AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

MAGİSTRATURA MƏRKƏZİ

Əlyazma hüququnda

Orucov Qabil Arif oğlu

BLOKÇEYN TEXNOLOGİYASININ İQTİSADİYYATA TƏSİRİNİN TƏDQİQİ

MAGİSTR DİSSERTASİYASI

İstiqamətin şifri və adı:	**060509 Komputer Elmləri**
İxtisaslaşma:	**İnformasiya sistemləri**
Elmi rəhbər:	**i.e.d., prof. Balayev R.Ə.**
Magistr proqramının rəhbəri:	**tex.e.d., akad. Abbasov Ə.M.**
Kafedra müdiri:	**tex.e.d., akad. Abbasov Ə.M.**

Bakı-2020

MÜNDƏRİCAT

Səh.

GİRİŞ

Mövzünun aktuallığı: İnformasiya texnologiyaları inkişaf etdikcə onların iqtisadi proseslərdə tətbiqi də sürətlə artmaqdadır. Bu texnologiyaların iqtisadiyyat sahələrində tətbiq olunması nəticəsində iqtisadi proseslərin yerinə yetirilməsi daha təhlükəsiz və sürətli olmuşdur.

Bu cür texnologiyalardan biri də Blokçeyn texnologiyasıdır. Bu texnologiya mahiyyəti üzrə sistem istifadəçiləri arasında istifadə olunan paylanmış verilənlər bazası və ya rəqəmsal tranzaksiyaların və ya hadisələrin qeyd olunması üçün açıq bir registerdir. Bitcoin yeni bir valyuta növü olub açıq komputerlər şəbəkəsi olaraq internetdə fəaliyyət göstərir. İnternetə çıxışı olan hər bir kəs bu texnologiya vasitəsi ilə pul transferlərini email göndərmək qədər sadə formada həyata keçirə bilər. Bu yeni rəqəmsal pul forması ilə biz yeni bir maliyyə dünyasının başlanmasını görürük.

Bitcoin 2008-ci ilin maliyyə krizisindən bir neçə ay sonra 2009-cu ilin yanvar ayında dövriyyəyə buraxılmışdır. Bu texnologiya elə formada dizayn edilmişdir ki, hər hansısa şəxsin pullarının kilidlənməməsinə və götürülməməsinə təminat verir. Yeni yaranmış bu valyuta dünya ekonomikasında olduqca təsirli effekt göstərmişdir. Biz artıq Bitcoin-in ABŞ valyutası ilə müqayisədə bir neçə sentdən neçə min dollara qalxdığının şahidi olduq.

Onun gizli yaradıcısı Satoşi Nakamato yalnız mənbə kodunun proqramçılar tərəfindən dəstəklənməsi üçün Bitcoin və onun başlanğıc xəbərləri haqqında paylaşımları ilə tanınır. Heç kəs onun əsl kimliyini bilməsə də Bitcoin-in mənbə kodunun testlənməsindən sonra ciddi bir səhvlərin olmaması onun işinin dəyərinin açıq göstəricisidir.

İndiki günümüzdə Bitcoin və kriptovalyuta texnologiyaları ətrafında böyük həyəcan yaranmışdır. Optimistlər bu texnologiyaların tədiyənin, ekonomikanın hətta siyasi prosesslərin də fundamental dəyişilməsinə gətirib çıxaracağını düşünürlər. Pessimistlərin isə iddiasına görə Bitcoin və digər kriptovalyuta texnologiyaların təbii şəkildə qırılması və möhtəşəm bir çöküşə məruz qalması

qaçılmazdır.

Kriptovalyutaların əsas özəlliyinin nə olduğunu başa düşmək üçün biz onların texniki səviyyədə necə işlədiyini başa düşməliyik. Növbəti paraqraflarda ekonomikada pul dövriyyəsindən, Bitcoin-nin adi puldan fərqi, Blokçeyn texnologiyası və perspektivlərindən, mərkəzləşdirilməmiş sistemlərdən və kriptovalyutaların gələcəkdəki talehlərindən bəhs edilir.

Problemin qoyuluşu və öyrənilmə səviyyəsi: İnformasiya təhlükəsizliyin çox vacib məsələ olduğu bir dövrdə İnternet üzərindən yerinə yetirilən mübadilələrin təhlükəsizliyinin təmin olunması və həqiqiliyinin yoxlanılması müxtəlif müəssisələr və dövlət orqanları tərəfindən ciddi formada tənzimlənən bir prosesdir. Bu cür tranzaksiyalar yerinə yetirilən zaman onların yoxlanılması və təsdiqlənməsi bu sahədə fəaliyyət göstərən aralıq vasitəçilər tərəfindən həyata keçirilir. Aralıq vasitəçilərin istifadəçi məlumatlarına baxış imkanın olması və ya həmin məlumatların götürülub başqa məqsədlər üçün istifadə olunması riski vasitəçilərə olan güvəni hər zaman sual altında saxlayır. Bu cür informasiya təhlükəsizliyi və bu sahənin yalniz bir neçə güclü üzvlər tərəfindən idarə olunması problemlərini aradan qaldırmaq məqsədi ilə Blokçeyn texnologiyası əsasında fəaliyyət göstərən yeni mübadilə sistemləri yaradılmışdır. Blochain texnologiyasının tətbiqi ilə sayılan problemləri aradan qaldırmaq imkanına malik olunmasına baxmayaraq eyni zamanda həll tələb edən yeni problemlər yaranır.

Blokçeyn texnologiyası əsasında yaradılmış sistemlər vasitələ iqtisadi proseslərin hansı formada aparılmasının bəzi məsələlərini Andreas M. Antonopoulos, Richard Caetano, Melanie Swan, Siraj Raval, Michael Crosby kimi iqtisadiyyatçılar və proqram təminatı mütəxəssisləri tərəfindən analiz edilmişdir.

Bu problemin mürəkkəbliyi və çoxölçülüyü, informasiya texnologiyalarının sürətlə inkişaf edərək iqtisadiyyat sahəsində daha geniş miqyasda tətbiq olunmaları tədqiqat mövzusunun aktuallığını müəyyənləşdirdi, dissertasiyanın predmetini, məqsədini və vəzifələrini seçdi.

Tədqiqatın obyekti və predmeti: Tətqiqatın obyekti iqtisadiyyat sahəsində fəaliyyət göstərən individual şəxslər, özət təşkilatlar və müəssisələrdirlər. Tədqiqatın predmet sahəsi iqtisadiyyat sahəsində üzvlərin qarşılıqlı mübadiləsi mexanizmlərinin qayda və qanunları götürulmüşdur.

Tədqiqatın məqsəd və vəzifələri: Tədqiqatın məqsədi Blokçeyn texnologiyasının tətbiqi nəticəsində müxtəlif maliyyə bazarlarının hansı formada modifikasiyalara uğraması və onun texniki səviyyədə necə fəaliyyət göstərməsi araşdırılırması və mümkün problemlərin həl yollarının tapılmasıdır. Dissertasiyanın məqsədinə çatması üçün aşağıdakı vəzifələr müəyyən edilmişdir:

- Ənənəvi maliyyə münasibətlərinin araşdırılması və dəyər daşıyan rəqəmsal pul vahidlərinə keçidin mərhələlərinin təyin olunması;

- İnternet üzərindən yerinə yetirilən tranzaksiyalar zamanı yaranan problemlərin araşdırılması;

- Blokçeyn texnologiyasının tətbiqi nəticəsində həll oluna biləcək problem və yeni yara biləcək problemlərin müəyyən olunması;

- Struktur və arxitektura baxımından dəyişilmiş marketlər üçün yarana biləcək perspektivlərin tapılması;

- Blokçeyn texnologiyası sayəsində yeni yaranacaq iqtisadi sahələrinin fəaliyyət formalarının araşdılırması;

- Kriptoqrafik funksiyaların araşdırılması

- Blokçeyn texnologiyasının texniki səviyyədə araşdılırması

Tədqiqatın informasiya bazası: Beynəlxalq təşkilatların hesabatları, İqtisadiyyat Nazirliyinin, Mərkəzi Bankın, Rabitə və Yüksək Texnologiyalar Nazirliyinin məlumatlarından və İnternet resurslarından istifadə edilmişdir. Dissertasiya işini Qərb iqtisadçılarının tədqiqatları və əsərləri təşkil edir. Eyni zamanda mənbə kodu açıq olan proqram təminatlarının analizi də təşkil edir. Təqdim edilən dissertasiyanın yazılışında paylanmış sistemlərin iqtisadi proseslərə

tətbiqi, biliklər iqtisadiyyatı, innovasiya iqtisadiyyatı, informasiya iqtisadiyyatı və digər elmlərin müddəalarından istifadə edilmişdir. Təqdim olunmuş magistr dissertasiya işinin bazasını biliklər iqtisadiyyatı, innovasiya iqtisadiyyatı və informasiya iqtisadiyyatı ilə bağlı elmlərin tədqiqat işlərinin spektri, meydana çıxan faktlar arasındakı qanunauyğunluq və əlaqələr təyin edilərək müxtəkif əlamətlər aşkar edilmişdir.

Tədqiqatın elmi yeniliyi: Əldə edilən və elmi yenilik təşkil edən ən əhəmiyyətli nəticələr:

- İqtisadi proseslərinin Blokçeyn texnologiyasının tətbiqi nəticəsində modifikasiyalarının analizi;

- Blokçeyn texnologiyası vasitəsi ilə yarana biləcək yeni marketlərin ortaya çıxarılması;

- Kriptoqrafik funksiyalardan və paylanmış sistemlərdən istifadə etməklə iqtisadiyyat sahəsində ciddi dəyişikliklərə gətirib çıxara biləcək proqram təminatlarının baza prinsiplərinin müəyyən olması;

Tədqiqatın praktiki əhəmiyyəti: Tədqiqat işi nəticə, təkliflərdən, tövsiyələrdən, elmi müddəalardan təşkil olunmuşdur. Magistr dissertasiya işində elmi-tədqiqat işlərinin səmərəliliyinin artırılması məqsədilə lazımi stimullaşdırma tədbirlərinin reallaşdırılması, iqtisadiyyat sahəsində innovativ texnologiyaların tətbiq olunma usullarının tapılması, yeni bazarların ortaya çıxarılması və onların fəaliyyətlərini analizi, Blokçeyn əsasında hazırlanana biləcək proqramlar üçün baza biliklərin formalaşdırılması, innovasiya fəaliyyətinin inkişafının ölkə iqtisadiyyatındakı təsiri kimi mövzuların araşdırılması tədqiqatın praktiki əhəmiyyətidir.

FƏSİL 1. Blokçeyn texnolgoiyası əsasında qurulmuş və ənənəvi rəqəmsal sistemlərdə maliyyə münasibətləri

1.1 Maliyyə münasibətlərinin inkişafı dövründə yaranmış problemlər

Qədim zamanlarda valyutalar olmamışdan əvvəl mal əldə edilməsi üçün yalnız bir sistem işləyirdi. Bu sistem barter sistemi idi. Fərz edək ki, X şəxsi aləta Y şəxsi isə dərmana ehtiyac duyur və X-in dərmanı Y-in isə aləti var. Bu halda onlar bir-birlərinin əşyalarına ehtiyac duyduqlarından rahatlıqla onları dəyişə bilərlər.

Digər tərəfdən fərz edək ki X şəxsinin ərzağı vardır və o bu ərzağı hər hansı bir alətlə dəyişmək istəyir. Eyni zamanda Y şəxsinin aləti var, o isə ərzağa yox dərmana ehtiyac duyur. Belə olduğu halda X və Y şəxsləri bir-birləri ilə ticarət edə bilməyəcəklər. Lakin, fərz edək ki, üçüncü bir Z şəxsinin də dərmanı vardır hansı ki ərzaqla dəyişməyə razıdır. Beləliklə, hər üç şəxsin istədiklərini əldə etmələri üçün üç tərəfli razılaşma yaranır.

Bu metodun çatışmazlığı koordinasiyadır, yəni eyni vaxtda eyni əşya və ya tələbatlara ehtiyac duyan bir qrup insanın istəklərinə nail olmasının təşkil edilə bilinməməsidir. Koordinasiya məsələsini həll etmək üçün iki sistem yaranmışdır: kredit və nəğd pul. Tarixçilər, antropoloqlər və iqtisadiyyatçılar hansının daha əvvəl yaranması barədə debatlar aparırlar.

Kredit əsasında olan sistemdə yuxarıdakı misalda X və Y şəxsləri bir-birləri ilə ticarət apara biləcəklər. Y X-ə istədiyi aləti verər və ona təmənnalı şəkildə yaxşılıq etmiş olar. Başqa sözlə desək, X şəxsində gələcəkdə Y şəxsinə qarşı bağlamalı olan borc yaranır. X öz material tələblərini ödədikdən sonra yaranmış borcu ləğv etməlidir. Əgər o, gələcəkdə Z şəxsi ilə qarşılaşıb öz ərzağını Z şəxsinin dərmanı ilə dəyişsə onda geri dönüb Y şəxsi qarşısında olan borcu dərman ilə ləğv edə biləcək.

Digər tərəfdən nəğd pul əsasında olan sistemdə isə X şəxsi Y şəxsindən aləti pulla alardı. Daha sonra Y əldə etdiyi pulla Z şəxsindən dərman alardı. Öz

növbəsində də Z şəxsi həmin pulla X şəxsindən ərzaq alaraq dövrü tamamlardı. Bu əməliyyatlar istənilən ardıcıllıqla yerinə yetirilə bilər o şərtlə ki, alıcıda hər bir tranzaksiya zamanı pul olsun. Əvvəl-axır elə vəziyyət yaranır ki sanki pullar əldən-ələ ötürülməyib.

