu hal açıq açardan qapalı açarı hesablamanı (xüsusilə daha uzun - 1024-dən 2048 bitə qədər olanlar üçün) çox çətinləşdirir. Hazırda istifadə olunan əsas asimmetrik şifrələmə alqoritmlərindən biri "RSA" (ilk dəfə 1977-ci ildə Rivest, Şamir və Adleman tərəfindən təsvir edilmişdir) alqoritmidir. "RSA" sxemində açarlar riyazi hesablamalardan əldə edilən moduldan istifadə olunmaqla yaradılır. Əsasən, modul iki açar yaradır: biri açıq, paylaşıla bilən, digəri isə məxfi saxlanılmalıdır. "RSA" alqoritmi açıq açar kriptoqrafik sistemlərinin əsas komponenti olaraq qalır.

Ümumilikdə blokçeyndə təklif olunan ideal kriptoqrafik şifrələmələrin aşağıdakı xarakterik xüsusiyyətləri mövcuddur:

- *Determinizm* - eyni qaydada daxil edilən məlumat eyni heş nəticə verməlidir.
- *Yüksək sürətlilik* - istənilən məlumat yüksək sürətlə heşə çevrilir.
- *Birtərəflilik* - əldə olunan heş nəticənin daxil edilməsi ilə ilkin məlumat müəyyən oluna bilinmir.
- *Lava effektinin olması* - daxil edilən məlumatda cüzi dəyişiklik nəticəsində heş nəticə tamamilə dəyişir.
- *Ziddiyyətin olmaması* - daxil edilən iki fərqli məlumata eyni bir bir heş nəticə verilmir.

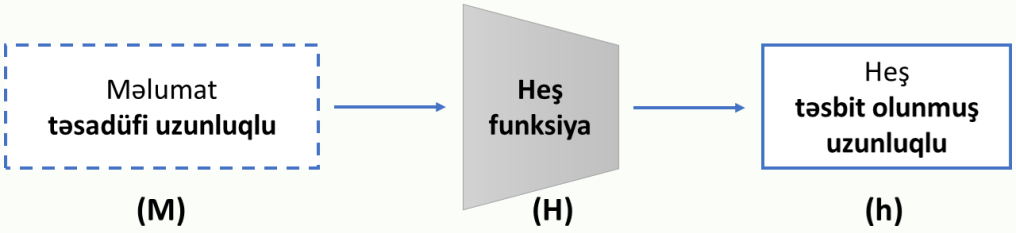
Beləliklə, açıq açar kriptoqrafiyası simmetrik alqoritmlərin çatışmazlıqlarından birini həll edir: bu, həm şifrələmə, həm də şifrənin açılması üçün istifadə olunan açarın ötürülməsi ilə bağlıdır. Müvafiq açarın etibar doğurmayan əlaqə üzərindən göndərilməsi riskli olmaqla, üçüncü tərəfin verilmiş açarla şifrələnmiş istənilən mesajı oxumasına imkan yarada bilər. Bu problemin həllini təmin edən mövcud kriptoqrafik üsullar (məsələn, Diffie-Hellman-Merkle açar mübadiləsi protokolu) hücumlara qarşı həssasdır. Açıq açar kriptoqrafiyasında isə əksinə, şifrələmə üçün istifadə olunan açar istənilən əlaqə üzərindən təhlükəsiz qaydada ötürülə bilər.

Beləliklə, simmetrik alqoritmlər ilə müqayisədə asimmetrik alqoritmlər daha yüksək səviyyədə qorunmanı təmin edir.

Heş funksiyalar. *Heş funksiyalar* – daha mühüm kriptoqrafik elementlərə aid olan və blokçeynin verilənlər strukturunun ayrılmaz tərkib hissəsini təşkil edən riyazi funksiyadır. Onlar rəqəmsal imzalar və məlumatın eyniləşdirmə kodları ("Message Authentication Code" – "MAC") kimi bir çox kriptoqrafik protokollarda və informasiya təhlükəsizliyi tətbiqlərində geniş istifadə olunur.

Kriptoqrafik heş funksiyalar – kriptoqrafiya üçün yararlı olan heş funksiyaların xüsusi bir sinfi olmaqla, giriş məlumatlarını təsadüfi uzunluğa dəyişən və təstib olunmuş uzunluqda olan çıxış məlumatları yaradan birtərəfli funksiyadır. Nəticə adətən, *heş-qiymət*, *heş-məbləğ* və ya *məlumat toplusu (daycest)* adlanır.

Ümumi şəkildə heş funksiyanı aşağıdakı kimi təsvir etmək olar:



Heş funksiyaların nəzərdə tutulmuş məqsədlərə xidmət etməsi və istifadəyə yararlı olması üçün onlar aşağıdakı əsas xüsusiyyətlərə malik olmalıdır:

- giriş məlumatları istənilən ölçülü istənilən sətir ola bilər, lakin çıxış məlumatları təsbit olunmuş uzunluğa – məsələn, 256 və ya 512 bitə malik olmalıdır;
- istənilən verilmiş məlumat üçün heş funksiya rasional şəkildə hesablanmalıdır;

- funksiya o mənada müəyyən olunandır ki, girişə eyni bir heş funksiya ilə verilmiş eyni ilkin məlumatlar hər dəfə eyni bir heş qiymət verə bilsin;
- məlumatın bütün mümkün variantlarının seçilməsi istisna olmaqla, məlumatın heş-qiymətindən istənilən üsulla ilkin məlumatı bərpa etməyin mümkün olmaması;
- məlumatda istənilən cüzi dəyişiklik çıxış heşinə güclü təsir göstərməlidir.

Qeyd olunan əsas xüsusiyyətlərdən əlavə, onlar kriptoqrafik protokol kimi nəzərdən keçirilməli olan təhlükəsizlik xüsusiyyətlərinə uyğun olmalıdır.

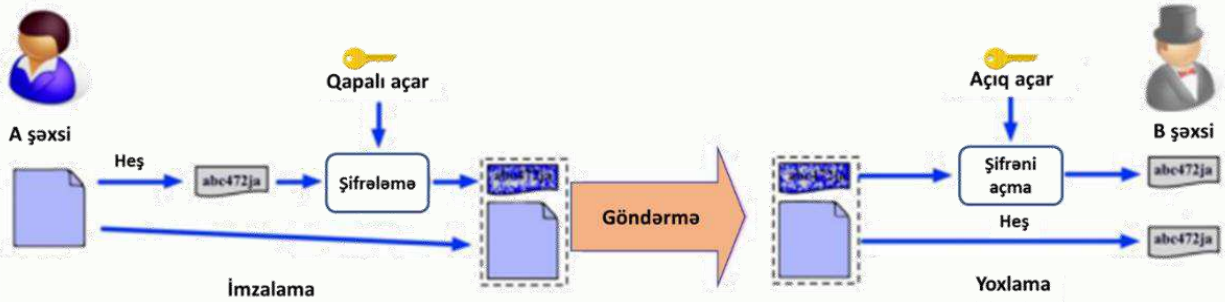
Assimetrik kriptoqrafiya vasitəsi ilə yanaşı blokçeyndə verilənlərin eyniləşdirilməsi məqsədilə **rəqəmsal imzalardan** da istifadə olunur.

Elektron rəqəmsal imza

Elektron rəqəmsal imza - imzalanacaq məlumatların kriptoqrafik alqoritmdən istifadə edilməklə təsdiqlənməsi və elektron sənədin müəllifliyini yoxlamaq üçün hazırlanmış bir bayt ardıcıllığıdır. Rəqəmsal imza əsasən mesajdakı məlumatlardan istifadə edərək yaradılan bir heş koddur. Bu mesaj göndərildikdə, alıcı mesajın mənşəyini yoxlamaq və onun dəyişdirilmədiyinə əmin olmaq üçün göndərənin açıq açarından istifadə edərək imzanı yoxlaya bilər. Bəzi hallarda rəqəmsal imza və şifrələmə birlikdə istifadə olunur, çünki heş kodun özü mesajın bir hissəsi kimi şifrələnə bilər (məsələn, "RSA" alqoritmi kimi). Qeyd etmək lazımdır ki, bütün rəqəmsal imza sxemləri şifrələmə metodundan istifadə etmir. Məsələn, "Bitcoin" və "Ethereum" əməliyyatları yoxlamaq üçün Elliptik Əyrili Rəqəmsal İmza Alqoritmi ("Elliptic Curve Digital Signature Algorithm" – "ECDSA") kimi tanınan xüsusi şifrədən istifadə edir.

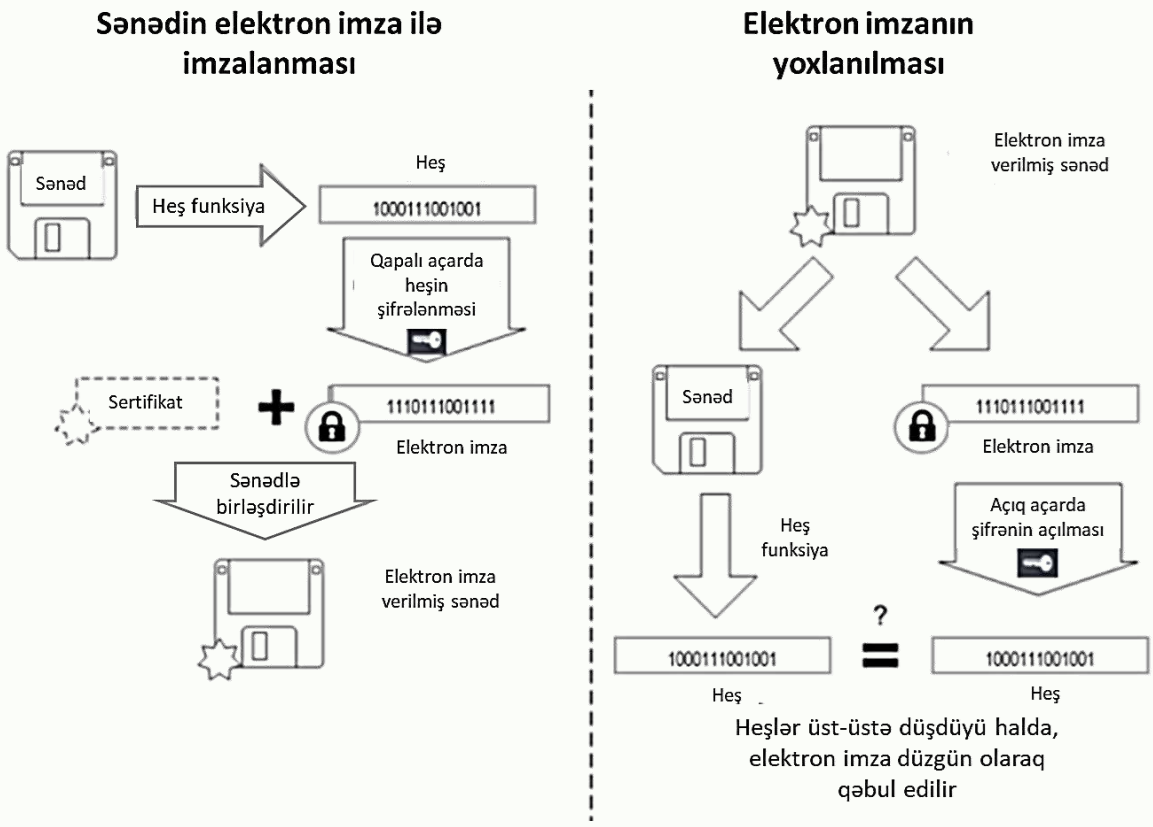
Blokçeyndə əməliyyat etmək üçün şəbəkə istifadəçisi bir cüt açara - açıq (ümumi) və qapalı (şəxsi) açara malik olmalıdır. Bu açarlar hər bir iştirakçının ünvanını formalaşdırır. Bir cüzdanda bir şəbəkə qovşağının *"n"* qədər ünvanı ola bilər. Vəsaitlər şəbəkə qovşağının açıq açarında görünür, lakin ondan istifadə etmək üçün o, müvafiq açıq açara bağlı olan qapalı açarı da bilməlidir. Şəbəkə qovşaqları açıq açarlardan vəsaiti qəbul etmək üçün istifadə edirlər. Açıq açarlar blokçeyn şəbəkəsinin hər bir istifadəçisi üçün əlçatandır.

Blokçeyn şəbəkəsində əməliyatın icra edilməsinə dair nümunə aşağıdakı şəkildə göstərilmişdir.



Köçürmə zamanı açıq açarda qeyd olunan hər hansısa bir dəyərin bir şəxsdən digər şəxsə ötürülməsi zamanı istifadə olunan qapalı açar rəqəmsal imza və nəticə etibarilə əməliyyatın ünvan sahibinin özü tərəfindən icra edilməsinin sübutu hesab olunur.

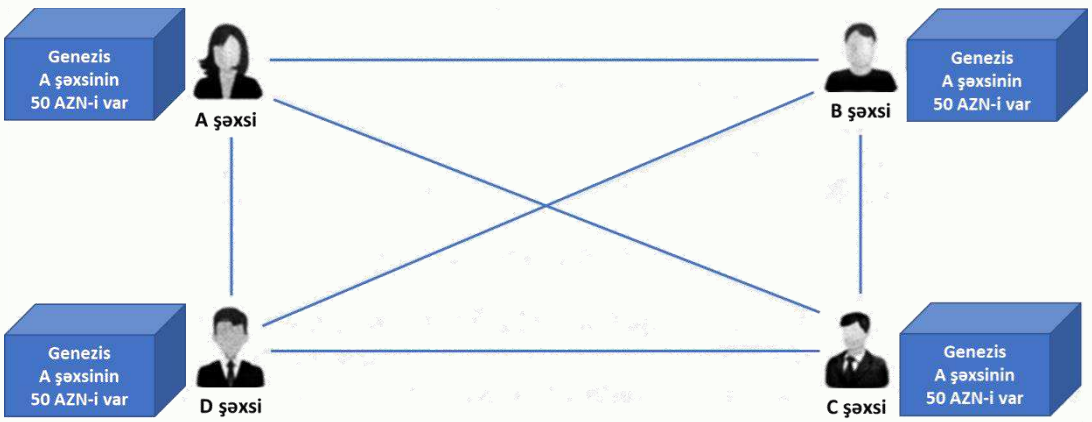
Elektron imzanın asimmetrik alqoritminin iş prinsipi



Blokçeyn sisteminin necə işlədiyini başa düşməkdən ötrü praktiki nümunəni nəzərdən keçirək və əməliyyatların necə baş verməsini, reyestrin necə yenilənməsini izləyək. Fərz edək ki, blokçeyn şəbəkəsində öz aralarında pul əməliyyatları aparan 3 iştirakçı – “A”, “B” və “C” şəxsləri mövcuddur. Blokçeynin açıq və əksmərkəzləşmiş funksiyalarının necə işləməsini başa düşmək üçün əməliyyatın yolu üzrə addım-addım izləmə aparaq.

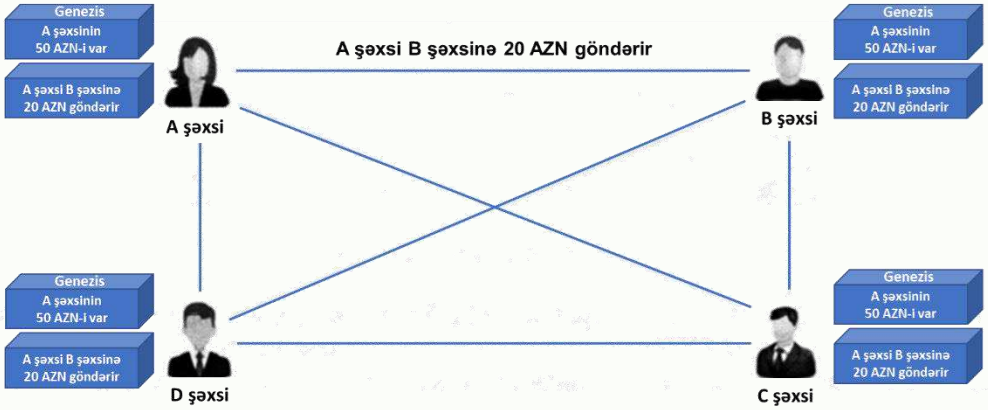
Addım 1

Fərz edək ki, “A” şəxsinin cüzdanında 50 manat var idi ki, bu da bütün əməliyyatların genezisini (başlanğıc nöqtəsini) təşkil edir və şəbəkənin hər bir qovşağı (“node”) da bunu bilir:



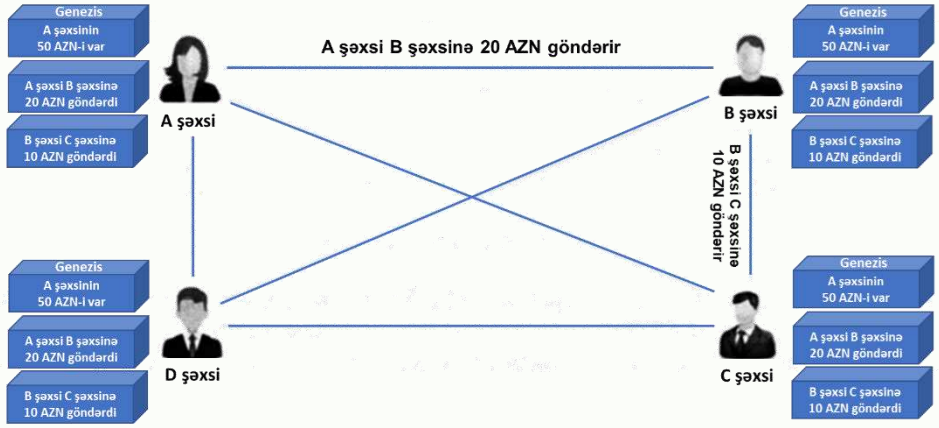
Addım 2

“A” şəxsi “B” şəxsinə 20 manat ödəməklə ilk əməliyyat həyata keçirir. Bu halda blokçeynin hər bir qovşaqda (“node”) yeniləndiyinə diqqət yetirin:



Addım 3

“B” şəxsi “C” şəxsinə 10 manat ödəməklə, “B” şəxsi digər əməliyyat (ikinci əməliyyat) həyata keçirir və blokçeyn bir daha yenilənir:



Bloklarda əməliyyatların məlumatları dəyişməz olaraq qalır. Bütün əməliyyatların tam olaraq geri dönüşü yoxdur. İstənilən dəyişmə yeni əməliyyatı doğurur ki, bu da bütün iştirakçılar tərəfindən təsdiqlənəcəkdir. Hər bir qovşağın (“node”) özünün blokçeyn surəti (nüsxəsi) vardır.

Konsensus alqoritmi və onun növləri

Hər bir açıq blokçeyn protokolunda konsensus alqoritmi yer almaqdadır. Qeyd olunduğu kimi, blokçeyndə şəbəkə qovşaqlarına iki növ məlumat ötürülür: əməliyyatlar və bloklar.

Əməliyyatlar sistem qovşaqlarının assimetrik şifrələmə metodlarından, açıq və qapalı açarlardan istifadə ilə icra edilir. Bu səbəbdən, bir əməliyyatın icrası üçün bütün şəbəkə qovşaqlarının razılıq verməsi heç bir əhəmiyyət kəsb etmir: məsələn, “bitcoin”lərin

göndərilməsinə başlamaq üçün heç bir razılaşmaya ehtiyac yoxdur, düzgün qapalı və açıq açarları bilmək kifayətdir. Lakin bir neçə əməliyyatların qruplaşdırılaraq blok şəklində blokçeynə əlavə edilməsi üçün ümumi razılığa gəlmək lazımdır. Bunu biz adi mağazalarda gün ərzində icra edilən əməliyyatlarla müqayisə edə bilərik. Məsələn, gün ərzində bir kassir bir sıra əməliyyat icra edir və bu əməliyyatları icra edən zaman iki şəxsin - kassir və alıcının iştirak etməsi kifayət edir. Lakin günün sonu hər bir kassirin icra etdiyi əməliyyatlar ilə kassada olan vəsaitlər tutuşdurulur və reyestr jurnala əlavə olunur. Bu prosesdə kassir ilə yanaşı, baş mühasib və rəhbərlik də iştirak edir. Yalnız gündəlik jurnal təsdiqləndikdən sonra, o, mağazanın yekun reyestrinə əlavə olunur. Müvafiq proses blokçeyndə də eyni qaydada aparılır, lakin burada aparılmış əməliyyyatları qrup şəklində bloka şəbəkə qovşaqları arasında olan validatorlar əlavə edirlər. Blokçeyndə müvafiq əməliyyatların blok şəklində hansı validator (qovşaq) tərəfindən blokçeynə əlavə edilməsinə vahid bir yanaşma tələb olunur. Blokçeyn protokolu daxilində qəbul edilmiş belə vahid yanaşmanı *konsensus alqoritmləri* təmin edir.

Konsensus alqoritmi - qrupdakı fərdlər (qovşaqlar) üçün ən uyğun qərarı formalaşdıran və dəstəkləyən qərar qəbul etmə prosesidir. Bu, konsensus alqoritminin texniki tərifidir. Sadə dillə desək, bu yalnız müəyyən qrup daxilində əvvəlcədən razılaşdırılmış metodologiya əsasında qərar qəbul etmə üsuludur.

Konsensusa gəlinməsi ilkin olaraq şəbəkə qovşaqlarının mümkün ola biləcək ikiqat xərcləməsinin qarşısının alınması məqsədilə istifadə olunur. Məsələn, Aişənin yalnız 1 “bitcoin”i var. O, eyni bitkoyni bir əməliyyatla Fəridə, digər əməliyyatla isə Səmədə göndərə bilər. Fərid və Səməd isə əməliyyat çıxarışlarını hər-hansı bir şəkildə uyğunlaşdırmasını aparmasalar, onların hər ikisi Aişənin ödənişini qəbul edəcəkdir. Buna səbəb əməliyyatların Aişənin elektron imzası ilə imzalanması və onun əməliyyat baş verməmişdən əvvəl müvafiq “bitcoin”ə sahib olması idi. Məhz bu səbəbdən də şəbəkə qovşaqları blokçeyndəki bütün əməliyyatları bir-biri ilə uyğunlaşdırmalıdır ki, eyni vəsaitin iki şəxsə göndərilməsinin qarşısı alınsın.

Konsensus alqoritmi vasitəsi ilə validatorlar Aişə tərəfindən göndərilmiş yalnız bir əməliyyatı təsdiqləyəcək, digərini isə yanlış əməliyyat kimi qəbul edəcəklər. Lakin digər mümkün bir ehtimal kimi validatorla Aişə arasında razılığın olması əsasında validatorun hər iki əməliyyatı təsdiqləyə bilməsidir. Belə halların qarşısının alınması validator tərəfindən təsdiqlənmiş əməliyyatın digər validatorlar tərəfindən də yoxlanılması ilə mümkün olur. Bu, hər bir qovşağın bütün əməliyyatlar barədə məlumatlılığını təmin etməklə mümkündür. Lakin bunun tətbiqi digər maraqlı sualı ortaya çıxarır. Hər bir qovşaq tərəfindən əməliyyatların bazası saxlanıldığı (dəstəkləndiyi) halda, onlar verilənlər bazasının ümumi vəziyyətini necə razılaşdıra bilərlər? Bir və ya bir neçə hesablama qovşağının bilərəkdən sistemi sarsıtmağa çalışdığı və verilənlər bazasının saxta vəziyyətini tətbiq etməyə cəhd etdiyi zaman sistem belə vəziyyətlərə necə qeyri-həssas qala bilər? Açıq blokçeynlərdə istifadə variantından asılı olaraq, qovşaqlar arasında konsensusa nail olunmasının müxtəlif üsulları tətbiq edilə bilər.

Blokçeynin təhlükəsizliyi və etibarlılığı məhz konsensus səviyyəsində formalaşır. Açıq blokçeynlərdə etibarlılıq və təhlükəsizliyə nail olmaq üçün **Bizans səhv tolerantlığından (“Byzantine Fault Tolerance”)** istifadə olunur. Bu həmçinin **Bizans generalları problemi** kimi də adlandırılır.

Bizans generalları problemi daha uzun müddət əvvəl məlum olsa da, blokçeyndə istifadə olunduqdan sonra daha da tanındı. Bizans generalları problemi Bizans ordusunun şəhərə hücumu zamanı qarşılaşdıqları qeyri-müəyyən vəziyyətlər və onların gedişi əsasında meydana çıxmışdır. Ümumilikdə problem sadədir, lakin onun həlli mürəkkəbdir. Bizans generalları problemini xülasə şəklində aşağıdakı kimi ifadə etmək olar.

Ayrı-ayrı generalların başçılıq etdiyi bir neçə ordu qruplaşması şəhəri götürmək üçün mühasirəyə alırlar. Qələbə üçün yeganə şans – bütün generalların şəhərə birlikdə hücum etməsinin baş verməsidir. Burada əsas məsələ qələbənin təmin edilməsi üçün bütün generalların müvafiq məsələdə konsensusu necə təmin etməsindən ibarətdir. Bu o deməkdir ki, ya bütün generallar hücum etməli, yaxud da onların hamısı geri çəkilməlidir. Əgər onlardan bəziləri hücum etdiyi halda, digərləri geri çəkilsə, onlar böyük ehtimalla döyüşü uduzacaqlar.

Vəziyyəti daha yaxşı başa düşməkdən ötrü onu konkret nümunədə nəzərdən keçirək. Fərz edək ki, şəhərə bizans ordusunun 5 qrupu yaxınlaşmışdır. Əgər beş generaldan heç olmasa üçü hücum etmək tərəfdarı olarsa, onlar şəhərə hücum edəcək, əks halda geri çəkiləcəklər. Generallar arasında satqın generalın olması ehtimalı da mümkündür. Həmin general hücum etmək istəyən generallarla hücum üçün səs verə, yaxud geri çəkilmək istəyən generallarla geri çəkilmək üçün səs verə bilər. Müvafiq halda o, belə hərəkət edə bilər, çünki ordu qruplar şəklində cəmləşib ki, bu da onların mərkəzləşdirilmiş koordinasiyasını çətinləşdirir. Əlaqələndirmənin çətinliyi isə yalnız iki generalın şəhərə hücum etməsinə və say baxımından üstünlüyü əldən verərək döyüşü uduzmalarına səbəb ola bilər. Bu vəziyyətdə daha mürəkkəb problemlər də meydana çıxa bilər:

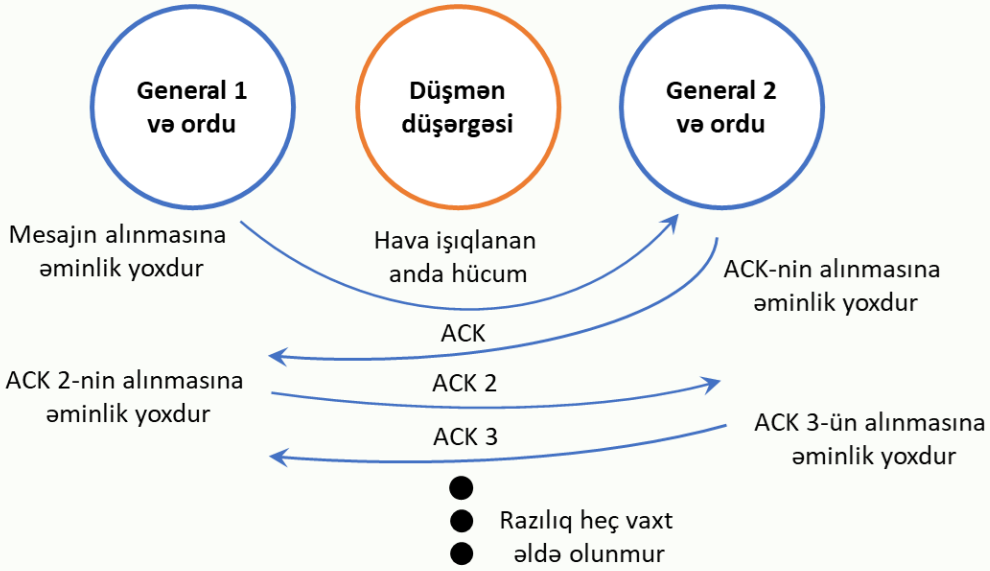
- birdən çox satqın olarsa, vəziyyət necə olar?
- generallar arasında məlumatların koordinasiyası necə həyata keçiriləcəkdir?
- generallar tərəfindən məlumatın həvalə edildiyi elçi şəhər qarnizon komandiri tərəfindən tutulduğu/öldürüldüy/ələ alındığı halda vəziyyət necə olacaq?
- satqın general xəbəri saxtalaşdırıb digər generalları aldadarsa, vəziyyət necə olar?
- generallardan hansılarının sədaqətli, hansılarının isə satqın olduğunu necə məyyən etməli?

Göründüyü kimi, şəhərə əlaqələndirilmiş şəkildə hücumun təşkil olunması üçün çoxsaylı məsələləri həll etmək lazım gəlir.

İlk dəfə 1975-ci ildə nəşr olunmuş (1978-ci ildə isə hazırkı adı ilə adlanıb) bu məsələ iki generalın ümumi düşmənə qarşı hücuma keçdiyi ssenarini təsvir etmişdir. General 1 lider, General 2 isə davamçı hesab olunur. Düşmən ordusuna uğurlu qələbə çalmaq üçün ayrılıqda hər bir generalın ordusu kifayət etmir, bu səbəbdən də onların əməkdaşlıq etməsi və eyni vaxtda hücuma keçməsi zəruridir. Bu sadə ssenari kimi görünür, lakin onların rabitə yaratması və uyğun zaman seçmələri məqsədilə General 2-yə hücum vaxtını xəbər verməkdən ötrü General 1 düşmən düşərgəsindən keçib gedən bir elçi göndərməlidir. Lakin elçinin düşmənlər tərəfindən tutulacağı və nəticədə xəbərin çatdılmayacağı ehtimalı da mövcuddur. Bu isə General 2 və onun ordusunun öz mövqelərini saxladığı halda (məlumatsız qalmaları səbəbindən), General 1-in təkbaşına hücuma keçməsinə gətirib çıxaracaqdır.

Hətta əgər birinci xəbər çatdırılsa belə, General 2 məlumatı aldığını təsdiq etməli (“ACK”, “TCP” protokoluna uyğunluğa diqqət edin) olduğundan, o, elçini geriyə göndərir, beləliklə də əvvəlki ssenari bu halda da təkrarlana bilər (yəni elçi ələ keçə bilər). Bu sonsuz sayda *təsdiq etmələrə (“ACK”)* genişlənə və bu səbəbdən də generallar razılığa gələ bilməzlər.

Hücum planına digər generalın razılaşdığına hər bir generalın əmin olması kimi ikinci tələbi təmin etmək mümkün deyildir. Hər iki general onların sonuncu elçilərinin düşmən düşərgəsini keçib-keçməməsini həmişə təxmin edəcəklər.



Xəbərin qarşı tərəfə çatmama ehtimalı həmişə 0-dan böyük olduğundan, generallar heç bir halda 100% əminliklə razılıq əldə edə bilməyəcəklər.

Əsasən açıq blokçeynlərdə bu kimi problemlərin aradan qaldırılması üçün blokçeyn protokollarda oyun nəzəriyyəsindən istifadə edirlər.

Oyun nəzəriyyəsi sosial iqtisadi problemlərin araşdırılması zamanı rəsmi olaraq Con fon Neyman tərəfindən təqdim olunmuşdur. Daha sonralar oyun nəzəriyyəsi "Neş tarazlığı" nəzəriyyəsi sayəsində Con Forbs Neş (kiçik) tərəfindən məhşurlaşdırılmışdır.

Oyun nəzəriyyəsi. *Oyun nəzəriyyəsi* – iki və ya daha çox tərəfin strateji davranışa cəlb olunduğu vəziyyətdir. Oyunlara nümunə olaraq, idman növü üzrə turnir, dondurma uğrunda mübarizə aparan qardaş və bacı, siyasi seçkilər, işıqforun işığı, məhkəmədə münaqişə tərəfləri və sairi göstərmək olar.

Bir konsepsiya olaraq oyun nəzəriyyəsi əsasında bir çox real vəziyyətlərdə mürəkkəb məsələlər həll olunur. Real həyatda qərarların böyük hissəsi müxtəlif tərəflərin davranışlarının öyrənilməsinə əsaslanır, oyun nəzəriyyəsi isə rasional qərar qəbulu üçün əsasları təmin edir.

Fərz edək ki, siz blokçeyn tətbiqinin hazırlayıcısı vəzifəsinə ərizə vermisiniz, sizin namizədliyiniz seçilir və sizə müəyyən əmək haqqılı iş təklif olunur, lakin siz tələb və təklifin böyük olduğunu və işəgötürənin təklifə yenidən baxaraq əmək haqqını artıracağını ehtimal edərək təklifi rədd edirsiniz. Siz bunun oyun olmadığını fikirləşə bilərsiniz. Lakin real vəziyyətlərdə bizim ətrafımızda olan hər bir şey oyundur. Beləliklə, *oyun - korrelyasiya olunan rasional seçimi* nəzərdə tutan vəziyyət kimi müəyyən oluna bilər. Bu o deməkdir ki, istənilən oyunçu üçün əlçatan olan perspektivlər təkcə öz seçimindən deyil, eləcə də verilmiş vəziyyətdə digər oyunçuların etdiyi seçimdən də asılıdır. Digər sözlə, əgər digər şəxslərin hərəkəti (fəaliyyəti) sizin taleyinizə təsir edirsə, deməli, siz oyundasınız.

Oyun nəzəriyyəsi – mürəkkəb oyunlarda istifadə olunan strategiyaların öyrənilməsidir. Bu, hər hansı vəziyyətdə məqsədə çatmaqdan ötrü yaxşı gediş etmək və ya yaxşı strategiyanı seçmək məharətidir. Bunun üçün rəqibin strategiyasını, eləcə də rəqibin fikrincə sizin mümkün gedişinizi başa düşmək lazımdır. Sadə bir nümunə göstərək: iki doğma qardaş vardır - böyük və kiçik qardaş. Fərz edək ki, soyuducuda iki növ dondurma vardır: biri portağal dadlı, digəri manqo ətirli. Böyük qardaş portağallı dondurmanı yemək istəyir, lakin bilir ki, əgər o, bu seçimi etsə, kiçik qardaş ağlayacaq və məhz portağallı dondurmanı tələb edəcəkdir. Bu səbəbdən, o, manqo ətirli dondurmanı seçir və gözlənildiyi kimi, kiçik qardaş da eynisini istəyir. Sonra böyük qardaş manqo ətirli

dondurmanı ona qurban etdiyi görünüşü yaradır, onu kiçik qardaşa verir və özü portağallı dondurmanı yeyir (istədiyi kimi). Vəziyyətə diqqət yetirin: bu hər iki tərəf üçün qazanclı variantdır, belə ki, böyük qardaşın məqsədi məhz portağallı dondurma idi. Əgər böyük qardaş sadə strategiya seçsə idi, o, kiçik qardaşı ilə dava edə və arzu etdiyini əldə edə də bilərdi. İkinci halda böyük qardaş kiçik qardaşın xəsarət almaması üçün harasına və nə dərəcədə güclü zərbə vurmasını müəyyən etməli idi, lakin o, portağallı dondurmadan imtina etdi. Oyun nəzəriyyəsinin məsələsi belədir: sizin məqsəd nədən ibarətdir və sizin yaxşı gedişiniz necə olmalıdır?

Digər bir nümunəni biznes sahəsindən gətirək. Təsəvvür edin ki, siz şəhərə tərəvəz tədarük edən satıcısınız. Fərz edək ki, şəhərə gedib çatmağın 3 üsulu mövcuddur ki, onlardan da biri ehtimal ki, qısa və yaxşı olduğu üçün hamının getdiyi adi marşrutdur. Bir dəfə siz görürsünüz ki, həmin yol təmir işlərinə görə bağlanıb və siz heç bir şəkildə həmin yol ilə gedə bilmirsiniz. İndi sizin iki digər yolunuz qalmışdır. Onlardan biri qısadır, lakin dar yoldur. Digəri daha uzundur, lakin kifayət qədər geniş yoldur. Burada siz gedilməsi lazım olan yolun seçim strategiyasını hazırlamalısınız. Vəziyyət elə ola bilər ki, yollarda intensiz hərəkət olsun və bir çoxları ən qısa marşrut ilə getmək istəsin. Bu dar hissələrdə güclü sıxlığa gətirib çıxara və böyük ləngimə yarada bilər. Beləliklə, siz yanacağa sərf olunmuş bir qədər əlavə vəsait hesabına şəhərə vaxtında çatmanı sığortalamaq üçün daha uzun yolu seçmək qərarı verirsiniz. Siz vaxtında çatdığınız və öz tərəvəzlərinizi başqalarından əvvəl yaxşı qiymətə satdığınız halda xərclərinizi asanlıqla kompensasiya ed biləcəyinizə əminsiniz. Bu da oyun nəzəriyyəsidir: adətən, optimal qərar axtarışından ibarət olan, qarşıya qoyulan məqsədə daha yaxşı necə nail olunması məsələsi.

Yuxarıda verilmiş nümunələrə əsasən, demək olar ki, oyun nəzəriyyəsi – real həyat vəziyyətlərinin oyun formasında modelləşdirilməsi metodu və arzu olunan nəticəyə nail olmaqdan ötrü bu və ya digər vəziyyətdə şəxsin və ya təşkilatın ən yaxşı strategiyası və ya hərəkətinin hansı olmasının təhlilidir. Oyun nəzəriyyəsindən irəli gələn konsepsiyalardan praktiki olaraq həyatın bütün aspektlərində (siyasət, sosial şəbəkələr, şəhər planlaması, sövdələşmələr, marketinq, paylanan hesablama və s.) geniş istifadə olunur. Oyun nəzəriyyəsi etibarlı qərarlar qəbul etməkdə və onları müxtəlif maraqlı ssenarilər ilə testdən keçirməkdə yardım edə bilər.

Blokçeyn protokollarda oyun nəzəriyyəsi sistemin davranışının müəyyən edilməsinə tamamilə yeni bir yanaşmanı irəli sürür. Oyun nəzəriyyəsinin metodları ən sərt üsullardır. Adətən, onlar qovşağın düzgün, bədniyyətli, etikalı olmasını və ya hər hansı digər oxşar xarakteristikalara malik olmasını heç vaxt nəzərə almır və yalnız iştirakçıların əldə etdiyi faydalara uyğun şəkildə fəaliyyət göstərdiyini və mənəvi qərəzlərə tabe olmadığını qəbul edir. Blokçeyndə oyun nəzəriyyəsinin yeganə məqsədi iştirakçılar arasında konsensus yaratmaqla sistemin stabilliyini, yəni *Neş tarazlığını* təmin etməkdir.

Oyun nəzəriyyəsində əgər siz başqa oyunçuların strategiyalarını bilirsinizsə və sizin öz strategiyanız mövcuddursa, lakin öz strategiyanızı dəyişməklə qazancı artıra bilmirsinizsə - bu vəziyyət *Neş tarazlığı* adlanır. Beləliklə, Neş tarazlığında hər bir strategiya verilmiş tarazlıqdakı bütün digər strategiyalara ən yaxşı cavabdır. Burada diqqət yetiriləsi məqam ondan ibarətdir ki, oyun nəzəriyyəsində oyunçu özünə fayda əldə etməsi üçün strategiya hazırlaya bilər, lakin rəqibə maksimum zərər verməyə çalışmaqla qalib gələ bilməz. Bundan əlavə, təkrar oynanılan istənilən oyun son nəticədə Neş tarazlığına düşə bilər (bir çox oyunlar Neş tarazlığı tapılanadək başa çatır. Oyunun təkrarlanması bütün oyunçular tərəfindən optimal strategiyanın hazırlanmasnı sürətləndirir). Neş tarazlığının praktiki təsvirini əldə etmək üçün *məhbus dilemmasını* konkret nümunə əsasında nəzərdən keçirək.

Məhbus dilemması. Fərz edək polislər “A” və “B” şəxslərini müxtəlif yerlərdə bir-birindən asılı olmayaraq narkotik satışı üstündə tutmuşlar. Onlar dindirilmək üçün iki

müxtəlif kameralarda saxlanılır və bu cinayət üçün onlara 2 il həbs cəzasının veriləcəyini bildirirlər. Lakin bir qədər sonra polislər keçən həftə baş vermiş oğurluq hadisəsində bu iki şəxsin də əlinin ola bildiyinə şübhələndilər. Lakin onlar oğurluq etməsələr belə, onsuz da 2 il azadlıqdan məhrum olunacaqlar.

Polislər həqiqəti üzə çıxarmaqdan ötrü strategiya hazırlamalıdırlar. Bu məqsədlə polislər "A" şəxsinin yanına gedərək ona belə bir yaxşı seçim imkanı verirlər: əgər "A" şəxsi törətdiyi cinayəti etiraf etsə, "B" şəxsi isə bunu etməsə, bu halda "A" şəxsinin cəzası iki ildən 1 ilədək azaldılacaq, "B" şəxsi isə 5 il iş alacaq. Əgər əksinə olsa, yəni "B" şəxsi cinayət törətdiyini etiraf etsə, "A" şəxsi isə etməsə, bu halda B şəxsi 1 il, "A" şəxsi isə 5 il həbs cəzası alacaqdır. Bundan əlavə, hər iki şəxs törətdiyi cinayəti etiraf etsə, bu halda hər biri 3 il azadlıqdan məhrum olunma cəzası alacaqdır. Eyni seçim imkanı "B" şəxsinə də verilir. Verilmiş şərtlərdə şəxslərin seçim qərarları təhlil olunur. Təsvir olunan vəziyyət *məhbus dilemması* adlanır.