Heç bir sistem bir-birini üstələmir. Nəğd pul əsasında olan sistem pul vəsaitlərinin hansısa ilkin paylanması ilə sistemə yüklənməlidir hansı ki, onlar olmadan heç bir əməliyyat yerinə yetirmək olmaz. Kredit əsasında olan sistemin isə belə bir paylanmaya ehtiyacı yoxdur. Lakin, çatışmazlığı ondan ibarətdir ki, borc verən hər bir şəxs eyni zamanda riskə getmiş olur. Çünki borc alan şəxsin heç vaxt borcunu ləğv etməmək ehtimalı vardır.

Nəğd pul əsasında olan sistem eyni zamanda bizə nəyinsə dəyəri haqqında mühakimə yürütməyə imkan verir. Əgər siz barter edirsinizsə bu zaman alət, dərman və ərzaq arasında hasının dəyərinin daha çox olduğu barədə bir söz söyləmək çətin olmur. Pul vəsaitləri bizə dəyər haqqında danışmağımız üçün rəqəmlərdən istifadə etməyə imkan yaradır. Buna görə də indiki günümüzdə qarışıq sistemdən istifadə edilir - hətta kreditdən istifadə edən zaman belə onu ləğv etmək üçün tələb olunan borc nəğd pul ilə ölçülür.

Bu ideyalar bir çox kontekstlərdə peyda olurlar, xüsusən də onlayn sistemlərdə harada ki, istifadəçilər bir-birləri ilə müəyyən virtual mal ticarəti ilə məşğul olurlar. Misal üçün peet-to-peer fayl mübadiləsi şəbəkələri freeloaders yəni qarşılıqlı paylaşım olmadan faylları yükləyən istifadəçilər problemi ilə qarşılaşır. Baxmayaraq ki fayl mübadiləsi işləyə bilər, eyni zamanda koordinasiya yəni sizin istədiyiniz faylı olan və sizin fayla ehtiyac duyan ideal şəxsi tapmaq problemi var. MojoNation və Karma kimi layihələrdə istifadəçilər müəyyən başlanğıc paylamı ilə virtual pullar əldə edirlər. Onlar bu pulları fayl almaq üçün xərcləməlidirlər və nüsxələrini digərlərinə göndərərək qazanmalıdırlar. Hər iki halda bir və ya daha çox mərkəzi serverlər istifadəçilərin qalıq pullarını izləyir və onlara daxili valyuta ilə və ya ənənəvi valyuta ilə mübadilə xidmətləri təklif edə bilər. MojoNation layihəsinin bu cür mübadiləni həyata keçirmək üçün uzun müddət yaşamamasına

baxmayaraq, indiki günlərimizdə istifadə olunan bir sıra protokolların (BitTorrent və Tahoe-LAFS) intellektual əsası oldu.

Kredit və nəğd pul fundamental ideyalardır. Beləliklə, elektron ödəniş metodlarını iki qrupa ayırmaq mümkündür. Aydındır ki Bitcoin nəğd pul qrupuna aiddir. İlk olaraq kredit qrupuna baxaq.

Kredit kartları ilə yerinə yetirilən tranzaksiyalar müasir günümüzdə internetdə istifadə olunan əsas ödəniş metodudur. İnternetdə kredit kartları ilə ticarət zamanı istifadəçi kartı haqqında məlumatları satıcıya göndərir və satıcı bu məlumatları sistemə daxil edir. Sistem rolunda banklar, kredit kart şirkətləri və ya digər qurumlar çıxış edə bilər.

Digər tərəfdən PayPal kimi vasitələrdə aralıq arxitekturadan istifadə olunur. Bu cür arxitekturada alıcı və satıcı arasında aralıq bir şirkət olur. Belə ki, alıcı öz kredit kartı haqqında məlumatları satıcıya yox aralıq vasitəçiyə göndərir. Aralıq vasıtəçi isə öz növbəsində tranzaksiyanın təsdiqi barədə satıcını məlumatlandırır. Bundan əlavə hər günün sonu satıcı ilə öz balansını tənzimləyir.

Bu arxitekturanın üstünlüyü ondan ibarətdir ki, alıcı öz kredit kartı haqqında təhlükəlilik riski olan məlumatları satıcıya vermir. Alıcı hətta satıcıya öz şəxsiyyəti haqqında belə məlumat verməyə ehtiyac duymur. Bu da gizliliyin qorunmasına təminat verir. Burada çatışmayan cəhəti ondan ibarətdir ki, alıcı və satıcı arasında olan birbaşa əlaqə mürəkkəbləşir. Elə hal yarana bilər ki hər iki tərəf həmin aralıq vasitəçi ilə hesaba sahib olmaq məcburiyyətində qalsınlar.

Bu gün əksər insanları internet üzərindən ticarət zamanı kredit kartları haqqında məlumatları paylaşmaq qane edir. Lakin, 1990-cı illərdə internet yeni idi, protokol səviyyəsində şifrələmə standartları yeni yaranmışdı və bu problemlər istifadəçiləri qərarsız qalmağa məcbur etmişdi. İnsanlara öz kredit kartları haqqında məlumatları nüfuzu bilinməyən satıcılara təhlükəli kanallarla göndərmək müəmmalı gəlirdi. Belə bir mühitdə aralıq arxitekturaya maraq getdikcə artmağa başladı.

FirstVirtual şirkəti 1994-cü ildə əsası qoyulmuş erkən ödəniş vasitəçisi idi. Bu

şirkətin təklif etdiyi sistem indi fəaliyyət göstərən PayPal-ın sisteminə bənzəsə də ondan uzun müddət əvvəl yaradılmişdı. Alıcı satıcıdan nə isə almaq istədikdə satıcı FirstVirtual şirkətinə tələb olunan ödəniş haqqında məlumatla müraciət edir. FirstVirtual şirkəti isə öz növbəsində əgər alıcı kredit kartı ilə ödənişə razıdırsa bu məlumatları ilə təsdiqləyir. Lakin bu cür ödəniş sistemində iki əsas məsələ var idi. Birinci, bütün əlaqələr emaillər üzərindən yerinə yetirilirdi. Veb brauzerlər HTTPS kimi şifrələmə protokollarını yeni dəstəkləyirdilər və ödəniş protokollarının çox partiyalı olması başqa çətinliklər əlavə edirdi. İkinci məsələ isə o idi ki, satıcı tələb olunan məbləği 90 gündən sonra əldə edirdi.

90-cı illərin ortalarında aralıq artitekturaya rəqib olan SET arxitekturası yaradıldı. SET həmçinin istifadəçilərə öz kartı haqqında məlumatları göndərməkdən azad edirdi. İstifadəçi ticarətə hazır olduğu zaman brauzer tranzaksiyanın detalları haqqında məlumatları və kredit kartı haqqında məlumatları kompüterdə yalnız aralıq vəsitəçinin deşifrələyə biləcəyi şifrələmə proqramına göndərir. Məlumatlar şifrələndikdən sonra onları təhlükəsiz şəkildə göndərmək olar. Satıcı şifrələnmiş məlumatları tranzaksiyanın detallarına öz baxışı ilə aralıq vasitəçıyə göndərir. Vasitəçi bu məlumatları deşifrə etdikdən və alıcının təsviri satıcınınki ilə eyni olduqdan sonra tranzaksiyanı təsdiqləyir.

SET arxitekturasını reallaşdıran şirkətlərdən biri CyberCash olmuşdu. Kredit kartları ilə ödənişlərin emalından əlavə CyberCoin adlanan rəqəmsal pul vahidləri də var idi. Lakin, onların proqram təminatları alıcıların internet üzərindən ticarəti zamanı ödənişlərini ikiqat artıran Y2K problemi ilə qarşılaşdığından şirkət 2001-ci ildə müflis oldu.

Bu arxitekturanın işləməmə səbəbi sertifikasiya olmuşdu. Sertifikat kriptoqrafik eyniliklərin təhlükəsiz bağlanması üsuludur. CyberCash şirkətində prosseslərdən və satıcılardan əlavə bütün istifadəçilərin də sertifikat alması qərarı alınmışdı. Uzun müddət əsas istifadəçilər kollektiv şəkildə bu qərardan imtina etdilər. Bitcoin bu problemi real şəxsi identifikasiyalardan qaçmaqla həll edir. Növbəti fəsildə bu barədə ətraflı açıqlanacaq.

91-ci illərin ortalarında nə vaxt ki, SET artıq standartlaşdırılmışdı. W3C konsoriumu da maliyyə ödənişlərin standartlaşdırılması barədə işlər aparırdı. Onlar bunu HTTP protokulunu genişləndirməklə istifadəçiləri tranzaksiyalar üçün əlavə proqram təminatından azad etməklə həyata keçirmək istəyirdilər. Lakin, onların bu cəhdləri uğursuzluqla nəticələnmişdi.

Rəqəmsal kommersiyanın sürətlə genişlənməsi ilə zamanla yerinə yetirilən tranzaksiyaları sayı artmağa doğru gedəcəkdir. İnsanların informasiya texnologiyaları inkişaf etdikcə həyat tərzlərinin necə dəyişməsinə əsasən söyləmək olar ki internetdə yeni yaradılacaq ödəniş metodları ənənəvi ödəniş metodlarını əvəz edəcəkdir. Bu ssenarinin həqiqi mümkünlüyünü nəzərə alan iqtisadiyyatçılar üçün kriptovalyutaların gələcəkdə iqtisadi bazarların formalaşmasında ciddi rol oynayacağı fikrini qəbul etmək məntiqli olardı. Cari vaxtda müxtəlif kriptovalyutalar pulun üç əsas funksiyasına görə bir-birlərindən fərqlənirlər. Ənənəvi pulları əvəz edə bilmək üçün kriptovalyutalar pulun növbəti üç funksiyasına sahib olmalıdırlar: 1) mübadilə imkanı; 2) mühasibat vahidi olmaq; 3) özündə müəyyən dəyər daşımaq; İqtisadi nəzəriyyələr ilk iki funksiyanın barterlərin tranzaksiya xərclərinin aşağı salması özəlliyinə görə daha vacib olduqlarını təklif edə bilərlər. Nəzərdə tutulur ki, əgər ilk iki funksiyanın dəyərləri təyin olunsa bu zaman üçüncü funksiyanın dəyəri avtomatik təyin olunacaq. Bu ona əsaslanır ki, istənilən innovasiyalar nəticə etibarı ilə biznesdə və relyasion tranzaksiyalarda iqtisadi problemləri həll etməlidir yoxsa ki, sadəcə innovativ riyazi bir alqoritm olmamalıdır. Riyaziyyat özü müstəqil məhsul kimi təmin incəlikdir. İncəliyin dəyəri isə metafizikidir. Beləliklə, əgər Blokçeyn texnologiyasının brendinqi yalnız üçüncü funksiyaya fokuslanırsa yəni ki valyuta ətrafında həyəcan yaradaraq onun dəyər almasına imkan verirsə və tək funksionallığı budursa bu halda o, pulun ilk iki funksiyalarının dəyər almasına imkan vermir. Likvidlik riski pulun dəyər daşıyıcısı kimi olması funksiyası ilə əlaqəlidir. Dəyərin saxlanılması ya qısa vadəli ya da uzun vadəli məqsədlər üçün olur. Qısa vadəli dəyər toplanması yatırımlar fəaliyyəti və yeni başlanğıclarda

itkilərin çox olması təbiətinə görə spekulyar ola bilir. Uzun vadəli dəyər toplanmasında isə valyutanın saxlanılması keçmiş qeydlərə görə əsaslandırıla bilinməz. Kriptovalyutanın uzun vadəli dəyəri kriptovalyuta ticarətlərdə nə dərəcədə geniş istifadə olunmasından asılıdır. Eyni zamanda mərkəzi bankların öz valyutalarının təminatını necə idarə etməklərindən və yeni texnologiyalara necə münasibət bəslədiklərindən də asılıdır. Bütün bu faktorlar konkret Blokçeyn sisteminin konkret tətbiqetmələrdə konkret ölkələr üçün uğurlu olub olmayacağını müəyyən edir. Blokçeyn texnologiyası alqoritm vasitəsi ilə təklif etdiyi kriptovalyutanın dəstəklənməsini təmin edir və mərkəzi bankınların pul siyasətlərinindən azad edir. Bu baxımdan kriptovalyutalar kağız pullardan fərqli olaraq dəyərin sığortalanması üçün daha yaxşı variant kimi görülür. Kriptovalyutaların dəstəkləyiciləri iddia edirlər ki, banklarda saxlanılan pullar risk altında olurlar, kriptovalyutalar isə müstəqil dəyər kəsb edən yeganə varlıqdır. Bu arqument yalnız kriptovalyutalar pulun ilk əsas funksiyasını yerinə yetirdikdə düzgün sayıla bilər. Əks halda kriptovalyular dəyər daşıyıcısı kimi qəpik stokunun dəyərinə oxşardır. Bu stok investorları qısa bir müddətdə zəngin edə bilər, lakin əgər qəpik stokunu buraxan şirktətin ona dəyər verəcək heç bir iqtisadi məhsulu yoxdursa onun dəyəri eyni zamanda sıfra da enə bilər. Bu yolla özündə dəyər saxlamaq məqsədi ilə yaradılmış hər hansı bir valyuta öz sərvətinin müstəqilliyinə təminat verə bilməz. Bundan əlavə idarəetmə orqanları istifadəçilər sıxışdıraraq onların kriptovalyutalarını müsadirə edə bilərlər. Buna görə də hansısa Blokçeyn texnologiyasının kriptovalyutasının dəyər daşıyıcısı kimi brendinqi düzgün fikir olduğunu demək olmaz. Əgər Blokçeyn texnologiyası öz potensialını mərkəzləşdirilməmiş tranzaksiyalar üçün tranzaksiyaların xərclərini azaltmaq mexanizmi formasında göstərmək istəyirsə bu zaman o pulun ilk iki funksıyasını yerinə yetirməlidir. Mübadilə vasitəsi funksiyası konkret Blokçeynin mübadilə birjalarında tranzaksiya xərclərinin necə azaltmasına fokuslanır. Tranzaksiya xərclərinin təbiəti iqtisadi ədəbiyyatlarda analiz edilmişdir. Xüsusi Blokçeyn sisteminin tranzaksiya xərclərini necə aşağı saldığını başa düşmək üçün