Hər iki şəxs müxtəlif kamerada yerləşir. Onlar bir-biri ilə danışa bilmir və verilmiş vəziyyətdə qlobal optimum kimi görünən - onların hər ikisinin oğurluqda iştiraklarını inkar etdikləri və hər ikisinin 2 il həbs aldıqları (yalnız narkotiklərlə ticarət üçün) strategiya barədə razılığa gəlmə imkanları mövcud deyildir. Lakin hətta onların bir-biri ilə danışma imkanları olsaydı belə, onlar bir-birilərinə etibar etməyə də bilərlər.

A şəxsinin (eynilə B şəxsinin də) 2 variantı vardır: oğurluqda iştirakını etiraf etmək və ya inkar etmək. O bilir ki, "B" şəxsi özü üçün sərf edən variantı seçəcək və o da "B" şəxsindən heç bir şeylə fərqlənmir (düşdüyü hal baxımından). Əgər "A" şəxsi günahını inkar etsə, "B" şəxsi isə əksinə, etiraf etsə, bu halda "A" şəxsini 5 il həbs, "B" şəxsini isə cəmi 1 il həbs gözləyir. Təbii ki, "A" şəxsi bu vəziyyətə düşmək istəmir. Əgər "A" şəxsi etiraf etsə, onda "B" şəxsinin iki variantı olur: etiraf etmək və ya inkar etmək. "A" şəxsinin etiraf etdiyi halda "B" şəxsinin hansı variantı seçməsindən asılı olmayaraq, ona 3 ildən artıq cəza verməyəcəklər. Beləliklə, "A" şəxsi üçün mümkün ssenarilər aşağıdakılar olacaqdır:

- "A" şəxsi etiraf edir, "B" şəxsi isə inkar edir: "A" şəxsi 1 il, "B" şəxsi isə 5 il həbs cəzası alır ("A" şəxsinin etiraf etdiyini nəzərə alsaq, bu hal "A" şəxsi üçün ən yaxşı haldır);
- "A" və "B" şəxsi hər ikisi etiraf edir: hər ikisi 3 il iş alır ("A" şəxsinin etiraf etdiyini nəzərə alaraq, ən pis halda).

Digər tərəfin seçimini nəzərə alaraq, hər bir tərəfin ən yaxşı gediş etdiyi halda, bu vəziyyət *Neş tarazlığı* adlanır. Bu hal aşkar olaraq qlobal optimum olmasa da, ayrılıqda hər bir şəxs üçün optimal seçimdir. Əgər siz bu vəziyyətə kənardan baxsanız, hər iki şəxsin oğurluğu inkar etməli və 2 il cəza almalı olduğunu deyəcəksiniz. Lakin siz özünüz oyun iştirakçısı olduğunuz halda, Neş tarazlığı – son nəticədə sizin düşdüyünüz haldır. Diqqət yetirmək lazımdır ki, Neş tarazlığı - qərarın dəyişilməsinin sizə heç bir fayda vermədiyi daha stabil vəziyyətdir. Onu əyani olaraq uduşlar matrisi şəklində təsvir etmək olar.

		B şəxsi: Etiraf	B şəxsi: İnkar
A şəxsi	Etiraf	**3** / **3**	1 / 5
A şəxsi	İnkar	5 / 1	2 / 2

Bizans səhv tolerantlığının (bizans generalları probleminin) olmadığı halda eyniranqlı qovşaq blokların zəncirinin etibarlılığını effektiv olaraq aradan qaldırmaqla,

səhv əməliyyatları ötürə və yayımlaya bilər. Bu isə daha pisdir, belə ki, zərəri öz üzərinə götürüb aradan qaldıra biləcək mərkəzi orqan mövcud deyildir.

Beləliklə, Bizans generalları probleminin blokçeyn şəbəkələrdə istifadəsi validatorların dələduzluq və manipulyasiya cəhdlərinin qarşısının alınması üçün validatorların yarısından çoxunun ən azı düzgün qərar verməsini tələb edir. Riyazi elementlərdən istifadə etməklə blokçeyn protokollarda konsensus əldə olunmasına nail olmaq mümkündür.

Blokçeyn protokoldan asılı olaraq Bizans generalları probleminin həlli üçün müxtəlif həllər (konsensus protokolları) təklif olunur. Belə həllərə nümunə olaraq “Proof of Work” (PoW), “Proof of Stake” (PoS), “Delegated Proof of Stake” (DPoS), “Proof of Activity” (PoA) və s.-i göstərmək olar.

“Proof of Work” (“PoW”, işin sübutu) **konsensus protokolu** ən resurstutumlu protokollarından biridir. Paylanmış sistemlərin kənar hücumlardan və sui-istifadə hallarından qorunması üçün istifadə olunan ən məşhur bir alqoritmdir (“DoS” hücumları, ikiqat xərc, spam poçtları və s.).

“PoW” protokolunda əməliyyatların təsdiqlənməsi və yeni blokların yaradılması üzrə validator funksiyasını mayninq qovşaqları yerinə yetirir. Onlar blokun formalaşdırılması üçün riyazi hesablamaları aparır və nəticəni blokçeyndə bütün qovşaqlarla bölüşürlər. Hesablamaların aparılması üçün lazım olan əsas meyar mayninq qovşağı tərəfindən istifadə olunan kompüter cihazının güc göstəricisidir.

“Proof of Work” konsepsiyası ilk dəfə 1993-cü ildə Cynthia Dwork və Moni Naor tərəfindən izah edilmişdir. Müəlliflər aşağıdakı fikri irəli sürmüşlər: “Paylanmış bir mənbəyə giriş əldə etmək üçün istifadəçi olduqca mürəkkəb, lakin icrası mümkün olan bəzi hesablamaları həll etməlidir. Şəbəkə bu şəkildə kənar hücumlardan qoruna bilər”.

1997-ci ildə Adam Bek spamlardan müdafiə məqsədilə “Hashcash” (heşkeş) layihəsini başlatdı. Layihədə tapşırıq belə tərtib edilmişdir: “Elə bir x nəticəni tapmaq lazımdır ki, SHA (x) öz daxilində *n* sayda sıfırlanmış bit olsun (yəni heş nəticənin önündə b sayda sıfırlar olsun)”. Sistem e-poçtla göndərilən məktublarda qismən də olsa şifrələməni təmin edirdi. Göndərilən hər e-mail-də başlığın hesablanması üçün hər dəfə 252 sayda heş hesablanması lazım gəlirdi. Bu hesablamalar bir neçə adi məktubun göndərilməsi üçün maneə yaratmasa da, davamlı şəkildə spam göndərişləri üçün böyük hesablamalar tələb edirdi. Təklif olunan həll “SHA-1” hesablama sistemindən istifadə etməklə funksiyanın heş kodunun hesablanmasını çox sürətlə yoxlamağa imkan verirdi.

“Proof of Work” (“PoW”) termini ilk dəfə 1999-cu ildə Markus Jacobsson və Ari Juels tərəfindən istifadə edilmişdir. “bitcoin” şəbəkəsində konsensusa çatmaq üçün bir vasitə olaraq “PoW”dan istifadə edilmişdir (blok zəncirinin düzgün hesab edildiyi bir konsensus). Satoşi Nakamoto qeyd olunan “Hashcash” (heşkeş) layihəsinin əsasını götürərək ona fərqli bir mürəkkəblik mexanizmi əlavə etmişdir.

Paylanan mühitdə *“nonce”* adlanan təsadüfi ardıcıllıqlardan istifadə edərək bütün qovşaqlar kriptoqrafik heş funksiyadan (məsələn, “SHA-256”) istifadə edilməklə fasiləsiz olaraq blokun heş qiymətini hesablayırlar.

Heşin məqsədli qiymətini əldə etdikdən sonra qalan iştirakçıların heşin düzgünlüyünü qarşılıqlı olaraq təsdiqləməsi lazımdır. Heşin hesablanması əməktutumlu proses olduğundan, burada stimullaşdırma mexanizmi tətbiq olunur, məsələn, “bitcoin” şəbəkəsində qovşaq əməliyyatların təsdiqinə və onların bloka birinci əlavə etməsinə görə bloku yaradan ilk mayner mükafat qismində kriptovalyutanın müəyyən hissəsini əldə edir. Bu prosesə *mayninq* deyilir.

Proses olaraq mexanizm mövcud mürəkkəblik səviyyəsi üzrə blok başlığına uyğun heş kodun tapılması cəhdlərini əhatə edir. Bu hesablamaların mürəkkəbliyi onların yalnız xüsusi hesablamalara imkan verən texnologiyalardan istifadə edilməklə aparılmasına

səbəb olsa da, müvafiq hesablamaların nəticələrinin yoxlanılması sadə bir prosesdir. Şəbəkə iştirakçıları qovşağın həmişə doğru dəyəri tapdığına əmin ola bilər, lakin hər hansı bir blokun tapılması prosesi çox zəhmətli və təsadüfi proses olduğundan, hansı konsensus qovşağının yeni blokun yaradılması üçün müvafiq alqoritmik hesablamaların daha tez həll edəcəyi və bloku tapacağını dəqiqliklə təxmin etmək mümkün deyildir. Sistemdə hər hansı bir blokun etibarlı olaraq tanınması üçün onun heş dəyərinin nəticəsi cari mürəkəbblik hədəfinin nəticəsindən az olmalıdır. Hər bir yeni blok ondan əvvəlki blokun heşini özündə saxlayaraq bir zəncir meydana gətirir. Bloku dəyişdirmək mümkün deyildir, yalnız eyni səviyyədə olan əvvəlki blokun heş dəyəri ilə bağlı bir blok yaratmaq mümkündür. Müvafiq prosesi həyata keçirmək üçün isə əvvəlki bütün blokları tapmaq və hər biri üzrə heşlərin tapılması üçün iş görmək lazım gəlir. Belə yanaşma prosesin mürəkkəbliyini artırmaqla, blokçeyn sistemini icazəsiz giriş və ikiqat xərclərdən qoruyur.

Beləliklə, “PoW” konsensus alqoritminin mahiyyəti iki əsas prinsipə söykənir:

- müəyyən səviyyədə mürəkkəb və uzun bir tapşırığın yerinə yetirilməsi imkanı;
- nəticənin tez və asanlıqla yoxlanılması imkanı.

“PoW” konsensus alqoritmi “Bitcoin”, “Ethereum” və “Litecoin” kimi kriptovalyutaların protokollarında istifadə olunur. Lakin müvafiq alqoritmin mənfi xüsusiyyətləri də mövcuddur. Texnologiya “bitcoin” protokolunda konsensus qovşağı (mayninq) sahəsini meydana gətirmişdir. Müvafiq sahənin yüksək gəlir vəd etməsi və yüksək həcmdə elektrik enerjisi istehlakını tələb etməsi “PoW” texnologiyasından istifadə edən bir çox ölkələrdə elektrik enerjisi ilə təhcizatlarda problemlər yaranmağa başlamışdır.

Bu kimi hallar isə digər konsensus alqoritmlərinin yaranmasına səbəb olmuşdur.

“Proof of Stake” (“PoS”) konsensus protokolu. 2012-ci ildə ilk dəfə “PoW”ya alternativ konsensus alqoritmi kimi təqdim edilmişdir. “PPCoin” kriptovalyutasında (hazırda “PeerCoin” kimi tanınır) hibrid sistemdən - “PoW” və “PoS” alqoritmlərindən birgə istifadə edirdi. “PoS” sisteminin əsas prinsipi növbəti blokun yaradılması hüququnun etibar edildiyi konkret şəbəkə iştirakçısının müəyyən olunmasıdır. “PoW”-də olduğu kimi “PoS” alqoritmində də qovşaqlar müəyyən bir bloklardan nəticə çıxararaq heş hesablamalıdılar, lakin “PoW”-dan fərqli olaraq bu sistemdə daha tez nəticə əldə edilməsi ehtimalı şəbəkə istifadəçisinin müəyyən dövr üçün dondurulmuş aktiv payının (tokenə) həcminə sahib olması ilə müəyyən edilir. Beləliklə, müvafiq şəbəkədə daha çox aktivə (dondudurlmuş tokenə) malik olan şəxs növbəti blokun yaradılması üçün daha böyük imkana (ehtimalına) malik olur. Müvafiq protokol ilk növbədə hesablama avadanlıqlarına qarşı böyük tələblər müəyyən etmədiyindən və işin görülməsi üçün əlavə mürəkkəb resursların xərclənməsinə ehtiyac yaratmadığından cəlbedici görünür.

“PoS” alqoritmindən istifadənin lehinə və əleyhinə müxtəlif arqumentlər irəli sürülür.

Lehinə olan əsas arqument hücum üçün əhəmiyyətli həcmdə vəsaitin tələb olunması ilə bağlıdır ki, bu da onu maliyyə baxımından lemək olar ki, mümkünsüz edir. Eyni zamanda, əlində çox sayda token cəmləşmiş təcavüzkarın özü hücumdan əziyyət çəkəcəkdir, çünki bu, kripto valyutanın sabitliyini pozacaqdır.

Əleyhinə olan arqumentlər aşağıdakılardır:

- “PoS” şəbəkə iştirakçılarına vəsait toplanması üçün əlavə motivasiyanı təmin edir ki, bu da şəbəkənin mərkəziləşdirilməsi ilə nəticələnə bilər;
- Kifayət qədər böyük vəsait toplamış kiçik bir qrupun yarandığı halda, müvafiq qrupa daxil olan şəxslər şəbəkənin digər iştirakçılarını özlərinin müəyyən etdiyi qaydalara əməl etməyə məcbur edə bilərlər.
- Blokçeyn sistemindən istifadə edən bir çox şəxslər tərəfindən “PoS” sistemləri qeyri-sabit bir mexanizm kimi xarakterizə olunur. Buna səbəb sistemə hücüm edən şəxslər tərəfindən “mövcud olmayan” mənbələr əsasında blokların (əlavə *çəngəllər* – növbəti bölmədə bu barədə ətraflı məlumat veriləcək) yaradılması üzrə manipulyasiyalar

ilə daha uzun alternativ zəncirin qurula bilinməsi imkanıdır. PoS validator (mayner) paralel olaraq hər iki zəncirdə (əsas və saxtalaşdırılmış) yeni blokları yarada və buna görə o, özünə məxsus olan aktiv ilə risk etməmiş olur. "PoS"da yaranan müvafiq problem *"Nothing at stake" problemi* adlanır.

Bir çox blokçeyn şəbəkələri konsensus əldə etmək üçün başlanğıcda "PoW" alqoritmindən istifadə etsələr də, daha sonra "PoS" alqoritminə keçmişlər. Məsələn, "PoW" ilə işləyən "Ethereum" blokçeyninin "PoS" protokolu ilə (bu variantda "Ethereum 2.0" adlanır) işləmə prinsipinə keçilməsi nəzərdə tutulur.

"Delegated Proof of Stake" ("DPoS") konsensus protokolu. Bu alqoritm "PoS"a çox oxşayır. "DPoS" protokolu "Graphene" layihəsi çərçivəsində 2014-cü ildə hazırlanmışdır və ilk dəfə "Bitshares", daha sonralar isə "Steemit" layihəsində aktivləşdirilmişdir.

Sistemin işləmə prinsipi "PoS"a oxşayır. Bu, dairəvi qaydada yeni blokların yaradılması üçün seçilmiş müəyyən sayda blok yaradıcılarının mövcud olduğu bir sistemdir. "DPoS" sistemində iki növ qovşaq şəbəkədə konsensusun düzgün fəaliyyət göstərməsini təmin edir. Bunlar blokları yaradanlar (validatorlar) və şəbəkə üzvləridir. Hər bir validatorun seçimi şəbəkə üzvü olan və ya şəbəkədə pay sahibi olan (blokçeyndən asılı olaraq) qovşaqların malik olduqları payların sayına proporsional qaydada verdiyi səslər əsasında həyata keçirilir. Adətən, bir neçə blok yarandıqdan sonra yenidən seçim olunmaqla validatorların siyahısı dəyişdirilir. Bəzi şəbəkələrdə istifadəçilər öz səsvermə hüquqlarını etibar etdikləri digər istifadəçilərə onların adından şəbəkənin digər üzvlərinə səs verə bilmələri məqsədilə verə bilərlər. Prosesin qalan hissəsi "PoS"da olduğu kimi icra edilir.

Beləliklə, "PoW" alqoritminindən istifadə zamanı validatorlar blokun əlavə edilməsi üçün müəyyən bir kriptoqrafik məsələni həll etməlidilər. Bu məsələni ilk həll edən şəxs bloku blokçeynə əlavə edir və bunun müqabilində mükafat alır.

"PoS"da iştirakçılar blok əlavə etmək imkanı əldə etmək üçün öz tokenlərini girov qoyur və qoyulan girovun həcminə proporsional sayda blok yaratmaq imkanı qazanırlar. Burada hər yaradılan bloka görə mükafat əldə olunur.

"DPoS"da isə iştirakçılar bloku əlavə edəcək şəxsi səsvermə üsulu ilə seçirlər. Seçilmiş qovşaqlar mükafat qarşılığında blokları yoxlayaraq blokçeynə əlavə edir. Səsvermənin nəticələrinə görə *validatorlar hovuzu* formalaşır və xüsusi alqoritm vasitəsi ilə validatorların növbəsi təşkil olunur. Əgər müəyyən edilmiş vaxt ərzində növbəsi çatan validator (qiymətləndirici) əməliyyatları bloka əlavə etmirsə, bu zaman blokun əlavə olunması hüququ növbəti iştirakçıya keçir. Tsikl başa çatdıqda, alqoritm yenidən validatorların hovuzunu təşkil edir və yerləri paylayır. Blokçeynlərdə mükafatlandırma və validasiya seçimləri müxtəlif və fərqli ola bilər. "DPoS"a nümunə kimi "EOS" blokçeyn platformasını göstərmək olar.

Beləliklə, "DPoS"un əsas üstünləklərinə (i) əməliyyatlarının sürətli olması, (ii) yüksək təhlükəsizlik və etibarlılıq və (iii) hər hansı bahalı avadanlıqlara ehtiyacın olmamasını aid etmək olar. Qeyd olunan üstünlükləri ilə yanaşı, müvafiq sistemin əsas boşluğu - böyük həcmdə tokenin (payın) bir şəxsdə cəmləşdiyi halda həmin şəxsin istədyi şəxsi validator qismində seçməsi hüququnu (səlahiyyətini) əldə etməsidir. "PoS" və "DpoS"un bir neçə modifikasiyası mövcuddur. Burada seçimin edilməsindən tutmuş girovun qoyulması və mükafatın ödənilməsi formalarına qədər fərqlər mövcüddur.

"Staking" (steykinq) - blokçeyn üzərindəki bütün əməliyyatlara dəstək vermək üçün vəsaitlərin kriptovalyuta cüzdanında saxlanılması prosesidir. Əslində bu, blokların yaradılması zamanı mükafat əldə etmək məqsədilə validatorlar tərəfindən öz kriptovalyutalarının müəyyən həcminin bloklanması prosesidir.

"PoS" alqoritmində validator olan şəxslər "PoW"da blokların təsdiqlənməsi işini görən maynerlərlə eyni funskiyanı daşıyırlar. Belə ki, öz vəsaitlərini bloklayan şəxslər blokun təsdiqlənməsində iştirak etdikdə, buna görə mükafat alırlar.

"Proof of Activity" ("POA" - fəaliyyətin sübutu) konsensus protokolu. Müvafiq alqoritm ən çox istifadə olunan "PoW" və "PoS" konsensus alqoritmlərini birləşdirən qarışıq bir yanaşmadır. "PoA"da proses aşağıdakı 2 mərhələdən keçir:

1) 1-ci mərhələdə "PoW"da olduğu kimi blokun yaradılması üçün xüsusi riyazi alqoritmlər vasitəsi ilə hesablamalar baş verir;
2) 2-ci mərhələdə blokun təsdiq edilməsi (imzalanması) üçün "PoS" sistemindən istifadə olunur.

Hazırda bir sıra digər növ konsensus alqortimləri də mövcüddur: "Proof of Burn", "Proof of Capacity" və s.

Konsensusda çəngəl anlayışı

Hər bir proqram təminatının müəyyən dövr ərzində təkmilləşdirilməsinə və ya işlək olmayan mexanizmlərinin dəyişdirilməsinə ehtiyac duyulur. Analoji proses blokçeyn platformalarında da baş verir. Məlum olduğu kimi açıq blokçeynlər açıq kodlardan ibarət olur və müvafiq ilkin kodlar istənilən şəxs və ya qrup tərəfindən köçürülə və dəyişdirilə bilər. Eyni zamanda belə dəyişikliklər blokçeyn üzvləri tərəfindən qəbul edilməyə də bilər ki, nəticədə bu hal şəbəkə qovşaqları arasında parçalanmaya səbəb ola bilər. Blokçeyn platformalarının ilkin və ya mövcüd kodlarının modifikasiyasına **çəngəl** deyilir.

Blokçeyn texnologiyasında **çəngəl ("fork")** – şəbəkə daxilində əvvəlcədən qəbul edilmiş qaydalardan kənar yeni qaydalarla işləmə prosesi hesab edilir.

Çəngəl bütün blokçeyn şəbəkəsinin işləmə mexanizmində böyük dəyişikliklər yarada bilər. Blokçeyn platformalarının ilkin və ya mövcüd kodlarının modifikasiyasının iki əsas növü mövcuddur: **yumşaq ("softfork") çəngəllər** və **sərt ("hardfork") çəngəllər.**

Yumşaq çəngəl modifikasiyası zamanı blokçeyn proqram təminatında qəbul edilmiş qaydaların dəyişməsi yeni qaydaların icrası üçün proqram təminatının yeniləməsini tələb etmir. Şəbəkədə qovşaqların bir hissəsinin yeni qaydalar qəbul etmədiyi halda belə müvafiq qovşaqların yeni qaydalardan istifadə edən qovşaqlarla qarşılıqlı əlaqə qurmasına manea yaratmır.

Yumşaq çəngəl modifikasiyasına aşağıdakıları aid etmək olar:

Şəbəkənin buraxılış imkanının genişləndirilməsi. Məsələn, belə bir dəyişiklik bir şəbəkə elementinə daha çox əməliyyatın daxil edilməsi üçün blokun ölçüsünün artımını nəzərdə tutur. Bu addım əməliyyat məlumatlarının bir istifadəçidən digərinə köçürülməsini sürətləndirməyə imkan verir ki, bu da blokçeyn sisteminin cəlbediciliyini artırır.

Şəbəkə iştirakçılarına məxsus ünvanların formatının dəyişdirilməsi. Buna məsələn, şəbəkə iştirakçılarının anonimlik imkanının artırılmasını aid etmək olar. Yumşaq çəngəldə eyni zamanda köhnə ünvanlar yenilərindən pul ala bilər və əksinə.

Komissiyanın yaradılması qaydalarının dəyişdirilməsi. Buna nümunə olaraq, köçürmə məbləğindən asılı olmayan sabit bir ödənişin təyin olunmasını göstərmək olar.

Yeni təhlükəsizlik protokollarının tətbiqi. Haker hücumunu və şəbəkə istifadəçilərinin şəxsi ünvanlarının sındırılması ehtimalını azaltmaq məqsədilə tərtibatçılar tərəfindən alqoritmlərin təyin edilməsi.

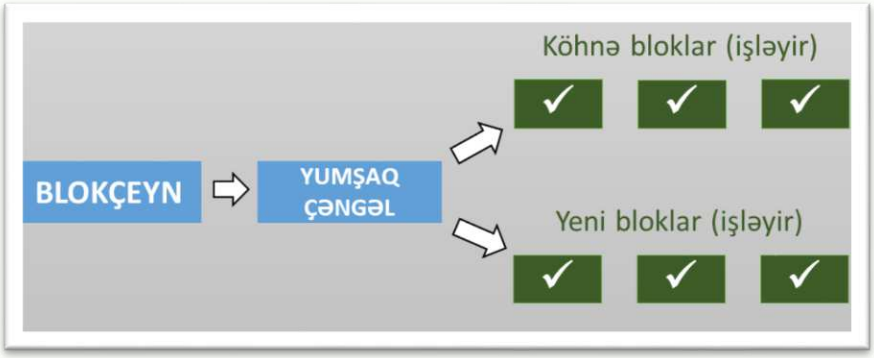
Yumşaq çəngəl (softfork) bir qayda olaraq, aşağıdakı məqamlara təsir göstərmir:

Blokçeyn üzərində qurulan kriptovalyutanın maksimum emissiyası. Bu, ilk növbədə məhdud tirajlı tokenlərə aid olmaqla, dəyişdirilə bilinməyən təməl bir parametrdir. Lakin

məhdudiyyətsiz emissiyaya sahib olan kriptovalyutalar yumşaq çəngəl həyata keçirə bilərlər.

Mayninq vaxtının bloklanması. Emissiyanın həcmini tənzimləyən digər əsas parametr olaraq müvafiq müvafiq zaman intervalının dəyişdirilməsi, demək olar ki, yalnız sərt çəngəl halında baş verə bilər.

Yumşaq çəngəl baş verdikdən sonra, həllərin tətbiqinə başlamaq üçün istifadəçilər proqram təminatını yeniləməlidirlər. Lakin belə keçid könüllü olaraq baş verir. Belə ki, yeniliklərdən razı olmayan hər hansı şəxs köhnə qaydalarla işləyən şəbəkədən istifadə etməyə davam edə bilər. Qeyd olunduğu kimi, yumşaq çəngəllərdən sonra eyni blok zəncirində həm köhnə, həçm də yeni alqoritmlər mövcud olduğundan, yeniliklərin mütləq şəkildə qəbul olunmasına ehtiyac qalmır.

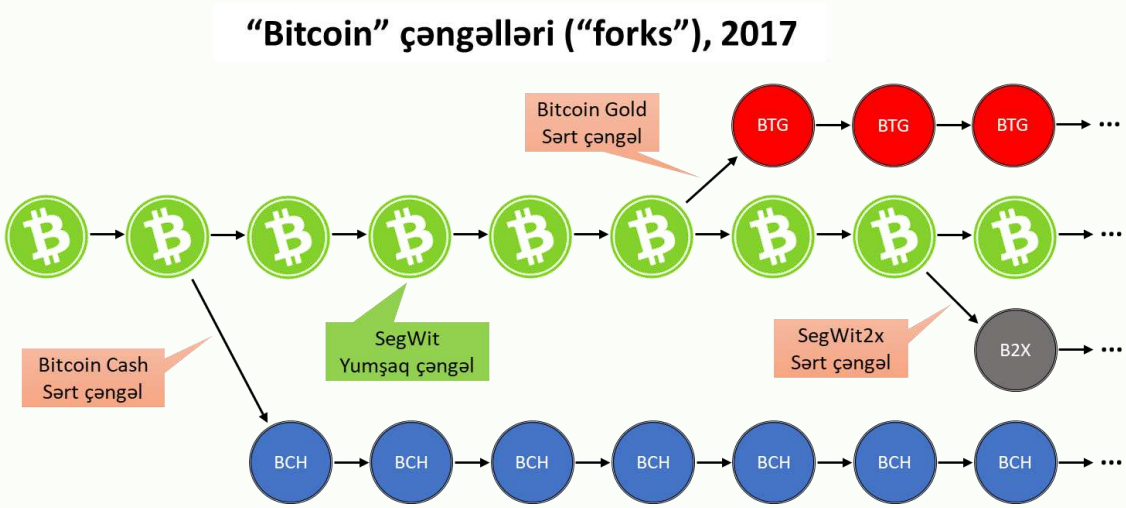


Sərt çəngəl (“hardfork”) - blokçeyn sistemi daxilində şəbəkə qovşaqları tərəfindən blok zəncirinə yeni qaydalara uyğun blokun əlavə edilməsidir.

Sərt çəngəl zamanı blokçeyn bir-biri ilə əlaqəli olmayan iki avtonom hissəyə bölünür. Bunun nəticəsi olaraq bir avtonom şəbəkə iştirakçıları digər tərəfin əməliyyatlarını izləyə bilmirlər və ikinci zəncirdə yaranan bloklar birinci zəncir üçün həqiqi hesab edilmir. Kriptovalyutalarda bu, bir kriptovalyutanın iki hissəyə bölünməsi ilə də nəticələnə bilər. Buna nümunə olaraq bitkoynda baş vermiş sərt çəngəlləri göstərmək olar.

2016-cı ildə bəzi bitkoyn tərtibatçıları əməliyyatlar üçün yerin azad edilməsi məqsədilə blokda yerləşən məlumatların bir hissəsinin blokçeynin hüdudlarından kənara çıxarılacağını nəzərdə tutan “SegVit” konsepsiyası haqqında təklif irəli sürmüşlər. Lakin bəzi şəxslər müvafiq yeniliyi müvəqqəti bir həll hesab edərək onunla razılaşmadı. Nəticədə, “SegVit”in aktivləşdirilməsindən əvvəl, 2017-ci ilin avqust ayında “bitcoin” tarixdə ilk dəfə olaraq səkkiz dəfə daha böyük blok vahidi (yeni “Bitcoin Cash Coin” – “BCH”) ilə əsas şəbəkədən ayrılmaq barədə qərar verdi. 2017-ci ilin oktyabrında ikinci sərt çəngəl nəticəsində “bitcoin”in əsas şəbəkəsindən “Bitcoin Gold” adlı kriptovalyuta ortaya çıxdı.

2017-ci ilədək “bitcoin” protokolunun proqram təminatlarındakı çəngəllərin sxemi aşağıda verilmişdir.



Blokçeynin növləri

Blokçeyn texnologiyasının geniş inkişafa nail olması və böyük imkanlar açması investorların marağına səbəb olmuşdur. Blokçeyn dedikdə, adətən, "bitcoin" kimi mərkəzləşdirilməmiş, hər kəsin daxil ola və iştirak edə biləcəyi blokçeyn başa düşülür. Lakin blokçeyn texnologiyasının imkanları yalnız mərkəzləşdirilməmiş texnologiya ilə məhdudlaşmayaraq, böyük investorlar və dövlətlərdə də ona maraq yaratmışdır. Belə marağın təzahürü kimi əşyaların interneti ("internet of things", "IOT") üçün əməliyyatların təsdiqlənməsi məqsədi ilə "IBM" və "Samsung" şirkətləri tərəfindən smart müqavilələrin yaradılmasını göstərmək olar. Blokçeyn texnologiyasının yaradılması kiçik şirkətlər üçün əlverişli hesab olunmasa da, iri korporasiyalar və dövlətlər üçün kifayət qədər geniş imkanlar yaradır. Bəzi hallarda dövlət orqanları böyük şirkətlərə hər-hansısa bir sahədə effektiv sistemin yaradılması üçün blokçeyn üzərindən platformalar hazırlayır. Lakin şirkətlər bu kimi formalarda blokçeynin hər kəs üçün açıq olmamasında və ya təhlükəsizlik baxımından şəbəkə iştirakçılarının məlumatlarının məxfi saxlanılması ilə əlaqəli şəbəkədə blokların əlavə edilməsinə, əməliyyatların icra edilməsinə və onlara baxışlara məhdudiyyət qoymaqda maraqlı olurlar.

Blokçeyn sistemində *əməliyyatların emalına olan tələblər* aşağıdakı kimidir:

1) əməliyyatlar sistemin mövcud vəziyyətinə uyğun olmalıdır;
2) əməliyyatlar eyniləşdirilə bilinən olmalıdır;
3) əməliyyatlar dəyişməz olmalıdır;
4) əməliyyatlar sonluğa malik olmalıdır (silinə bilinməməlidir);
5) əməliyyatlar şəbəkə qaydalarına uyğun olmalıdır.

Müxtəlif funksiya və arxitekturaya malik müxtəlif blokçeynlər çoxluğu mövcuddur. Onları əməliyyatların kimin oxuması, icra etməsi və yoxlamasından asılı olaraq fərqləndirmək olar.

İstənilən şəxsin oxuduğu və çıxışı olduğu blokçeyn ***açıq blokçeyn*** adlanır ki, bu da istənilən şəxsin bütün blokçeynə çıxış əldə etməsi və onun məzmununu oxuya bilməsi deməkdir. Blokçeynə yalnız səlahiyyətli şəxslərin çıxışı olarsa, belə blokçeyn **qapalı** blokçeyn adlanır.

Açıq və qapalı blokçeyn şəbəkələri aşağıdakı parametrlər üzrə müqayisə oluna bilər:

Konsensus əldə olunması. Açıq blokçeyn şəbəkələrində istənilən qovşaq konsensusun əldə olunması prosesində iştirak edə bilər. Qapalı blokçeyn şəbəkələrində isə yekun konsensus hər hansı qovşaq (təşkilat) tərəfindən müəyyən edilə və ona tamamilə nəzarət oluna bilər.

Şəffaflıq. Açıq blokçeyn şəbəkələrində əməliyyatlar ictimaiyyət üçün açıqdır və hər bir istifadəçi bütün hərəkətləri izləyə bilər, halbuki qapalı blokçeyn şəbəkələrində məlumatların oxunması şəbəkə parametrləri (sazlanmaları) ilə tənzimlənir.

Dəyişməzlik. Əməliyyatlar paylanan şəbəkədə saxlanıldığından, praktiki olaraq açıq blokçeyn şəbəkəsini dəyişmək mümkün olmur. Qapalı blokçeyn şəbəkələrdə idarə edən təşkilatın istəyi sayəsində əməliyyatı dəyişmək olar.

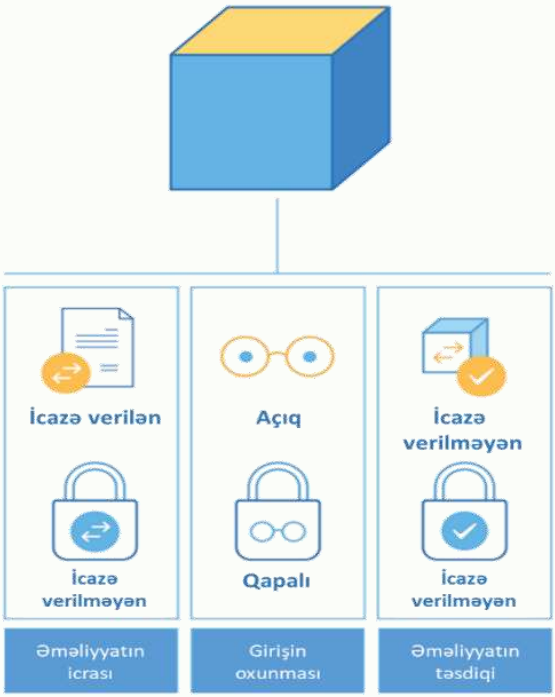
Effektivlik. Açıq blokçeyn şəbəkələrində böyük sayda qovşaqların mövcudluğu sayəsində əməliyyatların və blokların yayımlanması çox vaxt aparır. Bu səbəbdən, şəbəkənin buraxılış qabiliyyəti kifayət qədər aşağı düşür. Qapalı blokçeyn şəbəkələrində qovşaqların sayı idarə edən təşkilat tərəfindən nəzarət olunur ki, bununla şəbəkənin buraxılış qabiliyyətini yüksəltmək/aşağı salmaq olur.

Əksmərkəzləşmə. Qeyd edilən blokçeyn şəbəkələrinin əsas fərqləndirici xüsusiyyəti açıq blokçeyn şəbəkələrinin blokçeyn texnologiyasının mərkəzi ideyası olan əksmərkəzləşməni saxladığı halda, qapalı blokçeyn texnologiyalarının tam olaraq mərkəzləşdirilməsi və onlara qovşaqların müəyyən qrupu tərəfindən nəzarətin olunmasıdır. Blokçeyn şəbəkələrinin (BŞ) müqayisəli təhlilinin nəticələri aşağıdakı cədvəldə verilmişdir:

Parametr	Açıq BŞ	Qapalı BŞ
konsensusun əldə olunması	bütün qovşaqlar iştirak edir	bir təşkilat tərəfindən nəzarət olunur
şəffaflıq	əməliyyatlar hamı üçün əlçatandır	əməliyyatlar hamı üçün əlçatan ola və ya məhdudiyyətli ola bilər
dəyişməzlik	məlumatları dəyişmək praktiki olaraq mümkün deyildir	məlumatların dəyişdirilməsi imkanı mövcuddur
Effektivlik	aşağı / yüksək	yüksək
əksmərkəzləşmə	mövcuddur	mövcud deyil

Qeyd etmək lazımdır ki, açıq blokçeyn şəbəkələrinin heç də hamısı aşağı effektivliyə malik deyil. Tərtibatçılar açıq blokçeyndə istifadə olunan bir çox konsensus protokolları üçün məhsuldarlığın yüksəldilməsinin əlavə mexanizmlərini hazırlayırlar.

Əməliyyatı kimin göndərə bilməsi və kimin yoxlamasından asılı olaraq, blokçeynlər həmçinin **icazə verilən** və **icazə verilməyən** blokçeynlərə bölünə bilər. Əgər bir kimsə əməliyyatları göndərə və yoxlaya bilirsə, belə blokçeyn icazə verilən (icazə tələb olunmayan) blokçeyn adlanır. Əgər tərəflər əməliyyatın icrası və ya yoxlanılması, yaxud hər ikisi üçün eyniləşdirilməlidirlərsə, belə blokçeyn icazə verilməyən (icazə tələb edən) blokçeyn adlanır.

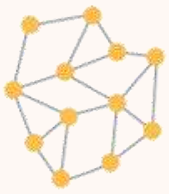
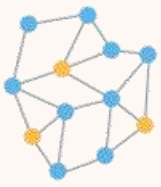


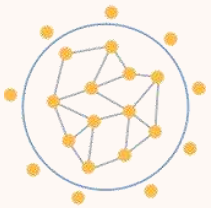
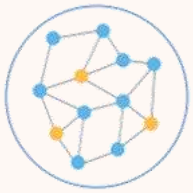
Blokçeyn atributları

Ümumilikdə, blokçeynin 4 əsas növünü müəyyən etmək olar:

- icazə tələb olunmayan açıq blokçeynlər;
- icazə tələb olunan açıq blokçeynlər;
- icazə tələb olunmayan qapalı blokçeynlər;
- icazə tələb olunan qapalı blokçeynlər.

Blokçeynin müvafiq növlərinə dair nümunələr aşağıdakı cədvəldə verilmişdir:

Blokçeynin növü	İzahı	Nümunə	Vizuallaşdırma
İcazə tələb olunmayan açıq blokçeynlər	Bu növ blokçeyn sistemlərdə hər bir şəxs blokçeynin konsensus mexanizmində iştirak edə bilər. Bundan əlavə, internetə qoşulmuş hər bir şəxs əməliyyatı icra edə və əməliyyat jurnalına (tam loqlara) baxa bilər.	Bitcoin, Litecoin, Ethereum	
İcazə tələb olunan açıq blokçeynlər	Bu növ blokçeyn sistemlərdə internetə qoşulmuş hər bir şəxs əməliyyatı icra edə və əməliyyat jurnalına (loqlarına) baxa bilər, lakin konsensus mexanizmində yalnız məhdud sayda qovşaq iştirak edə bilər	Ripple, Ethereum-un qapalı versiyaları	

İcazə tələb olunmayan qapalı blokçeynlər	Bu növ blokçeyn sistemlər konsensus mexanizminin hamı üçün açıq olmasına baxmayaraq, kimin əməliyyat icra etməsi və əməliyyat jurnalına (loqlara) baxış edə bilməsi baxımından məhduddur	Exonum (qismən)	
İcazə tələb olunan qapalı blokçeynlər	Bu növ blokçeyn sistemlər əməliyyat imkanını və əməliyyat jurnalına (loquna) baxış imkanını yalnız sistemdə iştirak edən qovşaqlar çərçivəsi ilə məhdudlaşdırır, blokçeyn sisteminin arxitektoru və ya sahibi isə blokçeyn sistemində kimin iştirak edə bilməsini və konsensus mexanizmində hansı qovşaqların iştirak edə bilməsini müəyyən edə bilər	Rubix, Hyperledger	

Cədvəldə sarı nöqtələr – yoxlayıcı qovşaqlar olmaqla, sistemdə əməliyyatları yoxlama və konsensus mexanizmində iştirak edə bilməni göstərir. Mavi nöqtələr əməliyyatları icra edə bilən, lakin yoxlama mexanizmində iştirak edə bilməyən şəbəkə iştirakçılarıdır. Bu nöqtələr konsensus mexanizmində iştirak etmir. Göy dairə yalnız onun daxilində olan qovşaqların əməliyyatın tarixini görə bilməsini ifadə edir. Dairəsiz təsvirlər isə internetə qoşulmuş hər bir kəsin blokçeyn əməliyyatlarının tarixini görə bildiklərini ifadə edir.

Blokçeyndə əməliyyatların uçot modelləri və Merkl ağacı

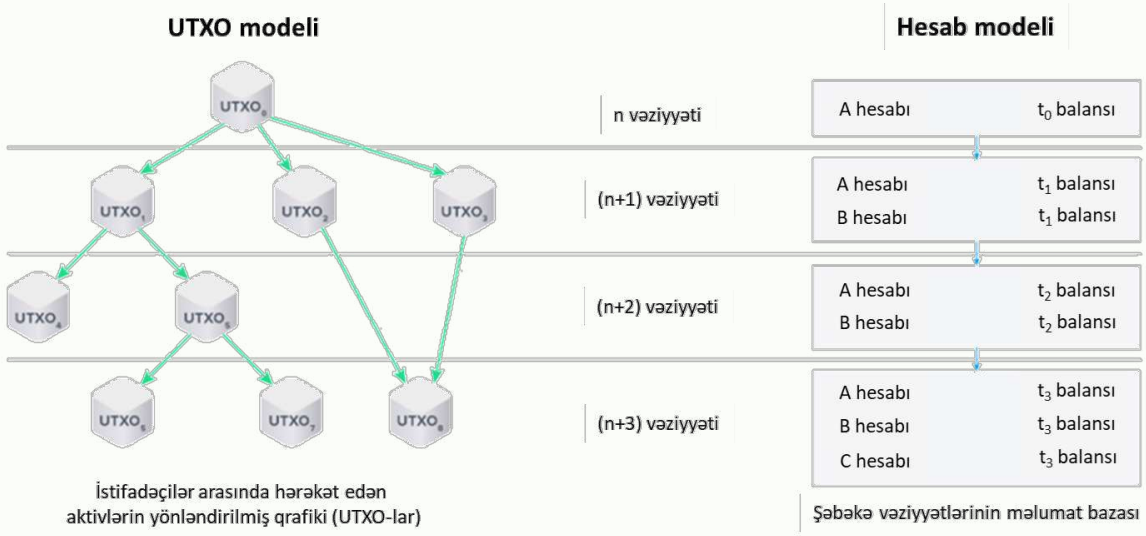
Müasir blokçeyn şəbəkələrində iki növ uçot modellərindən istifadə olunur. Bu modellərə *əməliyyatların uçota alınması arxitekturası və balansın (hesabın) vəziyyəti* də deyilir. İstifadə edilən birinci modelə “**UTXO”** (“Unspent Transaction Output” – xərclənməmiş əməliyyat çıxışı) modeli, ikinciyə isə **Hesab/Balans** (“Account based”) modeli deyilir.