tranzaksiya xərclərinin daxili təbiəti və vasitəçilərin tranzaksiyalar üçün tələb etdiyi bazar komissiyaları öyrənilməlidir. Tranzaksiya xərclərinin daxili təbiəti iki tipi əhatə edir: mənfi seçim və mənəvi risk. Mənfi seçim müqavilə qabağı risk də adlanırlar. Bu risk satıcının məhsul və xidmətləri heç bir əlaqəyə girmək istəmədiyi alıcıları cəlb etməsidir. Mənəvi risk isə müqavilə sonrası riskdir. Bu risk müqavilənin tərəflərindən birinin müqavilə şərtlərinə uymaması vəziyyətinin yaranması ilə bağlıdır. Bu tip problemlərin yaranma səbəbi müqavilə bağlayan tərəflər arasında asimmetrik informasiyasın olması və həmçinin məhsulların doğru xüsusiyyətlərinin göstərilməməsi olur. Blokçeyn texnologiyası iki müxtəlif şəxslər arasında tranzaksiyalar aparmağa imkan vermək üçün nəzərdə tutulursa o zaman ağıllı müqavilələrinin tətbiqi bu iqtisadi problemi həll edə bilər. Bütün tranzaksiyalar ya aşkar ya da ki qeyri-aşkar müqavilələrdirlər. Asimmetrik informasiya problemi nəticəsində tranzaksiya xərcləri aralıq vasitəçinin müəyyən etdiyi komissiyanın qat-qat çox ola bilir. Aralıq vasitəçilərin əldə etdiyi komissiyalar tranzaksiya xərclərinin azaldılması üçün nəzərdə tutulur. Həmin komissiyalar özlüklərində tranzaksiya xərcləri deyildirlər. Tranzaksiya xərclərinin tamamilə sıfra endirilmə imkanı demək olar ki mümkün deyildir. İqtisadiyyat üzrə Nobel mükafatı laureatı, müqavilələr nəzəriyyəsnin banisi olan Oliver Hart ağıllı müqavilələrin Blokçeyndə yaranan bütün problemləri həll edə biləcəyi fikrinə şübhə ilə yanaşırdı. Lakin, bir müddət sonra o, Blokçeyn şirkətlərindən birinə ağıllı müqavilələrin hazırlanması üzrə məsləhətçi olaraq qoşulmuşdur. Konkret Blokçeyn texnologiyasının mühasibat vahidi kimi olması funksiyasını necə yerinə yetirməli olması məsələsi də olduqca vacibdir. Mühasibat güclü etibarlılıq tələb edir hansı ki Blokçeyn sistemləri konsensual şahid mexanizmi vasitəsi ilə bunu təmin edə bilir. Yaxşı konsensual şahid mexanizmi hakim rolunu əvəz edə bilər. Lakin, yaxşı hakimin nə olması və öz işini kifayət qədər sürətli görə bilməsi kimi suallar yaranır. Bu suallara ağıllı müqavilələr cavab verə bilər. İddia olunur ki bitcoin-ə dəyər verən əsas ünsür bu sistemdəki hesablama gücüdür. Əgər autentifikasiya Blokçeyn sisteminin etibarlılıq göstəricisidirsə onda autentifikasiya

prosesi zamanı onun effektivliyinin qiymətləndirilməsi vacibdir. Məsələn orta hesabla bitcoin əldə olunması on dəqiqə çəkdiyi halda digər kriptovalyutanın başqa alqoritmdən istifadə etməsinə görə həmin vaxt da başqa olacaqdır. Bu effektivin qiymətləndirilməsi aspektlərindən biridir. Eyni zamanda Blokçeyn sistemlərinin mənbə kodunun açıq və ya qapalı olub ya olmaması da müzakirələrə səbəb olur. İddia olunur ki kirptovalyuta sisteminin uğurlu olması üçün onun mənbə kodu açıq olmalıdır.

Blokçeyn texnologiyasını başqa bir istiqaməti elektron ticarətdə sferasında yaradılan müxtəlif proqram təminatlarıdır. Hər hansısa bir Blokçeyn texnologiyasının brendinqi onun müxtəlif yeni texnologiyalarla uyğunluğu ilə də aparılır. Müxtəlif pay iqtisadiyyatları mövcuddur. Xüsusilə AirBnb şirkəti hansı ki on il əvvəl tranzaksiya xərcləri çox yüksək qiymətləndirilirdi. Səbəbi isə heç bir şəxsin öz yaşayış yerini bilinməyən şəxslərlə paylaşmaq istəməməsi idi. İndi isə effektiv ekranlaşdırma qolları texnologiyalarının yaranması ilə tranzaksiya xərclərinin azaldılması buna imkan verir. Blokçeyn texnologiyasının ən çox yayılmış kateqoriyaları bunlardır: 1) Pul xidmətləri və rəqəmsal cüzdanlar; 2) Kriptovalyutalar mədənçiliyi; 3) Kapital bazarları və maliyyə xidmətləri; 4) Ticarət xidmətləri və ticarət ödənişləri; 3-cü kateqoriya yüksək tranzaksiya komissiyaları lakin, az miqdarda tranzaksiya xərclərinin olması ilə xarakterizə olunur. Qeyd etmək lazımdır ki banklar və maliyyə müəssisələri ciddi formada informasiya asimmetriyası problemi ilə qarşılaşmamışdırlar. İnstitusional üzvlər banklar və maliyyə şəbəkəsinə daxil ola bilmək üçün müvafiq avtoritet təşkilatlar tərəfindən lisenziyalaşdırılır. Hər hansısa bir üzvün riskli olması zamanı mənəvi riski aradan qaldırmaq məqsədi ilə eyni zamanda həmin təşkilatlar tərəfindən üzv şəbəkədən uzaqlaşdırılır.

İlkin pul vahidləri rolunda daxili dəyəri olan dəyərli metallar çıxır edirdi. Fiziki metal pulların xarakteristikaları onlarının pulun əsas üç funksiyasını yerinə yetirməyə imkan verirdi. Onların əldə olunması üçün materialların tapılmasının çətin olması onlarının dəyərinin qorunmasını təmin edirdi. Pulların daxili

dəyərlərinin olmasına baxmayaraq onların dəyərlərinin müəyyən olunmasında hökümətlər vacib rol oynayırlar. Məsələn hər hansısa hökümət dəyərli metaldan hazırlanmış pul vahidinin üzərində öz nişanını əlavə edə bilər hansı ki, bu pul vahidlərinin təsdiqlənmiş sayda olmasının göstəricisidir. Fiat pullar isə hökumətlərinin rolunu bir adddım daha irəli aparır. Daxili dəyərə malik olan puldan fərqli olaraq fiat pulun dəyəri hökumətin qərarı ilə təyin olunur. Bir hökumət kifayət qədər güclü və etibarlıdırsa bu zaman o öz pul vahidini təyin edə bilər. Praktikada bu pullar bir sıra iqtisadi proseslərdə – vergilərin ödənilməsi, kreditlərin bağlanması üçün istifadə oluna bilir. Bu yolla əgər cəmiyyət üzvləri iqtisadi proseslərdə fəaliyyət göstərmək istəyirlərsə bu zaman onlar təklif olunan pul vahidini ödəniş vəsaiti kimi qəbul etməlidirlər. Bu yolla hökumət pulun dəyərinin qorunması və iqtisadi proseslərin imkanlarının genişləndirilməsi məqsədi ilə pul təminatını idarə edir. Müvafiq olaraq hökumətlər saxtakarlıqlarının və pul vasaitlərinin kopyalanmasının qarşısını almaq üçün müəyyən inzibatı cəzalar tətbiq edir. Müasir pullar o cümlədən ABŞ Dolları bir qayda olaraq fiat pullardırlar. Banklar iki tərəf arasında material vəsaitlərin fiziki mübadiləsinə alternativ yaradaraq pulların inkişafı üçün öz növbəsində vacib rol oynamışdırlar. Fiziki valyutanın mübadiləsinin təsdiqlənməsi nisbətən asan bir prosesdir. Ödəniş edən şəxs ödənişi qəbul edən şəxsə faktiki olaraq pula sahib olduğnu bildirir və vəsaiti ona verir və beləliklə ödənişi qəbul edən şəxs vəsaiti aldıqdan sonra mübadilə həqiqi sayılır. Lakin, bunun öz çatışmayan cəhətləri vardır. Fiziki pul vəsaitlərinə sahib olmaq onların oğurlanması, itirilməsi kimi problemlərlər qarşılaşır. Bundan əlavə bu cür mübadilələr üçün gərək iki tərəfdə fiziki olaraq bir məkanda olsunlar. Banklar yarandığı ilk vaxtdan etibarən bir məkanda olmayan müxtəlif tərəflər üçün vəsait mübadilələrini həyata keçirə bilməkləri üçün imkan yaradır. Bu, şəxslərə pul vəsaitlərinə fiziki olaraq deyil, mühasibat dəftərində rəqəmlər formasında saxlamaq imkanı verir. Ödəniş sistemləri müxtəlif banklara birgə işləyərək mübadilələr zamanı şəxslərin hesablarında kiyafət qədər pul vəsaitlərinin mövcudluğunu yoxlayırlar və uyğun olaraq hesaba vəsait əlavə olunması və ya

hesabdan vəsaitin silinməsi barədə banklara bildiriş göndərirlər. Burada əsas qeyd kimi müxtəlif tərəflərin banklara olan güvənini və mühasibat kitablarının yalnız həqiqi tranzaksiyalar zamanı dəyişməsini qeyd etmək olar. Əks halda fiziki şəxsin pul vəsaitləri itirilə və ya oğurlana bilər. Bir sıra mexanizmlər banklara olan güvəni təmin edə bilər. Banklarda bazarda dəqiq fəaliyyət göstərməsi üçün stimul vardır. Çünki pulların qorunması və mübadiləsi həyata keçirmək üçün nüfuzu aşağı olan banklar tez bir müddətdə bütün müştəriləri itirərək fəaliyyətlərini dayandırmalı olacaqdırlar. Əlavə olaraq hökumətlər banklarının fəaliyyətini gücləndirməkü üçün müəyyən normativlər və qaydalar tətbiq edirlər. Müasir günümuzdə vasaitlərin elektron formada mübadiləsi olduqca geniş yayılmışdır, lakin elektron ödəniş sistemləri aralıq vasitəçilərə olan güvən, ikiqat xərclər və digər müxtəlif problemlərlə qarşılaşırlar. Elektron mübadilələr müşahidəçilər tərəfindən ikiqat xərclər adlanan problemdən asılıdırlar. Vəsaitlərin elektron ötürülməsi zamanı bir istifadəçi özündə dəyər kəsb edən məlumatı bir neçə şəxsa göndərən zaman məlumatların kopyalanması kimi hal yarana bilir. Bu zaman sistemdə əsassız bir formada yeni vəsaitlərin yaranmasına yol açılır və buna görə də sistemdə dəyər kəsb edən vahid öz dəyərini itirməyə başlayır. Bu problem heç olmasa bir dənə mərkəzləşdirilmiş və güvənilir mərkəzi və ya özəl bank və ya iqtisadiyyat institutların mübadilələrə nəzarət etmələri üçün cəlb olunması ilə həll olunur. Güvənilir vasitəçilər hər bir şəxsin hesabında nə qədər vəsaitin olmasını nəzarət edirlər. Elektron ödəniş həyata keçirilən zaman vasitəçilər bir-birlərinə tranzaksiya barədə məlumatları ötürürlər və bu məlumatlar əsasında mühasibat kitablarını dəyişdirirlər. Vasitəçilərin göndərən şəxsin hesabını yoxlayırlar və kifayət qədər vəsait olduqda hesab müəyyən qədər azaldılır və göndərilən tərəfin hesabı nəzərdən keçirilir və hesabına əlavə olunur. Məsələn debit kart vasitəsi ilə həyata keçirilən ödəniş zamanı məlumat şəbəkə üzərindən göndərən şəxsin bankına müəyyən instruksiyalar halında göndərilərək digər şəxsin bankına vəsaitlərin köçürüləməsinə imkan verir. Bu cür ödənişlərin həyata keçirilməsinin altında dayanan nəzərə çarpacaq xərclər və böyük fiziki infrastruklar mübadilə sürətini və

əlçatanlığını təmin edir.

Bir çox Avropa ölkələri 2016-ci ilin sonundan başlayaraq blokçeyn proqram təminatlarının yaradılması üçün əlverişli şərait yaratmağa başlamışdırlar. Kriptovalyutalar yaranmağa başladığı ilk vaxtların onların tətbiq imkanları olduqca kiçik idi və Dünyanın hər yerində olduğu kimi bu cür valyutalardan yalnız qanunsuz ticarətdə istifadə oluna bilirdi. Kriptovalyutaların sərhədlərarası fəaliyyəti 2016-cı ildən başlayaraq aktivləşmişdir. Blokçeyn texnologiyalarına investisiyaların artması ilə müxtəlif ölkələr öz xidmətlərini bu texnologiyalar üzərindən yerinə yetirmək üçün müxtəlif təcrübələr aparmağa başladılar. Yeni proqram təminatlarının yaradılmasında məqsədlərdən biri də böyük miqdarda vasaitlərin transferini həyata keçirə bilmək üçün alternativin olmasıdır. Böyük Britaniya və Avstrraliya kimi ölkələr blokçeyn texnologiyasının perspektivleri barədə elmi araşdırmaları sürətlərdirirlər. Estoniya və Sinqapur kimi digər xırda ölkələr isə artıq bu texnogiyaları elektron hökümətin investisiya strategiyalarına daxil etmişdirlər. Dubay və ABŞ-ın İllinois kimi ştatları isə bir sıra hökümət xidmətlərinin blokçeynə köçürülməsi üçün təşəbbüslər görmüş və ya müəyyən kripto-iqtisadi zonalar yaratmışdırlar. Bir çox ölkələr hələ də bu sistem üzərində nəzarətsizliyi qoruyurlar. Bunun əsas səbəb kimi isə kripto-iqtisadiyyat sektorunun miqyasının kiçik olmasıdır.

Blokçeyn texnologiyası əsasında qurulan sistemlərin bazara daxil olması ilə yeni perspektivlər yarandı. Bitcoin şəbəkəsi özündə dəyər kəsb edən rəqəmsal kriptovalyutalar vasitəsi ilə aralıq vasitəçilər olmadan, məxfiliyin qorunması ilə və tranzaksiyaların heç kəs tərəfindən bloklanmasını təmin edərək onlayn ticarətlə məşğul olmaq imkanı təklif edirdi. Lakin, Bitcoin şəbəkəsinin hücumlara qarşı dayanıqlılığına baxmayaraq cari vəziyyətində mərkəzləşdirilmiş ödəniş sistemləri ilə müqayisədə daha az effektivdir. İcazəli Blokçeynlər elə sistemlərdirlər ki burada yeni üzvlərin sistemə yeni tranzaksiya daxil etməsi üçün icazəsi olmalıdır. Paylanmış hesabat sisteminin daxil olunması adətən bazarın ilkin strukturunun dəyişilmədən zamanla iştirakçıların sistemlə uyğunlaşması ilə motivasiya olunur.

Cari infrastruktudan rəqəmsal valyutalar strukturuna keçid etməklə mərkəzi banklar vətəndaşlara birbaşa kredit vermək imkanı əldə edə bilərlər. Bu cür keçid kommersiya banklarınının gəlir modellərni üçün risk yarada bilər beləki, vətəndaşlar daha güvənilir olan mərkəzi bankın pullarından istifadəyə keçə bilərlər. Daha sonra müxtəlif startaplar istifadəçilərin şəxsi rəqəmsal cüzdanlarının təhlükəsizliyinin təmin olunması və hesabatların aparılması üçün hazırlanmış proqram təminatları vasitəsi ilə rəqabətə girə bilərlər. Lakin bü cur sistemə keçid dövlətlərin vergilər sisteminin. Pul kütlələrinin idarə olunmasında köklü dəyişikliklər tələb edir. Bu cür rəqəmsal valyutalar ölkələr daxilində yaşayan və vətəndaşı olduğu ölkədə devalivasiya yaşanan əncəbilər üçün cəlb edicidir. Hindistan kimi ölkələrdə 500 və 1000-lik əskinazların demonetizasiya və tranzaksiyalara nəzarətin artırılması məxfilik baxımından istifadəçilərin kriptovalyutalardan daha həvəslə istifadəsinə itə bilər. Çin hökümətinin kriptovalyutaların istifadəsinə qoyduğu qadağadan sonra regulyatorlar və icazəsiz kriptovalyutalar arasında olan gərginliyi artırmışdır Eyni zamanda da Çin hökümәti Blokçeyn texnologiyasının imkanlarından istifadə edərək xərcləri azaltmaq və vətəndaşlar üçün yeni xidmət növlərinin araşdılırması ilə məşğuldur.

Kriptovalyutaların müəyyən xüsusiyyətlərinin analizi bu və ya digər kriptovalyutanın alternativ ödəniş vasitəsi kimi nə qədər əlverişli olmasını və gələcək prestpektivləri haqqında məlumat verə bilər. Lakin, müasir gündə bu cür analizləri aparmaq olduqca çətin məsələdir. Kriptovalyutaların mərkəzləşdirilməmiş təbiəti səlahiyyətli mənbələrin sənaye məlumatlarının müəyyən edilməsini çətinləşdirir. Bundan əlavə kriptovalyuta sistemlərinin genişlənməsi bu cür sistemlərinin analizi zamanla daha da mürəkkəbləşdirir. Bu cür çətinliklərin səbəbindən bütün kriptovalyuta sənayəsinin təhlil olunması mümkün deyildir.

Kriptovalyutalar tərərfindən yaranan risklər də öz növbəsində həll tələb edirlər. İqtisadiyyatçılar və siyasətçilər bir çox iqtisadi qanun və normativləri blokçeyn texnologiyasının icadından əvvəl tərtib etmişdirlər. Bu qanun və normativlərin

yeni yaradılmiş kriptovalyuta texnologiyaların risklərini də özündə saxlaya bilməsi problemi yaranır. Ən çox nəzərə çarpan risklər kriptovalyutaların qanunsuz proseslərdə işlədilməsi və tərəflərə tətbiq edilən istehlakçı müdafiəsinin olmamasıdır. Bir çox qanunsuz fəaliyyətlə məşğul olan şəxslər öz vəsaitlərinin köçürülməsi üçün bank və digər aralıq vasitəçilər əvəzinə nəğd puldan istifadə edirlər. Bunun səbəbi isə əvvəl də qeyd olunduğu kimi nəğd pullardan istifadə etməklə məxfiliyin təmin olunmasıdır. Bu halda heç bir üçüncü tərəf mübadilənin kimlər arasında və necə aparıldığını izləmək imkanına malik deyildir. Bir çox müşahidəçilər blokçeyn texnologiyasının mərkəzləşdirilmiş olmaması və yüksək anonimlik imkanlarının olması qanunsuz fəaliyyətlə məşğul olan şəxslərin sistem üzərindən öz vəsait mübadilələrini hökumət və güc strukturlarından gizli formada aparmaqlarına imkan yarada biləcəyindən sistemin fəaliyyətinə tərəddüdlə yanaşırlar. Kriptovalyutaların qanunsuz proseslərdə istifadə oluna bilinməsi onların cəmiyyəyə tamamilə ziyan verə bilməsi demək deyildir. Qeyd edilmişdir ki, blokçeyn texnologiyası tranzaksiyaların dəyişməz, açıq registeridir. Beləliklə, şəbəkə üzvü tərəfindən yerinə yetirilmiş hər bir tranzaksiyalarını müşahidə etmək mümkündür. Bu xüsusiyytə hüquqmühafizə orqanları üçün qanunsuz fəaliyyətlə məşğul olan hesabların izlənməsi izlənməsinə imkan verir. Bu yolla hüquqmühafizə orqanları tranzaksiya analizləri şablonları yaradaraq platformada fəaliyyət göstərən şəxslərlər həqiqi şəxslər arasında müəyyən bir əlaqə yarada bilərlər. Müxtəlif krptovalyutalar anonimlik dərəcələrinə görə bir-birlərindən fərqlənirlər. Lakin, çox yüksək anonimlik təmin edən blokçeyn şəbəkələrinin geniş miqyaslı istifadəsi müşahidə olunmur. Əlavə olaraq hüquqmühafizə orqanlarının cinayətləri araşdıra bilməsi üçün hökumət kriptovalyuta üzərində müəyyən tənzimləmə qaydaları tətbiq edə bilər. Mərkəzləşdirilməmiş sistemlər eyni zamanda vergidən yayınmaq istəyən şəxslər üçün də imkan yarada bilər beləki, gəlirlər saxlanılması üçün heç bir bankda hesab açmağa ethiyac yoxdur. Müşahidəçilər iddia edirlər ki, istifadəçilər kriptovalyutalar ilə mübadilələr aparan zamanı onlara səhv məlumatların verilməsi nəticəsində saxtakarlıqlarla üzləşə

bilərlər. Kriptovalyutalar yeni vəsait növü olduğundan bir çox istifadəçilər onunların necə faəliyyət göstərməsindən xəbərsiz ola bilərlər və nəticədə öz vəsaitlərinin digər şəxslər tərəfindən mənimsədilməsinə yol verə bilərlər. Eyni zamanda hesaba bağlı olan açarların itirilməsi istifadəçilərin vəsaitlərinin həmişəlik kilidlənməsinə yol açа bilər. Əlavə olaraq kriptovalyutalarla ödənişlərin dönməzliyi istifadəçiləri bir müddət sonra vəsaitsiz buraxa bilər.

Mərkəzi bankların pul siyasətinin fundamental səviyyədə əsas məqsədi iqtisadiyyatda dövriyyə edən pul vəsaitlərinin həcminin idarə olunmasıdır. Cari vaxtda bir çox ölkələrdə iqtisadiyyatda dövriyyə edən vəsaitlərin əksəri hökumətlərin fiat pullarıdır və bu pulların həcmi hökumət effektiv formada idarə olunur. Əgər bir və ya daha çox hökumətin idarə etmədiyi valyuta müxtəlif mübadilələr üçün istifadə olunmağa başlıdığı halda bir sıra nəticələr yarana bilər. Bu cür mübadilələrin artması mərkəzi bankların inflyasiyanı idarə etmək imkanlarına sərhəd qoya bilər. Mərkəzi banklar fiat pulların effektivliyini saxlamaq üçün müəyyən dəyişikliklər etməlidirlər ya da ki, kriptovalyutaların alışı və satışı ilə bağlı yeni proqram daxil edərək iqtisadiyyatda bu valyutaların idarəsinə təsir edə bilsin. Kriptovalyutalar global şəbəkədə fəaliyyət göstərdiyindən hər hansı bir ölkənin kritpvalyutaları idarə etməsi üçün alıb-satması eyni kriptovalyutalardan istifadə edən digər ölkələrin iqtisadiyyatına təsir edərək sabitliyi poza bilər. Beləliklə bir ölkənin kriptovalyuta siyasəti digər ölkələrin iqtisadiyyatında ciddi problemlərin yaranmasına səbəb ola bilər. İqtisadi sabitliyin pozulması nəticəsində ölkələr öz pul siyasətlərini dəyişmək məcburiyyətində qala bilərlər və eyni zaman müxtəlif ölkələr arasında siyası problemlər yarana bilər. Bir neçə valyutadan istifadə edən iqtisadiyyatlarda digər bir problem isə alıcılar və satıcılar arasında yarana bilər. Bütün alıcılar və satıcılar bütün valyutaların bir-birlərinə nəzərən dəyərlərini izləməlidirlər. Bu cür sistemə misal olaraq ABŞ göstərmək olar. Vətəndaş müharibəsi dövrünə qədər burada hər bir özəl bank şəxsi valyuta yaratmaq imkanına malik idi. Bu cür sistemin effektsizliyi və valyutaların bir-birlərinə nəzərən dəyərlərinin izlənməsi xərcli proses olduğundan sonda

mərkəzi bankın idarəsi altında vahid valyuta növü yaradıldı. Cari vaxta qədər hökumətlər bi qayda olaraq kriptovalyutaların yaradılmasında iştirak etmirdilər. Ümumiyyətlə bu texnologiyaların yaradılması zamanı məqsədlərdən biri kimi hökumətlərin pul hazırlanmasında və ödəniş sistemlərin qurulmasında iştirakı ehtiyacının aradan qaldırılması idi. Lakin, əvvəl də qeyd olunduğu kimi kriptovalyutaların anonimlik imkanları bir sıra qanunsuz fəaliyyətlərin daha da aktivləşməsinə yol açа bilər. Bu risklər müşahidəçilərin mərkəzi bankların blokçeyn texnologiyasının əsas prinsipləri əsasında öz rəqəmsal valyutasının hazırlana bilinməsi fikrinə gətirdi. Mərkəzi bank kirptovalyutaları haqqında yaranmış müzakirələr spekulyativ xarakter daşıyırlar. Bu və ya digər mərkəzi bank kriptovalyutaların yaradılması müxtəlif iqtisadi institutların bu cür valyutalara nə dərəcədə güvəninin olmasından asılıdır. Mərkəzi bank kriptovalyutaların hansı formada təşkil olunması öz növbəsində qeyri-müəyyənliklər yaradır. Məsələn mərkəzi bank kimi tranzaksiyaları təsdiqləyə biləcək vasitəçinin olması bu cür sistemlərdə kriptoqrafiyadan istifadə edilməsə ehtiyac duyulub ya duyulması kimi suallar yaradır. Digər tərəfdən bu cür kriptovalyutaların daxil edilməsinin bir sıra müsbət tərəfləri vardır. İddia olunur ki, bu cür valyutaların özəyində dayanan prinsiplər əsasında yaradılmış sistemlər ənənəvi sistemlərdən fərqli olaraq daha effektiv formada fəaliyyət göstərəcəkdir belə ki, kriptovalyuta əsasında qurulmuş sistemlərin fəaliyyətə buraxilması daha ucuz və asan başa gələ bilir. Eyni zamanda fiziki şəxslər öz hesablarını birbaşa mərkəzi bankda saxlaya bilərlər. Bu yolla yaradılan kriptovalyutalar vasitəsi ilə kommersiya bankları üçün yeni qaydalar daxil edərək sistemin sabitliyini artırmaq olar. Kommersiya bankları maraq dərəcələri və alternativ təhlükəsizlik variantları təklif edərək depositlərin saxlanılması üçün istifadəçiləri cəlb edə bilərlər. Mərkəzi bank kriptovalyutalarına qarşı rəsmi şəxslər tərəfindən ən böyük kritika cari sistemin minimum tələblərə cavab verdiyi halda yeni sktruktra keçidin ehtiyacı olmamasıdır. Əleyhdarların iddiasına görə bu cür sistem mərkəzi bankın fiziki şəxslərə kredit vermək imkanının yaranması bank sektorunda kreditvericilik imkanlarının daralmasına və

ekosistemin mərkəzi bank ətrafında cəmlənməsi halı baş verə bilər. Kreditvericilik imkanları azalan özəl banklar bu cür vəziyyətdə bankçılıq sektorunda kreditvericilik imkanlarının eyni səviyyədə saxlanılması üçün bütün qərarları mərkəzi banka buraxacaqlar. Bundan əlavə spektiklərin fikrincə kriptovalyutaların istifadəsi özəl bankların fəaliyyətlərinə manelər yaradaraq bank sektorundakı sabitliyi pozacaqdır. Bu kritiklər bildirirlər ki, hər hansı iqtisadi institutda və ya bank sektorunda həyəcan yaranarsa istehlakçılar cəld bir sürətdə öz vəsaitlərini hökumət tərəfindən dəstəklənən aktivlərə keçirəcəklər. Müşahidəçilər eyni zamanda mərkəzi bank kriptovalyutaları əsasında qurulmuş sistemin pul siyasətini gözlənilən effekti verməmək ehtimalı olmasını da bildirirlər. Mərkəzi banklar fiziki şəxslərin depositlərinə maraq dərəcəsi əlavə etməklə özəl banklara maraq dərəcəsi əlavə etmədən birbaşa makro-iqtisadiyyata çıxış əldə edə bilər. Digər tərəfdən kritiklərin fikcincə mərkəzi bankların makro-iqtisadiyyata bu cür böyük rol alması düzgün deyildir.