Blokçeyn texnologiyasında əsas məqsəd keçmiş hadisələri və istifadəçi münasibətlərində olan əlaqələri qeyd edərək yadda saxlamaqdır. Hər yeni blok yaradılanda, sistem öz protokolunda müəyyən edilmiş qaydada istifadəçilərə məxsus olan vəziyyətləri yenidən dəyərləndirir və yeni vəziyyət alır.

“UTXO” və Hesab uçot modellərinin əsas fərqlərindən biri sistem istifadəçilərinin aktivlərinin uçotunun necə aparılması ilə bağlıdır.

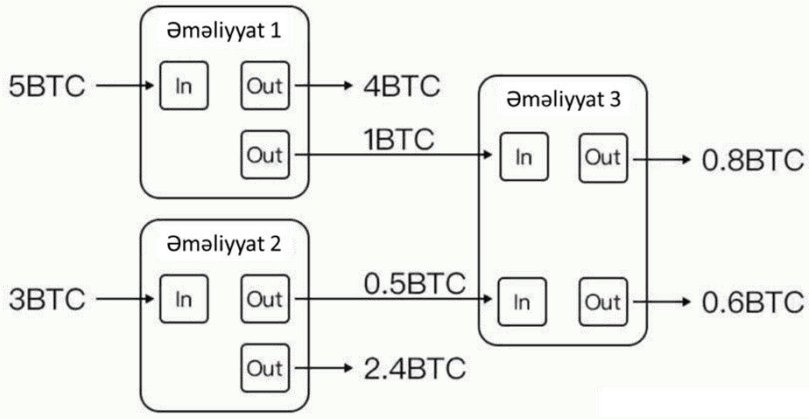
“UTXO” modelində aktivlərin hərəkəti ünvanlar arasında *yönəldilmiş asiklik qrafik* (“Directed Acyclic Graph” - “DAG”) formasında qeydə alındığı halda, Hesab əsaslı modeldə isə aktivlər istifadəşilərin hesabları ilə bağlı balansların dəyişməsi vəziyyəti formasında qeydə alınır.

SİSTEMİN VƏZİYYƏTİNİN QEYDƏ ALINMASI

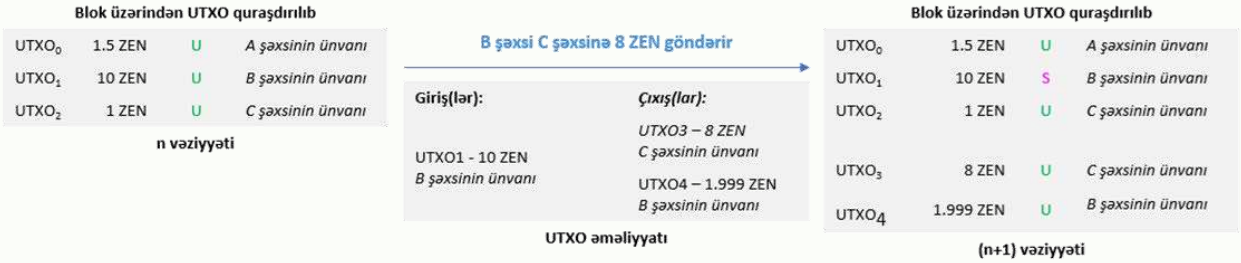


"UTXO" uçot modeli "Bitcoin", "Cardano", "Litecoin" və digər kripto-layihələr, Hesab uçot modeli isə "Etherium", "Tron", "Ripple" kimi layihələr tərəfindən istifadə olunur. Eyni zamanda, uçot modelləri blokların tərkib hissələri, Merkl ağacı prinsipinin quruluş forması və əməliyyatların icra edilməsi baxımından fərqlər yaradır.

"UTXO" modelinə malik blokçeyn platformalarında əməliyyatlar iki hissəyə bölünür: **Giriş** (Input) və **Çıxış** (Output) hissələr. *İstifadəçiyə olan mədaxil əməliyyatları giriş hissədə, onun etdiyi məxaric əməliyyatları isə çıxış hissədə əks olunur. Burada ən mühüm məqamlardan biri vəsaitin giriş hissədən tam məxaric edilməsinin zəruriliyidir.* Fərz edək ki, "A" şəxsinin giriş hissədə 8 "BTC"si var. Lakin bu vəsaitlər ona məxsus iki fərqli ünvanda 5 "BTC" və 3 "BTC" olaraq saxlanılır. Əgər "A" şəxsi "B" şəxsinə 4 "BTC" köçürmək istədikdə, bu zaman o, müvafiq vəsaiti 5 "BTC" olan cüzdanından "B" şəxsinə köçürməlidir. Vəsait "B" şəxsinə köçürülən zaman 1 "BTC" artıq qalan vəsaiti "A" şəxsi komissiya çıxıldıqdan sonra özünün ünvanına köçürür. Beləliklə, öz hesabından 4 "BTC"ni "B" şəxsinə xərcləmədiyi ana qədər bu vəsait xüsusi "UTXO" verilənlər bazasında saxlanılacaqdır. "A" şəxsi eyni əməliyyatı digər formada da edə bilər: 3 "BTC" olan cüzdanındakı bütün vəsaiti B şəxsinə köçürə, çatışmayan 1 "BTC"ni isə 5 "BTC" olan cüzdanından köçürə bilər. Beləliklə, hər bir yeni "UTXO" mövcud "UTXO"lardakı vəsaitlərin ona köçürülməsi (eyni zamanda da vəsaitin köçürüldüyü ilkin "UTXO" ünvanının ləğv edilməsi) ilə yaradılır. Girişlər mövcud "UTXO"lara xərclənir və çıxışlar yeni "UTXO"lar yaradır, əməliyyatlarda vəziyyətin dəyişməsi isə bir şəxsin digərinə çıxış əməliyyatı etdikdə baş verir.



UTXO MODELİNDƏ VƏZİYYƏTİN DƏYİŞMƏSİ



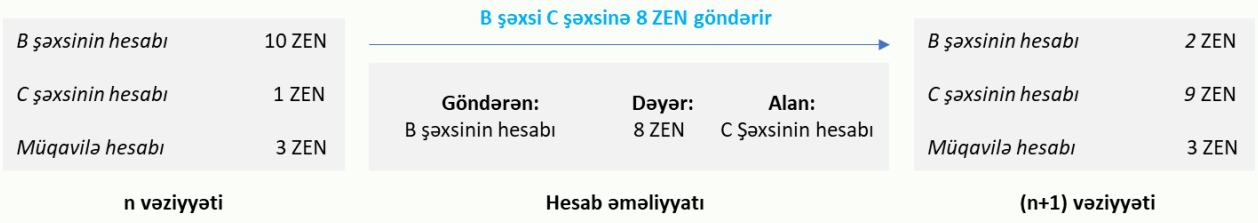
Məsələn, ənənəvi maliyyə sistemində əməliyyat bir hesabdan vəsaitin çıxarılmasını və digər hesaba yerləşdirilməsini nəzərdə tutur. Lakin "UTXO" modelinin hesabı olmadığı üçün göndərici hesabı/ünvanı da tələb etmir. Ünvanlar "UTXO"ları qəbul etmək üçün istifadə olunsa da, heç vaxt bu, blokçeyndə açıq şəkildə qeyd olunmur. Bunun əvəzinə, ünvanları hər bir əməliyyat çıxışına köçürmək üçün "**scriptPubKey"** skriptlərindən istifadə edilir. Vəsaitləri xərcləyərkən, əməliyyat girişinə yalnız "scriptPubKey"in icrası üçün tələb olunan imzalar və açıq açarlar istifadə olunur. "UTXO"da "bitcoin"lərin hansı ünvandan gəldiyi qeyd edilməsə də, bununla belə, əvvəlki "UTXO" ünvanını tapmaq asandır. *Əməliyyatın hər bir girişi əvvəlki əməliyyatın əməliyyat nömrəsi ("TXID") və oradakı çıxışın indeksi ilə mövcud "UTXO"ya istinad edir.*

"UTXO" modeli "Bitcoin" qovşaqlarına blokçeynindəki hər bir əməliyyatı effektiv şəkildə təsdiqləməyə imkan verir. Qovşaqlar müvafiq təsdiqləməni yoxlamaq məqsədilə *təsdiqlənməmiş əməliyyatların reyestrinə ("mempool")*, yaxud vəsaitin daxil olduğu ünvanın "UTXO" vəziyyətinə müraciət edirlər. Bu modeldən istifadənin özü "bitkocoin"də ikiqat xərcləmə problemini həll etməyə imkan verir.

Hesab modelində blokçeynin işləmə prinsipi adi banklardakı köçürmələrə oxşardır. Əsasən bu model smart müqavilələri dəstəkləyən blokçeyn platformalar tərəfindən istifadə olunur. Buna nümunə olaraq "Etherium"u göstərmək olar. Burada vəsait bir şəxsin hesabından digər şəxsin hesabına köçürülür. Bu zaman vəsait köçürülmədən öncə hesabda qalıq deyək ki, hər hansı *"n"* vəziyyətində olacaq, vəsait köçürüləndən sonra isə *"n+1"* vəziyyəti alacaqdır.

Hesab modelində yeni cüzdan yaradılarkən, ikiqat xərc yaranmaması üçün *"nonce"* rəqəmindən istifadə olunur. "Nonce" bir hesab üzrə əməliyyatın sayını göstərir və buna uyğun da əməliyyatın baş verdiyi ana hesabın balansı müəyyən oluna bilir.

HESAB MODELİNDƏ VƏZİYYƏTİN DƏYİŞMƏSİ



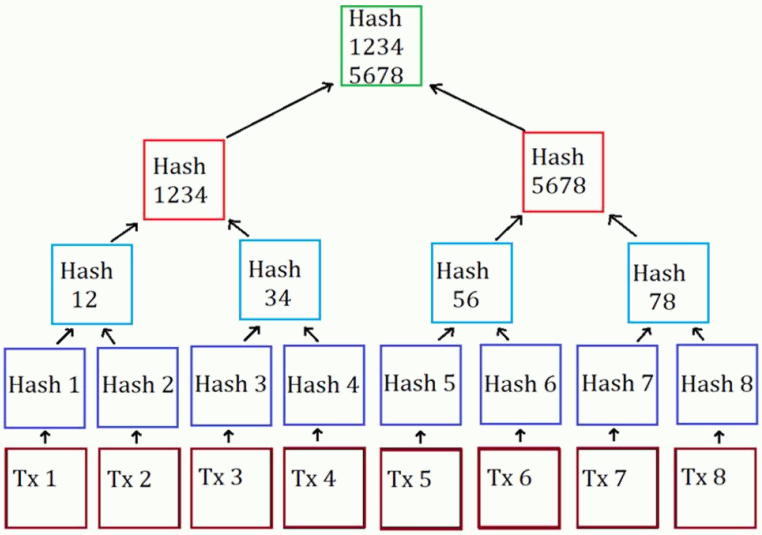
Blokçeyni başa düşmək üçün blokların əməliyyat hissəsində istifadə edilən **“Merkl ağacı”** texnologiyasınının prinsiplərini də başa düşmək lazımdır. Bu terminə bir çox halda *heş ağacı* da deyilir.

“Merkl ağacı” - ən ümumi anlamda böyük sayda məlumat elementlərini (chunk) heşləyən məlumat strukturudur. O, əsasən də eyniranqlı sistemlərdə şəbəkə qovşaqlarının məlumat mübadiləsi aparması və onu müstəqil şəkildə yoxlaması üçün geniş istifadə olunur.

“Merkl ağacı” konsepsiyası 1979-cu ildə professor Ralph Merkle tərəfindən patentləşdirilmişdir. Yuxarıdada qeyd edildiyi kimi, *texniki baxımdan blokçeyn* - ardıcıl bloklardan ibarət, bir-biri ilə kriptoqrafik heş funksiyalar ilə bağlı olan, hər bir blok və əməliyyatın doğrulunuğunu yoxlayan və təsdiqləyən şəbəkə üzvlərini birləşdirən sistem hesab edilir.

Merkl ağacının strukturu ağac şəklində (tərsinə çevrilmiş formada) tam məlumat strukturuna bənzəyir. Ağacın baş hissəsində blokun tərkibinə daxil olan əməliyyatların ümumiləşdirilmiş heş nəticəsi formalaşır. Belə ki, ilk əvvəl hər əməliyyatın heş nəticəsi alındıqdan sonra digəri ilə toplanaraq yeni heş nəticə alınır və vahid bir heş alınanadək bu proses eyni qaydada davam edir. Alınmış yekun heş nəticə blokda *Merkl heş* adlanır və blokun ümumi heşinin formalaşmasında istifadə olunur. “UTXO” uçot modelinə malik blokçeynlərdə blokda bir *Merkl heş* olur.

Çox vaxt daha sadə Merkl ağacı olan ikili ağacdan istifadə olunur. Onda hər bir blok iki heşə malik olur.



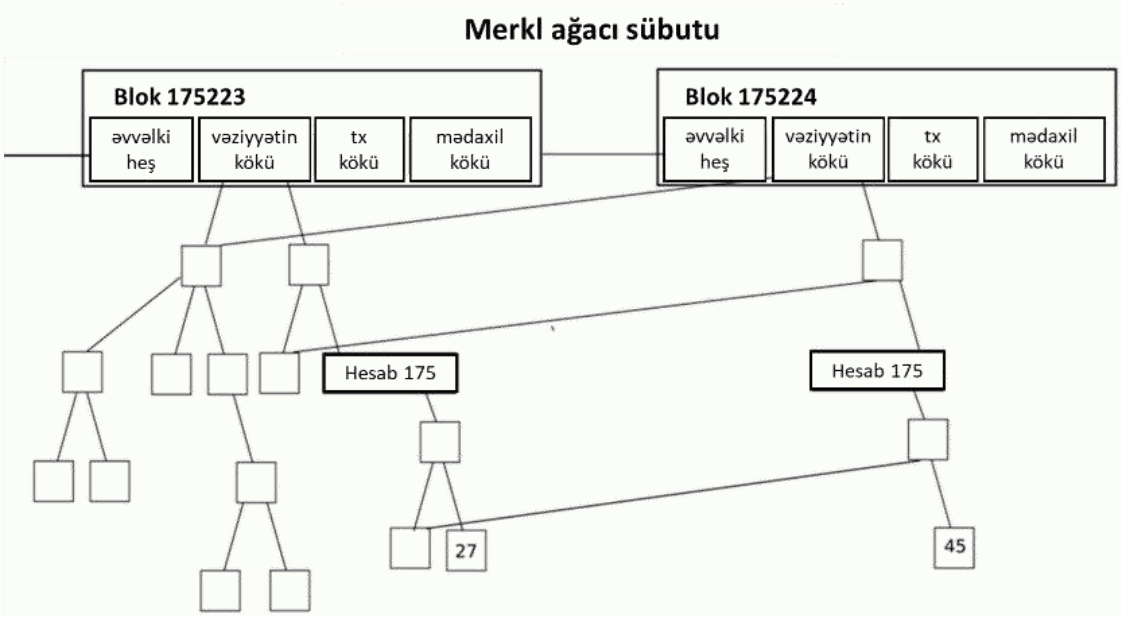
“Merkl ağacı”nın yaradılması sayəsində böyük bir əməliyyat siyahısı və ya hər hansı digər məlumat toplusu yalnız bir sətirdə təmsil oluna bilər.

Hesab modelinə malik blokçeynlərdə ikili Merkl ağacından fərqli olaraq mürəkkəb *Merkl ağacından* istifadə olunur. Məsələn, “Ethereum”da **“Prefiksli Merkl ağacı”** (yaxud “Merkle Patricia” ağacı da adlanır) prinsipindən istifadə olunur. Bunun sadə “Merkl ağacı” prinsipindən fərqi müvafiq blokçeynlərdə aktivlərin əməliyyatların vəziyyətinə görə deyil, hesabların balans vəziyyətinə görə dəyişməsinin qeydə alınmasıdır. Eyni zamanda, “Ethereum”un smart müqavilələrdən istifadə etməsi də “Merkl ağacı” prinsipinin işinə təsir edir. İkili Merkl ağacı – mahiyyətcə elementlərin ardıcıllığı şəklində təqdim olunmuş informasiyanın yoxlanılması üçün daha yararlıdır. Onlar həmçinin “əməliyyat ağacları”nın təqdim edilməsi üçün də yararlıdır, çünki onlara düzəliş edilməsi tələb olunmur: “əməliyyat ağacı” həmişəlik yaradıldığı kimi dəyişməz qalır.

Vəziyyət ağacı isə bir qədər mürəkkəbdir. Mahiyyətcə, “Ethereum”da vəziyyət – açar və qiymətlər cədvəlidir, hansı ki, burada açarlar ünvanlar, qiymətlər isə balansa, birdəfəlik koda və reyestrə malik hesablardır.

“Ethereum”da hər bir blok başlığı aşağıdakı üç müxtəlif növ obyekt üçün bir deyil, üç “Merkl ağacı”na malikdir:

- əməliyyatlar;
- qəbzlər (“receipt root” - mahiyyətcə, hər bir əməliyyatın icrasının nəticələrinə dair məlumatlar);
- balansın cari vəziyyəti.



“Ethereum”da əməliyyatlar və smart müqavilələrin təsdiq edilməsi zamanı validatorlar aşağıdakı suallara cavab verməlidir:

1. icra olunan əməliyyat hər-hansı bir blokda varmı?
2. son 30 gündə göndərən ünvan tərəfindən neçə əməliyyat/hadisə yaradılıb?
3. vəsait göndərən hesabın cari qalığı nə qədərdir?
4. belə bir hesab varmı?
5. müvafiq müqavilə üçün verilmiş əməliyyatın nəticəsi necə olacaq?

Birinci suala cavab “Merkl ağacı”nın əməliyyatlar hissəsinə, üç və dördüncü suallara cavab balans vəziyyətinə görə, ikinci suala cavab isə Merkl ağacındakı qəbzlərin verilənlər bazasına əsasən müəyyən etmək mümkündür. 5-ci sualın cavabı balansın dəyişmə vəziyyəti ilə müəyyən edilir, lakin bu bir qədər mürəkkəb prosesdir.

Bölmə
Üç

3

KRİPTOVALYUTALAR VƏ ONLARIN NÖVLƏRİ

- kriptovalyuta
- bitcoin
- altkoin
- steyblkoin

Kriptovalyutalar və onların növləri

Virtual aktivlərin hazırda ən geniş yayılmış forması kriptovalyuta hesab olunur. Mərkəzləşdirilmiş hesabda deyil, blokçeyn şəbəkəsində saxlanılan elektron pulların xüsusi forması kimi kriptovalyutalar eynilə fiat valyutalarda olduğu kimi bir şəxsdən dəgərinə köçürülə, yığım və ödəniş vasitəsi kimi istifadə oluna bilər.

"Bitcoin" kriptovalyutası blokçeyn texnologiyası vasitəsi ilə dünyada yaradılan ilk uğurlu layihədir. "Bitcoin" konsepsiyası ilə bağlı ilk dəfə 2008-ci ilin oktyabr ayında özünü Satoşi Nakamoto (şəxs özünü belə adlandırıdı, lakin bu ad altında əslində kimin olduğu hələ də bilinmir) adı ilə təqdim edən şəxs və ya şəxslər qrupu tərəfindən *"Bitcoin: A Peer-to-Peer Electronic Cash System"* paylaşımında edilmişdir. Müvafiq paylaşımda Satoşi "bitcoin"in işləyəcəyi *texniki sənədi ("white paper")* təqdim etmişdir.

Texniki sənəd (white paper) - şirkətin və ya layihənin strategiyasını təsvir edən sənədə deyilir. Bu, həm texniki, həm də digər layihənin icrası zamanı yarana biləcək çətinliklərin aradan qaldırılmasını təsvir edən həllər yoludur. Sənəddə layihə ilə əlaqəli bütün məsələlər yer almalıdır: iş planı, ideologiya, manifest, ideyanın təsviri, bazar təhlili, cəlb etmə metodları və funksionallıq. Müvafiq texniki sənəd yalnız onu öyrənəcək token alıcıları üçün deyil, həmçinin layihə yaradıcılarının özü üçün də əhəmiyyətlidir.

"Bitcoin"in "genesis blok" adlanan ilk bloku 3 yanvar 2009-cu ildə yaradılır və bu zaman ilk 50 "bitcoin" (BTC) emissiya olunur. Bu "bitcoin"ləri ilk dəfə Satoşi Nakamotonun özü əldə etmişdir. 12 yanvar 2009-cu ildə isə Satoşi Nakamoto və Hell Finn arasında ilk "bitcoin" əməliyyatı baş vermişdir (10 BTC).

"Bitcoin"in dəyərinin ilk dövrlər onun istehsalına sərf edilən xərclərə bağlanmasına dair qərar verilmişdir. 2009-cu ildə "New Liberty Standart" web saytı 1 dollara 1309.03 "bitcoin" emal etmənin mümkün olduğunu bildirmişdir (1 BTC = 0.000769 USD). Hell Finndən başqa ilkin "bitcoin"ləri əldə edən şəxslər arasında kriptoqrafiya ilə əlaqəli olan Vey Day və Nik Sabo da yer almışdır. "Bitcoin"in ən kiçik vahidi onun yaradıcı Satoşi Nakamotonun adına qoyulmuşdur. 1 "bitcoin" 10^{-8} (0.00000001 BTC) satoşiyə bərabərdir.

2010-cu ildə Laslo Hankyes ilk dəfə "bitcoin"dən ödəniş vasitəsi kimi istifadə edərək 10 000 BTC-yə (1 BTC = 25 USD) pizza almağa nail oluşdur. 2011-ci ildə isə Djed Makkaleb "bitcoin"in mübadiləsinə imkan verən ilk platforma yaratmaq məqsədilə "MTGox" adlı birja yaratmışdır. Buradan birja istifadəçiləri "bitcoin"i fiat valyutalar ilə mübadilə edə bilirdilər. 2014-cü ildə bir neçə birjaya olan kiberhücumlardan sonra müvafiq birja öz fəaliyyətini dayandırmışdır.

2021-ci ilin noyabr ayında "bitcoin"in bazar dəyəri tarixi rekord olan 68 000 USD səviyyəsinə çatmışdır.

"Bitcoin" eyniranqlı bərabərhüquqlu şəbəkə qovşaqlarından ibarət açıq kodlu sistemdir. Sistemin fundamental əsaslarını kriptoqrafiya, "PoW" ("Proof of Work") konsensus alqoritmi və "UTXO" əməliyyat modeli təşkil edir.

"Bitcoin"in fiat valyutalardan əsas fərqi emissiyanın mərkəzləşdirilmiş orqan tərəfindən deyil, bərabərhüquqlu qovşaqlar tərəfindən hər yeni blokun yaradılması zamanı həyata keçirilməsidir. Emissiya edilmiş vəsaitlər əməliyyatları təsdiqləyən və müəyyən alqoritm əsasında onları bloka əlavə edən validatorlara mükafat olaraq verilir. "Bitcoin"də validatorlar *"mayner"* adlanır. Buna səbəb "bitcoin"in hasil olunması üçün məsələn, qızılın istehsalı üçün zəruri işlərin görülməsinə analoji işlərin görülməsidir. "Bitcoin"in emissiya həcminə məhdudiyyət tətbiq edilmişdir. Belə ki, "bitcoin"in emissiya oluna biləcək maksimum mümkün sayı 21 milyon olaraq müəyyənləşdirilib. Müvafiq məhdudiyyət "bitcoin"in inflyasiyadan qorunması üçün daxil edilib. Eyni zamanda, hər bir köçürmə əməliyyatı zamanı köçürən şəxs tərəfindən müəyyən miqdarda komissiya

ödənilir ki, bu da blokun emissiyasından başqa validatorun əldə edə biləcəyi əlavə qazancdır. Komissiyanın ödənilməsi mütləq olmasa da, əməliyyatın bloka əlavə edilməsində mühüm əhəmiyyət daşıyır. Eyni zamanda deflyasiya hər dəfə bloklara görə "bitcoin" mükafatının azaldılması ilə əlaqələndirilir. Belə ki, hər 210 min blokdan bir *yarıya bölünmə (halving)* deyilən bir prosess baş verir və blokun yaradılmasına görə mükafat kimi nəzərdə tutulan "bitcoin"lərin sayı 2 dəfə aşağı düşür. Hazırda bir bloka görə nəzərdə tutulmuş mükafat 6.25 "bitcoin"ə bərabərdir.

İlk 36 288 blok yalnız bir kompüter tərəfindən yaradılmışdır və bu müddət ərzində həmin kompüter vasitəsi ilə 1 148 800 BTC emissiya edilmişdir. Hesablamalara görə "bitcoin"in tam emissiyası 2 140-cı ildə başa çatmalıdır.

"Bitcoin" heç bir tənzimləyici orqanın və ya mərkəzi bankın iştirakı olmadan fəaliyyət göstərir, şəbəkədə kriptovalyutaların emissiyası və əməliyyatların işlənməsi şəbəkədəki iştirakçılar tərəfindən kollektiv şəkildə həyata keçirilir. Şəbəkə bir neçə dəfə "hardfork" (sərt çəngəl) edilmişdir. "Bitcoin" şəbəkəsində hər saniyədə 7-8 əməliyyat təsdiqlənir.

"Bitcoin"də əməliyyatların təsdiqi və bloka əlavə edilməsi validatorların (maynerlərin) sayından aslı olaraq müəyyən "heş dərəcəsi" ("hash-rate") tələb edir. Validator sayına görə "heş dərəcəsi" daha mürəkkəbləşə bilər. Daha güclü "heş dərəcəsi"nə sahib olan validatorun məsələləri daha tez həll etmə imkanı yaranır. İlkin dövrdə bu hesablamaları bir kompüter və onun videokart gücünə etmək olduğu halda, hazırda müvafiq proses daha güclü yaddaş və hesablama cihazları tələb etdiyindən, *Konkret tətbiq üçün inteqral sxemlərdən ("Application Specific Integrated Circuit" - ASIC)* istifadə olunmağa başlanılmışdır. "ASIC" mayninqi xüsusi avadanlıqdan istifadə edərək əməliyyatların təsdiqi və blokların yaradılmasıdır. Xüsusi olaraq müəyyən bir kriptovalyutanın emissiyası üçün yaradılmış "ASIC"lər vasitəsi ilə hesablamalar xüsusi çiplərdən istifadə edilməklə aparılır ki, bu da adi kompüterlərdə istifadə olunan videokartlardan daha güclüdür.

Eyni zamanda, bir çox validatorlar emissiya prosesində iştirak etmək üçün xüsusi şəbəkələr – "Mayninq hovuzları" ("Mining Pool") ilə birləşirlər. Müvafiq "Mayninq hovuzları"nda qazanılan "bitcoin"lər onun iştirakçıları tərəfindən öz "heş dərəcəsi" ("hash-rate") ölçülərinə görə bölünürlər.

"Bitcoin" blokçeynində bloklar orta hesabla hər 10 dəqiqədən bir formalaşır. Hər blokun həcmi 1 meqabaytdır. Hazırda "segwit" texnologiyasından istifadə hesabına bir blok üzrə əməliyyat həcmi artmışdır.

Altkoinlər

"Ethereum" (Efirium). "Bitcoin"in uğurlu tətbiqi və açıq kodlu olması onun texnologiyasından istifadə edərək digər oxşar tipli əksmərkəzləşdirilmiş kriptovalyutaların yaranmasına səbəb olmuşdur. "Bitcoin"in sürətinin zəif olması, onda miqyaslanma və digər problemlərin mövcudluğu alternativ əksmərkəzləşməmiş kriptovalyutaların yaranması ilə nəticələnmişdir. Ümumiyyətlə, eyniranqlı açıq blokçeyn şəbəkələrdə miqyaslanma, əksmərkəzləşmə və təhlükəsizlik ilə bağlı olan çağırışların eyni zamanda həll edilməsi çox çətin məsələlərdəndir. Müvafiq məsələlər ilk dəfə Vitalik Buterin tərəfindən müəyyən olunduğundan, belə problem *Vitalik Buterin trilemması* adlandırılmışdır.

"Bitcoin"dən başqa, ondan sonra yaranmış bütün kriptovalyutalara altkoin deyilir. Altkoinlərin yaranma səbəbləri sırasına "bitcoin"in monopoliyasına qarşı mübarizə, onun alqoritm konsensusu, sürəti, əməliyyatların icra olunma növü və s. aid edilir. Hazırda "coinmarketcap.com" kripto-platformasında 7000-dən çox aktiv altkoin vardır. Funksiyalarına görə altkoinlər fərqlənirlər (*Əməliyyatların tezliyi və bahalı komissiyaların*

həlli (“XRP”), Anonimliyin həlli (“Dash”, “Monero”, “Zcash”), Mürəkkəb və bahalı mayninqin həlli, Funksionallığın çatışmazlığı (etherium) və s.).

2013-cü ildə “bitcoinmagazine.com” jurnalının həmtəsisçisi Vitalik Buterin “bitcoin”in proqram dilinin funksional çatışmazlığı səbəbindən yeni blokçeyni yaratmaq qərarına gəlmişdir. “bitcoin”də ən böyük boşluqlardan biri “bitcoin” blokçeyninin proqram dilinin tam tyurinqinin olmaması idi. Kompüter elmində *tam “tyurinq” (“full turing”)* proqramlaşdırma dili, müvafiq alqoritm, tələb olunan vaxt və yaddaş həcmi nəzərə alınmaqla, kompüterə istənilən konkret problemi həll etməyə imkan verən sazlama imkanıdır. 2013-cü ilin sonunda Vitalik Buterin öz yeni layihəsi olan “Ethereum”un *texniki sənədini (“white paper”)* buraxmışdır. Bu sənəddə vahid blokçeyn daxilində digər kriptovalyutaların, əksmərkəzləşdirilmiş proqramların yaradılması ilə bağlı məlumat verilirdi. 2013-cü ildə öz layihəsinə görə İsveçrədə 100 000 USD dəyərində olan Piter Till adına təqaüd aldıqdan sonra, 2014-cü ildə layihəyə əlavə vəsait cəlb etmək üçün Vitalik Buterin “kraudfandinq” elan etmişdir. Lakin bu “kraudfandinq” qiymətli kağız və ya hər hansı başqa formada deyil, “bitcoin” ilə qəbul edilirdi. Beləliklə, bu, virtual aktiv məkanında ilk *İlkin sikkə təklifi/yerləşdirilməsi (“ICO” – “Initial Coin Offering”)* hesab edilir. Müvafiq “ICO” nəticəsində Vitalik Buterin layihənin icrası üçün 31 000 BTC (18,5 mln. USD) toplamağa nail olmuşdur. Nəticədə, 30 iyul 2015-ci ildə “Ethereum” platforması yaradıldı.

İlk baxışdan “ehthereum”un “bitcoin”dən funksionallıq, əməliyyatların validasiyası, “coin”lərin alqı-satqısı və mübadiləsi baxımından fərqi yox idi. Lakin məhz “ethereum”un yaranması blokçeyn texnologiyasının yeni inkişaf mərhələsinə keçidinə səbəb olmuşdur. Onun təklif etdiyi smart müqavilələr blokçeyn texnologiyasının maliyyə sistemindən kənar istifadəsinə də geniş imkanlar yaratdı. “Ethereum” blokçeynində istifadə olunan proqram dilləri (“Solidity”, “Serpent”, “LLL”, “Mutan”) tam “tyurinq” funksiyalarına malikdir. Burada bir şəxs digərinə valyuta ilə yanaşı, hər hansı sənədi, hüquq və öhdəliyi də ötürmə qabiliyyətinə malik olur.

“Ethereum”un skripti “if-then” (“əgər-onda”) prinsipi ilə işləyir və bu ssenariyə uyğun əməliyyatlar “Ethereum” şəbəkəsinin qovşaqları tərəfindən avtomatik olaraq blokçeynə əlavə olunur.

Beləliklə, “Ethereum” - kodu açıq olan, “PoW” konsensus alqoritmi ilə işləyən, eyniranqlı əksmərkəzləşmiş tətbiqlər yaratmaq imkanı verən, smart müqavilə sistemi üzərindən işləyən bir platformadır. “Ethereum” platformasında hüquq, sənəd və digər dəyərlərin bir şəxsdən digərinə ötürülməsi üçün “PoW”dan istifadə edildiyindən, “bitcoin”də olduğu kimi burada da validatorların (maynerlərin) mükafatlandırılması zəruridir. “Ethereum”da bunun üçün özünün şəbəkədaxili valyutası olan “Ether”dən (ETH) istifadə olunur. “ETH” də “bitcoin”də olduğu kimi gündəlik əməliyyatlarda pul vasitəsi kimi istifadə oluna bilər. “Ethereum”da da minimal ödəniş vahidi mövcüddur: **1 ETH = 10^9 “gwei”.** Bəzən bu ölçü vahidini onun təsisçisinin adı ilə Şennon da adlandırırlar. Maynerlər (validatorlar) öz komissiyalarını “gwei” şəklində alırlar.

Lakin “bitcoin” blokçeynindən fərqli olaraq “ethereum” blokçeynində hər hansı bir əməliyyatın icrası üçün komissiyaların ödənilməsi könüllü deyil, bazar dəyərinə uyğun formalaşmışdır. Burada hər bir əməliyyatın icrası üçün müəyyən dərəcədə iş görülməlidir. Bunu avtomobilin işə salınması nümunəsində nəzərdən keçirək. Məsələn, bir avtomobilin işə salınması və sürülməsi üçün yanacaq lazımdır. “Ethereum” şəbəkəsində də vəsaitin göndərilməsi və smart müqavilənin yaradılması üçün “gas” adlanan komissiya haqqını efirlə ödəmək lazımdır.

“Gas” - “ethereum” üzrə hər-hansı bir əməliyyatın və ya smart müqavilənin icrası üçün tələb olunan hesablama resurslarına uyğun təyin olunmuş komissiya vahididir. “Gas”ın qiyməti şəbəkədəki tələbatdan asılı olaraq dəyişə bilər. Bunun səbəbi “Ethereum” şəbəkəsindəki mövcud olan hesablama resurslarının məhdudluğu ilə bağlıdır.

Şəbəkədə əməliyyatların sayı nə qədər çox olarsa, şəbəkənin yüklənməsi bir o qədər də artır və “gas”ın qiyməti tələbat əsasında yüksəlir. Eyni prinsip əksinə də doğrudur, şəbəkədəki əməliyyatların sayı azalanda, qazın qiyməti də aşağı düşür. “Ethereum” şəbəkəsinin bu formada çalışmasının əsas məqsədi əməliyyatının icrasına daha yükək xidmət haqqı ödəyən istifadəçiyə prioritet verməkdir.

“Gas”ın dəyəri gözləyən əməliyyat və Efirium Virtual maşınının görəcəyi işə görə dəyişə bilər. Məsələn, fərz edək ki, “A” şəxsi “B” şəxsinə 1 ETH köçürmək istəyir. Köçürmə üçün “gas” limitinin 21 000 olması məlumdur. Əməliyyat baş verən anda hesab edək ki, “gas”ın bir vahidinin orta dəyəri 200 “gwei”dir. Bu zaman “A” şəxsinin hesabından məxaric olacaq vəsait aşağıdakı kimi hesablanacaqdır:

“Gas” limiti × “Gas”ın bir vahidinin qiyməti = Məxaric olunan vəsait (“gwei” ilə)
Yəni: 21 000 × 200 = 4 200 000 “gwei”.

4 200 000 “gwei” isə 0.0042 ETH-yə bərabər olduğundan, “A” şəxsinin hesabından ümumilikdə 1.0042 ETH tutulacağını hesablamaq olar. Burada, 1 ETH “B” şəxsinin hesabına, 0.0042 ETH isə “mayner”ə (validatora) mükafat olaraq köçürülücəkdir. Sistem bu formada 2021-ci ilin avqust ayına kimi işləyirdi. Lakin avqust ayından sonra qəbul olunmuş “EIP 1559” protokoluna əsasən, köçürmələrdə istifadə olunan komissiyanın bir hissəsinin yandırılaraq yox edilməsi nəzərdə tutulmuşdur. Yandırılması nəzərdə tutulan komissiya *baza ödənişi (“base fee”)* adlanır. Müvafiq düstur aşağıdakı formada olacaqdır:

“Gas” limiti × (baza ödənişi + sürətli əməliyyat üçün ödəniş)

Məsələn, fərz edk ki, “A” şəxsi “B” şəxsinə 1 ETH göndərir və baza ödənişi (“base fee”) 100 “gwei”yə bərabərdir. “A” şəxsi baza ödənişindən başqa əməliyyatın daha tez keçməsi üçün əlavə olaraq 10 “gwei” də köçürmə etmək qərarına gəlir, yəni:

21 000 × (100 + 10) = 2 310 000 “gwei” = 0.00231 ETH

Beləliklə, alınmış məbləğdən validatora (maynerə) 0.00021 ETH köçürüləcək, 0.0021 ETH isə yandırılacaqdır. Bundan əlavə, “B” şəxsinə 1 ETH köçürüləcəkdir. Yandırılmanın səbəbi emissiyanın yuxarı həddinin olmaması ilə əlaqələndirilir. Şəbəkə yaradıcıları bu yolla “Ethereum”un giymətinin ucuzlaşmasının qarşısını almağa çalışırlar.

“Gas” limiti eyni zamanda blokun həcminə də təsir edir. Belə ki, yeni yaranacaq blok üçün ona əlavə olunan əməliyyatların ümumi sayına müəyyən “gas” limiti qoyulur ki, bu həddi aşmaq mümkün deyildir. “EIP 1559” protokolundan sonra “gas” limiti 15 mln.-dur. Lakin bu limit iki dəfəyədək artırıla bilər.

Əməliyyat üçün komissiya ödənişi köçürməni edən şəxs tərəfindən öz seçiminə əsasən təyin edilir. Lakin burada istifadəçilər müəyyən risklərlə qarşılaşa bilərlər, xüsusilə də çox aşağı xidmət haqqı qeyd edənlər əməliyyatların icrasını aylarla gözləyə bilər, yaxud müvafiq əməliyyat bir müddətdədən sonra geri qaytarıla bilər.

“Ethereum” üzrə tipik əməliyyat aşağıdakı məlumatları özündə saxlayır:

Əməliyyatın heşi:	0x652e51ac4b56b1dc82odc850fb2bde344b622df129a4vk
Əməliyyatın qəbul edilmə statusu:	Uğurlu
Blokun hündürlüyü:	5828416 (2 blokun təsdiqi)
Zaman qeydi:	45 saniyə əvvəl (İyun-21-2021 12:37:09 PM +UTC)
Göndərən:	0x1c40d52e51ac4b56b1dc82odc850fb2b
Alan:	0xc179fbd51ac4b56b1dc82odc850fb2b
Məbləğ (dəyər):	0.04981708 ETH ($26.67)

“Gas” limiti:	42000
“n” əməliyyatı tərəfindən istifadə olunmuş “gas”:	21080
“Gas”ın qiyməti:	0.0000000060003 ETH (6.0003 gwei)
Əməliyyatın cari dəyəri/ödəniş:	0.000126486324 ETH ($0.07)
Birdəfəlik kod (“nonce”) / (mövqe):	39 | {78}

“Ethereum” hesab əsaslı blokçeyndir. Burada iki növ hesablar mövcüddur: (i) *“mülkiyyətdə olan” (“externally owned”)* – bu hesablar məxfi açarı özündə saxlayan şəxslər tərəfindən idarə olunur; (ii) *“müqavilə” (“contract”)* – smart müqavilə formasında blokçeyndə yerləşdirilən və kodla ifadə olunan hesablar.

“Ethereum”da samrt müqavilə - müqavilənin müəyyən şərtlərinin yerinə yetirilməsi baş verdikdə, tərəflər arasındakı müqavilənin şərtlərinə əməl olunmasını təmin edən və əməliyyatı icra edən bir proqramlaşdırma kodudur. Məsələn, hesaba hər dəfə vəsait daxil olunanda göndərən şəxsə “təşəkkür edirəm” mesajının göndərilməsi ağıllı müqavilə adlanır. Bu müqavilələr daha mürəkkəb, çox miqyaslı və bir neçə pilləli olan daha mürəkkəb prosesləri idarə edə bilirlər və buna görə əksmərkəzləşdirilmiş tətbiqi proqram hesab olunurlar.

Steyblkoinlər

Adi kriptovalyutaların həddindən artıq volatil və təminatsız olması daha stabil kriptovalyutaların yaranmasına səbəb olmuşdur. Belə kriptovalyutalar “**Steyblkoin**” **(“Stablecoin”)** adlanır. Digər kriptovalyutalardan fərqli olaraq, “steyblkoin”lər volatil olmur və dəyərləri stabil fiziki aktiv (qızıl, neft) və ya valyuta ehtiyatları (məsələn, dollar) ilə təmin olunur.

Yaranma formasına görə “steyblkoin”lər mərkəzləşdirilmiş şirkətlər və əksmərkəzləşmiş avtonom şirkətlər tərəfindən yaradılır (“DAO”lar). Adətən, şəffaflığın təmin olunması üçün onların fəaliyyəti və aktivləri il ərzində bir neçə audit şirkəti tərəfinədən audit olunur. Funksional olaraq “steyblkoin”lərin öz blokçeynləri mövcüd olmur və onlar “Proof of Reserves” (“PoR”) konsensus alqoritmindən istifadə edir. Nümunə üçün “Tether” (“USDT”) və “Dai” (“DAI”) kimi fərqli steyblkoinləri nəzərdən keçirək.

Ehtiyatların milli valyutada tam təmin edilməsi sayəsində “Tether”in qiyməti dollara bağlıdır, digər sözlə hər bir “Tether”in emissiyası bir dollar ehtiyatla təmin edilib. “CoinGecko.com” portalının məlumatına görə, 2021-ci ildə ən iri kapitalizasiya “Tether” “steyblkoin”inə məxsusdur. Lakin ümumi qaydalara baxmayaraq, onun ehtiyatlarını yoxlamaq bu günə qədər mümkün olmayıb və bu səbəbdən, istifadəçilər yalnız “Tether” yaradıcılarının bəyanatına etibar edə bilirlər. Beləliklə, “Tether” dollarla təmin edilmiş mərkəzləşdirilmiş bir “steyblkoin”dir. Lakin bir sıra araşdırmalar nəticəsində “Tether”in təminatı kim tək ABŞ dolları deyil, digər valyutaların da çıxış etdiyi müəyyən olunmuşdur.

“DAI”nin ehtiyatları isə “ETH” (efir) kriptovalyutası ilə təmin olunub. Əksmərkəzləşdirilmiş bir avtonom təşkilat üzvləri və smart müqavilələr tərəfindən səsvermə yolu ilə idarə olunan protokollar vasitəsilə dəyəri dollara bağlanılıb və “USDT”nin əksinə olaraq onun ehtiyatları istənilən vaxt asanlıqla yoxlanıla bilər. Beləliklə, “DAI” kriptovalyuta ehtiyatları ilə təmin edilmiş əksmərkəzləşdirilmiş “steyblkoin”dir.

“Steyblkoin”lər tətbiqi maliyyə proqramı olmasa da, kriptovalyuta aləmində nisbətən aşağı riskli və qeyri-volatil alət rolunu yerinə yetirərək, “DeFi” tətbiqində hər kəs üçün risklərin azaldılması üzrə əlverişli bir alətə çevrilmişlər.

Ümumiyyətlə, ehtiyat bazasının növündən asılı olaraq, kriptovalyuta bazarında aşağıdakı növlərdə “steyblkoin”lər mövcuddur:

- fiat təminatlı “steyblkoin”lər;
- əmtəə təminatlı “steyblkoin”lər;
- kriptovalyuta ilə dəstəklənən “steyblkoin”lər;
- senyoraj (“seigniorage”) növlü “steyblkoin”lər.

Qeyd olunan “steyblkoin” növlərinin özünəməxsus iş prinsipi, üstünlükləri və çatışmazlıqları mövcuddur.

Fiat təminatlı “steyblkoin”lər. Müvafiq “steyblkoin”lərə məzənnəsi fiat pul (dollar, rubl və ya digərləri) ilə təmin edilən kriptovalyutalar aiddir. Burada məqsəd “steyblkoin” sahibinin hər an onları real pula dəyişdirməsi imkanının yaradılması baxımından “steyblkoin”in məzənnəsinin sabitliyini təmin etməkdən ötrü kriptovalyutanın dəyərini bank hesablarındakı real pullarla 1:1 nisbətində dəstəkləməkdir. Fiat təminatlı “steyblkoin”lərin iş prinsipi olduqca sadədir: emitent əvvəlcə bank hesabına depozit yerləşdirir, sonra isə depozit məbləğində tokenləri emissiya edir. Tokenlərin sahibi onları fiatla dəyişdirdikdə, ekvivalent miqdarda tokenlər dövriyyədən çıxarılır və ya məhv edilir.

Əmtəə təminatlı “steyblkoin”lər. Bu növ tokenlərin məzənnəsi fiziki aktivlərin (qızıl, qiymətli daşlar və s.) qiymətinə bağlıdır. Məsələn, təminat şəklində qızıldan istifadə edilərsə, bu halda bir “steyblkoin” qızılın müəyyən miqdarına (məsələn, 1 qram qızıla) bərabər götürülür və s. Aktiv ilə dəstəklənən “steyblkoin” nümunəsi kimi rübdə bir dəfə yoxlamadan keçirilən Sinqapurun “Safe house”da yerləşən “DGX” tokenini göstərmək olar.

Kriptovalyuta təminatlı “steyblkoin”lər. Bəzi “steyblkoinlər” digər virtual aktivlər, adətən, bazarda ən böyük kapitalizasiyaya malik olan “bitcoin”, “ethereum” kimi kriptovalyutalar ilə dəstəklənir. Eyni zamanda, risklərin minimum səviyyəyə salınmasında təminat üçün bir neçə virtual aktivdən istifadə olunur. Belə “steyblkoin”lər əsasən əksmərkəzləşdirilmiş “P2P” platformalarında istifadə edilir. Kriptovalyuta ilə dəstəklənən bütün “steyblkoin”lər demək olar ki, smart müqavilələr üzərindən çalışırlar.

Senyoraj (“Seigniorage” - alqoritmik) növlü “steyblkoin”lər. Bu növ tokenlər kriptovalyuta kütləsini artırmaq və ya azaltmaq üçün alqoritmik yanaşmadan istifadə edir. Eyni metod Mərkəzi Bank tərəfindən inflasiya səviyyəsinin tənzimlənməsi məqsədilə istifadə olunan pul kütləsinin tədavülünün artırılması və ya azaldılması alətinə analojidir. Bu cür sikkələrin əsas məqsədi məzənnəni eyni səviyyədə, məsələn, 1 dollar səviyyəsində saxlamaqdır.

Bölmə

Dörd

4

CÜZDANLAR VƏ ONLARIN NÖVLƏRİ

- cüzdan
- mnemonik ifadə
- ilkin ifadə
- heş-funksiya
- açıq açar
- qapalı açar
- hesab
- cüzdan zənciri
- ünvan açarı

Cüzdan anlayışı və növləri

Kriptovalyutaların alışı prosesinin ilkin pilləsi cüzdanların yaradılmasından ibarətdir. Lakin virtual məkanda istifadə olunan kriptovalyuta cüzdanları gündəlik həyatdakı ənənəvi cüzdanlardan bir qədər fərqlənir. *Kriptovalyuta cüzdanı* – funksional olaraq açarların anbarını, eləcə də cüzdan sahibinin əməliyyatlarını və balansını əks etdirən interfeysdir. Yəni cüzdan - açar sahibinə öz vəsaitlərini və əməliyyatlarını izləmə və idarəetmə səlahiyyəti verən vasitədir. Virtual məkanda cüzdanlar riyazi və kriptoqrafik funksiyalardan istifadə etməklə formalaşır. Kriptovalyuta cüzdanları sikkələri deyil, açarları saxlayır. Hər bir istifadəçinin açar cütündən - şəxsi (qapalı) və açıq açarlardan ibarət pul kisəsi mövcuddur. İstifadəçilər açıq açardan formalaşan ünvanla vəsaitləri bir-birinə göndərə bilir. Sistem validatorlarına əməliyyatın həqiqiliyini və vəsaitlərin ünvan sahibi tərəfindən icra edildiyini göstərmək məqsədilə şəxsi (qapalı) açardan istifadə olunur. Cüzdan üzrə əməliyyat göndərən tərəfin alan tərəfin açıq açarını daxil etməklə həyata keçirilir. Qapalı açar isə alan tərəfin əməliyyatı təsdiqləməsi üçün istifadə olunur. Qapalı açar məxfi olmaqla, yalnız cüzdan sahibində olur.

Virtual aktiv cüzdanı - virtual aktivlərin toplanılması, saxlanılması və ötürülməsi (köçürülməsi) üçün istifadə olunan vasitədir (proqram təminatı və ya digər mexanizm/daşıyıcıdır).

Cüzdanlar daima internet şəbəkəsinə qoşulu olub-olmamasına görə isti və soyuq cüzdanlara bölünürlər.

İsti cüzdanlar – daim internetə qoşulu olan cüzdanlardır. Misal üçün, “Binance” birjasında şəxs qeydiyyatdan keçdikdə bu cüzdan daima onlayn vəziyyətdə qalacaqdır. Bu növ cüzdanlar treyderlər üçün rahatlıq yaratsa da, kiberhücum və dələduzluq hallarına qarşı dayanıqlı deyillər.

Soyuq cüzdanlar – isti cüzdanlardan fərqli olaraq daim internetə qoşulu olmaya bilər. Əsasən bu, açarları özündə saxlayan fiziki daşıyıcılar formasında olur və avtonom rejimdə işləyə bilirlər. Bu cüzdanların işləmə mexanizmi daha mürəkkəb olsa da, onlar kiberhücum və dələduzluq hallarına qarşı dayanıqlı olurlar.

Mərkəzləşmiş birjalar öz vəsaitlərinin yalnız cüzi hissəsini isti cüzdanda, əsas hissəsini isə soyuq cüzdanlarda saxlayırlar. Mərkəzləşmiş birjalarda vəsaitlərini saxlamaq istəməyən şəxslərin öz vəsaitlərini əksmərkəzləşmiş birjalarda saxlamaq imkanı mövcuddur. Bu birjada açarlar birjada deyil, cüzdan sahiblərinin özündə olur.

Qapalı açarın kimdə saxlanılmasından asılı olaraq, cüzdanlar ***kastodial*** (qapalı açarın üçüncü tərəfdə olması) və ***qeyri-kastodial*** cüzdanlara bölünürlər.

Cüzdanların internetə daimi qoşulu olma xüsusiyyətinə və qapalı açarın kimdə saxlanmasına görə aşağıdakı növ cüzdanlar mövcüddur:

Proqram təminaltı cüzdanlar: istifadəçilər və qapalı açarlar barədə məlumatları özlərində saxlayan proqram təminatlı cüzdanlardır. Belə cüzdana nümunə olaraq *“trust wallet”i* göstərmək olar. Müvafiq növ cüzdanlar əsasən isti cüzdanlar kateqoriyasına daxil olur və aşağıdakı növlərə bölünür:

a. veb-cüzdanlar (onlayn cüzdanlar) – bu cüzdanlar blokçeyn şəbəkəyə çıxışı hər-hansı brauzer vasitəsi ilə etməyə imkan verirlər. Bu cüzdanlara birjada yaradılan cüzdanları və digər onlayn formada işləyən cüzdanları aid etmək olar. Adətən, bu növ cüzdanlarda məxfi açar istifadəçidə deyil, vasitəçidə olur.

b. mobil cüzdanlar lokal (desktop) cüzdanlar kimi işləyir. Yeganə fərq məlumatların kompüterdə deyil, digər elektron cihazlarda (telefon, planşet və s.) olmasıdır. Mobil cüzdanların ödəniş və hesablaşmalarda “QR” kod vasitəsi ilə istifadəsi çox rahatdır.

Lokal (masaüstü, desktop) cüzdanlar – kompüterə yüklənən və istifadə olunan proqram təminatı hesabına yaradılır. Veb-cüzdanlardan fərqli olaraq bu növ cüzdanlar onun sahibinə məxfi və açıq açara tam sahib olma imkanı yaradır. Bunun üçün öncədən müvafiq blokçeyn platformaya uyğun olan proqram yüklənməlidir. Yüklənən fayllardan *"wallet.dat"* faylı kompüterin yaddaşında qalmalıdır. Bu faylda cüzdana giriş icazəsi verən açarlar saxlanılır. Açar məlumatlarını məxfi saxlamaq üçün müvafiq fayl kodlaşdırılır. Fayl itirildikdə və ya parol unudulduqda, istifadəçi cüzdana giriş imkanını itirmiş olur. Bu səbəbdən, adətən, kompüterin əl çatan olmadığı halda digər avadanlıq vasitəsi ilə cüzdana giriş icazəsini təmin etməkdən ötrü bu faylların nüsxəsi çıxarılır, yaxud ilkin ifadə ("seed") və məxfi açar digər bir ünvana köçürülə bilər. Bu növ cüzdanların quraşdırılması zamanı kompüterdə virusların olmaması mütləqdir. *Lokal cüzdanların* da öz növbəsində iki növü mövcuddur: ağır və yüngül cüzdanlar.

"Ağır" cüzdanlar - bütün blokçeyni kompüterə yükləyir, istifadəçini blokçeyn şəbəkəsinin tamhüquqlu üzvü səviyyəsinə qaldırır və kompüterdə böyük həcmdə yaddaş tələb edir (məsələn, "bitcoin"də 2019-cu ilin əvvəlinə bu 236 GB-dən çox idi). *"Yüngül" cüzdanlar* isə əksinə, bütün blokçeyni şəxsi kompüterə köçürmür, saxlanılması zəruri olan bəzi məlumatları kompüterin yaddaşında saxlayır. Onlar əsas şəbəkə ilə, bəzi hallarda isə müxtəlif "API"lar vasitəsilə mübadilə aparır.

Cihaz cüzdanlar soyuq cüzdan olaraq daima internetə qoşulu olmurlar. Müvafiq cüzdanlar məxfi və açıq açarın yaradılması üçün xüsusi sözlərdən ("seed phrase") təşkil olunur, onlarda xüsusi hesablama formalarından istifadə edilir. Həmçinin bu cüzdanlardan bəzi əksmərkəzləşdirilmiş birjalarda və veb-birjalarda da istifadə etmək mümkünüdür.

Kağız cüzdan – ayrıca bir cüzdan növü olaraq, bir kağız üzərində məxfi və açıq açarların çap olunmuş formasıdır.

Qeyri-deterministik cüzdan. Satoşi özünün ilkin tezislərində anonimliyin qorunması üçün hər bir əməliyyatı bir ünvanla aparmağı tövsiyə edirdi, bu prinsipə "bir ünvan - bir əməliyyat" da deyilir. Qeyri-deterministik cüzdan növü Satoşi və digər ilk istifadəçilərin işlətdiyi ilk cüzdan növüdür. Bu cüzdanlar təsadüfi olaraq müəyyən sayda yaradılan şəxsi (qapalı) açarların toplusuna bənzəyir. Məsələn, "Bitcoin Core" müştərisi ilk 100 təsadüfi şəxsin açarını generasiya etmə qabiliyyətinə malik olurdu. Daha sonra, zərurət olduğu təqdirdə, əlavə şəxsi açarların yaradılmasına ehtiyac yaranırdı. Bu növ pul kisəsi **JBOK** ("Just a Bunch Of Keys" - sadəcə açar dəsti) adlandırılır. Müvafiq açarları idarə etmək, onlar üçün hər dəfə ehtiyat nüsxələr yaratmaq və əldə etmək çətin prosesdir. Hər yeni açar yaradıldıqda onun yeni ehtiyat nüsxələri də yaradılmalıdır. Bu baş vermədiyi halda, eləcə də açara bağlı ünvana giriş icazəsi itirildiyi halda, sikkələri bərpa etmək mümkün olmayacaqdır. Qeyd edilən nüanslar istifadəçilərin Satoşinin qeyd etdiyi "bir əməliyyat - bir ünvan" prinsipini icra etməməsinə və hər bir əməliyyat üçün bir ünvandan istifadə etməsinə səbəb olmuşdur. Bu isə sistemin təklif etdiyi anonimliyi aradan qaldırmış olur.

Deterministik cüzdan – bu növ cüzdanlar qeyri-deterministik cüzdanlardan fərqli *"n"* sayda cüt açıq və qapalı açarlar yaradırlar. Onların yaradılması üçün müəyyən ilkin (məxfi) ifadələrdən ("seed phrase") istifadə olunur. İlkin ifadə cüzdanla bağlı bütün açarları müəyyən etməyə imkan verən alətdir. Müvafiq cüzdanın əsas xüsusiyyəti cüzdan sahibi tərəfindən ilkin ifadədən "*n"* sayda açarın yaradılmasının mümkünlüyüdür. Bu cüzdanlarda bütün şəxsi (qapalı) açarları bərpa etmək üçün yalnız ilkin ifadəni bilmək kifayət edir. Deterministik cüzdanlarda hər açar üçün ehtiyat nüsxəsinin yalnız bir dəfə yaradılması kifayətdir (qeyri-deterministik cüzdanlarda isə hər dəfə yeni açar yaradılanda məlumatların ehtiyat nüsxəsi yaradılır). Eyni zamanda, cüzdanda olan məlumatların qəbul olunması və ötürülməsi prosesi də sadələşir. Həmçinin məlumatı bir cüzdandan

digərinə ötürmək üçün ilkin ifadəni bilmək kifayətdir. İlkin ifadə xüsusi birtərəfli “heş” (hash) hesablama vasitəsi ilə *mnemonik kodlardan* və *entropiyadan* hesablanır.

Entropiya heç kimin əvvəllər yaratmadığı və ya gələcəkdə yarada bilməyəcəyi çox böyük təsadüfi ədəddir. Bu ədədlər “*bit”* formasında olurlar (misal üçün: 10010001110). Bit (0 və ya 1) kompüterdə informasiyanın saxlanılması üçün istifadə olunan ən kiçik vahiddir. Entropiya minimum 128, maksimum 256 “bit”dən ibarət olmalıdır. Bu qədər “bit” təkrarlanmanın qarşısını almaq üçün kifayət edən həcmdir. Hasil olunmuş entropiya 32 bitə bölünməlidir.

Mnemonik ifadə (kod) və ya xüsusi söz (“seed phrase”) – entropiyada alınan rəqəm ifadələrinin onluq ədədə çevrilərək blokçeyndə istifadə olunan, əvvəlcədən müəyyən edilmiş ingilis dilli lüğətdə (BIP39) onun qarşı söz ifadəsidir. Mnemonik ifadə entropiya bitinin həcminə uyğun 12, 18 və 24 sözdən ibarət ola bilər. İlkin ifadənin hasil olunması üçün istifadə edilən lüğətdə 2048 söz vardır. Lakin ilk rəqəm sıfırdan başlamalı olduğundan, entopiyadan əldə edilən onluq rəqəmə 1 əlavə etmək və ona uyğun sözü mnemonik kodda istifadə etmək lazımdır. Bu koddan yaranan söz ardıcıllığı vasitəsi ilə ilkin ifadə yaradılır.

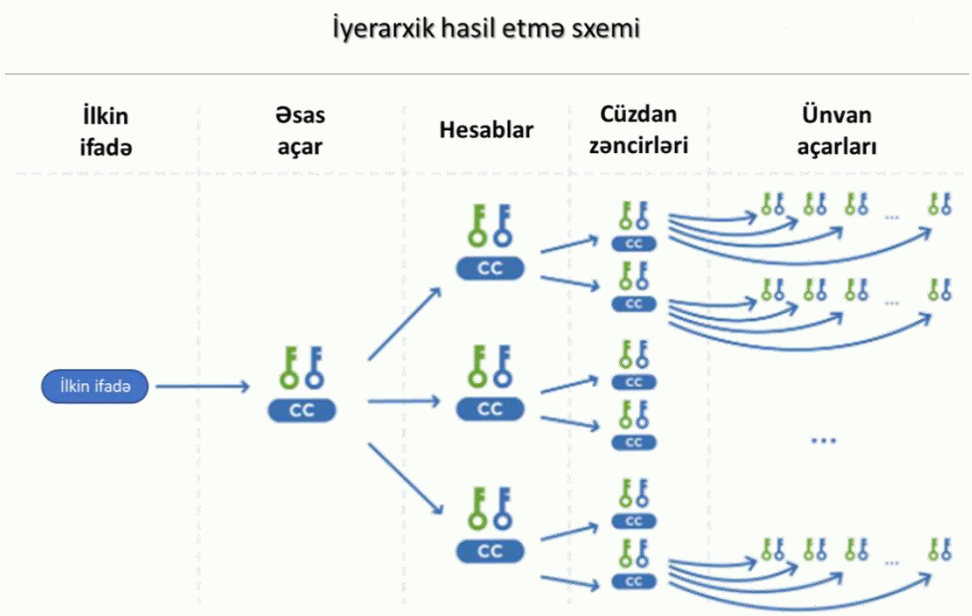
Deterministik cüzdanlar iki formada olur: ardıcıl deterministik cüzdan və iyerarxik deterministik cüzdan.

Ardıcıl deterministik cüzdanda ilkin ifadədən və indeks sıra nömrəsindən “heş” (hash) hesablanır. “SHA-256” funksiyasından istifadə etməklə 4 mlrd.-a (4 bayt) qədər məxfi açar formalaşır. Praktikada bu qədər açarın bütün ehtiyacları qarşılayacağı nəzərdə tutulur.

İyerarxik deterministik cüzdanların (“HD wallets”) açarları “BIP32” prinsipi üzrə hasil olunur. Burada ilkin ifadədən əsas açar alınır. İyerarxik deterministik cüzdana məxsus açıq açar məxfi açarın yarandığı anda formalaşır.

İyerarxik deterministik cüzdanın işləmə prinsipi aşağıdakı kimidir:

Hər şey ilkin ifadədən (buna bəzən “master-seed” də deyilir) başlayır. Onun vasitəsi ilə açar cütü və “0” nömrəli zəncir kodu (“chain code”) formalaşır. Yaranan bu açar cütünə əsas açar (“master key”) da deyilir. Əsas açardan şəxsi (məxfi) və açıq açar, eləcə də indeks nömrəsinə görə daha kiçik açarlar formalaşaraq yekunda ünvan üçün istifadə oluna bilirlər. “BIP32” üzrə açarın hasil olunması prosesinin ətraflı izahı aşağıdakı sxemdə verilmişdir:



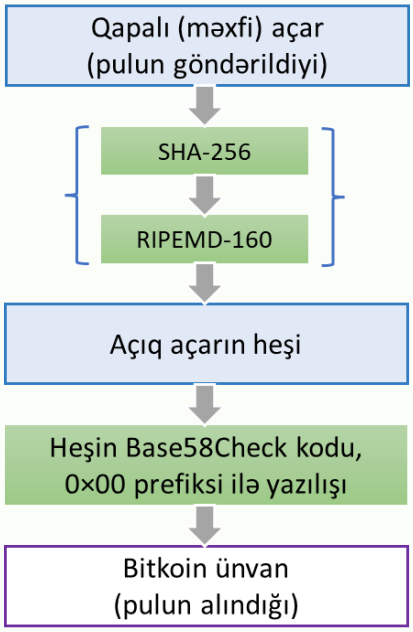
Qeyd: cc (“chain code”) – zəncir kodudur

İlkin ifadədən əsas açar "heş" funksiyanın digər növü olan "*HMAC" (Hash-based message authentication code – heş əsasında məlumatın eyniləşdirilməsi kodu)* vasitəsi ilə əldə olunur. Burada nəticənin əldə olunması üçün iki ifadə - sabit sətir və məxfi söz qeyd olunmalıdır. Bu məlumatlar "SHA-512" heş funksiyası ilə emal olunur. Nəticədə əsas qapalı açar və zəncir kodu əldə olunur. Zəncir kodu – eyni uzunluqlu ikili vektorların sıralanmasıdır.

Qapalı açardan ona bağlı açıq açar "Elliptik Əyrili Rəqəmsal İmza Alqoritmi"nin ("ECDSA") variasiyası olan "secp256k1" texnologiyası ilə əldə edilir. Müvafiq "heşinq" birtərəfli formada baş verdiyindən, digər tərəfi çıxarmaq demək olar ki, mümkün deyil.

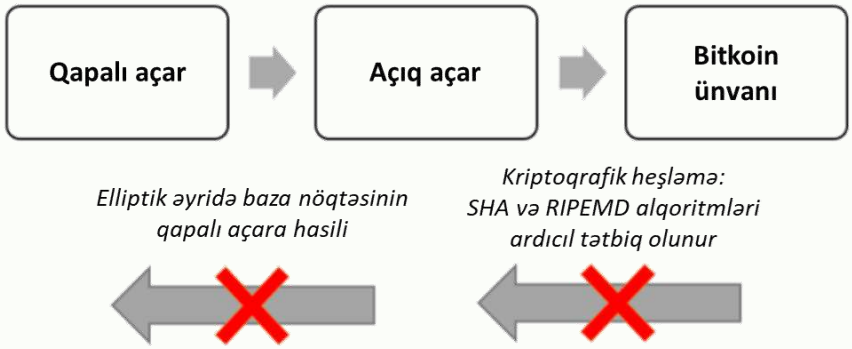
Əldə edilmiş açar cütlərindən xüsusi indeksləri olan çoxlu sayda digər açar cütləri yaradıla bilər. Yeni yaradılan iyerarxiya hesablara analoji qaydada isitifadə olunur. Fərz edək ki, ilkin ifadəsi olan hər hansı bir istifadəçi bir-birindən fərqli olan bir neçə ünvan yaratmaq istəyir. Bu ünvanlara məxsus sikkələrin qarışdırılmaması və başa çatmış əməliyyatlarda onlar arasında hər hansı əlaqənin aşkar edilməməsi, açarların tamamilə bir-birindən ayrı istifadəsi nəzərdə tutulur. Hesabların birində açarlar qrupu işçi büdcə üçün, digərində - şəxsi büdcə üçün, digər hesab isə şəxsi uçot üçün istifadə olunacaqdır. Bütün bu prosesdə isə sikkələr bir-birinə qarışmayacaq və ilk baxışda hesabların hər hansı bir şəxlə əlaqəliliyi müəyyən edilməyəcəkdir.

Məsələn, "bitcoin"də qapalı açarın ünvanı ardıcıl olaraq "Təhlükəsiz heşləmə alqoritmi" ("Secure Hash Alqorithm" – "SHA")" və "RIPEMD" ("RACE Integrity Primitives Evaluation Message Digest") kimi iki kriptoqrafik "heşinq" ("hashing") alqoritminin tətbiqi ilə əldə olunur. Birinci mərhələdə alınan heş uzunluğu 256 bit ("SHA-256" alqoritmi istifadə olunur), ikinci mərhələdə isə 160 bit ("RIPEMD-160") təşkil edir.



İyerarxik açarların ilk standardı "BIP32" standartı hesab olunur. Daha sonra, müvafiq standartlar bir qədər inkişaf eədərk "BIP44" və digər formalar yaranmışıdr. Cüzdanda olan ilkin ifadə vasitəsi ilə bir standartı qəbul edən açarlar digər standart formada açıldığı halda nəticə vermirlər. Müvafiq standartlar da öz növbəsində ilkin ifadənin və ya bitin uzunluğuna görə digərindən fərqlənir.

Kriptocütlük (qapalı və açıq açar) ilə “bitcoin” ünvanı arasında əlaqə aşağıdakı şəkildə verilmişdir:



Bölmə

Beş

5

KRİPTOVALYUTALAR İLƏ MÜBADİLƏ ALƏTLƏRİ. BİRJALAR VƏ ONLARIN NÖVLƏRİ

- kripto-birja
- DEX
- OTC
- mübadilə proqramları

Kriptovalyutalar ilə mübadilə alətləri

Kriptovalyuta bazarına təkan verən əsas texniki yeniliklərdən biri müxtəlif *mübadilə platformaları ("P2P")* hesab edilir. Bu mübadilə vasitələri arasında ən böyük pay kriptovalyuta birjalarının payına düşür. Kriptovalyuta birjalarının iş prinsipi adi səhm birjalarının iş prinsipi ilə çox oxşardır. Fərq yalnız istifadə olunan aktivlərdədir. Kriptobirjalar demək olar ki, kriptovalyutalar ilə eyni anda yaranıb.

Kriptovalyuta mübadiləsi ilk dəfə "New Liberty Standard" onlayn birjasında həyata keçmişdir. 2009-cu ilin oktyabrında yaranan bu birja "bitcoin" blokçeynində "bitcoin"lərin alına biləcəyi ilk onlayn birja hesab olunurdu. Həmin dövrdə "bitcoin"in dəyərinin müəyyən edilməsində problemlər olduğundan, "New Liberty Standard" saytı onun dəyərini özünün "mayninq" etdiyi "bitcoin"lərin əldə edilməsinə görə sərf edilən elektrik enerjisinə xərclənmiş vəsaitlə qiymətləndirmək qərarına gəlmişdir. Burada "bitcoin"in alqı-satqısı əsasən kriptoanarxistlər və həvəskarlar tərəfindən baş verirdi. Lakin "New Liberty Standard"ı birja olaraq adlandırmaq düzgün də olmazdı, o, daha çox vəsait mübadiləsini həyata keçirən servis funskiyasını həyata keçirirdi. 2010-cu ildə yeni birjalar - "Mt. Gox", "Bitcoin Market", "Tradehill" birjaları yaranmışdır.

"CoinMarketCap.com" saytının məlumatına (noyabr, 2021) əsasən, kriptovalyuta birjalarında ticarəti aparılan 14600-dən çox rəqəmsal aktivlərin ümumi bazar kapitallaşma həcmi 2.6 trilyon dollardır. 2020-ci ildən başlayan iqtisadi izolyasiya dövründə "bitcoin" və bəzi kriptovalyutalara tələb və etibar artmağa başlamışdır. Bunun nəticəsi olaraq, 2020-ci ilin I yarısından başlayaraq rəqəmsal aktivlərə edilən investisiyalar öz sahiblərinə kifayət qədər gəlir qazandırmışdır. "Bitcoin" və "ethereum" kripto-investorların əsas aktivləri olaraq qalsa da, digər rəqəmsal aktivlər (altkoinlər) də 2021-ci ildə yüksək marjaya malik olub.

Kriptoanarxistlər və liberallar üçün mərkəzləşdirilməmiş şəkildə alqı-satqı əməliyyatları fiziki olaraq mümkün olsa da, bu sistemin real iqtisadiyyata inteqrasiya cəhdlərində mühüm bir çatışmazlıq müəyyən edilmişdir. Müvafiq çatışmazlığın əsasında isə kriptoaktivlərin fiat pula çevrilməsi dayanır. Kriptovalyuta bazarında əməliyyatların həcminin (say və məbləğin) getdikcə artması ticarətin ədalətliliyinə zəmanət verəcək, mübadilə məqsədilə "bitcoin"ləri saxlayacaq, fiat ilə kütləvi əməliyyatlar aparacaq subyektlərin meydana gəlməsi zərurətini şərtləndirirdi. Müvafiq funksiyaları isə kriptovalyuta birjaları öz üzərinə götürdü.

Birjalar və onların növləri

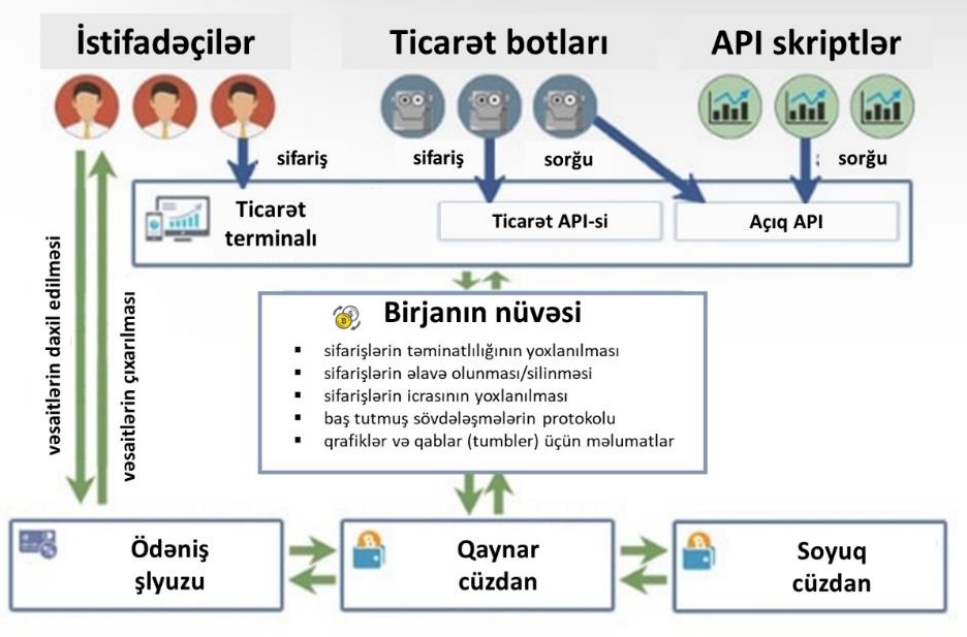
Funksiyalarına görə kriptovalyuta birjaları üç qrupa bölünür:

- müxtəlif növ kriptovalyutaların ("bitcoin", "litecoin", "ether" və s.) bir-biri ilə mübadiləsini və manipulyasiyanı təşkil edən birjalar;
- kriptovalyutaları fiat dünya valyutalarına (dollar, avro, rubl və s.) mübadilə edən birjalar;
- kriptovalyuta üzrə spekulyasiya əməliyyatlarının (manipulyasiyalarının) tam spektrini həyata keçirən birjalar (onlar birinci və ikinci qrupların funksiyalarını birləşdirir).

Likvidliyin kim tərəfindən təmin edilməsi, əməliyyatların blokçeyn şəbəkədə aparılıb-aparılmaması, qapalı açarın kimdə olması və digər parametrlərə görə kripto-birjalar *mərkəzləşmiş və əksmərkəzləşmiş* olur.

Mərkəzləşmiş kripto-birjalarda qapalı açar birjanın özündə qalır. Burada əməliyyatlar birjadaxili və blokçeyndə aparıla bilər.

Mərkəzləşmiş kripto-birjaların işləmə prinsipi aşağıdakı kimi təsvir oluna bilər:



Mərkəzləşmiş kriptobirjalar fiat valyuta ilə əməliyyatları dəstəklədikdə, onların müvafiq valyutaların saxlancı üçün müəyyən banklarda hesablarının olması zəruridir. Bu funksiyanın birjanın özü, yaxud ödəniş aqreqatorları tərəfindən təmin olunma imkanları vardır. Daxil edilən fiat valyutaların müqabilində birjanın təyin etdiyi məzənnə və komissiya haqqları tutulmaqla birja istifadəçilərinin hesablarına kriptovalyutalar köçürülür.

Birja daxilində istifadəçilərin məxfi açarları birjanın özündə saxlanılır. Burada birja istifadəçilərin hesablarını bir-birindən fərqləndirmək üçün ünvanlarda *“memo” kodlardan* (rəqəm, hərf və s.) istifadə edir ki, onlar da əsasən mərkəzləşdirilmiş birjada yerləşən kriptovalyutanın blokçeyn şəbəkəsi üzrə əməliyyatlarının aparılması üçün istifadə olunur.

Eyni zamanda, mərkəzləşdirilmiş birjalarda əməliyyatlar birjadaxili hər hansı iki istifadəçi arasında baş verdikdə, bu əsas blokçeyn şəbəkəsində əks olunmur, yəni əməliyyat yalnız birjadaxili olaraq bir ünvandan digərinə köçürülür. Birjalar bütün istifadəçilərin vəsaitlərini öz cüzdanında saxlayır. Özlərini kiberhücumlardan qorumaq məqəsdilə bir çox hallarda onlar vəsaitlərin yalnız cüzi hissəsini qaynar cüzdanda, əsas hissəsini isə soyuq cüzdanda saxlayırlar. Müvafiq birjalarda kriptovalyutaların likvidliyi birjanın səhmdarları, yaxud “marketmeyker”lər tərəfindən təmin olunur.

Əksmərkəzləşmiş kripto-birjaların iki növü mövcüddur: qapalı açarı istifadəçidə olan və qapalı açarı özündə saxlayan kripto-birjalar. Qapalı açarları özündə saxlayan bu birjaların mərkəzləşdirilmiş birjalardan fərqi yalnız belə birjalarda əməliyyatların blokçeyn şəbəkəsində baş verməsidir. Burada fiat valyuta ilə kriptovalyuta mübadiləsi müxtəlif provayderlər tərəfindən təmin olunur.

Qapalı açarı özündə saxlamayan əksmərkəzləşmiş kripto-birjaların yaranması smart müqavilələrin yaranması ilə eyni vaxta təsadüf edir. Əsasən ilk öncə "ethereum" blokçeynində, daha sonra müxtəlif smart müqavilələri dəstəkləyən blokçeynlərdə yaradılan belə birjalarda fiat valyuta ilə mübadilə birbaşa olaraq aparılmır. Eyni zamanda, müvafiq birjalarda bütün kriptovalyuta alqı-satqısı birbaşa olaraq blokçeyndə baş verir, kriptovalyutaların likvidliyi isə şəbəkə iştirakçıları tərəfindən depozit kimi qoyulan cüt kriptovalyuta "hovuz"ları vasitəsi ilə təmin olunur. Mərkəzləşmiş birjalarda vəsaitlərin qorunmasına zəmanət verildiyi halda, əksmərkəzləşmiş birjalarda bu məsələ nəzərdə tutulmamışdır.

Adi fond birjalarında olduğu kimi kriptovalyuta birjalarında da birja istifadəçiləri derivativ və spot ticarəti ilə məşğul olmaq imkanlarına malikdirlər.

Mümkün risklərdən qorumaqla peşəkar əsasda ticarəti aparılan və törəmə maliyyə alətləri olan (baza aktivinə nəzarən) derivativlər bağlanmış müqaviləyə əsasən qeyd edilmiş aktivin bir şəxs tərəfindən digər şəxsdən müəyyən müddət ərzində alınmasıdır. Derivativlərin fyuçers, opsion, istifadə olunmuş token və svop kimi növləri mövcuddur.

Spot ticarətdə isə aktivlərin alqı-satqısı qeyri-şərtsiz icra olunur.

Əksmərkəzləşmiş birjaların ("DEX") yaranması əksmərkəzləşmiş maliyyə tətbiqlərinin ("DeFi") yaranması ilə əlaqələndirilir. "*DeFi*" - əksmərkəzləşmiş maliyyə tətbiqi olaraq maliyyə xidmətlərindən istifadəyə, borc və ticarət əməliyyatlarını mərkəzi orqan olmadan icra etməyə imkan verən platformadır. Bu, əksmərkəzləşmiş tətbiqlər ("Dapps") vasitəsilə təmin edilir və bu tətbiqlərin əksəriyyəti "ethereum" platformasıda yerləşdirilib.

Kriptovalyutalar ilə digər mübadilə alətləri

Kriptovalyutalar ilə əməliyyatlarda birjalar ilə yanaşı, mübadilə şirkətlərindən də geniş istifadə olunur. Kriptovalyuta mübadiləsini həyata keçirən subyektlər kriptovalyutanı almaq, satmaq və ya mübadilə etməyə imkan verən proqram təminatlarını təklif edən şirkətlərə deyilir.

Mübadilə proqramlarına marağın artmasını onların öz istifadəçilərinin anonimliyini təmin etməsi, daha az komissiya ödənişinin tutulması və mübadilənin sürətli icra olunması ilə əlaqələndirilir.

Kriptovalyuta mübadiləsi proqramları ilk öncə kriptovalyutaların fiat valyutaya konvertasiyasını nəzərdə tutsa da, hazırda onlar kriptovalyutaların bir-birinə mübadiləsi xidmətini də öz müştərilərinə təklif edirlər. Kriptovalyutanın mübadiləsi üzrə əməliyyatların tərəflərin kimlər olmasından asılı olaraq, müvafiq mübadilə proqramları iki növə bölünür:

- *Mərkəzləşmiş mübadilə proqramları.* Burada müxtəlif şəxslər arasında alqı-satqı prosesində mərkəzləşmiş birjaların fəaliyyətinə oxşar formada bir vasitəçi iştirak edir.
- *"P2P exchange" mübadilə proqramları.* Burada mübadilə platforması yalnız iki fərqli şəxs arasında vasitəçilik və qarant funksiyasını yerinə yetirir. Ödəniş və mübadilə şərtləri isə alıcı və satıcının öz aralarında razılaşdırılır.

Mübadilə platfromalarından əlavə, kriptovalyutanın mübadiləsi və nağdlaşdırılması üçün digər növ alətlərdən də istifadə olunur. Bunlara *Kripto "ATM"ləri və Birjadan kənar ticarət platformalarını ("OTC")* aid etmək olar.

Kripto "ATM"lər - virtual valyutalar ilə əməliyyatları, nağd və ya debet kartının köməyilə hər hansı şəxs tərəfindən virtual valyutaların alqı-satqısını dəstəkləyir.

Birjadan kənar ticarət platformaları ("Over The Counter" - "OTC") - birjalardan kənar kriptovalyutaların alqı-satqı prosesidir. Kriptovalyutalar üçün birjadan kənar bazar klassik birjaların meydana çıxmasından əvvəl də inkişaf etmişdi, lakin böyük əməliyyatlar üçün "OTC" platformaları yalnız 2013-2014-cü illərdə meydana gəlməyə başladı. Belə platformalar keçmiş treyderlər, "hec fondlar"ı, ödəmə sistemləri və maynerlər arasında geniş yayılmışdır. Müvafiq birjadan kənar məntəqələrdə 100 milyon dollar və daha çox həcmdə olan əməliyyatlar gündəlik qaydada həyata keçirilir. "OTC"lərin təqdim etdikləri əsas üstünlüklərə adi birjalarda əldə oluna bilinməyən həcmdə kriptovalyutaların alınması imkanını, aşağı komissiya və stabil kursun olmasını aid etmək mümkündür.