Bütün iqtisadi müəssisələr öz sistemlərinə yeni müştəri əlavə etdikləri zaman KYC (müştərini tanımaq) və KYB (müştəri biznesini tanımaq) proseslərini yerinə yetirirlər. Bu proseslər çərçivəsində müştərilər uyğun beynəlxalq qayda və qanunlara əsasən identifikasiya olunurlar. Müştəri məlumatlarə və onalra tətbiq olunan qaydalar zamanla dəyişdiklərindən KYC və KYB proseslərinin icra olunması çətinləşir. Bundan əlavə müştərilər hər hansı bir xidmətdən istifadə etmək istədikdə müəyyən sənədləri təsdiqləmək məcburiyyətindədirlər. Bu cür problemləri aradan qaldırmaq mərkəzləşdirilmiş xidmət tərəfindən təmin olunur. Lakin, bu cür həll kiber hücumlara və məlumatların başqa məqsədlər üçün istifadə olunmasına yol açа bilər. Blokçeyn texnolgoiyasının tətbiqi mərkəzsizləşdirilmənin hesabına qeyd olunmuş problemləri həll edə bilər. Müştərilərin məlumatlarını blokçeyn şəbəkəsində saxlayaraq zaman keçdikcə tələb olunduqda həmin məlumatları yeniləyərək hər zaman müştərilərin ən son profillərini görmək imkanı əldə olunur. Bu kontekstdə blokçeyn texnologiyasının aşağıdakı üstünlükləri vardır.

1. Mərkəzsizləşdirilmə. Müştərilərin məlumatları paylanmış şəbəkədə saxlanılır hansı ki, mərkəzləşdirilmiş sistemlərdən fərqli olaraq kiber cinayətlərin həyata keçirilməsi daha çətindir. Təhlükəsizlikdən əlavə mərkəzləşdirilməmiş sistemlər KYC və KYB proseslərində məlumatların ardıcıllığının qorunmasını təmin edir.

2. Daha güclü məxfilik. İstifadəçilərin məlumatları heç bir etibarlı üçüncu şəxs tərəfindən idarə olunmur. Əvəzində isə mərkəzsizləşdirilmiş proqram təminatları olan ağıllı müqavilələr vasitəsi ilə idarə olunur. Bundan əlavə KYC prosesini həyata keçirmək üçün müştəri məlumatlarına baxış yalnız müştərinin icazəsi olduqdan sonra həyata keçirilə bilər.

3. Dəyişməzlik. Blokçeyndə bir dəfə əlavə olunmuş məlumat heç vaxt dəyişdirilə bilinməz. Bu, bütün iqtisadi müəssisələrə müştərilərin məlumatlarının dəqiqliklə izlənməsinə və istənilən vaxt icazə olduqda baxış imkanı verir. Lakin, müştəri öz hesabını bağladıqdan sonra bütün məlumatların silinməsini tələb edə bilər. Bu halda müşətəri ümumi məlumat qorunması tənzimləməsinə dayanaraq unudulmaq hüququndan istifadə edə bilər.

Hal-hazırda bir çox banklar xırda və orta müəssisələri yükəsk riskli müştərilər kimi qiymətləndirirlər. Bu xırda startaplardan əlavə eyni zamanda varlı olan xırda və orta müəssisələr üçün də keçərlidir. Bunun səbəblərindən biri kimi 2008-ci ilin maliyyə krizisindən sonra daxil edilmiş daha ciddi olan yeni qaydaları göstərmək olar. Bu qaydaların daxil edilməsi ilə bu cür müəssisələrin kredit əldə etmək imkanları azalmışdır. Banklar xırda və orta müəssisələrin kredit imkanlarının qiymətləndirilməsi üçün yeni metodların yaranmasını tələb edirlər. Bu metodlar banklar arasında məlumat mübadiləsidən və ya digər məlumat mənbələrindən istifadə edə bilərlər. Blokçeyn texnologiyası bir neçə tərəf arasında kredit reytinqləri haqqında məlumatların təhlükəsiz formada mübadiləsinə imkan verir. Şəbəkənin iştirakçıları müəssisələrin kredit qabiliyyətlərini qiymətləndirmək üçün məlumatlar daxil edə bilərlər. Yanaşmanın mərkəzsizləşdirilmiş olması kredit qabiliyyətinin qiymətləndirilməsi zamanı daxil olunmuş məlumatların doğruluğuna

təminat verir. Bundan əlavə kredit riskinin qiymətləndirilməsi konfidensial məlumatlar olmadan həyata keçirilir. Qeyd etmək lazımdır ki, bu cür blokçeyn sisteminin dəyəri şəbəkədən istifadə edən tərəflərin sayı artdıqca və onların daxil etdikləri məlumatların dəyərindən asılı olaraq artır. Sistemdə birgə fəaliyyət göstərən bankların sayı artdıqca kredit risklərinin qiymətləndirilməsinin dəqiqliyi də artır. Artıq bu cür qiymətləndirməni həyata keçirmək üçün startaplar da mövcuddur. Bu cür startaplara misal olaraq Bloom-u göstərmək olar hansı ki, Ethereum və İPFS-dən (InterPlanetary File System) istifadə edərək mərkəzləşdirilməmiş formada kredit risklərinin qiymətləndirilmsinə imkan verir.

Kredit risklərinin qiymətləndirilməsi və KYC prosesində olduğu kimi blokçeyn texnologiyası istehlakçıların və müxtəlif bizneslərin daha dəqiq, təhlükəsiz və məxfi formada profilləşdirməsi üçün şəraiti yaradır. Bir çox hallarda müştərilər eyni zamanda bir neçə bank və iqtisadi istitutlarla iş aparırlar. Bu müəssisələrin hər biri müştərilər öz qaydaları və normativləri əsasında profilləşdirirlər. Bu məqsədlə məlumatlar müxtəlif iqtisadi institutlardan əlavə eyni zamanda sosial şəbəkələrdən belə toplanıla bilər. Müxtəlif tip hesablardan məlumatların toplanması, struktursuz və strukturlu məlumatların analiz olunması əsasında müştərilərin daha düzgün profillərini yaratmaq mümkündür. Blokçeyn vasitəsi ilə bu cür məlumatların təhlükəsiz formada, güvən sərhədlərini aşaraq müxtəlif müəssisələr arasında mübadiləsinə nail olmaq olar. Eyni zamanda müştərilərin icazəsi olduğu halda məlumatların idarə daha da asanlaşdırıla bilinər. Daha dəqiq olan müştəri profili əsasında iqtisadi institutlar hər bir müştəri ilə tələb və istəklərindən asılı olaraq individual formada xidmətlərini təklif edə bilərlər. Bir neçə misal olaraq aktivlərin idarə olunması fərdiləşdirilmiş məsləhət proqramları, fərdiləşdirilmiş yatırım portfellərinin düzəldilməsi və s. Müştərilərin profilləşdirilməsi sözsüz ki, KYC və KYB prosesləri ilə əlaqəlidir belə ki, bu proseslər müştərilərin ilkin profillərinin yaradılmasının əsasını təşkil edir. Daha da irəli gedərək yeni imkanlar əldə etmək üçün müştərilər müəssisələri daha çox məlumatlarla təmin edə bilərlər. Bu istiqamətdə yeni bir bazar olan şəxsi məlumatlar bazarının yaranması mümkündür

hansı ki, fərdi şəxslər bu və ya digər müəssisələrlə iş apardıqda yeni və fərdiləşdirilmiş xidmətlər əldə edə bilərlər.

Bir sıra iqtisadi institutlar sığorta xidmətləri də təklif etdiyindən siğorta sektoru da iqtisadiyyat sektoru ilə sıx bağlıdır. Sığorta sektorunda tətbiq olunmaqla blokçeyn bu sektora dəyərli imkanlar gətirə bilər. Nümunə olaraq yorucu sığorta proseslərinin sürətləndirilməsi kimi vasitə olmasını göstərmək olar. İddiaların həll olunması prosesi çox vaxt çəkən və mürəkkəb bir prosesdir hansı ki, bir neçə tərəflərin və vasitəçilərin iştirakını tələb edir. Bütün maraqlı tərəflərin paylanmış mühasibat registerinə inteqrasiya olunması və bütün yoxlanışlar və təsdiqləmələr üçün ağıllı müqavilələrin hazırlanması bu prosesləri asanlaşdıra bilər. Ağıllı müqavilələr bütün tələb olunan addımları təhlükəsiz formada yerinə yetirə bilər. O cümlədən tələb olunan məbləğin hesanlanması da müəyyən edə bilər. Müştəri məlumatlarının mübadiləsinin ağıllı müqavilələrlə realizasiyası həmçinin saktakarlıqların da qarşısını almağa imkan verir. Sistemi zənginləşdirib daha da etibarlı etməyin çoxlu yolları vardır. Misal olaraq qəza anında çəkilmiş mediafaylların sistemə əlavə olunmasını gətirmək olar.

Maliyyə xidmətləri təklif edən təşkilatlar müştərilərin istəklərini yerinə yetirə bilmək üçün bir neçə prosesdə birgə fəaliyyət göstərirlər. SWIFT tranzaksiyalarının emalında iki və ya daha çox təşkilatlar cəlb olunur. Bu tranzaksiyaların əsasında dayanan kritik infrastrukturlar kiber cinayətkarlar üçün əsas hücum nöqtəsidir. Maliyyə institutlarının təhlükəsizliyə etdiyi yatırımların həcminin artmasına baxmyaraq həmin infrastrukturlar yenə də hücumlara qarşı həssas olaraq qalırlar. 2016-cı ildə kiber hücum nəticəsində Banqladeş mərkəzi bankından 81 milyon dolların oğurlanması bunun göstəricisidir. Maliyyə sistemləri hər zaman kiber cinayətkarlar üçün əsas olacaqdır. Bu cür hücumların qarşısının alınması üçün maliyyə təşkilatları bir-birləri qarşılıqlı əlaqələri gücləndirməli və daim öz infrastrukturlarının təhlükəsizliyi barədə məlumatların mübadiləsini həyyata keçirməlidirlər. Təhlükəsizlik məlumatlarının maliyyə institutları arasında mübadiləsi təhlükəsizlik sahəsində birgə fəaliyyət üçün fundament ola bilər.

Blokçeyn texnologiyası maliyyə təşkilatları arasında kiber təhlükəsizlik və fiziki təhlükəsizlik məlumatlarının mübadiləsini asanlaşdırır. Paylanmış registerdən istifadə etibarlı şəkildə təhlükəsizlik ekspertlərinin birgə fəaliyyət aparmasına imkan verir. Müxtəlif müəssisələrin təhlükəsizlik məlumatlarının birgə işlənməsi əsasında yeni təhlükəsizlik metodları yaradılar bilinər. Bu metodlar əsasında global maliyyə trazanzaksiyaları yerinə yetirilən zaman yüksək səviyyədə təhlükəsizliyə nail olmaq olar. Yeni təhlükəsizlik informasiyalarının daxil olunması bu metodlar daim yenidən işlənə və daha da təkmilləşdirilə bilinər. Beləliklə birgə fəaliyyət nəticəsində kiber hücumların və digər riskli proseslərin qarşısı müəyyən dərəcədə almaq imkanı əldə olunur.

Heç bir yeni texnologiya risklərsiz deyildir. Blokçeynin əsas üstünlüyünün paylanmış registər konsensusu vasitəsilə saxtakarlıqların praktiki olaraq tamamilə aradan qaldırılmasıdır. Lakin, bu o demək deyil ki mümkun deyil. Sistemdə hər zaman kiber hücumlar və ya saxtakarlıqla məşğul olan şəxslər olacaqdır. Blokçeyn sistemin konsensusu əmin edir ki, əgər hər hansı bir düyün kiber hücuma məruz qalaraq saxta məlumatlar yerləşdirilmişdirsə bu zaman həmin düyünü növbəti proseslərin icrasında iştirak etməyəcəkdir. Əgər sistemədəki əksər düyünlər eyni zamanda kiber hücuma məruz qalsalar bu zaman sistemin informasiya tamlığının pozalması mümkundur. Lakin, bunun baş verməsi ehtimalı olduqca aşağıdır.

Əksər böyük sistemlərin inkişaf formaları mərkəzləşdirilmiş formadan mərkəzləşdirilməmiş formaya doğrudur. Sistemlər qurulan zaman ilkin mərkəzləşdirilmiş formada dizayn edilir. Bunun səbəbi isə məzkəzləşdirilmiş sistemlərin qaydaların yaradılması və bu qaydalara riayət olunmasının izlənməsi üçün ən effektiv formadır. Bu forma dublikasiyaların qarşısını alır və yaranmış mübahisələrin həllinə imkan verir. Mərkəzləşdirilmiş sistemlərin yükləri artdıqca onların xərcləri də artmağa başladığı halda texnologiyaların inkişafı nəticəsində mərkəzləşdirilməmiş sistemlərin xərcləri aşağı düşməkdədir. Bu baxımdan mərkəzləşdirilməmiş sistem olan blokçeynə keçid təşkilatlar üçün yeni imkanlar açmağa və öz xərclərini azaltmaq şəraiti yarada bilər. Bu baxımdan təşkilatlar və

bazarlar eyni formada fəaliyyət göstərməyə başlayacaqdırlar. Beləki, bazarlar mərkəzləşdirilməmiş formada fəaliyyət göstərən sistemlərdirlər.

İnkişaf etmiş iqtisadiyyata malik ölkələrdə maliyyə institutlarına olan inam kifayət qədər yüksəkdir. Bir qayda olaraq inkişaf etmiş iqtisadiyyatlar sabitdirlər və inflyasiya dərəcələri aşağıdır. Bundan əlavə onların diqqətli tənzimlənən maliyyə və hökumət institutları vardır. Dünyada bütün iqtisadiyyatlar bu xüsusiyyətlərə malik deyildirlər. Beləliklə, kriptovalyutalar maliyyə institutlarına inamın az olduğu ölkələrdə bu inamın daha çox olduğu ölkələrdən fərqli olaraq daha geniş miqyasda tətbiq oluna bilinər. Fərdi şəxslərin maliyyə təşkilatlarına olan inamının itməsinin müxtəlif səbəbləri ola bilər. Təşkilatların müflis olmaq ehtimalı və ya da şəxslərin vəsaitlərinin qorunması üçün kifayət qədər resurs ayırmaması bu cür səbəblərdən sayıla bilərlər. Müəyyən fərdi şəxslər eyni zamanda hökumətin fiat pulların dəyərinin qorunması üçün kifayət qədər fəaliyyət aparmadığını düşünüb valyutalara inamını itirə bilərlər. Hiperinflyasiyaların baş verməsi halında fiat pulların bütün dəyərlərini itirməsi fərdi şəxslərin vəsaitsiz qalmaqlarına səbəb ola bilər beləki, fiat pullar heç bir daxili dəyərə malik deyildirlər.

İqtisadiyyatçılar iqtisadi nəzəriyyələri tətbiq etməklə praktiki bazar dizaynlarının formalaşmasında çox böyük uğurlara nail olmuşdurlar. Lakin, problemlər hələ də qalmaqdadır. Dövlət aktivlərinin birdəfəlik hərrəcalarından başqa ən yaxşı dizaynlar hələ də həyata keçirilmir. Misal olaraq Vilyam Vikeri tərəfindən hazırlanmış ikinci qiymət hərracını göstərmək olar. Bu dizayna əsasən iddiaçılar öz təklif etdikləri məbləği göstərirlər. Yekunda ən yüksək qiyməti təklif etmiş iddiaçı ikinci ən böyük məbləği ödəməlidir. Bu cür hərrac nəticələrinin effektiv olması xüsusiyyəti vardır və sadə sövdələşmə prinsiplərini özünə daxil edir. Buna baxmayaraq bu cür dizayn praktikada tətbiqi limitli olmuşdur. İstisna olaraq yalnız Google AdWord layihəsini göstərmək olar. Agentlərdən düzgün qiymətləndirməni tələb edən market dizaynlarının praktikada özünü doğru göstərməmək səbəblərindən biri də aralıq vasitəçilərə olan güvənin çatışmazlığıdır.

Açıq hərrac bu problemi həll edə bilərdi. Lakin, bu problemin həlli çoxlu resurs tələb edir beləki, eyni vaxtda və eyni məkanda bütün iddiaçıları toplamaq çətin və xərcli məsələdir və İnternet üzərindən təşkil olunması praktiki olaraq mümkün deyildir. Paylanmış sistemlər bu müsadirə problemi həll edə bilərlər. Misal olaraq eBay şirkəti istifadəçilərə öz ən böyük təkliflərini göstərmək üçün avtomatik iddaçı xidmətini təklif edir. Mahiyyəti üzrə bu xidmət ikinci qiymət hərrac dizaynını kopyalayır. Bir çox hallarda istifadəçilər avtomatik iddiaçıdan düzgün istifadə etmirlər və öz təkliflərini son dəqiqədə bildirirlər. Bunun səbəblərindən biri güvənin olmaması və ya istifadəmçilərin təkliflərinin düzgün formada təsdiqlənməməsi ola bilər. Paylanmış sistemlərdə ağıllı müqavilələrdən istifadə etməklə təklifləri heç bir şəxsə göstərmədən bir yerdə toplamaq olar. Hərrac bağlanandan sonra isə ağıllı müqavilə qalibi avtomatik formada müəyyən edir və artıq istifadəsi tələb olunmayan məlumatları silir. Ağıllı müqavilələr eyni zamanda iddiaçıların kifayət qədər vasəitlərinin olmasının yoxlanılmasını təmin edir və doğru olmayan iddiaları uzaqlaşdırmaqla hərracın təkrar keçirilməsinin qarşısını alır.

Şəxsiyyətin yoxlanılması məsələsi bütün iqtisadi sistemlər üçün ən vacib məsələdir. İstifadəçilər hər zaman bu və yə digər tranzaksiya yerinə yetirmək istədikdə həmin tranzaksiyanın icrasının düzğün olduğundan əmin olmaq üçün aralıq vasitəçi tərəfindən şəxsiyyətin doğruluğu yoxlanılır. Bu yoxlanış düzgün və qanuni tranzaksiyalarla fraud, rəqəmsal cinayətlər arasında dayanır. Yaxşı fəaliyyət göstərən market şəxsiyyətin yoxlanılmasının güclü olduğu və həmçinin müxtəlif mallar və xidmətlərin izlənməsinə imkan verən sistemlərə söykənir. Cari yoxlanış həlləri ədətən təhlükəli sirlərdən, sənədlərdən və ya aparat təminatında saxlanılan açıq açarlardan asılıdır. Bir çox hallarda aralıq vasitəçilər dövlətlər olur lakin, eyni zamanda müxtəlif özəl təşkilatlar və şirkətlər də bu rolda çıxış edə bilərlər. İnformasiyanın bu vasitəçilər vasitəsilər ötürülməsi çox hallarda məlumat sızıntısına və ya şəxsi məlumatlar digər məqsədlər üçün istifadə olunmasına səbəb ola bilir.

İqtisadiyyat sistemlərində atomar tranzaksiya elə tranzaksiyalara deyilir ki, onları icrası aralıq vasitəçi olmadan bütövlükdə paylanmış registerdə həyata keçirilsin. Bu cür tranzaksiyalara misal olaraq satıcı və alıcı arasında kriptovalyutalar mübadiləsini göstərmək olar. Atomar tranzaksiyaların keçirilməsinə imkan verən Blokçeyn texnologiyası saəyəsində iqtisadiyyət və hesabat səhalərində dəyişilməz audit jurnalı və hesabat işlərinin sadələşdirilməsinə nail olmaq olar. Bu səhalərdə blokchain texnologiyasının tətbiqi ikiqat mühasibat konsepsiyanı genişləndirərək daha açıq, çevik və proqramlaşdırıla bilinən mübadilə platformalarının yaradılmasına imkan yarada bilər. Zaman, zəhmət və resurslara qənaətdən əlavə yüksək funksionallığa malik mübadilə platformamaların hazırlanması ciddi tənzimlənən bazarlara yeni üzvlərin daxil olması üçün şərait yaradır.

2015-ci ildə Bitcoin və digər kriptovalyutalar ətrafında yaranmış həyəcan nəticəsində bir çox, o cümlədən təcrübəsiz və tez bir müddətdə qazanc əldə etmək istəyən investorlar kriptovalyulardan qazanc əldə etmək üçün külli miqdarda yatırımlar etməyə başlamışdırlar. Yatırımlar vasitəsi ilə Bitcoin kriptovalyutasının dəyəri sürətlə artaraq 20,000 ABŞ dolları dəyərini almışdır. Lakin, bir sıra investorlar qazanc əldə etmək məqsədi ilə tez bir sürətdə öz kriptovalyutalarını satmaq qərarına gəlmələri Blokçeyn bazarında iqtisadi köpüyü partlatmışdır. Nəticədə kriptovalyutaların dəyərinin aşağı düşməsi bazara gec gəlmiş investorların yatırımlarını doğrultmadı və bir çoxlarının kriptovalyutalar bazarından uzaqlaşmasına gətirib çıxardı. Kriptovalyutalar bazarının bu cür davranması bir çox individual şəxslər və özəl təşkilatlar üçün Blokçeyn texnologiyası əsasında qurulmuş layihələrin təhlükəli olması barədə məlumat verirdi. Lakin, tərcübəsiz investorların bazarı tərk etməsi və yeni innovativ fikirlərin daxil edilməsi kriptovalyutalar bazarının stabilləşməsinə səbəb oldu. Artıq uzun müddətdir ki, müxtəlif kriptovalyutaların ABŞ dolları ilə müqayisədə özünü stabil aparması individual şəxslər və müəssisələrin yenidən Blokçeyn şəbəkəsinə inamını artırmış oldu.

Hal-hazırda dünyada ən məşhur Blokçeyn şəbəkəsi Bitcoin şəbəkəsinin olmasına baxmayaraq bundan başqa da Blokçeyn şəbəkələri də mövuddur. Onlara misal olaraq Ethereum, Ripple və s. kimi şəbəkələri göstərmək olar. Bu şəbəkələr imkanlarına görə bir-birlərindən fərqləndiyindən onların tətbiq sahələri də müxtəlif ola bilər. Əsas məqəsdi banklar arası transferləri reallaşdırmaq üçün yaradılan şəbəkə Ripple şəbəkəsi olmuşdur. Ripple şəbəkəsinin əsas fərqləndirici xüsusiyyəti onun istifadəçilərinin heç bir rəqəmsal valyutadan istifadə etmədən istənilən valyutada transferlər edə bilməsidir. Ripple texnologiyası Silikon vadisində əsas məqəsdi pul daşınmalarının yüsək sürətlə yerinə yetirilməsini təmin etmək olan Ripple Lab şirkəti tərəfindən yaradılmışdır. Bu texnologiyanın istifadəçiləri bir-birləri ilə müxtəlif valuyatalarda ticarət etmək imkanına malikdirlər. Məsələn USD valyutasında göndərilən ödəniş digər tərəfdən YEN valyutası formasında qəbul edilə bilər. Lakin, bu cür bir-başa transferlər yüksək tələbə malik valyutalar arasında ola bilər. Az tələb olunan valyutalarla transfer zamanı isə istifadəçilər konvertasiya üçün Ripple şəbəkəsinin rəqəmsal valyutası olan XRP-dən istifadə etməli olacaqlar. Adətən az tələb olunan valyutalarla transferlər zamanı bir neçə mərhələli konvertasiyalar olur. Ripple-in təklif etdiyi forma ilə isə bu prosesi bir mərhələdə görmək imkanı əldə olunur. Digər Blokçeyn şəbəkələrindən fərqli olaraq Ripple müxtəlif iqtisadi institutlardan, o cümlədən banklardan, likvidlik təminatçılarından və ödəniş sistemlərindən asılıdır. Şəbəkənin valyuta konvertasiyaları və transfer sürəti bu iştirakçıların birgə fəaliyyətdən asılıdır. Ripple şəbəkəsi əvvəldə qeyd olunan valyutalardan əlavə digər rəqəmsal valyutaları və eyni zamanda fiziki mallar olan gümüş və qızılla olan ödənişləri də dəstəkləyir.

Bu nəticəyə gəlmək olar ki, Bitcoin şəbəkəsi insanların bir-birləri ilə ödəniş etmələri üçün yaradılmış sosial şəbəkə olduğu halda Ripple şəbəkəsi iqtisadi institutlar üçün ənənəvi transferlərini daha da sürətli və geniş formada apara bilməsi üçün yaradılmış global Blokçeyn şəbəkəsidir. Ripple şəbəkəsi elə formada dizayn olunmuşdur ki bu sistemdən istifadə edən iqtisadi institutlar onun

imkanlarını öz qanun və normativlərinə uyğunlaşdıra bilərlər.