Adi birjalar ilə müqayisədə "OTC"lərin üstünlükləri aşağıdakılardır:

- Adi birjada kifayət qədər likvidlik olmaya bilər. Nəticədə, böyük bir həcmdə köçürməni bir neçə platformaya bölmək və bir neçə mərhələdə almaq lazım gələcəkdir. Bu zaman, tələbin təklifi üstələməsi nəticəsində hər bir növbəti sifarişin qiyməti artacaq və ilkin alış giyməti ilə son alış qiyməti arasında böyük fərq yarana bilər. Birjadan kənar ticarət isə vahid qiymətə böyük həcmdə likvidlik problemi olmadan ticarət aparmağa imkan verir;
- Bir çox birjalarda əməliyyatın ən yüksək həddinə limitlər müəyyən edilib. Adi birjalar ilə müqayisədə "OTC" brokerlərin təqdim etdiyi bu limitlər daha yüksək olur;
- Kriptovalyutanın birbaşa likvidlik təminatçısından alınması daha sürətli üsuldur. Birja vasitəsilə böyük əməliyyatlar bir neçə gün çəkə bilər. Birjadan kənar brokerlər vasitəsi ilə isə bu müddət daha azdır;
- Birjalarda əməliyyatların aparılması daha təhlükəsiz hesab olunur, çünki bu əməliyyatlarda böyük likvidlik təminatçısı və broker iştirak edir;

"OTC"lərin adi birjalarla müqayisədə mənfi cəhətləri aşağıdakılardır:

- Broker daha çox komissiya əldə edir;
- Birjada əməliyyatlarını "API"lar vasitəsi ilə avtomatlaşdırmaq mümkündür, lakin "OTC"lərdə bu mümkün deyil. Məntiqi baxımdan da bu rasional addım kimi görünmür, belə ki, bir neçə milyonluq ticarət dövriyyəsi olan şəxsin gündəlik treyder fəaliyyəti ilə "OTC" platfromada ticarət aparması ağlabatan deyildir.
- əməliyyatlarda yüksək limit həddi.

"OTC" platforması üzərindən alqı-satqı prosesi adətən aşağıdakı kimi baş verir:

Valyuta almaq (və ya satmaq) istəyən şəxs sosial şəbəkədə, çat-bokslarda, brokerlərə kritpovalyuta alışı ilə bağlı müraciət edir. Müraciətdə alqı-satqı miqdarı, tarix

və dəyəri ilə bağlı qeydlər aparılır. Qiymət razlaşdırıldıqdan sonra əməliyyatlar aparılır. Sosial şəbəkələr üzrə kriptovalyuta alqı-satqısı əsasən fiziki şəxslərin öz aralarında birbaşa aparılır.

Blokçeyn üzrə təhlil proqramları və alətləri

Blokçeyn üzrə xüsusi analitik alətlər və proqramlar blok zəncirlərindəki məlumatların təhlil edilməsi və kriptovalyutanın anonimliyinə çalışan cinayətkarların aşkar edilməsi məqsədilə istifadə oluna bilər. Hazırda bu məqsədlə istifadə olunan əsas alətlər və proqramlar aşağıdakılardır.

“Chainalysis” (ABŞ). “Chainalysis” istifadəçi fəaliyyətinin monitorinqi hesabatlarının təhlili, şübhəli fəaliyyətin aşkarlanması üzrə vizuallaşdırma və araşdırma, eləcə də kiber təhdidlərə qarşı kəşfiyyat alətidir. Təşkilatın təklif etdiyi uyğunluq (komplayens) alətləri, əməliyyatları tanı prosedurları, blokçeyn şəbəkəsinin təhlil edilməsi imkanları dünyanın 44 ölkəsinin 180-dən çox təşkilatı tərəfindən istifadə olunur. Belə istifadəçilər sırasına “Barclays”, “Europol”, “BMT-nin Narkotik və Cinayətlər İdarəsi” və digər maliyyə institutları daxildir.

“Elliptic” (Böyük Britaniya). “Elliptic” - “bitcoin” şəbəkəsi üzərindən cinayət fəaliyyətini araşdıran və çirkli pulların yuyulmasının qarşısını almaq, əməliyyatları izləmək məqsədilə istifadə edilən blokçeyn analitik proqramıdır. Onun digər əsas alətlərdən fərqi şəbəkə daxilindəki məlumat bloklarının təhlilini süni zəka və maşın öyrənmə (“machine learning”) texnologiyası ilə birlikdə aparmasıdır.

“Whitestream” (İsrail). Blokçeyn təhlil texnologiyası kimi “Whitestream” blokçeyn şəbəkəsinin bloklarındakı xam məlumatları “axtarış edilə bilən” və icra edilə bilən məlumatlara çevirərək lazımi məlumatı asanlıqla əldə etməyə yardım edir. Bu təşkilat PL/TMM-ə, eyniləşdirməyə aid məlumatları və digər müxtəlif məqsədlər üçün olan məlumatları “API” (Application Programming Interface – tətbiqi proqramlaşdırma interfeysi) vasitəsilə müştərilərinə təqdim edir.

“CipherTrace” (ABŞ). “CipherTrace” PL/TMM, blok zəncirinin kriminalistika ekspertizası və kriptovalyuta təhdidlərinin kəşfiyyatı və həlli üzrə fəaliyyat göstərir. Maliyyə kəşfiyyatını həyata keçirən qurumlar, eləcə də tənzimləyicilər əməliyyatları və eyniləşdirmə prosedurlarının aparılmasını izləmək üçün “CipherTrace” blokçeyn analitik imkanlarından istifadə edirlər. Dünyanın bir çox aparıcı birjaları, fondları, bankları və “VAXT”ları öz risklərini və fəaliyyətlərini tam idarə etmək üçün “CipherTrace”dən istifadə edir.

“Elementus” (ABŞ). “Elementus” blokçeyn şəbəkəsindəki məlumatları paylaşmaq məqsədilə maliyyə institutlarının aktivlər üzrə menecerləri, VAXT-lar və dövlət orqanları üçün blokçeyn analitika platformasını təqdim edir.

“Coin Metrics” (ABŞ). “Coin Metrics” maliyyə təsisatları, fondlar, media və araşdırma vasitələri və məlumat / tətbiq təminatçıları da daxil olmaqla müxtəlif tədqiqat vasitələri üçün açıq mənbəli məlumat mənbəyidir. “Coin Metrics” şəbəkə məlumatlarını anlamaq üçün açıq blok zəncirində baş verən bütün əməliyyatların və aktivliyin müşahidə edilməsi üzərində qurulmuşdur.

Bölmə
Altı

6

BLOKÇEYNİN MİQYASLANMASI. YAN ZƏNCİRLƏR VƏ ÖDƏNİŞ KANALLARI

- miqyaslanma
- yan zəncir
- sürətli şəbəkə
- bölünmə

Blokçeynin miqyaslanması. Yan zəncirlər (“sidechain”) və ödəniş kanalları

Miqyaslanma qabiliyyəti artan tələbata cavab olaraq sistemin təkamül qabiliyyətinin göstəricisidir. Ödəniş sistemlərində miqyaslanma müəyyən tapşırıqları daha tez yerinə yetirmək üçün təklif olunan təkmilləşdirmə proseslərinin əksidir. Blokçeyndə isə miqyaslanma dedikdə, texnologiyanın daha çox əməliyyatları emal etmək qabiliyyətinin mümkünlüyü nəzərdə tutulur. Vitalik Buterin trilemmasına (miqyaslanma, əksmərkəzləşmə və təhlükəsizlik ilə bağlı olan çağırışların eyni zamanda həll edilməsi) daxil olna miqyaslanma probleminin həlli üçün müəyyən təkliflər olunur. Bu həllərdən biri də *yan zəncirlər (“sidechain”)* hesab olunur.

Yan zəncirlər (“sidechain”) - blokçeynin rəqəmsal aktivlərinin başqa bir blok zəncirində etibarlı şəkildə istifadə edilməsinə və zərurət olduqda, orijinal blok zəncirinə geri qaytarılmasına imkan verən texnologiyadır. Yan zəncirlər (“sidechain”) konsepsiyası ilk dəfə 2014-cü ildə daxil edilmişdir.

Yan zəncirlərin kommersiya məqsədləri üçün nəzərdə tutulması halları da mövcüddur. Məsələn, “Blockstream” tərəfindən hazırlanan “Liquid sidechain” - “bitcoin” mübadiləsi, emal xidmətləri və treyderlərə xidmət etmək üçün nəzərdə tutulmuşdur. Özünəməxsus bir blokçeyn olan “Liquid sidechain” bir çox müstəqil sistemdən fərqli olaraq, “bitcoin” blokçeyninin əsasında qurulmaqla birjalar arasında pul köçürmə müddətini bir neçə saniyəyə qədər azaltmağa yardım edir.

Yan zəncirlər (“sidechain”) - ana blokçeynə ikitərəfli bağlanan ayrı bir blokçeyn kimi də təqdim edilə bilər. Ana blokçeynə “əsas zəncir”, yan zəncirlərə isə “əlavə zəncirlər” deyilir.

Əsas blokçeynin istifadəçisi əvvəlcə kriptovalyutanı kənar şəbəkənin ünvanına göndərir, orada onların başqa yerdə xərclənməsinin qarşısını almaq üçün kriptovalyuta müvafiq ünvanda bloklanır. Bu proses başa çatdıqdan sonra iştirakçılar müəyyən bir gözləmə müddətindən sonra (əlavə təhlükəsizliyin təmin edilməsi məqsədilə) prosesin icra olunması barədə məlumat alırlar. Bundan sonra bərabər miqdarda kriptovalyuta yan şəbəkəyə köçürülür və istifadəçilər onlara məxsus vəsaitləri xərcləmək imkanı əldə edirlər. Kriptovalyuta yan zəncirdən əsas blokçeynə göndərilərkən proses əks istiqamətdə baş verir. Burada validatprlar qrupu (şəbəkədaxili əsas səsə malik şəxslər), yəni əsas zəncir ilə onun yan zəncirlərindən biri arasında əlavə təbəqə rolunu oynayan operatorlar qrupudur. “Birlik” istifadəçinin pullarının nə vaxt “kilidlənəcəyini” və nə vaxt xərclənə biləcəyini müəyyənləşdirir.

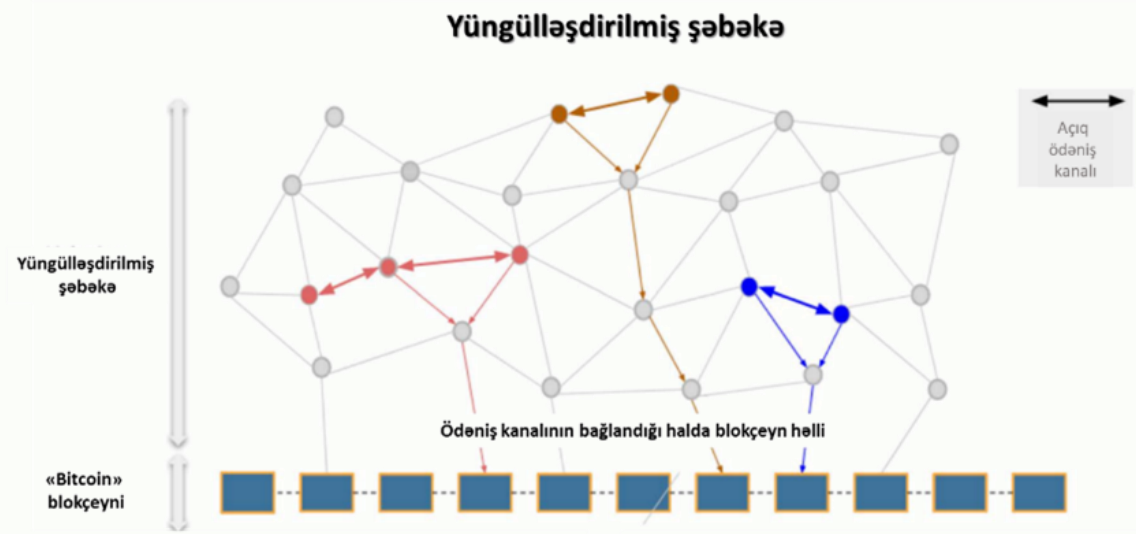
Yan zəncirlər (“sidechain”) şəbəkəsinin iştirakçıları özlərinin “birlik” üzvlərini seçə bilərlər və əməliyyayyatların şəbəkədaxili təsdiqi formasına dəyişiklik etmə qabiliyyətinə malik olurlar. Bu modelin çatışmazlığı - əsas zəncir ilə blokçeyn arasında əlavə bir təbəqənin olması və nəticə etibarilə mərkəzləşmə risklərinin mövcudluğudur.

2017-ci ilin yanvar ayında “Blockstream” yenilənmiş konsensus mexanizmini və etibar modelini, habelə uğursuzluq halında göndərilən vəsaitin ana zəncirə geri qaytarılmasını təmin edən mexanizmlərin təsvirini ehtiva edən yan zəncirlər üçün yeni bir *“White papers”* (hökumət və ya digər səlahiyyətli qurumun verilmiş məsələ üzrə məlumata və təkliflərə malik hesabatı) təqdim etmişdir.

Yan zəncirlər (“sidechain”) arasında uğurlu layihələrə əsas şəbəkədə olan kriptovalyutaları çoximzalı ünvanlarda “kilidləyən” layihələr aid olunur. Kiliddən çıxarılma yalnız hər bir açar sahibinin təsdiqi ilə mümkün olacaqdır. Bu xüsusiyyət hər hansı aktivin əksmərkəzləşmiş formada müxtəlif cüzdanlar arasında hərəkətinə imkan verən, ictimaiyyət tərəfindən yoxlanılan etibarlı əməliyyat şəbəkələri formalaşdıra bilər.

Yan zəncir (“sidechain”) şəbəkələri öz sistemlərindəki təhlükəsizliyə görə özləri cavabdehlik daşıyır. Hər bir yan zəncir müstəqil olduğu üçün onun daxilində baş verən hər hansı xəta və onun yaratdığı zərər həmin zəncirdə qalır və əsas blokçeynə təsir etmir.

Sürətli (yüngüllləşdirilmiş) şəbəkə (“lightning network”) - blokçeyn üzərində ikinci şəbəkə kimi də təqdim oluna bilər. Onun işləmə prinsipi aşağıdakı kimidir: əsas blokçeyndən kənarda (“offchain”) iki və daha artıq şəxs tərəfindən xüsusi kanal yaradılır. İki şəxs halında bir açıq açara bağlı iki qapalı (məxfi) açar formalaşır. Bu zaman şəxslər arasında dövriyyə müvafiq kanal üzrə baş verir və sadəcə şəxslərin öz aralarında olan balans dəyişir. Müvafiq kanalın əsas blokçeynlə əlaqəsi yalnız blokçeyndən vəsaitlərin köçürülməsi və ya qəbul edilməsi zamanı baş verir. Eyni zamanda, sürətli şəbəkələrdə bir çox şəxs müəyyən bir proqram təminatı ilə bir-biri ilə əlaqələndirə bilər. Sürətli şəbəkənin işləmə prinsi mərkəzləşmiş birjalara oxşar olacaqdır. Belə şəbəkənin əsas üstünlüyü “bitcoin” şəbəkəsində əməliyyatların ləng işləməsinin qarşısının alınması və komissiya xərclərinin azaldılması ilə bağlıdır.



Blokçeyndə miqyaslanma probleminin qarşısının alınması üçün istifadə edilə biləcək daha bir alətə bölünmə (“sharding”) deyilir. Bu üsul ilk öncə “ethereum” blokçeyn platformasında yaranmışdır.

Bölünmə (“sharding”) – blokçeyn məlumat bazasının göstərdiyi funksiyalara görə məntiqi əsasda bölünməsi və ayrıca saxlanması üsuludur. Bölünməyə (“sharding”) həmçinin *məlumatların üfüqi bölünməsi* də deyilir.

Blokçeyn baxımından, bölünmə (“sharding”) – hesab modelli blokçeynlərdə şəbəkənin ayrı-ayrı seqmentlərə bölünməsidir. Hər bir qovşağın (“nod”un - kompüterin) şəbəkədəki hər bir əməliyyatı yoxlamağa məsul olduğu sxemdən fərqli olaraq, bölünmədə (“sharding”) əməliyyatları yoxlayan hər bir hissəyə bir qovşaq təyin edilir. Blokçeynin daha çevik idarə olunan seqmentlərə bölünməsi əməliyyatın ötürücülük imkanını artıra və bununla da müasir blokçeynlərin üzləşdiyi miqyaslanma problemini həll edə bilər.

Bölünmənin (“sharding”) əsas ideyası hər bir qovşağın (kompüterin) hər bir əməliyyatı hesabladığı modelin əvəzinə, qovşaqların yalnız müəyyən hesablamaları emal etdiyi paralel icra modelini təklif etməsidir. Müvafiq model birdən çox əməliyyatı paralel şəkildə həyata keçirməyə imkan verir.

Blokçeyndə bölünmə üsulunun effektivliyi yüksək olsa da, onun praktiki reallaşdırılması bir qədər mürəkkəb prosesdir. Bu mürəkkəblik ilə əlaqəli onun praktikada tam reallaşması halları hələ ki, mümkün olmamışdır. Blokçeyndə miqyaslanma, eləcə də sürətin artırılması problemlərinin mövcudluğu bir çox hallarda şəbəkə istifadəçilərinin alternativ yollardan istifadə etməsinə səbəb olur. Müvafiq alternativ üsullara blokçeyn bloklarının həcminin artırılması və ya blokçeyn üzərindən yaradılan altkoinlərdən istifadə etməklə müxtəlif funksiya və layihələrin onların öz şəbəkəsində öz valyutaları ilə icrası halları aiddir.

Bölmə

Yeddi

7

TOKEN ANLAYIŞI. TOKENLƏRİN NÖVLƏRİ

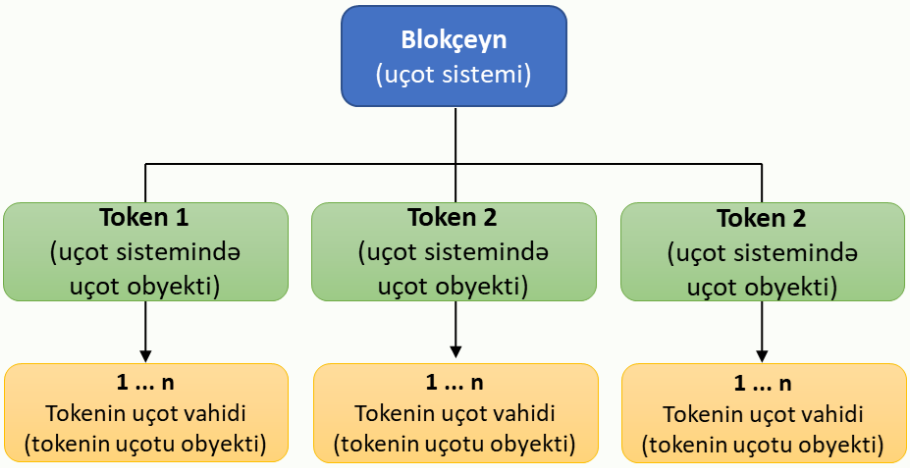
- token
- tokenləşdirmə
- FT
- NFT
- kraudfandinq
- airdrop
- baunty
- ICO
- IEO
- IDO
- STO

Token analyışı. Tokenlərin növləri

Blokçeyn texnologiyasında ***token*** ən mürəkkəb anlayışlardan biridir. Buna səbəb onun müxtəlif formalarda çox müxtəlif hüquq və əşyaları ifadə etməsidir. Texniki baxımdan blokçeyn - rəqəmsal məkanda müasir mühasibat uçotunu təmin edən texnoloji həll, *token* isə - müvafiq paylanmış reyestr texnologiyasına əsaslanan rəqəmsal məlumat uçotu sistemində orijinal bir aktivə və ya onun törəməsinə dair qeydlərdir.

Beləliklə, **token** - blokçeyn texnologiyası əsasında həyata keçirilən sistemlərin mühasibat obyektidir.

Blokçeyndə rəqəmsal məlumat obyektlərinin uçotu sisteminin sxemi aşağıda verilmişdir:



Tokenin aşağıdakı xüsusiyyətləri onu mühasibat obyekti hesab etməyə imkan verir:

- blokçeyn sisteminin istifadəçilərinin müstəqil olaraq şəbəkə daxilində tokenlər yarada bilməsi;
- tokenin bir identifikator kimi olması imkanı və mühasibat sistemində (blokçeynin) öz vahidlərinə malik olması;
- blokçeyn sisteminin istifadəçisi token yaradarkən, emissiya olunan tokenlərin son həddini göstərə bilməsi;
- blokçeyn sisteminin istifadəçiləri arasında tokenin özünün deyil, onun fərdi vahidinin köçürülməsi;
- tokenin ikili mahiyyət daşıması (ölçü vahidi və eyni zamanda blokçeyn şəbəkəsindən kənar əmlakın uçot obyekti olması).

Paylanmış reyestr texnologiyasına əsaslanan rəqəmsal məlumat uçotu sistemində mövcud orijinal (eləcə də törəmə) aktivdən əldə edilmiş məlumat identifikatoruna **tokenləşdirilmiş aktiv** deyilir.

Orijinal (ilkin) aktiv - paylanmış reyestr texnologiyasının rəqəmsal məlumat uçotu sistemində yaradılmış tokenləşdirilmiş aktivin real ifadəsidir.

2015-ci ildə “ethereum” blokçeyn platformasının yaradılması ilə *əksmərkəzləşmiş smart müqavilələr* konsepsiyası formalaşdı. “Ethereum” sistemi nəinki yeni ödəniş tokenlərinin yaradılmasına (efir), həmçinin əməliyyatlar üçün etibarlı vasitəçilər olmadan açıq elektron internet üzərindən digər elektron tokenlərin rahatlıqla yaradılmasına və avtonom idarəçiliyinə yol açdı.

Tokenlərin yaradılması, onların digər elektron token qarşılığında bölüşdürülməsi və paylanması prosesi *İlkin sikkə təklifi/yerləşdirilməsi* (“ICO” - “Initial coin offering”) analyışının yaranmasına səbəb olmuşdur.

Bir çox iqtisadçılar və hüquqşunaslar tərəfindən tokenlərə virtual aləmdə qiymətli kağızların analoqu funksiyasını daşıyan obyekt kimi baxılsa da, əslində tokenlərin yalnız bu çərçivə ilə məhdudlaşdırılması tam olaraq düzgün yanaşma olmazdı. Buna səbəb tokenin istənilən bir əşya - həm fiziki, həm də rəqəmsal məhsulun ifadəsi ola bilməsidir. Blokçeyn texnologiyasında *tokenin əsas üstünlüyü* - hər hansı bir vasitəçi olmadan bir şəxsin digər şəxsə token ötürmə hüququnun olmasındadır. Öz qarşılığı ilə əvəz oluna (özü kimi identik bir əşya ilə əvəz olunma) bilmə qabiliyyətindən asılı olaraq, tokenlər aşağıdakı növlərə bölünür:

- eyni qarşılığı ilə əvəz oluna bilən tokenlər (“fungible tokens” – “FT”s);
- eyni qarşılığı ilə əvəz oluna bilməyən tokenlər (“non-fungible tokens” – “NFT”s).

Özünün eyni qarşılığı olan əşya ilə əvəz oluna bilən fikizi əşyalara ən yaxşı nümünə kimi pul nişanlarını göstərmək olar. Məsələn, 1 AZN nominala malik valyuta digər 1 AZN nominallı valyutadan heç bir fərqi olmur və bunlar qarşılıqlı əvəz oluna bilən aktiv hesab edilir (lakin bu, köhnə pul nişanlarına şamil edilmir). Eyni funksiya kriptovalyutalara da aid edilir. 1 “bitcoin”in digər 1 “bitcoin”dən heç bir fərqi olmadığından, onlar qarşılıqlı əvəz oluna bilən token kimi qəbul edilir.

Qarşılıqlı əvəz oluna bilməyən tokenlərin (“NFT”) tərifi isə bir qədər daha çətindir. Bu növ tokenlərin ən yaxşı fiziki nümunəsi kimi vətəndaşın pasportunu göstərmək olar. Hər bir vətəndaşın pasportu görünüşcə eyni olsa da, onlar hər şəxsin özünə uyğun fərdi məlumatları əks etdirdiyindən, bir-biri ilə əvəz oluna bilməzlər. Bu səbəbdən, vətəndaş pasportu qarşılıqlı əvəz oluna bilməyən sənəd kimi çıxış edir. Bu növ tokenlərə həmçinin tələbə diplomu, əmlak çıxarışı və bu kimi digər sənədləri nümunə göstərmək olar. “NFT” tokenlər - qarışılığı ola bilməyən və müəyyən dəyər ifadə edə bilən aktivlərdir. Məsələn, bəzi dövlətlər tərəfindən artıq istifadəyə verilmiş rəqəmsallaşmış diplomlar, müəyyən elektron tətbiqlərə giriş icazələri belə aktivlərə nümunə ola bilər.

Qarşılığı ilə əvəz oluna bilən tokenlər (“FT”) də öz növbəsində aşağıdakı növlərə bölünür: ödəniş tokenləri, xidməti tokenlər, investisiya tokenləri.

Ödəniş tokenləri (“Payment tokens”). Ödəniş tokenlərinə həmçinin valyuta tokenləri və ya kripto-tokenlər də deyilir. Ümumiyyətlə, ***ödəniş tokenləri*** – bir çox halda sadəcə kriptovalyutaları əhatə edir və geniş mənada pul və ya qızıl kimi daxili dəyərə

malik olur. Yəni belə tokenlər ABŞ dolları, avro və digər fiat valyutalarla eyni funksiyaları daşımaqla, alış, satış və digər maliyyə əməliyyatlarının aparılması məqsədləri üçün istifadəni nəzərdə tutur. Bu kriptovalyutalara "bitcoin", "monero", "ethereum" və öz blokçeyni üzərində qurulmuş və ödəmə vasitəsi kimi xidmət edən bir çox digər kriptovalyutalar da daxildir.

Xidməti tokenlər ("Utility tokens") – müəyyən layihə yaradıcıları tərəfindən təqdim olunan məhsul və xidmətlərin ödənişi üçün istifadə olunur. Müvafiq tokenlər müəyyən platformalara daxil olma, məhsul və xidmətləri əldə etməyə imkan verən imtiyazlar, proqram tətbiqi istifadəçilərinin platformadan istifadəsinin təşviqi üçün edilən mükafatlandırmadan ibarətdir.

Ümumiyyətlə, xidməti tokenlər gələcəkdə şirkətin məhsullarından və ya xidmətlərindən istifadəyə icazə verən tokenlərdir. Xidməti tokenlərin yaranması və geniş yayılmasının əsas səbəbləri onların kütləvi formada vəsait cəlb etmə imkanı və eləcə də şirkətlərin maliyyə tənzimləyici orqanlarının qanunvercilik ilə tənzimlənən qaydalarının təsir dairəsinə düşməməsi ilə bağlıdır. Şirkətlər hər hansı bir tokeni pay olaraq tanıdığı təqdirdə, ortaya çıxacaq çətinlik və mürəkkəb sənədləşmə prosesindən yan keçmək üçün yalnız rəsmi olaraq xidmətləri daxilindəki tokenləri bir dəyər olaraq təqdim etdiklərini bildirirlər. Eyni zamanda, layihə rəhbərləri potensial investorlara gələcəkdə layihənin uğurlu olması nəticəsində yalnız xidmət və ya məhsulun deyil, tokenin dəyərinin də artması ehtimalının olduğunu vurğulayırlar.

Xidməti tokenlərin ən məşhur nümunəsi **"BAT"**dır *("Basic Attention Token" - əsas diqqət tokeni)*. ERC-20 standartına uyğun token kimi "BAT"dan "Brave" veb-brauzerinin reklam platformasında istifadə olunur. "BAT"dan istifadə etməklə istifadəçilər ziyarət etdikləri saytlarda reklamları bloklamaq, marketoloq və məhsul yaradıcıları isə reklam yerləşdirməklə əlavə müştəri kütləsini cəlb etmək imkanı qazanırlar. Şəbəkənin təqdim etdiyi alqoritmlər istifadəçilərin maraqlandığı sahələr üzrə marketinq təklifləri etməsində geniş imkanlar açır. "BAT"ın yaradıcısı olan Brendon Eyç "Javascript"in və eyni zamanda "Firefox", "Mozilla" kimi veb-brauzerlərin yaradıcılarından biridir. "BAT" 31 may 2017-ci il tarixindən "ICO" elanına başlamışdır. Cəmi 30 saniyədə satışa çıxarılmış bütün "ICO"lar realizə edilmişdir. 130 şəxs layihə tokenini almağa müvəffəq olmuşdur. Onlardan biri 20000 ETH (4.7 mln. USD ekvivalentində) dəyərində token almışdır. Layihə tokenlərinin emissiyası birdəfəlikdir. ERC-20 standartı üzərindən yaradılan belə tokendən cəmi 1.5 milyard sayda emissiya edilmişdir. Bu tokenlərin 1 milyardı 156250 "EHT"ə realizə edilmiş, digərləri isə 2 smart müqaviləyə yerləşdirilərək rezerv olunmuşdur (200 milyonu layihənin qurulmasına, 300 milyonu isə gələcəkdə istifadəçilərin cəlb edilməsi üçün). İzdihamlı satışdan ("Crowdsale") sonra layihə yaradıcıları tokenlərin 6 ay işlənməyəcəyi təqdirdə, öz likvidliyini itirəcəyi barədə qərar qəbul etdilər. Lakin tokenlərin məhv olunma məqsədi ilə deyil, sadəcə yeni içtirakçıların cəlb olunması üçün şəbəkəyə geri qaytarılması nəzərdə tutulurdu.

Ümumiyyətlə, "BAT" tokenlərini aşağıdakı formada əldə etmək mümkündür:

- "Brave" brauzerinin yüklənilməsinə görə;
- "Brave" brauzerində reklama baxmaqla;
- Birjada tokenin alınması ilə;
- İştirakçıların müxtəlif aktivləri (müxtəlif ölkə valyutaları, kriptovalyutalar, qiymətli daşlar və s.) dəyişdirmək imkanına malik olduqları yükləmə xidməti (upload service) ilə.

Beləliklə, "BAT" sistemi iki hissədən ibarətdir: "BAT" tokendən və "Brave" brauzerdən. Sistemdə platforma iştirakçıları kimi aşağıdakı şəxslər çıxış edir:

- *Marketoloqlar. "*BAT" tokenlər vasitəsi ilə əməliyyatlar aparıb müxtəlif reklamlar yerləşdirərək, şəbəkə iştirakçılarına öz məhsullarını təklif edirlər. Şəbəkənin təqdim etdiyi məqsədli yanaşma buna geniş imkan yaradır.
- *Kontent yaradıcıları (saytlar).* Sayta yerləşdirilmiş reklamlardan və iştirakçıların marağından gəlir əldə edirlər.
- *İstifadəçilər.* Reklamlara baxışlara görə tokenlər əldə edə, onları saxlaya, maraqlı olan kontentlərə baxış üçün icazə hüququ əldə etmə üçün istifadə edə, tokenlərlə müxtəlif investisiya edə və ya istənilən tokeni dəstəkləyən tətbiqdə tokeni istafadə edə bilərlər.

İnvestisiya tokenləri ("Security tokens" – "SEC") / Aktivlərin tokenləri ("Asset tokens", "FINMA"). Tokenlərin vahid tərifi olmadığından, bu növ tokenlərə yanaşmalar da fərqlidir. Bu istiqamətdə araşdırmalar aparan ABŞ Qiymətli Kağızlar və Mübadilə Komissiyası ("SEC") və İsveçrə Maliyyə Bazarları İdarəsinin ("FINMA") investisiya tokenlərinə olan yanaşmaları fərqlənir. "SEC" tokenlərə daha çox qiymətli kağızlara analoji qaydada yanaşır, "FINMA" isə daha çox tokenlərin iqtisadi funksiyasına diqqət yetirir.

Qeyd olunmuş token növlərinin bəzi funksiyalarını eyni zamanda daşıya bilən hibrid formalı tokenlər də mövcuddur.

Tokenlərin emissiya formaları və növləri

Eyni qarşılığı ilə əvəz oluna bilən tokenlərin ("FT"s) emissiyası

Hər bir layihənin yaradılması üçün layihə yaradıcılarına layihənin reallaşdırılması üçün əlavə vəsaitlər tələb olunur. Məsələn, şirkətlər öz layihələrinə vəsait lazım olduqda, onlar əlavə qiymətli kağızlar emissiya etməklə əlavə vəsaitlər cəlb etməyə nail olurlar. Bu prosesə "İlkin açıq yerləşdirmə" ("Initial Public Offering" – "IPO") – şirkət səhmlərinin ilk açıq satışı prosesi deyilir. "IPO" zamanı şirkət öz səhmlərini birjada yerləşdirir, potensial investorlar isə şirkətin səhmlərini əldə etmə imkanı qazanırlar. Bu proses ***kraudfandinq ("crowdfunding")*** adlanır.

Kraudfandinq – layihələrin kütləvi (kollektiv) maliyyələşdirilməsi üçün edilən yığımdır. Bu yığım müxtəlif məqsədlərə xidmət edə bilər: fəlakətlərin aradan qaldırılması, azarkeş dəstəyi, siyasi kampaniyaya dəstək, yeni fəaliyyətə başlayan və kiçik müəssisələrin maliyyələşdirilməsi, pulsuz proqram təminatı, mənfəət bölgüsü və s. Vəsait üçün müraciət edənə, layihənin təmsilçisinə təsisçi deyilir. İnvestorlara, layihəyə maddi töhfə verən insanlara isə himayədar ("backer") deyilir.

Kraudfandinqin əsas tələbləri başlanğıcda hədəfin elan olunması, tələb olunan pul miqdarının müəyyənləşdirilməsi, bütün xərclərin hesablanmasının aparılması və maliyyə yığımı prosesinin hər kəs üçün açıq olmasıdır. Yaranacaq şirkətə maliyyə yardımı yalnız fiziki şəxslərdən deyil, həmçinin hüquqi şəxslərdən də edilə bilər.

İlkin sikkə (token) təklifi/yerləşdirilməsi ("Initial Coin Offering" – "ICO") – hər hansı bir layihə və ya şirkət tərəfindən öz pul-tokenlərini emissiya etməklə vəsait, investisiya cəlbidir. Müvafiq elanı etmiş şirkətlər layihə daxilində istifadəsi mümkün olan tokenlər müqabilində layihənin maliyyələşdirilməsi üçün müəyyən müddət ərzində kriptovalyuta cəlb edirlər. "ICO"nun əsas məqsədi - layihə yaradıcıları tərəfindən şirkət (və ya layihə) yaranmazdan öncə blokçeyn şəbəkəsindən borc götürməkdir. Mahiyyət etibarı ilə "ICO" - qiymətli kağızlar birjasında yerləşdirilmiş "IPO"ların blokçeyn üzərindən olan analoqudur. Lakin "IPO"lardan fərqli olaraq "ICO"ların öz fərqli xüsusiyyətləri vardır:

- səhm alıcılarından fərqli olaraq, token alıcıları mülkiyyət hüququ əldə etmirlər;

- tokenlər ümumiyyətlə blokçeyndə qorunan bir mühitdə satılır və IPO-lardan fərqli olaraq token alıcılarının anonim olmasını nəzərdə tutur (hal-hazırda bəzi ölkələrdə buna icazə verilmir);
- tokenlərin istiqrazlara bənzəməsinə baxmayaraq, emitentinin satışdan sonra götürdüyü borc öhdəliklərini yerinə yetirməməsi halında onun alıcılarının qanunvericiliyə uyğun müdafiəyə sahib olmama ehtimalı var.

"ICO" vasitəsi ilə vəsaitlərin cəlbi kraudfandinqə bənziyir. Lakin ənənəvi formadan fərqli olaraq, "ICO" üzrə vəsaitlər fiat valyutada deyil, kriptovalyutalarda cəlb olunur.

"ICO"nun elan edilməsi üçün minimal tələblər yaranacaq müvafiq platforma barədə məlumat vermək üçün veb-saytın yaradılması, layihənin məqsədi, risklərini və üstünlüklərini izah edəcək texniki sənədin ("white paper") yazılması və "ICO"nun buraxılması üçün emissiya ediləcək tokenlərin miqdarı və onun dəyərinin müəyyən edilməsidir. Bütün bu işlərdə əlavə vəsaitlər tələb edildiyindən, bəzən "İlkin ICO" ("Pre ICO") elan edilməsi müşahidə olunur.

"ICO"nun əsas problemi hüquqi tənzimləmə mexanizmlərinin olmamasıdır. İnvestorların layihəyə borc verməklə yerləşdirdiyi maliyyə vəsaitlərini tam olaraq itirmə riski (ehtimalı) mövcuddur. Daha yüksək risk isə layihə təsisçilərinin fırıldaqçı olma ehtimalı ilə bağlıdır. Müvafiq riskləri minimuma endirmək üçün kripto sahədə nüfuzlu şirkətlər hesab edilən "AngelList" və "Protocol Labs" tərəfindən şübhəli "ICO" startupları və layihələrinin yerləşdiriləcəyi "Coinlist" platforması (https://coinlist.co/) yaradılmışdır. Bu platformada əlamətlərinə görə şübhəli hesab olunan layihələr platformanın siyahısından çıxarılır və token alıcıları nisbətən daha etibarlı platformalara yatırım etmə imkanı qazanırlar. Adətən, "ICO"lar 1 aydan 2 ilədək "kilidlənmiş" ("lock up") müddətə nəzərdə tutulur. "Kilidlənmiş pəncərə" ("lock up window") **–** "ICO" alıcıları və investorları tərəfindən tokenlərin geri alınmasına və ya satılmasına icazə verilmədiyi bir zaman pəncərəsidir. ABŞ-da "ICO"lar qiymətli kağızlara oxşarlıq analogiyasına uyğun olaraq qəbul edilmişdir. Lakin buna baxmayaraq, 2017-ci ildə "Satis Group LLC" tərəfindən aparılan araşdırmanın nəticələrinə əsasən, "ICO"ların 80%-nin əsas məqsədlərinin fırıldaqçılıq və şəbəkə iştirakçılarını aldadaraq dolayı yol ilə vəsait toplanması olduğu müəyyən edilmişdir (https://research.tokendata.io/ saytı isə müvafiq rəqəmin 90% olduğunu və "ICO"ların yalnız 8%-nin birjalara əlavə olunduğu bildirmişdir).

İlkin mübadilə təklifləri - ("Initial Exchange Offerings" – "IEO") – "ICO"lardan fərqli olaraq daha yenidir və burada vəsaitlərin cəlb edilməsi kriptobirjaların rəhbərliyi altında edilir. "IEO" zamanı birja tərəfindən startap layihənin maliyyə-hüquqi aspektlərinin yoxlanışı aparılır. Müvafiq yoxlamalar hüquqi şəxsin qeydiyyatdan keçməsi, nizamnamə sənədləri və investisiya potensialı məsələləri, eləcə də şirkətin maddi vəziyyətinin, investisiya risklərinin, uzunömürlülüyünün və digər göstəriciləri əhatə edir. Bu platforma ilk dəfə "Binance" birjası tərəfindən təqdim olunmuşdur. "Binance" birbaşa birjadan tokenlərin satışı üçün 2017-ci ilin dekabr ayında ayrıca bir platforma yaratmışdır. Platformaya yerləşdirilən layihələrin qısa müdət ərazində böyük investisiyalar toplamağa nail olması sahəyə digər birjaların da marağını artırmışdır.

"IEO"nun "ICO" ilə müqayisədə bir çox **üstünlükləri** mövcuddur:

- tokenlərin yerləşdirilməsinə başladıqdan sonra mübadilə istifadəçilərinin geniş auditoriyası üçün istifadəyə verilməsi təşkilatçılar üçün əlverişlidir.
- mübadilə birjaları üçün "IEO"nun müsbət tərəfi daha çox istifadəçi diqqətini cəlb edə bilmə imkanıdır. Mərkəzləşdirilmiş mübadilə birjalarının komissiya qazancını da birjalar üçün "IEO"nun üstnlüklərinə aid etmək olar.
- investorlar baxımından isə "IEO"ların üstünlüyünə birjada olan hesab vasitəsi ilə tokenlərin birbaşa alınması imkanı və layihənin yerləşdirilməzdən əvvəl birja mütəxəssisləri qrupu tərəfindən yoxlanılmasını aid etmək olar.

“IEO”ların çatışmazlıqlarına aşağıdakılar aid edilir:

- layihənin təqdim edilməsi mürəkkəb prosesdən keçməni tələb edir. Hər bir mübadilə birjası yerinə yetirilməli olan qeyri-şəffaf layihələr üçün öz tələblərini irəli sürür.
- layihə yerləşdirilmədən əvvəl yoxlanıldığından, bu, müəyyən bir vaxt tələb edir. Bunun üçün birjalar əlavə işçi cəlb etməli və onları əmək haqqı ilə təmin etməlidilər ki, bunun da mənbəyini layihəyə edilən yatırımlardan komissiya formasında tutulmalar təşkil edə bilər.
- investorlar üçün əsas çatışmazlıq isə mərkəzləşdirilmiş mübadilə birjalarının bir çoxu tərəfindən istifadəçilərin identifikasiya olunma tələbini irəli sürməsidir. Bununla yanaşı, ticarət zamanı vəsaitin birjanın cüzdanında olması ilə əlaqəli digər risk də mövcuddur ki, bu da onlara tam nəzarətin olmadığını göstərir.

İlkin əksmərkəzləşdirilmiş mübadilə təklifi (“Initial Dex Offering” – “IDO”) - əksmərkəzləşdirilmiş birjada bir token yaradaraq vəsait cəlb etmə modelidir. Digər növlərlə müqayisədə vəsait cəlb etmənin nisbətən daha yeni üsuludur. Ümumiyyətlə, “IEO” və “IDO” bir-birinə oxşar olsalar da, “ICO”dan fərqli olaraq “IDO”da tokenlərin satışı mərkəzləşmiş birjada yox, əksmərkəzləşdirilmiş birjada yerləşdirilir.