Hal-hazırda konkret bir kriptovalyutanın qəbul olunması onun texniki imkanlarının iqtisadiyyatda nə qədər geniş istifadə tətbiq oluna biləcəyindən asılıdır. Bu konteksdə Ripple şəbəkəsinin saniyədə 15 tranzaksiya emal edən Ethereum və saniyədə 3-6 tranzaksiya emal edən Bitcoin şəbəkəsi ilə müqayisədə 1500 tranzaksiya emal edə bilməsini qeyd etmək lazımdır. Bu rəqabət effektivlik nöqteyi nəzərdən vacib olsa da, şəbəkələrin istifadə rahatlığı, likvidlik və şəbəkənin miqyası özündə daha çox dəyər kəsb edir.

1.2 Blokçeyn sistemləri və ənənəvi rəqəmsal sistemlərinin müqayisəsi

Bazarlar alıcılar və satıcılar arasında könüllu mal və xidmətlər mübadiləsini asanlanlaşdırır. Bir əməliyyatın uğulu başa çatması üçün mübadilədə iştirak edən tərəflərin mübadiləni təsdiqləməsi əsas şərtdir. Mübadilə tərəflər arasında şəxsən baş verdikdə alıcı nəğd pulu birbaşa satıcıya verə bilər və satıcı pulun orijinallığını yoxlaya bilər. Bu ssenaridə vəsitəçi olaraq istifadə olunan valyutanı dəstəkləyən mərkəzi bank çıxış edir. Əməliyyat şəbəkə üzərindən onlayn formada yerinə yetirildikdə isə bu cür mübadilə bir neçə aralıq maliyyə vasitəçilərinin təsdiqi vasitəsilə həyata keçirilir. Vasitəçilərin iqtisadi sistemlərə daxil etdikləri əsas dəyər informasiya asimmetriyasını aradan qaldıraraq mübadilədə iştirak edən tərəflərin informasiyalarının tamlığının qorunmasıdır. Bu əksər hallarda iştirakçıların monitorinqini, etibarlı sistemlərin dəstəklənməsini və müqavilə şərtlərinin icrasını da özünə daxil edir. Bazarlar miqyasına və coğrafi olaraq əlçatanlığına görə genişləndiyindən əvvəlcədən bir-birləri ilə heç bir əlaqəsi olmamış tərəflərin hansı bir dəyər kəsb edən malların və ya xidmətlərin mübadiləsi zamanı təhlükəsizliyi və informasiya tamlığının qorunmasını təmin etmək məqsədilə aralıq vasitəçilərdən daha çox asılı olduqlarından yoxlanış və təsdiqləmə xidmətləri daha çox dəyər əldə etmiş olurlar. Bu cür yoxlanış və təsdiqləmə xidmətlərin dəyəri yüksək olduğu halda bazarın əlçatanlığı aşağı düşür. Vasitəçilər bir-birləri ilə birbaşa effektiv mübadilə apara bilməyən tərəflər üçün bu cür xidmətlər qarşılığında müəyyən

ödəniş tələb edirlər.

Vasitəçilər üzərindən yerinə yetirilən mübadilələr zamanı həmişə üçüncü şəxslərin mübadilə məlumatlarına baxış imkanı olduqlarından bu məlumatların daha sonra digər məqsədlər üçün istifadə olunmaması ehtimalı aşağı düşür. Üstəlik sosial və iqtisadi proseslərin rəqəmsallaşmasının sürətlə inkişaf etdiyi bir dövrdə informasiya təhlükəsizliyinin təmini daha problemli olmuş və məlumat sızıntıları daha da artmışdır. Klassik nümunə olaraq kredit kartları məlumatların və sosial təhlükəsizlik nömrələrinin oğurlanmasını misal göstərmək olar. Blokçeyn texnologiyası mübadilə məlumatların təsdiqlənməsi üçün üçüncü bir aralıq vasitəçiyə ötürmədən şəbəkənin təklif etdiyi imkanlarla təsdiqlənməsini təmin edir. Şəbəkə istifadəçilərinin cari tranzaksiya məlumatlarının bir hissəsinin yoxlanılması kiyafət edir ki, mübadilə uğurl yekunlaşdırılsın.

Rəqəmsallaşdırma müxtəlif növ tranzaksiyaların yoxlanılması və təsdiqlənməsi xərclərini nəzərə çarpacaq dərəcədə aşağı salmışdır. Blokçeyn texnologiyası isə öz növbəsində bu xidmətlərin dəyərini sıfra endirdi. Blokçeyn tətbiqetmələri oflayn yazıların və onların rəqəmsal formları arasındakı interfeysdə hələ də müəyyən çəkişmələrə məruz qalır və son mil problemi ilə qarşılaşır. Bu problemə əsasən Blokçeyn texnolgiyasının imkanlarının hüdudları iqtisadi texnologiyalar və kriptovalyuta sahələri ilə limitlənir. Şəbəkə üzərindən yerinə yetirilən zəncirvari transaksiyalar və oflayn formada yerinə yetirilən tranzaksiyaların əlaqəsi üçün innovatik, tamamlayıcı layihələr hazırlanması tələb olunur. Bitcoin Blokçeyn şəbəkəsi vasitəsi ilə sahibkarlığın təsdiqlənməsi və rəqəmsal aktivlərin mübadiləsini aparmaq mümkündur. Bu şəbəkə texniki olaraq istifadəçilərin bir-birlərinə aralıq vasitəçi olmadan Bitcoin göndərilməsini və alınmasını təmin etsə də, offayn formada ödənişlər son mil probleminə gəlib çıxır. Bitcoin mübadilə vahidi kimi limitli olduğundan və fiziki və rəqəmsal dünya arasında rəqəmsal aktivlərin necə istifadə olunmasını idarə edə bilən hiperinfilyasiya dərəcəsinə çatmış dövlətlər devolivasiyadan xilas olmaq üçün Bitcoin-dən istifadə edirdilər.

Rəqəmsal tranzaksiya yaranan zaman bu mübadilədə iştirak edən tərəflərin

müəyyən məlumatları və tranzaksiyanın yaranma tarixi kimi məlumatlar qeyd olunur. Növbəti tədbirlərin icrası faktiki olaraq bu məlumatlar əsasında yerinə yetirilir. Bir sıra tədbirlər təsdiqlənmə üçün əlavə məlumatlar tələb edə bilərlər. Misal olaraq hər hansı bir tranzaksiya icra olunan zaman yaranan problemin həlli üçün tranzaksiyasın məlumatları audit tərəfindən nəzərdən keçirdilməlidir. Audit problemin həlli üçün hazırlanmış daxili prosesin icrası üçün tərəflərdən əlavə məlumatlar tələb edə bilər. Bu cür struktur tərəflər arasındakı problemi həll etmək üçün əlavə xərclər, işçi qüvvəsi və ya digər bir vasitəçi tələb edə bilər. Blokçeyn texnologiyası bu cür problem ortaya çıxdığı zaman məlumatların xərcsiz təsdiqlənə bilməsini təmin edir. Tranzaksiyanın yerinə yetməsi üçün tələb olunan şəbəkədə qeyd olunmuş istənilən atribut və ya məlumat istənilən vaxt və xərcsiz təsdiqlənə bilər. Göründüyü kimi, aralıq vasitəçilərə olan güvən şəbəkənin əsasını təşkil edən proqram təminatı və həmin proqram təminanlarının fəaliyyət göstərdiyi konsensus qaydaları ilə əvəz olunur. Bu qaydalar müntəzəm əsaslarla paylanmış məlumatların həqiqi vəziyyətini dəstəkləyərək tərəflər arasında razılığının necə əldə olunmasını müəyyən edir. Paylanmış məlumat olaraq keçmiş tranzaksiyalar haqqında məlumatlar ola bilərlər. Daha mürəkkəb proqram təminatlarında müəyyən proseslərin icrası üçün paylanmış məlumatlar həmçinin qaydaları əhatə edə bilər. Bu cür proseslər ağıllı müqavilələr adlanır. Ağıllı müqavilələr vasitəsi ilə bir sıra biznes prosesləri Blokçeyn şəbəkəsi üzərindən aparmaq olar. Müxtəlif təşkilatlar bir sıra tranzaksiyaların icrasını blokchain şəbəkəsinə köçürərək aralıq vasitəçilərdən azad olmaq və xərcləri minimuma endirmək üçün müxtəlif eksperimentlər aparırlar. Nəticədə bu cür proqramlar rəqəmsal aktivlərin sahibkarlığının və ticarətinin izlənməsinin xərcləri bazar iştirakçılarının güclərini itirmədən aşağı saldığıdan cari işçilərin tamamlayıcısı rolunu almağa başladılar. Bundan əlavə aralıq vasitəçilər yoxlama və təsdiqlənmələrin avtomatlaşdılırmasına nail olsalar belə normativ qanuna uyğunluqları və bazarın təhlükəsizliyini dəstəkləyərək öz iqtisadi güclərini qoruyub saxlaya bilərlər. Rəqəmsal atributların Blokçeyn şəbəkəsində yoxlanılması ucuz olmasına baxmayaraq oflayn hadisələrlər

onların rəqəmsal təsvirləri arasında əlaqə yaratmaq olduqca xərcli və dəstəklənməsi çətin olan bir prosedurdur. Bu problem identifikasiya və təsdiqlənmə məsələlərinə hədəflənmiş texnologiyanın nəyə görə gec yayıldığını izah edir.

Digər tərəfdən də Blokçeyn texnologiyası rəqəmsal aktivlərin sövdələşmələrinin hesabatını aparmaq üçün istifadə oluna bilər. Konsensus qaydalarına əsasən fəaliyyət göstərən proqram tokenlərin necə yaranmasını, əldə olunmasını və şəbəkənin razılıq vəziyyətinə gəlib çıxmasını müəyyən edir. Token adı altında Blokçeyn şəbəkəsində istifadə olunan və müəyyən dəyər daşıyıcısı olan əsas məhfumu adlandırmaq olar. Avtonom tokenlər üçün tranzaksiya atributlarının yoxlanılması və sadə müqavilələrin tətbiqi xərci olduqca aşağı ola bilər. Bu Bitcoin şəbəkəsində rəqəmsal vahidlərin global formada ötürülməsinə imkan verir. Əlbəttə ki KYC və AML qaydalarına uyğunluğun təmin olunması individual təşkilatlardan oflayn identifikasiya məlumatları ilə Bitcoin şəbəkəsindəki identifikasiya atributları ilə əlaqəsini təmin etməlidirlər. İnsanlar hələ ki Bitcoindən dəyər daşıyıcısı kimi istifadə etməyə üstünlük verirlər.

Digər tərəfdən əgər blokchain şəbəkəsindəki yazı oflayn şəxsiyyətin, xidmətin və onlarla bağlı olan tranzaksiyaların təmsilçisidirsə, bu zaman xərcsiz yoxlanışın əldə olunması çətin məsələdir. Bu ssenariyə əsasən yoxlama xərclərinin aşağı salınması oflayn hadisələrlərlə onların onlayn yazıları arasında uyğunluğun dəstəklənməsi ilə əldə oluna bilinər. EverLedger blockchian şəbəkəsi dəyərli daşların çatdırılma zəncirində izlənməsi üçün rəqəmsal barmaqizi kimi onların fiziki xüsusiyyətlərindən istifadə edir. Bir çox hallarda oflayn hadisələr və onların Blokçeyn şəbəkəsindəki yazıları arasında əlaqənin qurulub saxlanılması olduqca xərcli bir məsələdir. Bundan əlavə bu cür əlaqələrin qurulması üçün güvənilir aralıq vasitəçilər və həmçinin bü cür vasitəçilərin informasiya təhlükəsizliyini təmin edə biləcəkləri müəyyən qaydalar toplusu yaradılmalıdır. Oflayn hadisələr və onların Blokçeyndəki yazıları arasında güclü əlaqənin olmaması informasiya asimmetriyası və mənəvi zədə yaradaraq bazarlara təhlükə ola bilərlər. Bu

kontekstdə İOT (İnformation of thing) cihazları real dünya haqqında məlumatları özlərində saxlaya bildiklərindən Blokçeyn şəkəbəsində avtomatlaşdırıla bilən müqavilə dəstlərinin geniş yayılmasında böyük rol oynaya və ağır iş tələb edən yoxlama məsələlərini ucuz zihazlarla həll etmək imkanı yarada bilərlər. Ümumiyyətlə isə son mil problemi aradan qaldırıldıqda mərkəzləşdirilməmiş yoxlanış bahalı proses olmaqdan ucuz və güvənilir proses olmağa doğru irəliləyəcəkdir. Bu proses tranzaksiya icrası baxımından mərkəzləşdirilmiş sistemlərlə müqayisədə daha çox effektivlik verməsə belə, iqtisadiyyatda rəqabətin artması nəticəsində resusların qorunmasına, daha yüksək məxfilik və yeganə inkar nöqtəsinin aradan qaldırılmasını təmin edə bilər. Eyni zamanda oflayn hadisələr və onların Blokçeyndəki yazıları arasında əlaqə yaratmaq üçün innovasiyalar yaradılmadığı müddətcə aralıq vasitəçilər bu cür əlaqələrin qurulmasını öz qərar verdikləri formada idarə edərək bazarda öz təsir qüvvələrini saxlayacaqdırlar. Mərkəzləşdirilməmiş sistemlərdə yoxlama dəyəri aşağı düşdükcə onların effektiv formada qurulub fəaliyyət göstərmək miqyası da aşağı düşür. Bu cür sistemlərdə informasiyanın tamlığı ilk tranzaksiya atributlarından başlayaraq son tranzaksiyaya atributları əsasında qurula bilər.

Aktivlərin vəziyyətinin aşağı qiymətlərlə yoxlanılması imkanı Blokçeyn protokuluna rəqəmsal aktivlərin tarixçəsi haqqında konsensusa gəlməkdən əlavə şəbəkə üçün dəyərli olan bir vəziyyətdən digərinə keçid qaydalarının müəyyən edilməsi imkanını yaradır. Bu vəziyyət keçidləri şəbəkənin dəyərinin artıran və rifahını yüksəldən şəbəkə üzvlərinin şəbəkədən daha çox istifadəsi üçün təşviq oluna bilər. Protokol şəbəkənin müxtəlif vəziyyətlərdə özünü necə aparması, kifayət qədər resusların olmasının və onun təhlükəsizliyinin yoxlanılması üçün prosesləri simulyasiya etmək imkanı verir. Birlikdə bu stimullar iqtisadi şəbəkənin ilkin yüklənmə, eksplutasiyasını və miqyaslanmasını dəyərini aşağı salır. Vəziyyətin yoxlanılması imkanı iqtisadi agentlərə aralıq vasitəçilərdən asılı olmadan şəbəkə resurslarına sahibkarlıq hüququ verdiyindən yoxlanış dəyərinin aşağı düşməsi şəbəkənin dəyərinin aşağı düşməsi üçün zəruri faktordur. İcazəli

Blokçeyn şəbəkəsində sistemin vəziyyətinin idarə olunması tam olaraq proqram tərərfindən deyil, hər hansı xarici tərəflər tərəfindən idarə oluna bilər. Nəticədə iqtisadi nöqteyi nəzərdən şəbəkə ənənəvi rəqəmsal platformaların fəliyyət göstərdiyi şərtlər daxilində fəaliyyət göstərəcəkdir.

İcazəsiz Blokçeyn şəbəkəsi isə üçüncü bir tərəfin müdaxiləsi olmadan iqtisadi agentlərə ümumi məlumatların vəziyyətini öz aralarında müəyyən etmək imkanı verir. Ümumi məlumatların nələri təmsil etməsi baxımından çevik olması bu texnologyanı ümumi məqsəd texnologiyası (ÜMT) edir. ÜMT-lər bir qayda olaraq iqtisadiyyatda geniş miqyasda yayılmaları uzun müddət çəkir. Lakin, bir çox sahələrdə performansın artmasına gətirib çıxarır. Klassik ÜMT nümunələri kimi daxili yanma mühərrikini, elektrik enerjisini və interneti göstərmək olar. Bir çox hallarda icazəsiz şəbəkələr TCP/İP kimi protokollarla müqayisə olunsalar belə onlar tamamilə müxtəlif məqsədlər üçün yaradılmışdırlar. TCP/İP protokolunun əsas məqsədi marşrutlaşdırma və informasiyanın paketləşdirilməsidir. İcazəsiz şəbəkələrdə platformanın operatoruna olan güvən şəbəkənin fəaliyyət göstərdiyi proqram və konsensusla əvəz olunur. Nəticədə vasitəçilərin təsir gücü, senzura və məxfilik riski azaldıla bilinər. Güvən modelinin dəyişdirilməsi ciddi problemlərə gətirib çıxara bilər. Beləki, proqram təminatının kodunda olan səhv informasiya tamlığının pozulmasına gətirib çıxara bilər. Yeni güvən modeli ilə bağlı olan problemlər proqramlaşdırma səhvlərindən, investorlara heç bir biznes model olmadan böyük qazanc sözü və zərərli hücumlardan irəli gəlir. İcazəli şəbəkələr yoxlama dəyərinin aşağı olmasından faydalandığı halda icazəsiz şəbəkələr vəsitəçilərə güvənmədən şəbəkənin idarəsinin dəyərinin aşağı olmasından da faydalana bilərlər. Şəbəkə xərclərinin aşağı olmasının nəticəsi xüsusən şəbəkənin ilkin yüklənməsində və eksplotasiyasında hiss olunur. Birinci mərhələdə şəbəkənin tokenlərini onun genişlənməsi və dəstəklənməsini gücləndirmək üçün istifadə etmək olar. Məsələn sikkələrin ilkin paylanması və ya şəbəkədə mədənçilik fəaliyyəti ilə məşğul olanlara mükəfat təklif etməklə kapitalın artırılması. İkinci mərhələdə şəbəkə nümayəndələrinin şəbəkəyə yeni resurs daxil etdikləri üçün

qazanc əldə edilən bazar modelinə keçilir. Sistemin ilkin yüklənməsində şəbəkə miqyasının kiçik olması istifadəçilərə digər ənənəvi prinsiplər əsasında fəaliyyət göstərən sistemlərlə müqayisədə eyni imkanları təklif edə bilməyəcəkdir. Bu mərhələdən uğula keçid istifadəçilərin sistemə verdiyi töhfədən və investorların sistemin gələcək dəyərinə gözləntilərinin pozitivliyindən asılıdır. Mənbə kodu açıq olan layihələrdə olduğu kimi ilk istifadəçilər sistemin stabil fəaliyyət vəziyyətinə çatması üçün onun dəstəklənməsinə müəyyən qədər vaxt sərf etməlidirlər. Digər tərəfdən də investorlar ilkin yatırımlarından qazanc əldə edilməsi üçün sistemin tokeninin bazarda dəyərinin qalxmasını gözləməlidirlər. Bu cür sistemlərin tokenlərinin bazarda dəyər alması mələk investorlar və müəssisə kapitalistlərindən yatırım almadaın Blokçeyn startapları qurulan zaman istedadların cəlb olunmasına imkan verir. Sikkələrin ilkin yüklənməsinə sadəcə bir neçə sətirlik kod yazmaqla nail olmaq imkanı, heç bir hüquqi idarəetmənin olmaması və onların bazarda ticarətinin idarə olunması sistemə spekulyatorların cəlbinə səbəb oldu. Nəzəri baxımdan sistemə giriş maneələrinin az və texniki yatırımların olması yeni tip sahibkarlıq növləri üçün kapital açа bilər. Lakin, idarəetmənin olmaması saxtakar proektlərin qanunlarla qarışaraq tərcübəsiz investorların yatırımlası ilə bazarda problemlər yarana bilər. Nəzərə alsaq ki, şəbəkə tokeninin bazar dəyəri şəbəkənin gələcək uğurundan asılıdır, texniki və hüquqi qeyri-müəyyənliklər bazarda riskin yaranmasına və tokenlərinin dəyərinin stabilliyin pozulmasına gətirib çıxara bilir. Bazardə yaranan həyəcan və təcrübəsiz investorların cəlb olunması Blokçeyn texnologiyası ilə fəaliyyət göstərən sistemlər bazarında spekulyar köpük yaratdı. Nəticədə investorların keyfiyyətli layihələrin tapılıb yatırımlar etməsi olduqca çətin bir məsələyə çevrildi.

Əgər birinci mərhələdə sistemin istifadəçilər tərəfindən cəlb olunması və miqyasının genişləndirilməsi məqsəd qoyulmuşdursa, ikinci mərhələdə isə sistemin məqsədi şəbəkə üzvlərinin şəbəkəni dəstəkləməsini davam etdirərək və resurs itkisinə imkan verməyərək şəbəkə ekosisteminin qorunmasıdır. Blokçeyn ideyasına görə protokol səviyyəsi şəbəkənin bütün istifadəçiləri arasında paylanmış əsas

resusrdur. Bu resursun təhlükəsizliyin artılıması, texniki problemlərin aradan qaldırıması, məlumat ötürülməsi sürətinin yuxarı olması şəbəkının bütün istifadəçiləri üçün müxtəlif mənalarda qazanc gətirə bilər. Digər tərəfdən uyğun sistem idarəetməsinin olmadığı halda protokol səviyyəsinin dəstəklənməsi üçün kiyafət qədər yatırım olmaya bilər. Qiymətləndirmə nöqteyi nəzərdən sistemin ilkin yüklənməsi zaman bazardakı qeyri-müəyyənlik sistemin bütün imkanlarının kəşfinə imkan vermir. Nəticədə bazar dəyəri kiçik qiymətləndirilən Blokçeyn startapları daha stabil mərhələyə keçdikləri zamanı bazar dəyərləri yüksək qiymətləndirilir.

Ümumiyyətlə Blokçeynin realizasiyasının hansı ki əsas üstünlüyü yoxlanış dəyərinin aşağı və şəbəkə əlaqələrinin dəstəklənməsi üçün olan xərclərin azaldılması olan dörd əsas ölçüsü vardır. Birincisi, bu sistemlər bazar gücünü sistemin ilkin qurucularının və ilkin iştirakçılarının əlində qalmasına imkan vermir. Bu, şəbəkənin hər hansısa bir üzvünun tranzaksiyaları öz maraqlarına görə bloklaması, digər iştirakçıların sistemdən uzaqlaşdırılması və yalnız bir neçə sistem üzvündən asılı olmadan fəaliyyət aparmağa imkan verir.

İkinci, bu sistemlər planlaşdırıldığı kimi şəbəkə xərclərinin azaldılması üçün digər sistemlərlə müqayisədə xarici idarəetmədən, relyasion müqavilələrdən və öz əməliyyatlarının dəstəkləməsi üçün qanunlardan daha az asılıdırlar. Əlbəttə ki, icazəsiz şəbəkələrdə ziddiyyətlərdin qarşısının alınması üçün oflayn idarəetməyə və maraq tərəflərinin koordinasiyasını təmin etməyə ehtiyac vardır. Lakin, ənənəvi sistemlərlə müqayisədə aralıq vasitəçilərin təsiri azaldılmış və proseslərin bir çoxu proqram təminatının vasitəsi əsasında icra olunur.

Üçüncü, məxfilik riskinin aşağı olması nəticəsində heç bir tərəfin istifadəçilərin məlumatlarına bir-başa baxış imkanı olmur. Ənənəvi sistemlərdə məxfilik riski xüsusən də bazarlarda güclü hiss olunur beləki, istifadəçilərin şəxsi məlumatları və fəaliyyətləri süni intellekt alqoritmlərinin təkmilləşdirilməsində istifadə olunur. İstehlakçıların şəxsi məlumatlarının rəqəmsal xidmətlərdə qapalı qapılar arxasında necə istifadə olunması haqqında necə istifadə olunması gizli olduğundan ənənəvi

rəqəmsal xidmətlər istifadəçilər tərəfindən sorğulana bilinər.

Dördüncü, Blokçeyn sistemlərinin realizasiyası şəbəkə xərclərinin azaldılmasına kömək etsə də, təşkilatların daxili arxitekturasınn dəyişilməsini tələb edir. Arxitektura dəyişiklikləri təşkilatların və ya müəssisələrin insan resusrlarının illərlə qazanılmış biliklərinin dəyərinin aşağı düşməsinə və dəyərlərin dəyişilmısinə səbəb ola bilər. Bu cür dəyişikliklər təşkilatların və ya müəssisələrin yeni biznes modelinə keçidinə və bazarın imkanlarının mənimsədilməsinə imkan yaradır. Ənənəvi rəqəmsal marketlərdə platformanın operatorları əlaqələri izləmək üçün böyük görmə qabiliyyətinə malikdirlər və istifadəçilər aktivləri saxlayıb idarə etməyi və onların ticarəti ilə məşğul olmağı birbaşa yerinə yetirə bilməzlər. Bu, bu cür sistemlərdə rəqəmsal aktivlərin sahibkarlığının müəyyən edilə bilinməməsinin nəticəsidir. Bitcoindən əvvəl heç bir mərkəzi hesabat palatası olmadan rəqəmsal pulların ikiqat xərclər probleminin və kopyalanmağın qarşısını almaq mümlün deyil idi. Bitcoin bu problemi rəqəmsal tokenlərin idarəsini heç bir üçüncü şəxsə vermədən istifadəçilərin özlərinə verir. Bu rəqəmsal cüzdanlar arasında mübadilə dəyərinin aşağı olmasını və məxfiliyi təmin edir. Blokçeyn sistemləri istifadəçilərə vasitəçi olmadan tranzaksiyalar yerinə yetirmək imkanı versə belə, bu sistemlərin mərkəzləşdirilmiş sistemlərdən fərqli olan rahat istifadəçi interfeysləri yoxdur. Bitcoin istifadəçiləri öz şəxsi açarlarını özlərində saxlaya bilmələrinə baxmayaraq bir çox istifadəçilər bir sıra onlayn Blokçeyn cüzdanlarından istifadə edirlər. Bu da öz növbəsində ənənəvi sistemlərdən fərqlənmir.

Beləliklə, bazarların inkişaf etməsi üçün iştirakçılar hesabat məlumatları, tərəflərinin nüfuzu, mübadilə olunan aktivlərin xarakteristikaları və müqavilələr üçün dəyər kəsb edən hər hansısa bir xarici faktor kimi tranzaksiya atributalarının effektiv yoxlanılması təmin olunmalıdır. Təşkilatların sərhədləri xaricində bu yoxlanışlar vasitəçilər vasitəsi ilə aparılır. Bazardakı bütün tranzaksiyalara nəzarət etmək bacarıqlarına görə öz xidmətləri qarşılığında onlar müəyyən qazanc əldə edirlər. Bu cür informasiya üstünlüyü qazanan vasitəçilər bazarda digər iştirakçılar üzərində gücə sahib olurlar. Nəticədə bazarda məxfilik riski, yeganə inkar mərkəzi,

innovasiyalara maneələr və yüksək xərclər yaranmış olur. Blokçeyn texnologiyası isə öz növbəsində şəbəkə və yoxlanış xərclərin azaldılması sayəsində və paylanmış rəqəmsal infrastrukturdan istifadə olunması ilə heç bir tərəfə bazarda monopoliya yaratmaq imkanı verməməklə yeni ekosistemin yaradılmasına imkan verir. Mərkəzi hesabat palatasının olmaması bazara giriş maneələrini azaldır və innovasiyaların yaranmasına şərait yaradır. Proqram təminatları