“IDO”ların “ICO” və “IEO”lar ilə müqayisədə əsas üstünlüklərinə “IDO”nun həyata keçirilməsi üçün təşkilatçıların müstəqil olması, tokenlərin likvid olması, anında ticarətə başlama imkanı və layihə xərclərinin azaldılmasını aid etmək olar. İlk “IDO”lardan biri 2019-cu ilin iyun ayında “Binance DEX”də siyahıya alınan “RAVEN” idi. Emissiya sayı və tokenlərin dəyəri digər formalarda olduğu kimi qalmaqdadır. “IDO”lar daha çox “Polkastarter”, “Paid network”, “Duckstarter” kimi əksmərkəzləşdirilmiş birjalarda yerləşdirilir.

Qiymətli kağız tokeni təklifi (“Security Token Offering” – “STO”). “STO”nun “ICO”dan əsas fərqi satılan tokenlərin qiymətli kağız funksiyasını yerinə yetirməsi və demək olar ki, ənənəvi səhmləri əvəz etməsidir. Digər bir fərq səhmlərin adi fiziki şəxslər tərəfindən deyil, şirkətlər tərəfindən emissiya edilməsidir. Token sahibləri “STO” zamanı şirkətin qazancından mənfəət əldə etməyə, həmçinin şirkətdaxili qərar vermələrdə iştirak imkanına malik olurlar. Bu növ tokenlərin buraxılışı üçün bir çox ölkələrdə şirkətlər token satışı təklifindən öncə səhmlərin buraxılışı ilə analoji qaydaları yerinə yetirmək məcburiyyətində olurlar (KYC, qeydiyyat və s.). İlk “STO” 2018-ci ilin oktyabr ayında “indiegogo.com” platformasında ABŞ-ın “Regis Aspen Resort” şirkəti tərəfindən elan edilmişdir. Şirkət bu yolla 18 mln. ABŞ dolları cəlb edə bilmişdir. “STO” modeli yuxarıda qeyd edilən modelllərdən daha etibarlı və cəlbedici göründüyündən, ona olan maraq getdikcə artmaqdadır.

Tokenlərin paylanılması kraudfandiq (tokenlərin pulla alınması) ilə yanaşı, aşağıdakı digər üsullar ilə mümkündür.

“Airdrop” üsulu – şəbəkə yaradıcıları tərəfindən müəyyən bir sosial şəbəkədə və digər forumlarda paylaşım və ya layihə haqqında şərh yazılması müqabilində pulsuz tokenlərin təqdim edilməsidir. Müvafiq proses adətən, çox vaxt tələb etmir. Bu növ layihələr haqqında məlumat bir çox forum və saytda əldə oluna bilər, lakin hazırda ilkin məlumat mənbəyi “bitcointalk.org” forumudur.

“Bounty” üsulu. Bu üsulun “Airdrop” üsulundan fərqi yalnız tokenlərin paylanmasının daha çox zəhmət tələb edən iş müqabilində verilməsi ilə bağlıdır. Bunlar bəyənmələr, mesajlar, məqalələrin tərcüməsi, forumlar və bloqlarda mövzu və

məqalələrin təbliği ola bilər. Sosial şəbəkələrdə, ixtisaslaşmış forumlarda və bloqlarda, populyar mesaj mübadilələrində hesablara ehtiyac duyulur. “Bounty” üsulu ilə “ICO” elanı bir neçə ay davam edə və bu müddətdə bir neçə pulsuz token paylanması ola bilər. “Bounty”də mükafatın həcmi adətən, “Airdrop”dan daha böyük olur.

“Bounty” üsullu “ICO”lar şərti olaraq iki növə bölünür:

- “ICO”dan əvvəlki mərhələdə baş verənlər: sosial şəbəkələrdə tanıtım, sistem boşluqlarının axtarışı və s.;
- “ICO”dan sonrakı mərhələdə fəaliyyət göstərənlər: müəyyən işin görülməsi, məlumat toplanması və s.

Eyni qarşılığı ilə əvəz oluna bilməyən tokenlərin (“NFT”lər) emissiyası

Virtual mülkiyyətə sahiblik ifadəsi əsasən fiziki dünyada hər-hansı bir dəyəri olan aktivə sahib olmanı ifadə etsə də, bu, bütün halları əhatə etmir. Müxtəlif oyun personajlarına görə ödənilən vəsaitlər oyun tərtibatçılarının özləri tərəfindən təqdim olunur, onların mülkiyyəti hesab edilir, lakin mülkiyyət hüququ tam olaraq oyun iştirakçısına ötürülmür. Belə problemlərin (hüquqların ötürülməsi, alqı-satqı və digər hallar) aradan qaldırılması ilə bağlı blokçeyndən istifadə edilməyə başlanılmışdır. Blokçeyn virtual aktivlərin köçürülməsi, saxlanması və digər funksiyaları yerinə yetirməyə imkan verir və şəxsin aktiv üzərindəki hüququnu tanıyır. Təqdim edilən bu funksiyanı **eyni qarşılığı ilə əvəz oluna bilməyən tokenlər (“NFT”lər)** yerinə yetirə bilir.

“NFT”lər - blokçeyn şəbəkəsində bir-birinə dəyişdirilə bilməyən və bir-biri ilə əlaqələndirilməyən tokenlərə deyilir. “NFT”lər rəqəmsal obyektlərin (aktivlərin) əldə edilməsi üçün istifadə olunur: şəkillər, videolar, səs, oyundakı bir xarakter və ya obyekt, beysbol kartı, domen adı və s. “NFT”lərin yaranması rəqəmsal cüzdanlarda saxlanılan sənət əsərlərinin yalnız onların sahiblərinə məxsus olmasını təsdiqləməyə imkan vermişdir. “NFT”nin və onun sahibinin həqiqiliyi tokenin kodunda dəqiqləşdirilə bilər. Bu, metaməlumatlar üzərindən təmin olunur. Hər bir tokenin ifadə etdiyi obyektə dair məlumatların saxlamasının son dərəcə bahalı olması müvafiq məlumatların blokçeyndə saxlanılmasını çətinləşdirir. Bunun əvəzinə blokçeyndə hər bir virtual obyektə əlaqələndirici link yaratmaq (“IPFS” – heş kod və ya “HTTP” ünvan kimi) mümkündür ki, bunun köməyilə xarici tətbiqlər müxtəlif alqoritmik funksiyalar ilə müvafiq obyektdə attributları aşkarlayıb əlaqə yaratsın. Bu növ əlaqələrə verilənlər barədə məlumat və ya metaməlumatlar deyilir.

“NFT” tokenləri blokçeynin daxilində və ya ondan kənarda saxlamaq mümkündür.

Metaməlumatların blokçeyn daxilində yerləşdirilməsinin üstünlükləri aşağıdakılardır:

- tokenlə birgə blokçeyn platformada olması. Gələcəkdə virtual obyektin yaradıldığı tətbiqin ləğv edildiyi, yaxud bağlanıldığı təqdirdə belə blokçeyndə qalmasına imkanı yaradır;
- Blokçeynin məntiqinə uyğun şəkildə dəyişmə imkanının olması.

Metaməlumatların blokçeyn daxilində saxlanılması üsulu daha üstün olsa da, “etherium” platformasının tətbiq etdiyi limitlər bir çox halda məlumatların blokçeyndən kənarda saxlanılmasına səbəb olur. Belə metaməlumatları “ERC721” standartında token “URI” metodu ilə əldə etmək mümkünüdür. Bu növ metaməlumatdan istifadə etməklə, token obyektinin harada olmasının müəyyən edilməsi imkanı yaranır. “Opensea” platforması bunu daha da inkişaf etdirərək, müxtəlif vizual formalı obyektin təsvir olunması imkanı yaratmışdır.

Metaməlumatların blokçeyndən kənarda saxlanılmasının iki üsulu mövcuddur: Mərkəzi (vahid) serverdə saxlama və Planetlərarası Fayl Sistemi serverində (“Interplanetary File System” – “IFPS”) saxlama.

Mərkəzi (vahid) serverdə saxlama. Müvafiq üsul verilənlərin ən rahat saxlanılması üsulu olsa da, aşağıdakı çatışmazlıqlara malikdir:

- proqramçıların metaməlumatları öz mülahizələrinə görə dəyişə bilmə imkanı;
- məlumat saxlanılan hostun oflayn olduğu halda, metaməlumatlara çıxışın əldə edilməsinin mümkün olmaması.

Planetlərarası Fayl Sistemi serverində ("Interplanetary File System" – "IFPS") saxlama – eyniranqlı faylların saxlama sistemi olaraq, məlumatların bir neçə kompüterdə saxlanmasına imkan yaradır. Bu isə (i) faylın heş ilə unikal şəkildə ünvanlanması səbəbindən metaməlumatların dəyişməz qalmasına və (ii) müvafiq məlumatları yerləşdirmək istəyən qovşaqların olduğu müddətdə məlumatlara çıxışın əldə edilməsinə zəmanət verir.

Rəqəmsal incəsənətə olan marağın artması nəticəsində ənənəvi auksionları təşkil edən "Christies" auksionu tərəfindən 2018-ci ildən kripto-obyektlərin auksionunun təşkilinə başlamışdır. "NFT" tokenlərə digər bir maraq müxtəlif idman yarışlarını təşkil edən federasiyaların oyunlarda baş vermiş xüsusi halların video və foto görüntülərinin obyekt kimi blokçeynə daxil olunub satılmasıdır. "Flow Blockchain"in təqdim etdiyi platformada "NBA Top Shot" (eləcə də "UFC" və "Warner Bros. Music") belə tokenləri satışa çıxarmağa başlamışdır. "NFT" tokenlərin xalis kriptoaktiv kimi qəbul edilməsi, kripto sahədə artıq ixtisaslaşmış şəxslərin valotil kriptovalyutalar və "ICO"lardan çox bu növ məhsullara yatırım etməsini stimullaşdırmışdır. "NFT" tokenlərin fərqli platformalara əlavə edilməsinin təmin olunması məqsədilə "ethereum" tərtibatçıları tərəfindən bütün tokenlər vahid standart formasına salınmışdır. "NFT" tokenlərin işləmə prinsipləri "ERC" token standartları ("ERC721" və digər) üzərindən qurulmuşdur.

Bölmə
Səkkiz

8

VİRTUAL AKTİVLƏR VƏ VİRTUAL AKTİVLƏR ÜZRƏ XİDMƏT TƏMİNATÇILARI-NA DAİR FATF TƏLƏBLƏRİ

- FATF Tövsiyələri
- Köçürmə qaydaları

Virtual aktivlərə və Virtual aktivlər üzrə xidmət təminatçılarına dair FATF tələbləri

2015-ci ilin iyununda FATF-ın virtual valyuta ilə əlaqəli PL/TM risklərinin idarə olunması məsələləri üzrə tövsiyələrini əks etdirən "Virtual valyutalara risk əsaslı yanaşmanın tətbiqi üzrə rəhbərlik" adlı müvafiq sənədi nəşr olunmuşdur. FATF-ın müvafiq rəhbərliyinin tətbiq dairəsi "konvertasiya olunan virtual valyuta" və "konvertasiya olunan virtual valyutanın mübadiləsi üzrə xidmət təminatçıları" ilə məhdudlaşırdı. Müvafiq rəhbərlik konvertasiya olunan (və ya açıq) virtual valyutanı real (fiat) valyutada ekvivalent dəyərə malik olan və real (fiat) valyutaya və əksinə mübadilə oluna bilən virtual valyuta olaraq müəyyən edir. Konvertasiya olunan virtual valyutanın mübadiləsi üzrə xidmət təminatçıları yalnız konvertasiya olunan virtual valyuta ilə real (fiat) valyuta arasındakı mübadiləyə töhfə verdikləri halda FATF Tövsiyələrinin təsiri altına düşürdü.

2018-ci ilin oktyabrında FATF öz Tövsiyələrinin virtual aktivlərin istifadəsi ilə aparılmış maliyyə fəaliyyətinə tətbiq edildiyini dəqiq aydınlaşdırmaq üçün onlara düzəlişlər etdi. FATF Tövsiyələrinə əsas düzəlişlər "virtual aktivlər" və "virtual aktivlər sferasında xidmət təminatçıları" anlayışlarının və onların izahının daxil edilməsi ilə bağlı olmuşdur. FATF-ın 15-ci Tövsiyəsinə edilmiş düzəlişə əsasən, VAXT-lar PL/TMM məqsədləri üçün tənzimlənməli, lisenziyalaşdırılmalı və ya qeydiyyatdan keçirilməli, eləcə də onlara münasibətdə effektiv nəzarət sistemi tətbiq olunmalıdır.

2019-cu ilin iyununda VA və VAXT-lara münasibətdə FATF tələblərinin necə tətbiq olunmasını əlavə olaraq aydınlaşdırmaqdan ötrü FATF 15-ci Tövsiyəyə izahedici şərhi təsdiq etdi. Xüsusilə bu, VA və VAXT-lar ilə əlaqəli fəaliyyət və əməliyyatlara münasibətdə risk əsaslı yanaşmanın tətbiqi, PL/TMM məqsədləri üçün VAXT-lara nəzarət, lisenziyalaşdırma və qeydiyyat, preventiv tədbirlər, o cümlədən müştərilərin eyniləşdirilməsi, sənədlərin saxlanılması və şübhəli əməliyyatlara dair məlumatların ("STR") göndərilməsi, sanksiyalar və digər tədbirlər, beynəlxalq əməkdaşlıq məsələlərini əhatə edirdi.

2019-cu ilin iyununda FATF həmçinin VA və VAXT-lara münasibətdə risk əsaslı yanaşmanın tətbiqi üzrə rəhbərliyi təsdiqlədi. Müvafiq rəhbərlik VA və VAXT-lar ilə əlaqəli fəaliyyətlərə münasibətdə tənzimləyici və nəzarət tədbirlərinin başa düşülməsində və hazırlanmasında ölkələrin dövlət qurumlarına yardım etmək, eləcə də VA ilə əlaqəli fəaliyyət həyata keçirmək istəyən özəl sektor subyektlərinin özlərinin PL/TMM öhdəliklərini başa düşməsinə və bu tələbləri effektiv şəkildə icra etmələrini aydınlaşdırmaqda onlara yardım etməkdir.

FATF üzv ölkələrdən "virtual aktivlər ilə bağlı risklərin idarə olunması və yumşaldılması üçün VAXT-ların PL/TMM məqsədləri üçün tənzimlənməsini və lisenziyalaşdırılmasını və ya qeydiyyata alınmasını, eləcə də FATF Tövsiyələrində nəzərdə tutulan effektiv monitorinq sisteminin tətbiqini və müvafiq tədbirlərə riayət olunmasını" tələb edir. FATF yurisdiksiyalardan virtual aktivlərə münasibətdə müştərilərin kompleks yoxlanışının və davamlı monitorinqinin aparılmasını, şübhəli əməliyyatlara dair hesabatların tərtib olunmasını, sənədləşmənin aparılmasını və PL/TMM üzrə digər preventiv tədbirlərin tətbiq olunmasını tələb edir.

Blokçeyn texnologiyalarının yaranması və onlardan maliyyə/ödəniş xidmətləri üçün istifadə olunması son onillikdə dünya maliyyə sistemində baş vermiş mühüm dəyişikliklərdən biri olmuşdur. Bu yeni tendensiya innovasiyalar gətirməklə, effektivliyi yüksəltmiş və alternativ maliyyə alətlərinin yaranmasına gətirib çıxarmışdır. Maliyyə

bazarlarının bir hissəsi kimi virtual aktivlər və kriptovalyutalar tənzimləyici orqanların, eləcə də FATF-ın diqqətini çəkmişdir. PL/TMM sahəsində standartları müəyyən edən beynəlxalq qurum olaraq FATF həmçinin maliyyə köçürmələrinin həyata keçirilməsi qaydalarını da müəyyən edir. Bu standartlar isə maliyyə vasitəçiləri arasında müştərilər barədə məlumatların mübadiləsini tələb edir.

FATF bildirir ki, bir sıra hökumətlər virtual aktivlər (VA) və Virtual aktivlər üzrə xidmət təminatçılarının (VAXT) tənzimlənməsi üçün artıq müəyyən tədbirləri nəzərdən keçirirlər. Lakin bütün dünyada VA-lar ilə əlaqəli fəaliyyətlərin miqyasının artmasına və VAXT-ların müxtəlif yurisdiksiyalar arasında daha çox dərəcədə əməliyyat keçirməsinə baxmayaraq, bir çox yurisdiksiyalarda VA-lar ilə əlaqəli fəaliyyətlərin doğurduğu PL/TM risklərinin azaldılması məqsədilə effektiv PL/TMM sistemi mövcud deyildir. VA-ların sürətli inkişafını, artan funksional imkanlarını, qlobal, transmilli xarakter daşımasını nəzərə alaraq, FATF-ın prioritet vəzifələrindən biri VA və VAXT-ların yaratdığı PL/TM risklərinin azaldılması üçün ölkələrin təcili tədbirlər qəbul etməsini təmin etməkdən ibarətdir.

FATF-ın 15-ci Tövsiyəsinə (Yeni texnologiyalar) əsasən, ölkələr və maliyyə təsisatları aşağıdakı səbəblərdən meydana çıxan PL/TM risklərini müəyyən etməli və qiymətləndirməlidir:

a) yeni təchizat mexanizmləri də daxil olmaqla, yeni məhsulların və yeni işgüzar praktikanın işlənib hazırlanması;
b) yeni, eləcə də artıq mövcud olan məhsullar üçün yeni və ya inkişaf etməkdə olan texnologiyalardan istifadə olunması.

Maliyyə təsisatları halında belə risk qiymətləndirilməsi yeni məhsulların, işgüzar praktikanın işə salınmasınadək və ya yeni və ya inkişaf etməkdə olan texnologiyalardan istifadəyədək aparılmalıdır. Bundan əlavə, onlar belə risklərə nəzarət olunması və onların aşağı salınması üçün müvafiq tədbirlər görməlidir.

Virtual aktivlərin yaratdığı risklərin idarə olunması və minimuma endirilməsi üçün ölkələr VAXT-ların PL/TMM məqsədləri üçün tənzimlənməsini, lisenziyalaşdırılmasını və ya qeydiyyata alınmasını, eləcə də effektiv monitorinq sisteminə cəlb olmasını və FATF Tövsiyəsinin tələblərinə uyğun müvafiq tədbirlərə riayət etməsini təmin etməlidir.

FATF-ın 15-ci Tövsiyəsinə dair izahlı qeydə əsasən, FATF Tövsiyələrinin tətbiqi məqsədləri üçün ölkələr virtual aktivləri “mülkiyyət”, “gəlirlər”, “vəsaitlər”, “fondlar və ya digər aktivlər” və ya “digər müvafiq (əlaqəli) dəyər” kimi nəzərdən keçirməlidir. Ölkələr FATF Tövsiyələrinə uyğun olaraq VA və VAXT-lar üçün müvafiq tədbirlər həyata keçirməlidir.

FATF-ın 15-ci Tövsiyəsində həmçinin aşağıdakı tələblər müəyyən olunmuşdur:

- VAXT-lar lisenziyalaşdırılmalı və qeydiyyata alınmalıdır. Artıq lisenziyalaşdırılmış və qeydiyyata alınmış VAXT fəaliyyətini həyata keçirən maliyyə təsisatlarının ayrıca lisenziyalaşdırılması və qeydiyyata alınması tövsiyə olunmur;
- VAXT-lara, onların direktorlarına və yüksək rəhbərliyinə bir sıra intizam və maliyyə sanksiyası tətbiq etmək hüququna malik səlahiyyətli orqan tərəfindən VAXT-lar PL/TMM üzrə adekvat tənzimlənməli və nəzarət olunmalıdır;
- Xarici həmkarları ilə operativ və konstruktiv informasiya mübadiləsi təmin edilməlidir;
- PL/TMM tələblərinin məlumatların qorunması, konfidensiallığının təmin edilməsi qaydalarına və analoji müddəalara uyğunluğunun təmin edilməsi üçün müvafiq orqanlar ilə fəaliyyət koordinasiya olunmalıdır;
- VAXT-lardan (həmçinin VA-lar ilə fəaliyyətdə iştirak edən digər təşkilatlardan) PL/TM risklərinin aşkar edilməsi, qiymətləndirilməsi və aşağı salınması üzrə effektiv tədbirlərin tətbiqi tələb olunmalıdır;

- FATF Tövsiyələrinə uyğun olaraq, öz müştərini tanı (“KYC”), uçotun aparılması, şübhəli əməliyyatlara dair hesabatlılıq və sanksiyalara riayət olunmasının yoxlanılması da daxil olmaqla, PL/TMM üzrə preventiv tədbirlərin tam spektri həyata keçirilməlidir.

FATF-ın 1-ci Tövsiyəsinə uyğun olaraq ölkələr virtual aktivlərin, eləcə də VAXT-ların fəaliyyəti və ya əməliyyatları nəticəsində meydana çıxmış PL/TM risklərini aşkar etməli, qiymətləndirməli və başa düşməlidir. Bu qiymətləndirmə əsasında PL/TM-in nəticələrinin qarşısının alınması və ya yumşaldılması üzrə tədbirlərin aşkar olunmuş risklərə mütənasibliyini (uyğunluğunu) təmin etmək məqsədilə ölkələr risk qiymətləndirməsinə əsaslanan yanaşma tətbiq etməlidir. Ölkələr VAXT-lardan PL/TM risklərinin azaldılması məqsədilə belə risklərin aşkar edilməsi, qiymətləndirilməsini və effektiv tədbirlərin tətbiqini tələb etməlidir.

VAXT minimum təsis edildiyi yurisdiksiyada lisenziyalaşdırılmalı və ya qeydiyyata alınmalıdır. VAXT-ın fiziki şəxs olduğu hallarda, onlar kommersiya müəssisəsinin (biznesin) yerləşdiyi (və ya fəaliyyətini həyata keçirdiyi) yurisdiksiyada lisenziyalaşdırılmalı və ya qeydiyyata alınmalıdır. Həmçinin yurisdiksiyalar VAXT-ların öz müştərilərinə məhsul və / və ya xidmət təklif etdiyi və ya əməliyyatlar həyata keçirdiyi yurisdiksiyada lisenziyalaşdırılmasını və ya qeydiyyata alınmasını tələb edə bilərlər. Səlahiyyətli orqanlar cinayətkarların və ya onların ortaqlarının VAXT-da əhəmiyyətli və ya nəzarət payına sahib olmasının və ya benefisiar mülkiyyətçi olmaqla idarəetmə funksiyasına sahib olmasının qarşısını almaq üçün lazımi hüquqi və ya tənzimləyici tədbirləri görməlidir. Ölkələr zəruri lisenziya olmadan və ya qeydiyyatdan keçmədən VAXT fəaliyyətini həyata keçirən fiziki və ya hüquqi şəxsləri müəyyənləşdirmək və uyğun sanksiyalar tətbiq etmək üçün tədbirlər görməlidir.

Verilmiş ölkədə maliyyə təsisatı kimi artıq lisenziya almış və ya qeydiyyatdan keçmiş, eləcə də belə lisenziya və ya qediyyatla VAXT fəaliyyətinə də icazə verilmiş (və bununla da FATF Tövsiyələrinə uyğun olaraq tətbiq olunan öhdəliklərin bütün spektrini əhatə edirsə) fiziki və ya hüquqi şəxslərə münasibətdə ayrıca lisenziyalaşdırma və ya qeydiyyat sisteminin tətbiq edilməsinə ehtiyac yoxdur.

Ölkələr VAXT-ların PL/TMM baxımından uyğun qaydada tənzimlənməsini, nəzarət və ya monitorinq olunmasını və virtual aktivlərin doğurduğu PL/TM risklərinin azaldılması üçün FATF-ın müvafiq Tövsiyələrinin effektiv şəkildə icra olunmasını təmin etməlidir.

VAXT-lara münasibətdə effektiv monitorinq və PL/TMM üzrə milli tələblərə uyğunluğun təmin olunması sistemi fəaliyyət göstərməlidir. VAXT-lar risk-əsaslı nəzarət və ya monitorinqi təmin edən səlahiyyətli orqan (SRB, yəni özünütənzimləyən orqan olmayan) tərəfindən nəzarət və ya monitorinq olunmalıdır.

Nəzarət orqanları yoxlama aparmaq, informasiya təqdim edilməsinin tələb olunması və sanksiyalar tətbiq etmək səlahiyyəti də daxil olmaqla, VAXT-ların nəzarət və ya monitorinq, PL/TM ilə mübarizə üzrə tələblərə riayət olunmasının təmin edilməsi üçün müvafiq səlahiyyətlərə malik olmalıdır.

Nəzarət orqanları VAXT-ların lisenziyasını və ya qeydiyyatını geri götürmə, məhdudlaşdırma və ya dayandırma səlahiyyəti də daxil olmaqla bir sıra intizam və maliyyə sanksiyaları tətbiq etmə səlahiyyətlərinə sahib olmalıdır.

Ölkələr FATF-ın 35-ci Tövsiyəsinə uyğun olaraq, PL/TMM tələblərinə əməl etməyən VAXT-lar ilə mübarizə aparmaq üçün cinayət, mülki və ya inzibati xarakterli bir sıra təsirli, mütənasib və çəkindirici sanksiyaların olmasını təmin etməlidirlər. Sanksiyalar yalnız VAXT-lara deyil, eləcə də onların direktorlarına və yüksək rəhbərliyinə qarşı da tətbiq edilə bilən olmalıdır.

Preventiv (xəbərdaredici) tədbirlərə gəldikdə, FATF-ın 10-21-ci Tövsiyələrində ifadə olunmuş tələblər aşağıdakı normalara riayət olunması şərtilə VAXT-lara tətbiq olunur:

a) VAXT-lar 1000 USD/EUR məbləğindən (limit həddindən) yuxarı olan təsadüfi (müəyyən müddətdən bir olan, müəyyən məqsəd üçün olan) əməliyyatlar həyata keçirən müştərilərin tam eyniləşdirilməsi və verifikasiyasını həyata keçirməlidir.

b) Tövsiyə 16-a əsasən, ölkələr virtual aktivlərin köçürülməsi zamanı köçürməni göndərən VAXT-ın göndərən haqqında zəruri və dəqiq informasiyanı və alan tərəf (benefisiar) barədə tələb olunan informasiyanı əldə etməsi və saxlamasını, köçürməni əldə edən VAXT-a və ya maliyyə təsisatına (əgər varsa) dərhal və etibarlı (təhlükəsiz) şəkildə göndərilməsini və eləcə də qeyd olunan məlumatların müvafiq orqanlar tərəfindən verilən sorğu üzrə əldə edilə bilən olmasını təmin etməlidir. Ölkələr virtual aktivlərin köçürülməsi üzrə benefisiar VAXT-ların (qəbul edən tərəf) göndərən (əməliyyatın başlandığı) tərəf barədə zəruri informasiyanı, benefisiar (alan) tərəf barədə zəruri və dəqiq məlumatı əldə edərək saxlamasını, eləcə də qeyd olunan məlumatların müvafiq orqanlar tərəfindən verilən sorğu üzrə əldə edilə bilən olmasını təmin etməlidir.

16-cı Tövsiyənin digər tələbləri (informasiyaya çıxışın monitorinqi, siyahıda olan şəxslərin əməliyyatlarının dondurulması və qadağan olunması üzrə tədbirlərin görülməsi daxil olmaqla) müvafiq Tövsiyədə müəyyən edilmiş eyni əsaslarla tətbiq olunur. Eyni öhdəliklər müştərinin adından virtual aktiv göndərən və ya alan maliyyə təsisatlarına da tətbiq edilir.

Ölkələr 37-40-cı Tövsiyələrdə qeyd olunmuş əsaslar ilə virtual aktivlərlə əlaqəli çirkli pulların yuyulması, predikat cinayətlər və terrorçuluğun maliyyələşdirilməsi üzrə beynəlxalq əməkdaşlığın maksimum geniş spektrini sürətli, konstruktiv və səmərəli şəkildə təmin etməlidir.

Xüsusilə, VAXT-ların fəaliyyətinə nəzarətə cavabdeh olan orqanlar nəzarət orqanlarının xarakteri və statusundan asılı olmayaraq və VAXT-ların nomenklaturası və ya statuslarındakı fərqlərdən asılı olmayaraq, xarici həmkarları ilə operativ və konstruktiv şəkildə məlumat mübadiləsi aparmalıdır.

Virtual aktivlərə dair FATF-ın 2021-ci ilin oktyabrında yenilənmiş Tövsiyələri

2021-ci ilin oktyabrında FATF özünün ilkin olaraq 2019-cu ildə nəşr etdirdiyi “Virtual aktivlər və VAXT-lara risk əsaslı yanaşma üzrə Rəhbərliyi”ni yeniləmişdir. 2021-ci ilin mart-aprel aylarında aparılmış ictimai məsləhətləşmənin töhfəsini əks etdirən müvafiq rəhbərlik FATF Tövsiyələrinin VA və VAXT-lara münasibətdə necə tətbiq olunmasını (müvafiq nümunələr əsasında), yumşaldıcı tədbirlərin tətbiqi üçün manelərin aşkar edilməsini izah edir və mümkün həllər təklif edir.

Yeni tərifə görə VAXT-lara *istifadə olunan texnologiyadan asılı olmayaraq*, VA-ların ötürülməsi və mübadiləsində iştirak etmə meyarına görə kriptovalyuta şirkətlərinin aid edilməsi təklif olunub. Bu, öz istifadəçilərinə vəsaitlərin köçürülməsi və mübadiləsi xidmətlərini təqdim edən “DeFi”lərin (“DeFi” protokolları) də VAXT kimi tənzimlənəcəyi anlamına gəlir.

Qeyd olunan rəhbərlikdə yeniliklər əsasən aşağıdakı 6 əsas istiqaməti əhatə edir:

- virtual aktivlər və VAXT-ların tərifərinin aydınlaşdırılması;
- FATF standartlarının steyblkoinlərə necə tətbiq olunduğuna dair təlimat;
- eyniranqlı (“peer-to-peer”) əməliyyatların PL/TM risklərinin aradan qaldırılması üçün ölkələr üçün əlçatan olan risklər və alətlər üzrə əlavə təlimat;
- VAXT-ların lisenziyalaşdırılması və qeydiyyatı üzrə yenilənmiş təlimat;
- dövlət və özəl sektor üçün “köçürmə qaydaları”nın tətbiqi üzrə əlavə təlimat;
- VAXT-a nəzarət edən təsisatlar arasında məlumat mübadiləsinin və əməkdaşlığın prinsipləri.

Sənəddə əsas yeniliklər “DEX”lər (əksmərkəzləşmiş birjalar) və kriptovalyuta üzrə depozit xidmətlərinin VAXT hesab olunması; steyblkoinlərin VA hesab olunması və onlara FATF standartlarının tətbiq olunması; PL/TM-i təşviq edən “NFT”lərin (eyni qarşılığı ilə əvəz oluna bilməyən tokenlər) VA hesab olunması; VAXT-lar üçün kütləvi qırğın silahlarının yayılmasının maliyyələşdirilməsi risklərinin qiymətləndirilməsi və aşağı salınması tələbinin müəyyən edilməsi; VAXT-ların kontragentlərinin kompleks yoxlanılmasının həyata keçirilməsinin ən yaxşı təcrübələrinin müəyyən olunması; eyniranqlı (“P2P”) əməliyyatlar üçün risklərin aşağı salınması variantları; FATF-ın yeni “köçürmə qaydaları”nın şərhi və tövsiyələr ilə bağlı olmuşdur.

2019-cu ildə nəşr olunmuş FATF rəhbərliyi ilə müqayisədə yenilənmiş 2021-ci il rəhbərliyi VA və VAXT-ların daha müfəssəl tərifini ehtiva edir. Ölkələr tərəfindən müvafiq anlayışların tərifl ərinə daha geniş yanaşmanın tətbiq edilməsi tövsiyə olunur. Qeyd olunan tərif lər istifadə olunan terminologiyaya deyil, aktivlərə və ya xidmətlərə aiddir. Rəhbərlik VAXT tərifinə daxil olan komponentlərin hər birinə dair ətraflı məlumat verməklə onların hər biri üzrə nələrin əhatə olunduğunu göstərir. Buraya steyblkoinlərin, eyni qarşılığı ilə əvəz oluna bilməyən tokenlərin (“NFT”), əksmərkəzləşmiş maliyyələşmənin (“DeFi”) və əksmərkəzləşmiş və ya paylanmış tətbiqlərin (“DApp”), eləcə də çoximzalı razılaşmaların FATF satndartlarına necə uyğun olması məsələləri daxildir.

Əksmərkəzləşmiş birjalar (“DEX”), platformalar və ya tətbiqlər VASP hesab olunur. FATF standartlarına uyğun olaraq əksmərkəzləşmiş tətbiqlər (“DApp”) VAXT hesab olunmur, lakin onun sahibləri və operatorları qismində çıxış edən “DApp” təşkilatları VAXT ola bilərlər.

Bundan əlavə, smart müqavilə texnologiyaları, broker xidmətləri, müxtəlif ticarət və kastodial xidmətlər də daxil olmaqla, VA üzrə şərti depozit xidmətləri VAXT hesab olunur.

İlkin olaraq VA kimi nəzərdən keçirilə bilinməyən “NFT”lər əslində dəyərləri ötürməyə və ya mübadilə etməyə imkan verən, yaxud PL/TM-i təşviq edən təkrar bazarların hesabına VA ola bilər.

Beləliklə, VA-nın hər hansı bir xüsusi formatı onları FATF satndartları çərçivəsindən istisna edə bilməz. Yəni heç bir aktiv FATF satndartları çərçivəsindən tam olaraq kənara çıxma kimi şərh oluna bilməz.

Yenilənmiş rəhbərliyə əsasən, FATF mərkəzi bankların rəqəmsal valyutalarını (“Central Bank Digital Currencies” - “CBDC”) virtual valyuta hesab etmir, lakin mərkəzi bank tərəfindən buraxılmış fiat valyutanın istənilən digər formasına analoji olan standartları tətbiq edir. Sənəddə həmçinin biznes modellərindən asılı olmayaraq, VAXT-ların istənilən müxtəlifliyinin tənzimləmə və nəzarət baxımından bərabər əsaslarda nəzərdən keçirilməli olduğu qeyd edilir.

İkinci istiqamət üzrə steyblkoinlər konsepsiyası “kütləvi tətbiq olunma” riski baxımından müzakirə olunur, eləcə də PL/TM risklərinə təsir edə bilən spesifik dizayn xüsusiyyətləri əhatə olunur. Ölkələr, VAXT-lar və digər məsul təsisatlar steyblkoinləri tətbiq etməzdən öncə onlar ilə əlaqəli riskləri daimi və perspektiv əsasda aşkar etməyə, qiymətləndirməyə və müvafiq risklərin idarə olunması və azaldılmasına çağrılır.

Yenilənmiş üçüncü istiqamət üzrə ölkələr və VAXT-lar eyniranqlı (P2P) əməliyyatlar ilə əlaqəli riskləri başa düşməyə çağrılır.

Yenilənmiş rəhbərliyə həmçinin məlumat təqdim etmə öhdəliyinə malik təsisatlara yardım etmək üçün steyblkoinlərin və *ilkin sikkə təklifinin/yerləşdirilməsinin* (“ICO”) hipotetik olaraq tematik araşdırmaları da daxil edilmişdir. Bundan əlavə, müvafiq sənəddə FATF-ın VA şəbəkəsi üçün köməkçi xidmət və ya məhsulları təqdim edən fiziki və ya hüquqi şəxsləri (onların istənilən VA fəaliyyəti ilə əhatə olunan biznesi təmsil etmədikləri və ya fəal yardım etmədikləri, yaxud öz müştəriləri adından çıxış etmədikləri çərçivədə) VAXT kimi tənzimləməyə çalışmadığı qeyd olunmuşdur.

Yenilənmiş rəhbərlikdə üçüncü istiqamət “P2P” əməliyyatları üzrə risklərin başa düşülməsi və azaldılması üçün ölkələrin nəzərə almalı olduqları tədbirləri əhatə edir. Nəzərdən keçirilmiş müvafiq bölmədə VA və VAXT fəaliyyətlərini qadağan edən və ya onu qanunsua elan edən ölkələrin VA və VAXT-lar ilə əlaqəli PL/TM risklərini dövri olaraq qiymətləndirməli olduğu bildirilir. Burada həmçinin lisenziyalaşdlrma və qeydiyyat prosesi ilə bağlı mülahizələr də daxil olmaqla, lisenziyalaşdlrma/qeydiyyatın təsviri dəqiqləşdirilir. Daha sonra, müvafiq bölmədə FATF standartlarında “müxbir bankçılıq və digər münasibətlərin” tərifinin necə şərh olunması məsələləri təsvir olunur. FATF-ın 16-cı Tövsiyəsi konteksində müvafiq rəhbərlik “köçürmə qaydaları”nın mətnini dəqiqləşdirir (əməliyyatlar üçün müəyyən komissiyaların və “köçürmə qaydaları”nın avtomatik geri qaytarmaların həyata keçirildiyi əməliyyatlara necə tətbiq edildiyi də daxil olmaqla). Rəhbərlikdə həmçinin aşağıdakılar dəqiqləşdirilir:

- Qarşı VAXT-ın (kontragentin) kompleks yoxlanılmasına və sahibi müəyyən edilməyən cüzdanlar üzrə əməliyyatlara münasibətdə hansı məlumatların toplanmalı olduğuna yanaşma;
- FATF-ın sanksiyaların yoxlanılmasına, “köçürmə qaydaları”na və toplu köçürmələrə yanaşması (xüsusən də FATF-ın “köçürmə qaydaları” üzrə məlumatların əməliyyat baş verdikdən sonra ötürülməsini qəbul etməməsi);
- Ölkələrin və VAXT-ların “günəşin çıxması” məsələsinə (bütün hökumətlərin “köçürmə qaydaları”nı eyni vaxtda həyata keçirməməsi bütün VAXT-ların mövcud olan həlləri tətbiq etməmələri ilə bağlı olması deməkdir) necə yanaşmalı olması.

Rəhbərliyin 4-cü bölməsində VAXT-lara və FATF-ın VA/VAXT təriflərinə uyğun olaraq VA ilə məşğul olan və ya belə xidmətlər göstərən digər təşkilatlara (öhdəliyə malik) FATF standartlarının tətbiqi nəzərdən keçirilir. Bu bölmədə aşağıdakı yeni istinadlar müəyyən olunub:

- müxbir bankçılıq və digər analoji münasibətlər;
- VAXT-ların “köçürmə qaydaları”na effektiv riayət etməsinə imkan verən texnoloji həllər;
- Qarşı VAXT-ın (kontragent VAXT-ın) eyniləşdirilməsi və kompleks yoxlanılması;
- Sahibi müəyyən olunmamış cüzdanlara və ya onlardan VA köçürmələri;
- VA-lar üçün əsas şübhəlilik meyarları.

Beşinci istiqamət üzrə VA/VAXT-lara risk qiymətləndirməsinə əsaslanan ölkə yanaşmaları və yeni tematik araşdırmalar verilir.

Rəhbərliyin yeni əlavə olunmuş altıncı bölməsində FATF-ın VAXT-lara nəzarət edən orqanlar arasında məlumat mübadiləsi və əməkdaşlıq prinsipləri müzakirə olunur. Nəzarət orqanları üçün məcburi olmayan müvafiq prinsiplər tələblərin geniş spektrini (məsələn, nəzarət orqanları sorğu aldığını təsdiq etməli, məlumat sorğularına cavab verməli, cavabları vaxtında təqdim etməlidir) əhatə etməklə, partnyorlar arasında əməkdaşlığa və müvafiq məlumatların mübadiləsinə yardım etmək məqsədi daşıyır.

FATF-ın 2020-ci ilin iyun müayinəsi (təftişi)

2019-cu ilin iyununda VA-lar ilə iş zamanı PL/TM üzrə tələblərə dəqiq aydınlıq gətirilməsi məqsədilə FATF özünün qlobal standartlarına düzəlişlər üzərində işini tamamlamışdır. FATF həmçinin yurisdiksiyalar və özəl sektor tərəfindən yenilənmiş standartların tətbiqi templərinin qiymətləndirilməsi, eləcə də VA sektorunun tipologiyalarında, sektorun riskləri və bazar strukturunda istənilən dəyişikliyin monitorinqi üçün 12 aylıq təftişin keçirilməsini razılaşdırdı.

FATF-ın yenilənmiş məruzəsində 2020-ci ilin iyunundan başlayaraq 12 aylıq dövr üçün FATF-ın yenilənmiş standart və tövsiyələri ilə əlaqəli bir sıra problemlər müəyyən

olundu. Məruzədə PL/TMM üzrə yeni tələblər FATF üzvü olan bir çox ölkələr tərəfindən qəbul olunur. Analoji şəkildə köçürmə qaydaları (“travel rule”) üçün texnoloji həllərin hazırlanmasında tərəqqiyə nail olunmuşdur. Lakin FATF-ın heç də bütün üzvləri 2020-ci ilin iyunu üçün dəyişmiş standartlara uyğun olaraq tədbirlərin həyata keçirildiyi barədə məlumat vermədilər. FATF tərəfindən aparılmış araşdırma göstərdi ki, bir çox ölkələrdə hələ də köçürmə qaydalarına riayət olunmaması halı geniş yayılmış, həmçinin yeni tələblərin tam inkar edildiyi hallar da aşkar edilmişdir.

Yurisdiksiyalar özlərinin milli qanunvericiliklərini FATF-ın yenilənmiş standartlarına adaptasiya etməli olduqlarını nəzərə alaraq, ətraflı aydınlıq gətirilməsi tələb olunan bir sıra məsələlər müəyyən olunmuşdur. Məsələn, yurisdiksiyaların steyblkoinlərə (“stablecoins”) ənənəvi, yaxud virtual aktiv kimi yanaşması lazım gəlir? Bundan əlavə, VA-ların saxlanılması, idarə edilməsi və ya ötürülməsinə münasibətdə daha dəqiq göstərişlər hazırlamaq lazımdır.

FATF-ın son tənzimləmə tədbirləri kripto sənaye ilə əlaqəli PL/TM risklərinin sonrakı anlaşılmasını dəstəkləmək məqsədilə riskləri müəyyən edən tematik nəşri (“red flags indicators”) də əhatə edir. Nəzərdən keçirmə tələb edən digər məsələlər sırasına VAXT-ın vasitəçi kimi iştirak etmədiyi və belə növ əməliyyatların FATF-ın yenilənmiş standartlarına uyğun olaraq PL/TM əməliyyatları üzərində nəzarət üzrə öhdəliklərinin təsirinə altına birbaşa düşmədiyi VA-ların xüsusi köçürmələri daxildir.

Şəxsi cüzdanlar üzərindən eyniranqlı əməliyyatların (“peer-to-peer”) dəqiq əhatəsinin olmaması bir sıra yurisdiksiyalarda, o cümlədən İsveçrədə narahatlığa səbəb olur. Məruzəyə əsasən, 2019-cu ilin iyunundan anonim və ya şəxsi sövdələşmələr əhəmiyyətli dəyişikliyə məruz qalmamışdır. Sübutların kifayət qədər olmaması ilə əlaqədar müəlliflər müvafiq şəxsi (eyniranqlı) sövdələşmələrin yüksək PL/TM riski yaratmadığı nəticəsinə gəlmişlər.

Lakin yeni VA-ların dövriyyəyə daxil olması, xüsusilə də anonim şəxsi sövdələşmələri aparmağa imkan verən aktivlərin kütləvi şəkildə qəbul olunduğu halda PL/TM riskləri dəyişə bilər.

Köçürmə qaydalarına (“travel rule”) uyğunluğun təmin edilməsi məqsədilə kontragent ilə qarşılıqlı əlaqə prosesində VAXT sövdələşmənin aparıldığı yurisdiksiyada kontragentin hüquqi statusunu müəyyən etmək və PL/TM risklərinin yoxlanılması qaydalarını nəzərə almaqla, əməliyyatların lazımi şəkildə icra olunduğunu yoxlamaq iqtidarında olmalıdır. Burada əsas məsələ kontragentin vaxtında və təhlükəsiz qaydada zəruri yoxlanışını aparmaqdan ibarətdir. Təklif olunan üsullardan biri bütün yurisdiksiyalardan olan informasiyanın cəmləşdiyi və razılaşdırılmış mərkəzi məlumat bazası üzərindən ona çıxışın həyata keçirildiyi kontragentlərin qlobal siyahısının yaradılması ola bilər. Lakin belə məlumat bazasının idarə edilməsi əksmərkəzləşmiş olacaq və bazar iştirakçıları tərəfindən koordinasiya olunacaqdır. Bu təklif ilə bağlı informasiyanın toplanması və saxlanmasına kimin cavadeh olacağı, bu prosesə kimin nəzarət edəcəyi və məlumatlara kimin çıxışına icazə veriləcəyinə dair özəl sektorda suallar meydana çıxır.

FATF standartlarından fərqli olaraq, İsveçrə qanunvericiliyində tənzimlənməyən cüzdan təchizatçılarının iştirakı ilə olan ödənişlər üçün heç bir istisna nəzərdə tutulmur. Belə məhdudiyyət nəzarət olunmayan təchizatçılar ilə olan sövdələşmələrə maneə yaradır və şübhəli ödənişlərin qarşısını alır.

İsveçrənin maliyyə bazarlarına nəzarət orqanı olan “FINMA”nın nəzarət etdiyi hər hansı bir monitorinq iştirakçısının ödəniş (köçürmə) əməliyyatlarının aparılması üçün zəruri olan informasiyanı ala və göndərə bilmədiyi hallarda, yalnız həmin təsisatın müştərisinə məxsus təsdiqlənmiş pul cüzdanları ilə aparılan müvafiq əməliyyatlara icazə verilir. Cüzdana mülkiyyət hüququ müvafiq texniki vasitələrin köməyilə sübut olunmalıdır.

Eyni bir təsisatın müştəriləri arasında aparılan sövdələşmələrə (köçürmələrə) icazə verilir. Üçüncü şəxsə məxsus olan xarici cüzdandan və ya xarici cüzdana olan köçürmə yalnız sövdələşməyə nəzarət edən təsisatın ilkin yoxlama apardığı, üçüncü şəxsin və benefisiar mülkiyyətçinin kimliyini müəyyən etdiyi və uyğun texniki vasitələrin köməyilə üçüncü şəxsin xarici cüzdana olan mülkiyyət hüququnu sübut etdiyi halda mümkündür.

Tənzimlənməyən cüzdan təchizatçılarının iştirakı ilə olan ödənişlər üzrə 3 ölkənin FATF standartlarına uyğunluğunun müqayisəli cədvəli aşağıda verilmişdir:

	FATF **T 16 – Köçürmə qaydası**	İsveçrə **AMLO 02/2019**	ABŞ **FinCEN Köçürmə qaydası**	Sinqapur **PSA**
Əməliyyatın yoxlama tələb edən minimum məbləği	Maliyyə vasitəçisi 1000 USD və ya EUR olan əməliyyatlar üzrə informasiya barədə məlumat verməlidir	1000 CHF-dən yuxarı (01/2021-dən tətbiq olunur)	1000 USD-dən yuxarı	1500 dollardan yuxarı
Göndərən şəxsin məlumatları	- Adı - Hesab nömrəsi - Yaşayış ünvanı, pasport nömrəsi və ya doğum tarixi və yeri	- Adı - Hesab nömrəsi - Yaşayış ünvanı, pasport nömrəsi və ya doğum tarixi və yeri	- Adı - Hesab nömrəsi - Yaşayış ünvanı	- Pasport və ya doğum haqqında şəhadətnamə - Pasport və ya biznes sertifikat
Benefisiarın məlumatları	- Adı - Hesab nömrəsi	- Adı - Hesab nömrəsi	- Adı - Hesab nömrəsi - Unikal identifikator	- Adı - Hesab nömrəsi - Unikal identifikator

Köçürmə qaydalarına (“Travel rule”) olan tələblər

“Köçürmə qaydaları” (“Travel Rule”) - birdən çox maliyyə təsisatının iştirakı ilə vəsaitlərin müəyyən köçürmələrində bütün maliyyə təsisatlarının müəyyən məlumatlarını digər maliyyə təsisatına ötürməsini tələb edir.

Köçürmələr ilə bağlı müvafiq qaydaların təkamülünə əsasən, ilk dəfə 1996-cı ildə ABŞ-ın maliyyə monitorinqi orqanı olan “FinCEN” tərəfindən köçürmələr üzrə qayda (“Travel Rule”) daxil edilmişdir. Bu qaydaya əsasən, pul xidmətləri göstərən banklar və şirkətlər 3000 ABŞ dolları və ondan yuxarı məbləğlərdə həyata keçirilən köçürmələr ilə bağlı göndərən və alan tərəf barədə informasiya mübadiləsi aparmalıdır. 2012-ci ildə hesabatı verilən əməliyyatların siyahısına elektron pul köçürmələrini daxil edən düzəlişlər edilmişdir. FATF yalnız 2012-ci ildə öz tövsiyələrinə uyğun olaraq köçürmə qaydasını (“Travel Rule”) qəbul etmişdir. 2018-ci ildə bütün dünya üzrə tənzimləyicilər kripto tənzimləni sərtləşdirdilər və nəticədə virtual aktivlər və VAXT-lar üçün köçürmə qaydasının tətbiqinə zərurət yarandı. FATF 2019-cu ilin iyununda “FinCEN” tərəfindən hazırlanmış “Kripto” qaydalar (“Travel Rule”) əsasında VAXT-lar arasında benefisiar və göndərən barədə informasiya mübadiləsinə münasibətdə qlobal standartları təklif etdi. Bu qaydalar kriptovalyuta birjaları, saxlanc cüzdanları, əksmərkəzləşdirilmiş birja operatorları və ya digər subyektlərə (hər bir konkret yurisdiksiyada qaydaların aid olunduğu) aid edilir.

Vəsaitlərin köçürülməsi üzrə bu “qaydalar” vəsaitlərin köçürülməsi sistemi vasitəsilə vəsaitləri göndərən və alan şəxslər barədə informasiya izlərinin saxlanılması yolu ilə PL və digər maliyyə cinayətləri ilə əlaqəli cinayətlərin aşkar edilməsi, istintaqının aparılması

və təqib olunmasında hüquq mühafizə orqanlarına (HMO) dəstək verilməsi üçün nəzərdə tutulub.

Şübhəli əməliyyatların müəyyən olunması və ötürülməsi, informasiyanın əlçatan olmasına nəzarət edilməsi, şübhəli şəxslər və təşkilatlar ilə aparılan əməliyyatların dondurulması və ya onların qadağan olunması tədbirlərinin görülməsi üçün göndərən və alan tərəf barədə tələb olunan məlumatların əldə edilməsi, saxlanılması və ötürülməsi üzrə öhdəliklər də daxil olmaqla FATF-ın 16-cı Tövsiyəsində ifadə olunmuş bütün tələblər VAXT-lar və virtual aktivlərin köçürülməsi ilə əlaqəli olan digər iştirakçı təşkilatlar üçün tətbiq olunur. Bu səbəbdən, ölkələr vasitəçi təsisatlar və virtual aktivlərin ötürülməsində iştirak edən maliyyə vasitəçiləri kimi öhdəlik daşıyan təşkilatlar tərəfindən göndərən və alan barədə tələb olunan etibarlı məlumatın əldə edilməsi və saxlanılması, eləcə də belə məlumatların benefisiar-təsisatlara təqdim olunmasını təmin etməlidir. Dəqiq məlumat FATF-ın “VA və VAXT-lar üçün risk əsaslı yanaşmanın tətbiqi üzrə rəhbərliyi”ndə ifadə olunmuşdur. Köçürmə üzrə tələb olunan məlumatlara aşağıdakılar daxildir:

- Köçürməni edən şəxsin (göndərən tərəfin) adı;
- Köçürməni edən şəxsin (göndərən tərəfin) hesab nömrəsi (məsələn, virtual aktivlərə malik cüzdan);
- Köçürməni edən şəxsin (göndərən tərəfin) fiziki (coğrafi) ünvanı, yaxud milli identifikasiya nömrəsi, yaxud müştərinin eyniləşdirmə nömrəsi (əməliyyatın nömrəsindən fərqli olaraq, sifarişçinin təsisatında göndərəni eyniləşdirir), yaxud doğum tarixi və yeri;
- Köçürməni qəbul edən şəxsin adı;
- Köçürməni qəbul edən şəxsin hesabı (əgər əməliyyatın işlənməsi üçün belə hesabdan istifadə olunarsa, məsələn, virtual aktivlərə malik cüzdan).

Müvafiq məlumatları virtual aktivlərin birbaşa olaraq özünə qoşmaq (əlavə etmək) üçün zərurət mövcud deyildir. Məlumatlar 15-ci Tövsiyənin izahlı qeydində göstərildiyi kimi, birbaşa, eləcə də dolayı olaraq təqdim oluna bilər.

Bölmə
Doqquz

9

VİRTUAL AKTİVLƏR İLƏ ƏLAQƏLİ POTENSİAL RİSKLƏR

- risk
- risk amilləri
- risk faktorları

Virtual aktivlər ilə əlaqəli potensial risklər

PL/TM məqsədləri üçün qanunsuz istifadəsi baxımından virtual aktivlər (real pullara və ya digər virtual aktivlərə mübadilə oluna bilən) potensial zəifliyə malikdir. Birincisi, onlar nağdsız ödənişlərin ənənəvi üsulları ilə müqayisədə daha yüksək dərəcədə anonimliyi təmin edə bilirlər. İnternet vasitəsilə ticarəti aparıla bilən virtual aktivlər sistemi ümumilikdə müştərilər ilə birbaşa qarşılıqlı əlaqənin olmaması ilə xarakterizə edilməklə yanaşı, anonim maliyyələşdirməni həyata keçirməyə imkan verir (maliyyələşmə mənbəyi zəruri şəkildə müəyyən edilməyən virtual mübadilə məntəqələri üzərindən nağd pullar və ya üçüncü şəxslər tərəfindən maliyyələşdirmə). Həmçinin onlar göndərən və alan tərəfin şəxsiyyətinin lazımi şəkildə müəyyən edilmədiyi hallarda anonim köçürmələrin həyata keçirilməsi imkanını təmin edə bilir.

Mərkəzləşməmiş sistemlər anonimlik riski baxımından xüsusilə həssasdır. Məsələn, hesablar kimi fəaliyyət göstərən “bitcoin-ünvanlar” mahiyyət etibarilə müştərilərin adları və ya onların digər eyniləşdirmə məlumatlarına malik deyildir, sistemin özündə isə mərkəzi server və ya xidmət təminatçıları mövcud deyildir. Bitcoin-protokol iştirakçıların şəxsiyyətinin müəyyən olunması və yoxlanılmasını, yaxud hər hansı bir şəkildə real dünyada iştirakçıların şəxsiyyətləri ilə əlaqəli olan əvvəlki dövrün əməliyyatları barədə məlumatların formalaşdırılması və aparılmasını tələb və təmin etmir. Bundan əlavə, mərkəzi nəzarət orqanı və hazırda PL-ə qarşı mübarizə məqsədləri üçün şübhəli əməliyyatların izlənilməsi və aşkar edilməsinə imkan verən proqram təminatı da mövcud deyildir. Hüquq mühafizə orqanları (HMO) istintaq aparılması və ya aktivlərin üzərinə həbs qoyulması üçün hər hansı bir mərkəzi yerin və ya şəxsin (inzibatçının) müəyyən edilməsi iqtidarında deyillər (müvafiq orqanların müştəriləri barədə məlumat əldə etmək üçün mübadilə xidmətləri üzrə ayrı-ayrı provayderləri aşkar edə bilmələrinə baxmayaraq). Beləliklə, bütün bunlar potensial anonimliyin kredit və debet kartları və ya “PayPal” kimi onlayn ödənişlərin daha köhnə ənənəvi sistemi halında sadəcə mümkün olmayan səviyyəsini təmin edir.

Virtual aktivlərin geniş yayılması və unikal xarakteri onların PL/TMM sahəsində olan potensial risklərini də yüksəldir. Virtual aktivlər sistemi internet (o cümlədən, mobil telefonlar) vasitəsilə əldə oluna və pul vəsaitlərinin transsərhəd ödənişləri və köçürmələrinin həyata keçirilməsi üçün istifadə oluna bilər. Bundan əlavə, virtual aktivlər bir qayda olaraq, bir sıra müxətlif ölkələrdə yerləşən, pul vəsaitlərinin köçürülməsini və ödənişlərin edilməsini təmin edən bir sıra şəxsləri özündə birləşdirən mürəkkəb infrastruktur çərçivəsində fəaliyyət göstərir. Xidmətlərin belə seqmentasiyası nəyin tam aydın olmadığını, PL/TMM tələblərinə riayət olunmasının təmin edilməsinə və nəzarətin həyata keçirilməsinə (məcburi tədbirlərin tətbiqinə) konkret olaraq kimin cavabdeh olduğunu göstərir.

Bundan əlavə, əməliyyatlar və müştərilər barədə məlumatlar və sənədlər çox vaxt müxtəlif yuridiksiyalarda yerləşən müxtəlif şəxslər tərəfindən aparıla və saxlanıla bilər ki, bu da belə məlumatlara HMO və tənzimləyici orqanların çıxışını əlavə olaraq çətinləşdirir.

Bu problem mərkəzləşməmiş virtual aktiv texnologiyalarının və biznes modellərinin sürətlə dəyişən və inkişaf edən xarakteri, o cümlədən virtual aktivlərdən istifadə edən ödəniş sistemləri çərçivəsində xidmətlər göstərən iştirakçıların sayı və növləri/funksiyaları ilə dərinləşir. Həmçinin virtual aktivlər sisteminin müxtəlif elementlərinin PL/TMM

sahəsində uyğun nəzarət tədbirləri olmayan yurisdiksiyalarda yerləşə bilməsi faktını da nəzərə almaq lazımdır. Mərkəzləşmiş virtual aktivlər sisteminin iştirakçıları PL-də iştirak edə bilər və bilərəkdən zəif PL/TMM rejiminə malik yurisdiksiya axtara bilərlər. Şəxslər arasında anonim əməliyyatlar həyata keçirməyə imkan verən mərkəzləşməmiş konvertasiya olunan virtual aktivlər hər hansı istənilən dövlət üçün tam olaraq əlçatmaz olan rəqəmsal məkanda mövcud ola bilər.

Hazırda **VA-lar üzrə** müşahidə olunan **əsas risklərə** - virtual valyutalarla əlaqəli risklər, "FinTech" firmaları vasitəsi ilə maliyyə məhsulları və xidmətlərinin təqdim edilməsi ilə bağlı risklər, TM-ə qarşı mübarizə sistemində və nəzarət sahəsində yaranan risklər, riskdən uzaqlaşmaqdan ("de-risking") yaranan risklər, nəzarət orqanlarının fikir ayrılığından yaranan risklər, transsərhəd VA fəaliyyəti ilə əlaqəli risklər, vergi cinayətlərinə qarşı mübarizəyə fərqli yanaşmalardan irəli gələn riskləri aid etmək olar.

Virtual aktivlər ilə əlaqəli digər potensial PL/TMM riskləri aşağıdakılardır:

- eyniranqlı ("peer-to-peer") onlayn əməliyyatların əksmərkəzləşməsi səbəbindən virtual aktivlər yüksək riskli hesab olunur;
- internet üzərindən virtual aktivlər ilə aparılan əməliyyatlar yüksək anonimliyi ilə seçilir ki, bu da əməliyyatlarda iştirak edən şəxsləri və vəsaitlərin mənbəyini müəyyən etməyi çətinləşdirir;
- virtual aktivlərin qiymətlərinin volatilliyi və spekulyativ xarakteri onları riskli edir;
- virtual aktivlər ilə əməliyyatlar dərhal icra olunur və ləğv oluna bilinmir;
- virtual aktivlər fiat pullara və ya əksinə asanlıqla konvertasiya olunur və potensial olaraq PL/TMM tələbləri altına düşmür;
- bir sıra ölkələrdə VA ilə əməliyyatlar üzrə PL/TMM komplayensi, nəzarət və məcburi tələblərə riayət edilməməsinə görə müəyyən edilən məsuliyyətlər baxımından aydınlığın olmaması;
- virtual aktivlər ilə əlaqəli şübhəli əməliyyat modellərinin monitorinqi və aşkar edilməsi üçün mərkəzi nəzarət orqanının və proqram təminatının olmaması;
- virtual aktivlərin istintaqı və müsadirəsi üçün HMO-ın mərkəzi bir yerə və ya təsisata (inzibatçıya) hədəflənə bilməməsi;
- istintaq (araşdırma) prosesində əməliyyatların izlənilməsinin çətin olması;
- virtual aktivlər sisteminə girişin internet (o cümlədən, mobil telefonlar) vasitəsilə əldə oluna bilinməsi və ondan beynəlxalq ödənişlər və pul vəsaitlərinin köçürülməsi üçün istifadə edilməsi;
- cinayətdən əldə olunan gəlirlərin gizlədilməsinin asanlığı hesabına istənilən regionda cinayət fəaliyyətini gücləndirə bilməsi;
- qanunsuz kapital qaçışı ilə ölkələrin iqtisadiyatlarına ziyan vura bilməsi;
- virtual aktivlər və onlarla aparılan əməliyyatların potensial olaraq TM üçün həssas olması;
- virtual aktivlər ilə əməliyyatların "darknet"dən istifadə edilməklə aparıla bilinməsi və adətən, "darknet"də başlanmış qanunsuz ticarətdə istifadə olunması imkanı;
- virtual aktivlərlə ticarət zamanı aldatma və dələduzluq risklərinin mövcudluğu.

VA-ların yuyulması müvafiq ekosistemin dizaynında insan, təşkilati və texniki amillərin mürəkkəb qarşılıqlı əlaqəsi nəticəsində baş verir. VA-ların PL/TM-ə məruz qalmasının başa düşülməsi mühüm həyati əhəmiyyət kəsb edir, çünki müvafiq qanunvericilik, monitorinq və nəzarətin olmaması verilmiş yurisdiksiyanı cinayətkarlar üçün virtual cəhətdən təhlükəsiz sığınacağa çevirə bilər. Müxtəlif yurisdiksiyalarda tənzimləmə çərçivəsinin müəyyən olunmasındakı böyük fərqlərin olması, təşkilatların və fəaliyyətlərin ümumi başa düşülməsinin (anlayışların vahid standart tərifl ərinin) olmaması səbəbindən, bir çox ölkələr VA-lar üzrə qanunvericiliyin qəbulu və qaydalara riayət olunmasının təmin edilməsinin müxtəlif mərhələlərində yerləşirlər. VA-ların qlobal

tənzimlənməsi ekosistemində müşahidə edilən müvafiq boşluqlar cinayətkarlara VA-ların anonimlik üstünlüklərindən istifadəsi üçün platformanı təmin edir.

FATF-ın 15-ci Tövsiyəsi tərəfindən irəli sürülmüş "köçürmə qaydası"nın ("travel rule") implementasiyasını təmin etməyə imkan verən texnoloji həllərin hazırlanmasında tərəqqi əldə olunmuşdur. Predikativ cinayət nəticəsində yaranmış VA-ları blokçeyndə qeydə alınmış əməliyyatlar üzrə izləmək olar. Blokçeyn texnologiyası bütün əməliyyatların şəffaflığını və izlənilə bilinməsini təmin edir, lakin buna baxmayaraq, "köçürmə qaydası"nın ("travel rule") implementasiya olunmadığı halda, iştirakçının əsl şəxsiyyəti heç vaxt məlum olmaya bilər. Lakin unikal "IP" ünvanlar, əməliyyatın tarixi və geolokasiya kimi bir sıra atributlar istifadəçinin anonimliyini azalda bilər. VA-ların PL/TM risklərini başa düşmək üçün onlar müxtəlif meyarların köməyilə təhlil oluna bilər. Belə meyarlara nümunə olaraq funksionallıq, stabilləşdirmə mexanizmi və sistem əhəmiyyətliliyi çıxış edir. Bazarda yeni biznes modellərin meydana çıxmasına uyğun olaraq, ehtimal ki, təsnifləşdirmə meyarları da inkişaf edəcəkdir.

VA-ların müxtəlif ölkələrə köçürülməsinin asanlığı və bütün dünyada nəzarət və preventiv tədbirlərin eyni olmaması səbəbindən, VA-lar əhəmiyyətli PL/TM riski daşıya bilərlər. Cinayətkarlar anonim formada dəyərin ötürülməsi və ya malların alışı (virtual birjalar vasitəsilə pul maliyyələşməsi və ya üçüncü tərəflərin maliyyələşməsi) üçün VA sistemindən istifadə edirlər. Xüsusilə terrorçuluğun maliyyələşdirilməsi baxımından VA-lar adətən, texnoloji vasitələrdən istifadə etməklə birbaşa əlaqə qurmadan yaradılan müştəri münasibətlərini özündə birləşdirə və anonim maliyyələşdirmə və alışlara (maliyyələşmə mənbəyi lazımi şəkildə müəyyən olunmadığı halda virtual birjalar vasitəsilə pul maliyyələşməsi və ya üçüncü tərəflərin maliyyələşməsi) icazə verə bilər. Onlar həmçinin göndərən və alan tərəfin lazımi şəkldə müəyyən edilmədiyi halda anonim köçürməyə imkan verə bilər. VA-lar ilə əlaqəli fəaliyyətər artmaqda olan PL/TM təhdidləri doğurur.

VA-ların təbiətini başa düşmək və onlar ilə əlaqəli riskləri qiymətləndirmək üçün ölkələr bir sıra amilləri nəzərə almalıdır. Belə amillərdən bəzi əsas olanlarına aşağıdakıları aid etmək olar:

- VA-nın emitentinin xarakteri (məsələn, eyniləşdirilə bilinən, eyniləşdirilə bilinməyən; dövlət, özəl; tənzimlənən, tənzimlənməyən);
- VA-ların nəzərdə tutulan (ehtimal olunan) istifadəsi (məsələn, vəsaitlərin yığımı, investisiya qoyuluşu, ödəniş, xidmətlərə hüququn verilməsi kimi istifadə / şəbəkədə və ya şirkətin ekosistemində məhsullardan istifadə olunması);
- VA sahiblərinin hüquqları (məsələn, əsas aktivin təminatı, verilmiş pay, şəbəkə və ya platformada xidmətlərə çıxış və ya onlardan istifadəyə dair tələblər);
- ödəmə tələbi (qiymətlərin dinamikasından asılı olaraq ödəməyə dair müqavilə tələbi, təsbit olunmuş ödəmə tələbi);
- reyestr ("ledger") üzərində nəzarət (ictimaiyyət üçün açıq, bəzi tərəflər üçün açıq, məhdud sayda səlahiyyətli tərəflərə açıq);
- reyestrin yoxlanılması (icazə verilən, icazə verilməyən);
- VA-lara sahibliyin ötürülməsi mexanizmi (məsələn, mərkəzləşmiş, "peer-to-peer" – "P2P", mərkəzləşməmiş).

Ümumilikdə, beynəlxalq təcrübədə VA və VAXT-lar üzrə müşahidə olunan riskləri (təhdid və zəifliklərı) qiymətləndirmək üçün onları aşağıdakı risk faktorları üzrə təsnifləşdirmək olar:

- VA-ların təbiəti (xarakteri) və profili;
- cinayətkarlar üçün əlçatanlığı;
- VA-ların maliyyələşmə mənbələri;
- VA-ların əməliyyat xüsusiyyətləri;

- cinayətkarlığın asanlığı;
- iqtisadi təsir.

VA-ların özünün təbiətindən irəli gələn riskin qiymətləndirilməsində istifadə olunan əsas risk elementlərinə anonimlik, "P2P" transsərhəd köçürməsi və daşına bilmə, birbaşa (üz-üzə) təmasın olmaması, izlənilə bilmə və köçürmənin sürəti daxil edilir.

VA-ların təbiətindən irəli gələn *anonimlik və konfidensiallıq* VA-ların baza texnologiyası şifrələmə/kriptoqrafiya ilə bağlıdır ki, bu da cinayət fəaliyyətinin aşkar edilməsini çətinləşdirir. VA-lar ilə bağlı anonimliyə nümunə olaraq aşağıdakıları göstərmək olar:

- axınların şifrəsinin açılmasını çətinləşdirməkdən ötrü əməliyyatların izini qarışdırmaqla, çoxsaylı istifadəçilərdən VA-ları toplayan və onları yenidən bölüşdürən servislər olan "mikserlərdən" və "qablardan" ("tumbler") istifadə edilməsi;
- "Bitcoin" kimi açıq, şəffaf blokçeyndə işləyən VA-nın mərkəzləşmiş birjaya köçürülməsi və daha sonra onun dərhal anonimiliyi yüksək olan kriptovalyutaya və ya konfidensial sikkəyə mübadiləsi;
- VA-ların sərhəddən keçirilməsi (çıxarılması) üçün mərkəzləşməmiş/sahibsiz cihazlardan və ya kağız cüzdanlardan istifadə olunması.

VA-ların təbiətindən irəli gələn "*P2P" ("peer-to-peer") transsərhəd köçürməsi və daşına bilmə* xüsusiyyəti bank və ya hər hansı digər maliyyə təsisatından keçmə zərurəti olmadan dünyanın istənilən yerində yerləşən qurbanlardan ödənişlər qəbul edən cinayətkarlar üçün cəlbedicidir.

VA-ların təbiətindən irəli gələn *birbaşa (üz-üzə) təmasın olmaması* xüsusiyyəti VA-ların bütün növləri üçün xas olan riskdir. Lakin şəxsi iştirak olmadan VA-lara çıxışın əsasında yerləşən anonimliyin ifşa edilməsi üçün "DLT" ("Distributed Ledger Technology" – Paylanan reyestr texnologiyası – bir sıra obyektlər və ya ərazilər arasında paylanan şəbəkədə məlumatlara eyni vaxtda girişini, yoxlanması və yenilənməsini təmin edən protokollar olmaqla, əksmərkəzləşmiş rəqəmsal məlumat bazasının təhlükəsiz fəaliyyətini təmin edir) texnologiyadan istifadə imkanları mövcuddur. VA sistemlərinin internetdə satılıb alına bilinməsi səbəbindən onlar bir qayda olaraq, birbaşa (üz-üzə) iştirak etməyən müştərilər ilə münasibətlər ilə xarakterizə oluna və anonim maliyyələşməyə (mliyyələşmə mənbəyini müvafiq şəkildə müəyyən etməyən virtulal mübadiləçilər vasitəsilə pul maliyyələşməsi və ya kənar – üçüncü tərəfin maliyyələşməsi) yol verə bilər.

VA-ların təbiəti ilə bağlı *izlənilə bilmə* xüsusiyyətinə gəldikdə, VA-ların növlərindən asılı olaraq, bir çox VA-lar konfidensiallığı vurğulayırlar ki, bu da izləmə imkanlarını çətinləşdirir, lakin "DLT" həlləri əməliyyatları asanlıqla izləməyə və yoxlamağa imkan verir.

VA-ların təbiəti ilə bağlı *köçürmənin sürəti* xüsusiyyətinə gəldikdə, qeyd etmək lazımdır ki, VA-ların bir sıra növləri digərlərinə nisbətən əməliyyatların daha yüksək sürətini təklif edirlər. Açıq mənbəli ekosistemlərdə ("IOTA") insanlar və maşınlar dəyəri (yəni pulu) və/və ya məlumatı etibar olmayan, icazəsiz və mərkəzləşməmiş bir mühitdə heç bir əməliyyat haqqı ödəmədən köçürə bilərlər. Bir çox digər sikkələrin əsasında dayanan texnologiyaya nisbətən daha geniş miqyaslı texnologiyadan istifadə etməklə "IOTA" əməliyyatların daha yüksək sürətini vəd edir.

VA-ların cinayətkarlar üçün əlçatan olması riskinin qiymətləndirilməsində istifadə olunan əsas risk elementlərinə VA-ların cinayətkarlar tərəfindən mayninq olunması, vəsaitlərin toplanması, vəsaitlərin köçürülməsi, "Dark-web"ə ("dark market"ə) çıxış imkanları və vəsaitlərin xərclənməsi imkanları üzrə göstəricilər aid olunur.

VA-ların cinayətkarlar üçün əlçatanlığı üzrə risk faktorundan irəli gələn *cinayətkar tərəfindən mayninq* adlı risk elementi kriptovalyutaların mayninqi üçün cinayətkarlar

tərəfindən oğurlanmış hesablama güclərindən istifadə olunmasını nəzərdə tutur ki, bu da gəlirli cinayət sahəsi hesab olunur. Kriptocekinqdə (“cryptojacking”) iştirak edən cinayətkarlar proqram təminatını quraşdırmaq üçün korporativ və fərdi kompüterləri, noutbukları və mobil cihazları kibercinayət üsulları ilə sındırmaqla zərərli VA mayninqini həyata keçirirlər. Müvafiq proqram təminatı isə kompüterin gücü və resurslarından kriptovalyutaların mayninqi üçün istifadə edir və ya heç bir şeydən şübhələnməyən qurbanlara məxsus kriptovalyuta cüzdanlarını oğurlayır. Kodu yerləşdirmək asandır, arxa planda (fonda) işləyir və onu aşkar etmək çətindir. Adətən, mayninq hovuzlarının operatorları tərəfindən iştirakçılara münasibətdə KYC/PL-TMM üzrə kompleks yoxlama tədbirləri həyata keçirilmədiyindən, iştirak edən maynerlərin bədniyyətli davranışlarının müşahidə edilməsi və ya cinayət mənşəli aktivlər təqdim etmə ehtimalları yüksələcəkdir.

VA-ların cinayətkarlar üçün əlçatanlığı üzrə risk faktoruna daxil olan *vəsaitlərin toplanması* adlı risk elementi TM üçün geniş imkanlar açır. Belə ki, VA-ların təbiətini nəzərə alaraq, bu gün kağız (fiat) pullar ilə müqayisədə rəqəmsal valyutaların terrorçuluğun maliyyələşdirilməsində (TM) və terror hücumlarında daha effektiv istifadə oluna bilməsi ehtimalı mövcuddur. VA-lar müxtəlif üsullar ilə maliyyələşmənin əldə eidlməsində terrorçulara yardım edə bilər. Ekstremist qruplaşmanın tərəfdarları özlərinin şəxsi VA-larını bağışlaya və ya vasitəçi brokerlər köməyilə pul vəsaitlərinin köçürülməsi üçün VA-lardan istifadə edə bilərlər. Vəsaitlər terror təşkilatı tərəfindən təcavüzkarın maliyyələşdirməsinin əlverişli bir üsulu olan “kraudfandinq” (crowdfunding - adətən internet vasitəsi ilə çox sayda insandan az miqdarda olmaqla pul vəsaitləri toplayaraq bir layihə və ya müəssisənin maliyyələşdirilməsi təcrübəsidir) yolu ilə də toplana bilərdi.

VA-ların cinayətkarlar üçün əlçatanlığı üzrə risk faktoruna daxil olan *vəsaitlərin köçürülməsi* adlı risk elementi xüsusilə bəzi VA növləri üçün xas olan riskdir. Bəzi VA növləri daha yüksək məxfilik dərəcəsi təklif edir və köçürməni daha rahat edir. Buna baxmayaraq, o, xüsusən də əməliyyatların etibarlı şəkildə və anonimliyi pozmadan həyata keçirildiyi təqdirdə, hələ də əhəmiyyətli texnoloji inkişaf səviyyəsi tələb edir. Terrorçu qrupların fəaliyyət göstərdiyi zəif inkişaf etmiş bölgələrə bu üsulla mümkün pul köçürməsi çətin məsələ olsa da, yüksək təhdid olaraq qəbul edilir.

VA-ların cinayətkarlar üçün əlçatanlığı üzrə risk faktoruna daxil olan *qaranlıq internetə (şəbəkə bazarına) çıxış (“Dark Web”, “Dark Market” access)* adlı risk elementi qanunsuz mallara cinayətkarların çıxışının asanlaşması ilə bağlıdır. Özü-özlüyündə qaranlıq bazarlar (“Dark Market”) mütləq olaraq qanunsuz deyildir. Bu adətən, VA-nın əsasında yerləşən eyni növ texnologiyadan istifafdə etməklə yaradılmış rəqəmsal ticarət meydançalarıdır. Cinayətkarlar yarı anonim xüsusiyyətlərinə görə ticarət üsulu kimi bu vasitəni seçirlər. Qaranlıq bazarların bir çoxu satılmasına icazə verilmiş məhsul növləri üzündən tez bir zamanda qanunsuz bazarlara çevrilirlər. Araşdırmalar HMO tərəfindən yoxlamaların çətinliyi üzündən qaranlıq bazar fəaliyyətlərinin həcminin artdığını göstərir.

VA-ların cinayətkarlar üçün əlçatanlığı üzrə risk faktoruna daxil olan *vəsaitlərin xərclənməsi* adlı risk elementi VA ekosisteminin bir hissəsi kimi çirkli pulların yeni texnologiyalara cinayət motivi ilə tətbiqini nəzərdə tutur. Bir çox iştirakçıların hökumətə və mərkəzi hakimiyyət orqanlarına arxalanmadan maliyyə həlləri sahəsində radikal innovasiyalar və sahibkarlığın təmin edilməsi məqsədilə VA bazarının imkanlarını öyrəndiyini nəzərə alaraq, bu vəsaitlər cinayətkarları çirkli pulların inteqrasiyası işinə qoşulmağa təşviq edə bilər.

VA-ların maliyyələşmə mənbələri üzrə riskin qiymətləndirilməsində istifadə olunan əsas risk elementlərinə kart (yaxud bank), nağd köçürmələr və natural ifadədə qiymətli mallar, virtual valyutalardan istifadə imkanları üzrə göstəricilər daxil edilir.

VA-ların maliyyələşmə mənbələri üzrə risk faktoruna daxil olan *kart (yaxud bank)* adlı risk elementi qanunsuz fəaliyyət, yaxud, məsələn, cinayətkarlar üçün daha cəlbedici

ola bilən PL/TMM nəzarətinin zəif olduğu platformalardan əldə olunan vəsaitlər ilə bağlı ola bilər. Ayrıca bir VA cüzdanı böyük məbləğdə pul vəsaitlərinin çıxarılması üçün istifadə olunan bir neçə bank/kredit kartlarına bağlı ola bilər. VA cüzdanlarında adi depozitlərə nəzərən daha yüksək olan depozitlər də verilmiş əməliyyatdan dərhal sonra fiat valyuta şəklində məxaric olunur. Vəsaitlərin mənbəyi yüksək riskli yurisdiksiyalarda olan bank hesabları və ya oğurlanmış kart ola bilər.

VA-ların maliyyələşmə mənbələri üzrə risk faktoruna daxil olan *nağd köçürmələr və natural ifadədə qiymətli mallar* adlı risk elementi VA-ların "birjadan kənar" ("OTC" – "Over the Counter") brokerlər vasitəsilə əldə edilməsi ilə bağlıdır. Cinayətkarlar yeni növ PL-in əsası kimi çıxış edən "birjadan kənar" ("OTC") brokerlər vasitəsilə VA-ları əldə etməkdən ötrü oğurlanmış natural formada olan qiymətli mallar yolu ilə (yaxud qəsb olunmuş proqramlardan v-köçürmə yolu ilə) VA-lara müraciət edə bilərlər. Birjadan kənar brokerlər ("OTC" brokerlər) adətən, onların fəaliyyət göstərdiyi birjalar ilə müqayisədə daha aşağı öz müştərini tanı ("KYC") tələblərinə malikdir. Onlardan bir çoxu bu boşluqdan istifadə edir və cinayətkarlara vəsaitlərini yumaq və nağdlaşdırmaqda yardım edirlər. Belə yuma ehtimal ki, fiat pullara nağdlaşdırmadan əvvəl ilk olaraq bitkoyn və digər kriptovalyutaların stabil vasitəçi valyuta kimi Tether-ə mübadiləsi yolu ilə həyata keçirilir.

VA-ların maliyyələşmə mənbələri üzrə risk faktoruna daxil olan *virtual valyutalardan istifadə* adlı risk elementi cinayət fəaliyyətləri ilə bağlı ola bilər. VA-lar cinayət fəaliyyətinin əsasən 4 əsas istiqamətinə məruz qalırlar: vergi ödəməkdən yayınma, pulların yuyulması, qaçaqmalçılıq və qəsb etmə (o cümlədən VA-nın özünün oğurlanması da daxil olmaqla).

Məsələn, altcoin-lər kimi bəzi VA-lar "sıfır açıqlamaya malik sübut texnologiyası"nı ("A zero-knowledge proof") təmin edir. Belə ki, bu texnologiya (və ya protokol) PL-ə qarşı mübarizə, yəni əməliyyatı izləmək imkanlarına aid işlərdə blokçeyn reyestrindən (blockchain's ledger) istənilən eyniləşdirmə məlumatını (göndərən və alan tərəf, əməliyyatın məbləği) silməklə faktiki olaraq blokçeyn texnologiyasının ən mühüm funksiyalarından birini aradan qaldırır. "Sıfır açıqlamaya malik sübut texnologiyası" - məlum informasiyanı birbaşa açıqlamadan nəyinsə məlum olmasının sübutu üçün kriptoqrafiyada istifadə olunan metoddur. Mahiyyətcə, bu, mübadilə zamanı şəxsi məlumatların məxfi saxlanılmasına imkan verir. Müvafiq protokol ("A zero-knowledge proof") sirri heç kəsə açmadan belə sizin sirri bildiyinizi sübut etməyə imkan verən dolayı sübutlardır. Siz yalnız düz danışdığınızı sübut edirsiniz. Digər bir misal olaraq, müştərinin sərvətinin mənbəyinin əsas hissəsini VA-lara, "ICO"-lara, eləcə də dələduzluq məqsədli "ICO"-lara olan investisiyalar təşkil edə bilər. Yaxud müştərinin maliyyələşmə mənbəyini qeyri-mütənasib olaraq böyük dərəcədə PL/TMM nəzarəti üzrə vasitələrə malik olmayan və ya qeydiyyatdan keçməmiş digər VAXT-lardan əldə olunmuş VA-lar ola bilər.

VA-ların əməliyyat xüsusiyyətləri üzrə riskin qiymətləndirilməsində istifadə olunan əsas risk elementlərinə tənzimlənən VA-lar, tənzimlənməyən VA-lar, mərkəzləşmiş mühit və mərkəzləşməmiş mühitlər adlı göstəricilər aid olunur.

VA-ların əməliyyat xüsusiyyətləri üzrə risk faktoruna daxil olan *tənzimlənən VA-lar* adlı risk elementi VA-ların xüsusi tənzimləməyə məruz qalıb-qalmaması ilə bağlıdır. Tənzimləmələrin yumşaldıcı amil olmasına baxmayaraq, VA ekosisteminin yeniliyi tənzimləmələrin (normativ tələblərin) effektivliyi və təsirliliyinə kölgə salır.

VA-ların əməliyyat xüsusiyyətləri üzrə risk faktoruna daxil olan *tənzimlənməyən VA-lar* adlı risk elementi əvvəlki risk elementi ilə eynidir, lakin bu element VA-lara tənzimlənməmə nəzərindən baxır. Bu istiqamət ənənəvi maliyyə sektorunda olan eyni tənzimləyici qorumanın (normativ mühafizənin) olmadığı VA sektorudur. Sektoru tənzimləmək üçün hər hansı tənzimləyici təşviq olmasa, bu sektor əvvəlki kimi cinayətkarların hücumuna və sui-istifadəsinə qarşı zəif olacaqdır.

VA-ların əməliyyat xüsusiyyətləri üzrə risk faktoruna daxil olan *mərkəzləşmiş mühit* adlı risk elementi əməliyyatların ənənəvi maliyyə sisteminə qoşulmuş birjada və ya digər qovşaqda qeydə alındığı qapalı mühitdir.

VA-ların əməliyyat xüsusiyyətləri üzrə risk faktoruna daxil olan *mərkəzləşməmiş mühit* adlı risk elementi mərkəzləşməmiş maliyyə ("DeFi") ilə bağlıdır. Mərkəzləşməmiş maliyyə ("DeFi") - mərkəzləşməmiş kompüter şəbəkələri vasitəsilə əməliyyatlarda vasitəçilərin sayını azaltmağı və ya aradan qaldırmağı hədəfləyən maliyyə xidmətləri ekosistemidir. Sistem banklar kimi vasitəçilər olmadan işləyir və smart müqavilələr vasitəsilə idarə olunur. VA ekosisteminin çoxsaylı iştirakçıları ilə (məsələn, maynerlər, birjalar, cüzdan proyavderləri, ödəniş prosessorları, "ATM" provayderlər və s.) VA şəbəkələrində məhz kimin hesabatlılıq öhdəliyinə malik olması (məsul olması) heç də həmişə aydın deyil. Hüquq mühafizə orqanları istintaq və ya aktivlərin ələ keçirilməsi (müsadirəsi) məqsədi ilə bir mərkəzi yeri və ya təşkilatı hədəf ala bilməz.

Cinayətkarlığın asanlığı üzrə riskin qiymətləndirilməsində istifadə olunan əsas risk elementlərinə vergi ödəməkdən yayınma, TM, cinayət yolu ilə əldə olunan gəlirlərin tənzimlənməyən VA-lar ilə gizlədilməsi, izləmə və ələ keçirmənin çətinliyi, valyuta nəzarətindən yan keçmə ("Circumvent Exchange Control") göstəriciləri daxil edilir.

VA-ların cinayətkarlığın asanlığı üzrə risk faktoruna daxil olan *vergi ödəməkdən yayınma* adlı risk elementi. FATF, VA-ları PL/TM, xüsusilə də vergi ödəməkdən yayınma və fırıldaqçılıq cinayətləri üçün yeni əsas risklərdən biri olaraq vurğulayır. Tənzimlənən sektor xaricində fəaliyyət göstərmək üçün yaradılmış hər hansı bir VA-nın vergidən yayınanları cəlb etməsi təəccüblü deyildir. Qeyri-formal sektorda fəaliyyətin miqyası və məlumat mübadiləsi ilə əlaqəli məhdudiyyətlər səbəbindən bir çox ölkələrdə VA-lar üzrə vergi ödəməkdən yayınmanın qarşısını almaq çətin olacaqdır. Qiymətləndirmə sistemi və hüquq sistemi vasitəsi ilə fəaliyyət göstərəcək qlobal vergi harmonizasiyasının və vergi problemlərinin olmaması nəzərə alınmaqla, VA-ların istifadə xarakterindən asılı olaraq ölkələr arasında və hətta eyni ölkə daxilində fərqli vergi rejimləri mövcuddur.

VA-ların cinayətkarlığın asanlığı üzrə risk faktoruna daxil olan *terrorçuluğun maliyyələşdirilməsi (TM)* adlı risk elementi. Terrorçu şəbəkələr rəqəmsal dünyada, o cümlədən VA-lar vasitəsilə mürəkkəb maliyyə əməliyyatları həyata keçirməklə texnologiyalara uyğunlaşmışlar. Yeni texnologiyaların imkanları törətdiyi cinayətlərə görə bədniyyətli şəxsləri məsuliyyətə cəlb etmək məsələsində HMO-ın işini çətinləşdirir.

VA-ların cinayətkarlığın asanlığı üzrə risk faktoruna daxil olan *cinayət yolu ilə əldə olunan gəlirlərin tənzimlənməyən VA-lar ilə gizlədilməsi* adlı risk elementi. Bu üsulla pullar, ənənəvi bank hesablarından fiat valyutanı qəbul edən rəqəmsal valyuta birjalarında onlayn hesablar vasitəsilə VA-lar üzərindən yuyulur. Sonra onlar "təmizləmə" prosesini (qarışdırma və təbəqələrə ayırma) işə salırlar, yəni mikserlər, tumblerlər (tumblers) və zəncir keçirmələrinin (həmçinin kross-valyuta da adlanır) köməyilə pulları kriptovalyuta sisteminə keçirməyə başlayırlar.

VA-ların cinayətkarlığın asanlığı üzrə risk faktoruna daxil olan *izləmə və ələ keçirmənin çətinliyi* adlı risk elementi. Köçürülə bilmə qabiliyyətinin asanlığı və onun izlənilə bilən təbiəti VA-nın ələ keçirilməsini (müsadirəsini) çətinləşdirir. Belə çətinlik xüsusilə də bütün dünya üzrə HMO, maliyyə təsisatları və tənzimləyici orqanlar arasında məlumat və təcrübə mübadiləsi məqsədilə sıx əməkdaşlığın zəruri olduğu fəaliyyətlərdə müşahidə olunur.

VA-ların cinayətkarlığın asanlığı üzrə risk faktoruna daxil olan *valyuta nəzarətindən yan keçmə* adlı risk elementi. Valyuta nəzarətinin qanunvericilik ilə tənzimləndiyi ölkələrdə VA-lar valyuta nəzarəti qaydalarından yan keçmə (yayınma) vasitəsi ola bilər. Transsərhəd köçürmələrində VA-lardan istifadə olunduğu hallarda ənənəvi ödəniş

sistemləri tərəfindən müşahidə oluna və qeydə alına bilinməməsi səbəbindən valyuta nəzarətinin tətbiqi və kapital axınlarının idarə olunması çətin olur.

İqtisadi təsir üzrə riskin qiymətləndirilməsində istifadə olunan əsas risk elementlərinə kölgə iqtisadiyyatı – ölkənin monetar siyasətinə təsiri, maliyyə xidmətləri bazarı ilə tam inteqrasiya imkanı, maliyyə institutları ilə virtual valyuta bazarı arasında hər hansı əlaqənin qadağan olunması, məhsul təchizatçılarının yüksək məsuliyyətlilik səviyyəsi üzrə göstəricilər aid olunur.

İqtisadi təsir üzrə risk faktoruna daxil olan *kölgə iqtisadiyyatı – ölkənin monetar siyasətinə təsiri adlı risk elementi.* VA-ların baza texnologiyasının ("DLT") və mərkəzləşməmiş VA-ların həssas və aşağı gəlirli əhali qruplarının ədalətli, davamlı və şəffaf şəkildə maliyyə xidmətlərinə əlçatanlığı (maliyyə inklüzivliyi) baxımından faydaları təmin etsə də, ölkələr VA-ların həddindən artıq istifadəsinin iqtisadiyyata və pul təklifinə təsirlərini nəzərə almalıdır. Tənzimlənən sektor xaricində VA-ların həddən artıq istifadəsi ölkənin iqtisadi nəticələrinə təsir edə bilər. Bu, VA-ların hazırda stabil monetar (pul-kredit) rejimlər və monetar stabilliyin üç əsas riskindən (struktur deflyasiya riski, pula tələbin müvəqqəti şoklarına cavab verməyə və bu yolla işgüzar tsikli hamarlaşdırmağa imkan verən çeviklik və son instansiya kreditoru kimi fəaliyyət göstərmək qabiliyyəti) qorumaq kimi çox mühüm funksiyalara malik olmaması səbəbindən baş verə bilər.

İqtisadi təsir üzrə risk faktoruna daxil olan *maliyyə xidmətləri bazarı ilə tam inteqrasiya imkanı adlı risk elementi.* Bütün dünyada mövcud maliyyə qurumları VA artımını izləyir və VA əsaslı texnologiyalara əhəmiyyətli həcmdə sərmayə qoyur, lakin buna baxmayaraq, ödəniş üsulu kimi VA-ların istifadəsində fəal iştirakın səviyyəsi aşağı olaraq qalır.

İqtisadi təsir üzrə risk faktoruna daxil olan *maliyyə institutları ilə virtual valyuta bazarı arasında hər hansı əlaqənin qadağan olunması adlı risk elementi.* VA-ların mərkəzləşməmə xarakterinə malik olması onları mövcud tənzimləyici (normativ) çərçivələrə və strukturlara asanlıqla uyğun gəlməsinə imkan vermir. VA-ların sərhədsiz xarakterdə olması və alətin müəyyən edilə bilən (eyniləşdirilə bilinən) "emitentinin" olmaması tənzimləyici orqanlar üçün çətinliklər yaradır.

İqtisadi təsir üzrə risk faktoruna daxil olan *məhsul təchizatçılarının yüksək məsuliyyətlilik səviyyəsi adlı risk elementi.* VA, hesabatlılığı təmin edən və sistemin qanuniliyini qoruyan bir sosial institutun yaradılmasına imkan verən idarəetmə strukturu tələb edir.

Qeyd olunanlardan əlavə, digər bir risk faktoru kimi "Təqdim olunan mal və xidmətlər, eləcə də VA növləri üzrə riskin qiymətləndirilməsində istifadə olunan əsas risk elementlərinə ölkədə, yaxud xaricdə lisenziya alması, biznesin təbiəti, ölçüsü və mürəkkəbliyi, məhsullar/xidmətlər, müştəri növləri, ölkə riski, VAXT fəaliyyəti göstərən institutlar, VA-lar (anonimlik), sürətli əməliyyat hesablaşmaları, xaricdə qeydiyyata alınmamış VAXT-lar ilə işləmə kimi göstəricilər daxil edilir.

Müvafiq risklər hər hansı nəzarət və risklərin azaldılması tədbirlərinin tətbiqindən əvvəl mövcud olan rsiklərdir.

VA-lar ilə əlaqəli PL/TM risklərinin qiymətləndirilməsi göstərir ki, mütəşəkkil cinayətkar birliklər VA-dan "təmiz pullara" çıxış əldə etmək üçün istifadə edə bilərlər. Cinayət fəaliyyətindən əldə olunan gəlirlərin daşınması və yuyulması məqsədilə kibercinayətkarlar, narkotik ticarətçiləri və digər mütəşəkil cinayətkar dəstələr getdikcə VA-dan daha çox istifadə etməyə başlayıblar. VA-lar (o cümlədən virtual valyutalar) belə qrupların nağd pullara anonim çıxış əldə etmələrinə və əməliyyatların izinin itirilməsinə imkan verir. Cinayətkarlar elektron cüzdanlar üçün qapalı açarları əldə edə və ya bankomatlardan nağd pul çıxara bilərlər. VA-ların doğurduğu risklərin qiymətləndirilməsi zamanı ölkələrin VA-ların təbiətini (xarakterini) nəzərə alması zəruridir.

VA-ların öz yurisdiksiyalarında istifadə xarakterinə xüsusi diqqət yetirilməlidir. Konfidensiallığın qorunmasının qanunsuz əməliyyatlara ekvivalent olmamasına baxmayaraq, məhz bu cəhət cinayətkarlarda daha çox rezonans doğurur. Məsələn, "Monero" kimi VA-lar ardıcıl əməliyyatların izlənilməsini çətinləşdirmək üçün gizli reyestr texnologiyasından ("obfuscated ledger technology") və "üzük imzalarından" ("ring signatures") istifadə edir. VA-ların belə növü qanunsuz fəaliyyətə yardım edə və PL/TM məqsədləri üçün istifadə üçün böyük risk doğura bilər.

Verilmiş ölkədə yuxarıda qeyd edilən risklərin azaldılması (yaxud yumşaldılması) üzrə həyata keçirilməsi gözlənilən tədbirləri aşağıdakı istiqamətlər üzrə təsnifləşdirmək olar:

Tədbirlərin istiqaməti	Tədbirlər	Tədbirlərin təsviri
Hökumət tədbirləri	PL/TMM üzrə hüquqi çərçivənin tamlığı (hərtərəfliliyi)	Ölkədə VA-lar və VAXT sektoru ilə əlaqəli PL/TMM üzrə preventiv tədbirlərə aid adekvat qanun və qaydaların (normativ-hüquqi bazanın) olub-olmamasını göstərir
	Giriş nəzarətinin mövcudluğu və effektivliyi	Bazara giriş üzrə nəzarət vasitələrinin mövcudluğunu və effektivliyini (lisenziyalaaşdırma, qeydiyyat və iş icazəsinin digər formaları da daxil olmaqla) qiymətləndirir. Səlahiyyətli orqanlara öz öhdəliklərini yerinə yetirmələri üçün müvafiq səlahiyyətlər, kifayət qədər sayda təlim keçmiş heyət və digər resurslar verən hərtərəfli normativ-hüquqi bazanın (hüquqi və tənzimləyici çərçivənin) olduğu təqdirdə, ölkədə effektiv giriş nəzarəti mövcudd olur. Effektiv giriş nəzarətinin olması PL və TM zəifliklərini azaldır və PL/TMM tələblərinə yüksək uyğunluğu təmin edir.
	Adekvat nəzarət və monitorinq mexanizmi	VAXT sektoru üçün adekvat nəzarət və monitorinq mexanizminin olmasını, eləcə də PL-ə qarşı mübarizə üzrə nəzarət/monitorinq prosedurlarının və praktikasının effektivliyini qiymətləndirir. Effektiv nəzarət/monitorinq rejimi: (1) müvafiq səlahiyyətlər və resurslar ilə təmin edilmiş hərtərəfli hüquqi və tənzimləmə çəçivəsinə malikdir və (2) on-site/off-side monitorinq və yoxlamalar üçün risk əsaslı yanaşmadaan istifadə edir.
	Müştərilərin eyniləşdirilməsi və vəsaitlərin mənbəyi üzrə tənzimləmə, etibarlı eyniləşdirmə infrastrukturunun mövcudluğu	VAXT-lar, maliyyə institutları və DNFBP-lərdən etibarlı, müstəqil mənbə sənədləri, məlumatları və ya informasiyasından istifadə etməklə müştərilərinin şəxsiyyətini yoxlama tələbinin olduğu halda, maliyyə şəffaflığı, eləcə də müştərilərin eyniləşdirilməsi və verifikasiyası prosesləri təkmil hesab olunur
	HMO-ların virtual aktivlərin istintaqı və izlənməsi üçün maliyyə və insan resursları potensialı	HMO-ların virtual aktivlərin istintaqı, izlənməsi, müsadirəsi və qorunması üzrə səlahiyyətlərini və imkanlarını qiymətləndirir. Bu sahədə effektiv mexanizm – (1) HMO-lara müvafiq səlahiyyətləri təmin edən hərtərəfli hüquqi/tənzimləyici

		çərçivəyə (normativ hüquqi bazanın) və ya onun ekvivalentinə malik olan və (2) öz funksiyalarını yerinə yetirmək üçün yaxşı resurslara və zəruri texnoloji alət və imkanlara malik olan mexanizmdir
	Beynəlxalq əməkdaşlığın effektivliyi	Kriptovalyuta ilə əlaqəli bir çox halların transmilli xarakterdə olmasını nəzərə alaraq, müvafiq göstərici VA və VAXT-lara münasibətdə verilmiş ölkənin səlahaiyyətli orqanları tərəfindən qəbul edilmiş (o cümlədən təqdim olunmuş) beynəlxalq əməkdaşlığın dərəcəsini və effektivliyini qiymətləndirir
	Daxili əməkdaşlığın effektivliyi	Vəsaitlərin hərəkətinin yüksək sürətini təmin etməyə imkan verən kriptovalyuta hallarının rəqəmsal xarakterini nəzərə alaraq, VA sektorunda PL/TMM siyasətlərinə münasibətdə milli əməkdaşlıq və koordinasiyanın dərəcəsi əhəmiyyətli məsələdir
	VAXT-lar üçün rəhbər sənədin və VAXT-lar ilə əlaqənin keyfiyyəti	VAXT sektoru ilə hökumətin qarşılıqlı əlaqəsinin səviyyəsini və onun səmərəliliyini qiymətləndirir
VAXT-lar üzrə tədbirlər	VAXT-ların səhmdarlar strukturunun şəffaflığı	VAXT-ların səhmdar, mülkiyyət və nəzarət strukturunun şəffaflıq səviyyəsini qiymətləndirir
	İdarəetmə strukturunun keyfiyyəti və VAXT-ların hesabatlılıq səviyyəsi	VAXT-ların idarəetmə strukturunu, VAXT və onun əməkdaşlarının hesabatlılıq səviyyəsini qiymətləndirir
	Komplayens funksiyasının və daxili nəzarət mexanizminin effektivliyi	PL/TM risklərinin aşağı salınması üçün VAXT-ların effektiv daxili nəzarət mexanizminin və komplayens (uyğunluq) funksiyasının olub-olmamasını qiymətləndirir. Effektiv kompayens funksiyası – (i) daxili nəzarət mexanizmi vasitəsilə riskləri başa düşməyə, preventiv və cavab tədbdirlərini həyata keçirməyə imkan verən, (ii) PL/TMM qanunvericiliyinə riayət edilməsini təmin edən yaxşı resurslara, adekvat vərdişlərə, texnoloji və digər resurslara malik olan funksiyadır
	VAXT heyətinin PL/TMM bilikləri	VAXT əməkdaşlarının PL/TMM üzrə vəzifə və öhdəliklərini nə dərəcədə yaxşı bilməsi və başa düşməsini qiymətləndirir
Maliyyə institutları və DNFBP-lər (ənənəvi öhdəliyə malik təsisatlar) üzrə tədbirlər	Maliyyə institutları və DNFBP-lər tərəfindən risk qiymətləndirməsi və risklərin azaldılması üzrə görülmüş tədbirlər	Ənənəvi öhdəliyə malik təsisatların VA-lar və yeni texnologiyaları özündə birləşdirən yeni və mövcud xidmətlər, məhsullar və tədarük mexanizmlərinə aid PL/TM risklərinin aşkar edilməsi və idarə olunması üzrə effektiv və adekvat tədbirlərdən istifadə edib-etməməsini qiymətləndirir
	Komplayens funksiyasının və daxili	Ənənəvi öhdəliyə malik təsisatların VAXT-lar və VA-lar ilə əlaqəli PL/TM risklərinin azaladılması üçün effektiv daxili nəzarət mexanizminə və

	nəzarət mexanizminin effektivliyi	komplayens (uyğunluq) funksiyasına malik olub-olmamasını, eləcə də belə funksiyasnın effektivlik səviyyəsini qiymətləndirir

Bölmə

On

10

TÖVSİYƏLƏR

VAXT-ların fəaliyyətinin PL/TMM baxımından tənzimlənməsi və effektiv monitorinq sisteminə cəlb olması üzrə tövsiyələr

Beynəlxalq təcrübə əsasında VA sektorunun inkişaf etdirilməsi, eləcə də VAXT-ların fəaliyyətinin tənzimlənməsi və PL/TMM üzrə effektiv monitorinq sisteminə cəlb olunması məqsədilə aşağıdakı ilkin tədbirlərin həyata keçirilməsi məqsədəuyğun hesab olunur:

- Rəqəmsal transformasiyanın tələblərindən irəli gələrək və VA sektorunun bir sıra fəaliyyət sahələrinin məcmusunu əhatə etdiyini nəzərə alaraq, VA sektorunun fəaliyyət mexanizmi, onun iştirakçıları, müvafiq sahədə ölkələrin beynəlxaq təcrübəsinin öyrənilməsi, bu sektorun doğurduğu risklər və onların qarşısının alınması, müvafiq sahədə əməkdaşlığın və koordinasiyanın təmin olunması, eləcə də VA-ların idarə olunması üzrə hüquqi/tənzimləyici çərçivənin inkişaf etdirilməsi məqsədilə milli səviyyədə işçi qrup, komissiya və ya hər hansı uyğun formatda *yüksək səviyyəli qrupun yaradılması*;

- Komissiya və ya qrup tərəfindən VA sektorunun inkişafı və tənzimlənməsi üzrə *proqramın hazırlanması*;

- Blokçeyn texnologiyasından mümkün istifadə də daxil olmaqla, təşkilati səviyyədə rəqəmsal dəyişikliklərin geniş şəkildə başa düşülməsinin təmin edilməsi üçün *rəqəmsal inkişaf prinsiplərinin və ya strategiyasının təsdiq olunması*;

- VA sektorunun fəaliyyəti üçün ölkə üzrə kompleks *rəqəmsal infrastruktur sisteminin* inkişafının təmin edilməsi üzrə *tədbirlərin planlaşdırılması və həyata keçirilməsi*;

- VA sektoru ilə əlaqəli anlayışların ətraflı araşdırılması, müvafiq sektor üzrə fəaliyyət mexanizmi, tənzimləmə imkanları, vergiyə cəlb olunma, VA-ların uçotu, VA sahiblərinin hüquq və vəzifələrinin müəyyən olunması, VA-lara sahibliyin ötürülməsi, VA sektorunun iştirakçılarının öhdəliklərinə dair tələblər, VAXT ekosisteminin hansı əsaslar üzrə qurulması, VAXT-ların lisenziyalaşdırılması və qeydiyyatı, VA sektorunun fəaliyyəti üçün zəruri olan texniki protokollar, VAXT-lara adekvat tənzimləmə və nəzarətin təmin edilməsi, VAXT-ların PL/TMM rejiminin subyektləri olaraq cəlb edilməsi, müvafiq sahədə preventiv tədbirlər, məlumat mübadiləsi sahəsində ölkədaxili və beynəlxalq əməkdaşlıq və digər zəruri məsələlər üzrə praktiki nümunələrin öyrənilməsi, beynəlxalq standartların tələbləri də nəzərə alınmaqla *qanunverici əsasların yaradılması*;

- VA sektorunda *lisenziyasız fəaliyyət* göstərən fiziki və hüquqi şəxslərin *siyahısının müəyyən edilməsi*. Zəruri lisenziya olmadan və ya qeydiyyatdan keçmədən VAXT fəaliyyətini həyata keçirən fiziki və ya hüquqi şəxslərin müəyyənləşdirilməsi və uyğun *sanksiyaların tətbiq edilməsi qaydalarının (mexanizmin) müəyyən olunması*;

- VA sektorunu *tənzimləyən*, eləcə də VAXT-ları lisenziyalaşdıran və onların fəaliyyətinə *nəzarət edən* və *monitorinqini həyata keçirəcək məsul qurumların müəyyən edilməsi*;

- VAXT-ların *lisenziyalaşdırılması mexanizminin müəyyən olunması*;

- VA ekosisteminin çoxsaylı iştirakçılarının (məsələn, maynerlər, birjalar, cüzdan proyavderləri, ödəniş prosessorları, ATM provayderlər və s.) *hesabatlılıq öhdəliklərinin müəyyən edilməsi*;

- Cinayətkarların qanunsuz maliyyələşməsi risklərini aradan qaldırmaq məqsədilə VA-ların Birjadan kənar brokerlər ("OTC" brokerlər, xüsusilə də xarici yurisdiksiyada qeydiyyatdan keçmiş) vasitəsilə əldə edilməsinə *nəzarət mexanizminin müəyyən edilməsi*;

- Ölkədə VA-ların, VAXT iştirakçılarının təsnifatlaşdırılması və beynəlxalq təcrübə əsasında milli hesablar sistemində kriptoaktivlərin (tokenlərin) və VAXT-ların *uçotunun aparılması qaydalarının müəyyən edilməsi* (o cümlədən, VA-ların funksionallıq, stabilləşdirmə mexanizmi və sistem əhəmiyyətliliyi meyarları üzrə təsnifləşdirilməsinin aparılması);

- *VA sektoruna risk əsaslı yanaşmanın tətbiq edilməsi*: VAXT-ların fəaliyyətindən (təklif etdiyi xidmətlərin xarakterindən) irəli gələn PL/TM risklərinin müəyyən edilməsi, qiymətləndirilməsi və başa düşülməsi sisteminin tətbiqi;

- *Anonimilik* imkanları xüsusilə yüksək olan sistem əhəmiyyətli kriptovalyutalara münasibətdə *xüsusi tədbirlərin tətbiqinə dair qaydaların müəyyən edilməsi*;

- VA sektorunun *fəaliyyətinin tənzimlənməsi qaydalarının* (müştərilərin, o cümlədən qarşı tərəfin eyniləşdirilməsi, benefisiar mülkiyyəçinin, PEP-lərin müəyyən olunması, daxili nəzarət qaydaları, köçürmə qaydaları, şübhəli əməliyyatlar üzrə hesabatlılıq sisteminin tətbiqi qaydaları) müəyyən olunması;

- FATF-ın 15-ci tövsiyəsi tərəfindən irəli sürülmüş *"köçürmə qaydası"nın* ("travel rule") implementasiyasını təmin etməyə imkan verən *texnoloji həllərin hazırlanması*;

- "ICO", "IEO" və "STO"ların fəaliyyətini tənzimləyən *qaydaların müəyyən olunması*;

- Predikativ cinayət nəticəsində yaranmış VA-ların blokçeyndə qeydə alınmış əməliyyatlar üzrə izlənilməsini, axınların şifrəsinin açılmasını, VA-ların qanunsuz mayninqinin və anonimliyin ifşa edilməsini ("DLT" texnologiya), "Dark web" üzrə təhlili təmin edən *IT infrastrukturun yaradılması*, eləcə də unikal IP ünvanlar, əməliyyatın tarixi və geolokasiya kimi bir sıra atributları müəyyən edə bilən *proqram təminatlarının müəyyən edilməsi və zəruri qurumların istifadəsinə*

verilməsi (o cümlədən, PL/TM-ə qarşı mübarizə məqsədləri üçün şübhəli əməliyyatların izlənilməsi və aşkar edilməsinə, eləcə də istintaq aparılması və ya aktivlərin üzərinə həbs qoyulmasına imkan verən proqram təminatlarının müəyyən olunması və zəruri qurumların təchiz olunması);

- Mərkəzləşmiş VA sisteminin iştirakçılarının fəaliyyətini tənzimləyən *qayda və mexanizmlərin müəyyən edilməsi*; o cümlədən, mərkəzləşmiş VA sistemində blokçeyn texnologiyası vasitəsilə yeni *aktivlərin emissiya edilməsi mexanizmi və qaydalarının müəyyən olunması*;

- Əksmərkəzləşmiş sistemlərdə VA sektoru iştirakçılarının fəaliyyətindən irəli gələn *anonimlik* məsələlərinin (anonim maliyyələşmə, üçüncü şəxslər tərəfindən maliyyələşmə və s.) tənzimlənməsi üzrə *prosedur qaydaların və ya mexanizmlərin müəyyən edilməsi*;

- "Sıfır açıqlamaya malik sübut texnologiyası"nı ("A zero-knowledge proof") təmin edən VA-lar üzrə əməliyyatları izləmək məqsədilə blokçeyn reyestrində *eyniləşdirmə məlumatlarının saxlanılmasına dair tələblərin müəyyən edilmə imkanlarının araşdırılması*;

- VA sahəsində *PL/TM əlamətlərinin (indikatorlarının) müəyyən olunması;*

- VA-lar üzrə *vergi rejimlərinin, vergitutma mexanizmlərinin müəyyən edilməsi və tətbiqi üzrə tədbirlərin həyata keçirilməsi*;

- VA-ların *emitentinin eyniləşdirilməsi məsələlərinin müəyyən olunması*;

- Eyni VA-ların müxtəlif yurisdiksiyalarda istifadə xarakterinin (xüsusilə konfidensiallıq imkanları baxımından) *öyrənilməsi və mümkün tənzimləmə mexanizminin müəyyən edilməsi*;

- VA sektorunun fəaliyyətinə *nəzarət edən və monitorinqini həyata keçirən müxtəlif qurumların* müvafiq sahədə *potensiallarının artırılması* məqsədilə onların aidiyyəti əməkdaşlarının müvafiq peşəkar təlimlərdə və beynəlxalq təcrübə mübadiləsində davamlı iştirakının, eləcə də bu subyektlərdə *texniki infrastrukturun qurulmasının təmin edilməsi*;

- Monitorinq subyektlərinin VA-lar barədə *məlumatlılığının artırılması* üzrə tədbirlərin görülməsi;

- PL/TMM üzrə *milli risklərin qiymətləndirilməsində* VAXT-ların fəaliyyəti və ya əməliyyatları nəticəsində meydana çıxmış PL/TM risklərinin aşkar edilməsi, qiymətləndirilməsi və başa düşülməsi məsələlərinin *nəzərə alınması;*

- *Blokçeyn texnologiyasının tətbiqinin* potensial imkanlarının öyrənilməsi və s.

İstifadə olunmuş ədəbiyyat siyahısı

1. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html
2. https://www.ramonmillan.com/documentos/bibliografia/BlockchainForDummies_Wiley.pdf
3. http://flibusta.site/b/514022/read
4. https://hub.forklog.com/fatf-nastupaet-chto-nuzhno-znat-o-novyh-rekomendatsiyah-po-virtualnym-aktivam/
5. https://forklog.com/chto-takoe-”bitcoin”/
6. https://www.iso.org/ru/news/isofocus_142-5.html
7. https://www.investopedia.com/terms/b/blockchain.asp
8. https://dtf.ru/flood/757034-blokcheyn-dlya-chaynikov-ultimativnyy-gayd
9. https://selectel.ru/blog/about-blockchain/
10. https://www.tsu.ru/podrobnosti/chto-takoe-tekhnologiya-blokcheyn-prostymi-slovami/
11. https://fincult.info/article/blokcheyn-chto-eto-takoe-i-kak-ego-ispolzuyut-v-finansakh/
12. https://www.oracle.com/ru/blockchain/what-is-blockchain/
13. http://loveread.ec/read_book.php?id=71809&p=26
14. http://flibusta.site/b/514022/read
15. https://dtf.ru/flood/757034-blokcheyn-dlya-chaynikov-ultimativnyy-gayd
16. https://selectel.ru/blog/about-blockchain/
17. https://www.tsu.ru/podrobnosti/chto-takoe-tekhnologiya-blokcheyn-prostymi-slovami/
18. https://fincult.info/article/blokcheyn-chto-eto-takoe-i-kak-ego-ispolzuyut-v-finansakh/
19. https://www.oracle.com/ru/blockchain/what-is-blockchain/
20. https://www.researchgate.net/publication/351233808_Analysis_of_Blockchain_Technology_Architectural_Basics_Application_Examples_Future_Trends_Problems_and_Disadvantages
21. https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-tehnologii-blokcheyn-i-kriptovalyuty-v-rossii
22. https://cyberleninka.ru/article/n/tehnologiya-blokcheyn-i-ee-prakticheskoe-primenenie?gclid=EAIaIQobChMI7bi-ueGW8wIVmrWyCh2EMwaIEAAYBCAAEgInNfD_BwE
23. https://currency.com/ru/chto-takoe-blockchain-tehnologiya
24. https://mcs.mail.ru/blog/blokcheyn-dlya-bankov-otlozhennaya-revolyutsiya-ili-pereotsenennaya-tekhnologiya
25. http://wiki.rocit.ru/articles/blockchain-just-about-the-complex/
26. https://www.ibm.com/ru-ru/topics/what-is-blockchain
27. https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain)
28. https://ru.euronews.com/2018/09/07/blockchain-long-read-ru
29. https://safe-surf.ru/specialists/article/5278/658923/
30. https://alpari.com/ru/beginner/glossary/blockchain/
31. https://forklog.com/polozhitelnye-storony-blokchejn-sistem-i-problemy-meshayushhie-ih-vnedreniyu/

32. https:// forklog.com/blokchejn-i-mirovye-regulyatory-osnovnye-pretenzii-k-tehnologii/
33. https://ichi.pro/ru/ponimanie-osnov-blokcejna-cast-1-vizantijskaa-otkazoustojcivost-39991631578137
34. https://exbase.io/ru/wiki/masshtabiruemost-blokchejna
35. https://marknelson.us/posts/2007/07/23/byzantine.html
36. https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/
37. https://101blockchains.com/byzantine-fault-tolerance/
38. https://ru.0xzx.com/2020042090297.html
39. https://habr.com/en/post/560566/
40. https://ru.bitcoinethereumnews.com/technology/what-is-solana-sol-and-how-does-it-work/
41. https://ru.euronews.com/2018/09/07/blockchain-long-read-ru
42. https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/
43. https://builtin.com/blockchain
44. https://selectel.ru/blog/about-blockchain/
45. https://www.tsu.ru/podrobnosti/chto-takoe-tekhnologiya-blokcheyn-prostymi-slovami/
46. https://currency.com/ru/chto-takoe-blockchain-tehnologiya
47. https://mcs.mail.ru/blog/blokcheyn-dlya-bankov-otlozhennaya-revolyutsiya-ili-pereotsenennaya-tekhnologiya
48. https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034
49. https://www.processmaker.com/blog/blockchain-workflow-automation-why-you-should-embrace-it/
50. http://loveread.ec/read_book.php?id=71809&p=4#gl_2
51. https://4cio.ru/uploads/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B8%CC%86%D0%BD%20(%D0%B8%D1%82%D0%BE%D0%B3%D0%BE%D0%B2%D1%8B%D0%B8%CC%86).pdf
52. https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-tehnologii-blokcheyn-i-kriptovalyuty-v-rossii
53. https://dtf.ru/flood/757034-blokcheyn-dlya-chaynikov-ultimativnyy-gayd
54. http://wiki.rocit.ru/articles/blockchain-just-about-the-complex/
55. https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-tehnologii-blokcheyn-i-kriptovalyuty-v-rossii
56. https://tc26.ru/events/smi-o-nas/vavilonskaya-bashnya-pochemu-blokcheynu-nuzhen-standart.html
57. https://www.dummies.com/personal-finance/blockchain-dummies-cheat-sheet/
58. https://vk.com/doc576778753_560366337?hash=59a999d30393da95d5
59. https://kniga.biz.ua/pdf/5351-Blockchain.pdf
60. https://www.researchgate.net/publication/351233808_Analysis_of_Blockchain_Technology_Architectural_Basics_Application_Examples_Future_Trends_Problems_and_Disadvantages
61. https://litmore.ru/8705-osnovy-blokchejna-vvodnyj-kurs-dlya-nachinayushhih-v-25-nebolshih-glavah.html
62. https://openknowledge.worldbank.org/bitstream/handle/10986/30584/AUS0000158-RU.pdf
63. https://unctad.org/system/files/official-document/ecn162021d3_ru.pdf
64. https://www.it.ua/ru/knowledge-base/technology-innovation/blockchain
65. https://www.oracle.com/ru/blockchain/what-is-blockchain/

66. https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain)
67. https://www.ibm.com/ru-ru/topics/what-is-blockchain
68. https://fincult.info/article/blokcheyn-chto-eto-takoe-i-kak-ego-ispolzuyut-v-finansakh/
69. https://www.oracle.com/ru/blockchain/what-is-blockchain/
70. https://www.iso.org/ru/news/ref2540.html
71. https://cyberleninka.ru/article/n/tehnologiya-blokcheyn-i-ee-prakticheskoe-primenenie?gclid=EAIaIQobChMI7bi-ueGW8wIVmrWyCh2EMwaIEAAYBCAAEgInNfD_BwE
72. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_russian.pdf
73. https://safe-surf.ru/specialists/article/5278/658923/
74. https://alpari.com/ru/beginner/glossary/blockchain/
75. https://forklog.com/polozhitelnye-storony-blokchejn-sistem-i-problemy-meshayushhie-ih-vnedreniyu/
76. https://forklog.com/blokchejn-i-mirovye-regulyatory-osnovnye-pretenzii-k-tehnologii/
77. https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348
78. https://www.it.ua/ru/knowledge-base/technology-innovation/blockchain
79. https://www.iso.org/ru/news/ref2540.html
80. https://palmina-invest.com/analytical-research/Travel_Rule_Report_RU_2020_12.pdf
81. https://www.golosameriki.com/a/nft-explained/5846708.html
82. https://rspectr.com/articles/773/iota-alternativa-blokchejnu
83. https://ru.bitcoinethereumnews.com/technology/what-is-solana-sol-and-how-does-it-work/
84. https://www.investopedia.com/terms/b/blockchain.asp
85. https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034
86. https://www.processmaker.com/blog/blockchain-workflow-automation-why-you-should-embrace-it/
87. https://builtin.com/blockchain
88. https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/
89. https://medium.com/@chrshmmmr/so-when-should-you-consider-a-blockchain-answers-with-flow-charts-376936432ce8
90. https://www.rbc.ru/crypto/news/5bbca2929a79475a3db778e6
91. https://prostocoin.io/blog/how-exchange-works
92. https://merehead.com/ru/blog/how-get-cryptocurrency-liquidity-providers/
93. https://info.exmo.me/ru/kriptovalyuty/stejblkoin/
94. https://info.exmo.me/ru/valyuty/halving-bitcoin-chto-izmenilos-god-spustya/
95. https://tgraph.io/CHto-takoe-halving-05-04
96. https://info.exmo.me/ru/obuchenie/birzha-kriptovalyut-ili-obmennik/
97. https://www.fxmag.ru/blog=56188_chem_otlichaetsya_birzha_kriptovalyut_ot_obmennika/
98. https://www.sravni.ru/enciklopediya/info/birzha-kriptovaljuty/
99. https://www.interkassa.com/anti-money-laundering-policy/
100. https://globaldigitalfinance.medium.com/banks-are-most-likely-exposed-to-crypto-assets-unknowingly-66922508fd54
101. https://www.chainalysis.com/

102. https://www.lawfareblog.com/merchant-crypto-payments-new-national-security-frontier
103. https://www.coindesk.com/first-mover-how-a-defi-trader-made-an-89-profit-in-minutes-slinging-stablecoins
104. https://sanctionscanner.com/blog/examining-the-aml-risks-and-red-flags-of-crypto-exchanges-258
105. https://analyticsindiamag.com/top-blockchain-analytics-companies-and-what-they-do/
106. https://www.acfeinsights.com/acfe-insights/3-companies-developing-blockchain-analytics-tools
107. https://complyadvantage.com/knowledgebase/crypto-aml-red-flags/
108. https://kompanion.online/birzhi-kriptovalyuty/birzha-i-obmennik/
109. https://cryptocurrencyhub.io/exchanger-vs-exchange-which-one-to-choose-73af890dea0a
110. https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/
111. https://www.lexology.com/library/detail.aspx?g=4c461fed-99b5-46e4-8f27-d4497957be4c
112. https://www.prostobank.ua/finansovyy_gid/investitsii/stati/chto_takoe_token_na_blokcheyne
113. https://academy.binance.com/ru/articles/hard-forks-and-soft-forks
114. https://sumsub.com/blog/aml-red-flag-indicators/#first
115. https://academy.horizen.io/technology/expert/utxo-vs-account-model/
116. https://impgun.wordpress.com/2015/11/22/merkling-in-ethereum/
117. https://eth.wiki/en/fundamentals/patricia-tree
118. https://easythereentropy.wordpress.com/2014/06/04/understanding-the-ethereum-trie/
119. https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/
120. https://academy.horizen.io/technology/expert/cross-chain-transactions/
121. https://forklog.com/sidechains-faq/
122. https://bitnovosti.com/2020/06/03/trilemma-masshtabiruemosti-blokchejna/
123. https://bytwork.com/articles/trilemma
124. https://academy.binance.com/ru/articles/what-is-staking
125. https://bytwork.com/articles/seed
126. https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch04.html
127. https://www.youtube.com/watch?v=skLvrhv8etU
128. https://www.youtube.com/watch?v=J3gzwh2F8aU
129. https://iancoleman.io/bip39/#english
130. https://www.pelock.com/products/hash-calculator
131. https://habr.com/ru/company/distributedlab/blog/413627/
132. https://bitnovosti.com/2021/08/07/bip39-i-mnemonic-phrase/
133. https://coderoad.ru/51152264/%D0%9F%D1%83%D1%82%D1%8C-%D0%B2%D1%8B%D0%B2%D0%BE%D0%B4%D0%B0-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%BE%D0%B2-HD-wallet-bip32
134. https://www.russianblogs.com/article/2264311352/
135. https://www.russianblogs.com/article/46391177811/
136. https://bitnovosti.com/2017/07/16/sozdayom-bekap-vashih-bitcoinov/
137. https://intuit.ru/studies/courses/3520/762/lecture/32518

138. https://habr.com/ru/company/bitfury/blog/340378/
139.
140. https://www.russianblogs.com/article/3455379956/
141. Stable Coins: тихая криптовалютная гавань | ForkLog
142. https://webhamster.ru/mytetrashare/index/mtb0/15490372385259ppaijw
143. https://habr.com/ru/company/distributedlab/blog/417337/
144. https://bytwork.com/articles/seed
145. https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt
146. https://iancoleman.io/bip39/#english
147. https://academy.binance.com/ru/articles/what-is-symmetric-key-cryptography
148. https://academy.binance.com/ru/articles/what-is-public-key-cryptography
149. https://2bitcoins.ru/chto-takoe-digicash-istoriya-tsifrovoj-valyuty/
150. https://bitcoinmagazine.com/culture/the-genesis-files-how-hal-finneys-quest-for-digital-cash-led-to-rpow-and-more
151. https://blockchainwiki.ru/o-tehnologii-blokchejn-prostymi-slovami/
152. https://freeton.house/ru/blokchejn-nachalo-istoriya-poyavleniya-samogo-pervogo-blokchejna/
153. https://habr.com/ru/company/wirex/blog/397999/
154. https://cryptonew.ru/mining/562-chto-takoe-nonce.html
155. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf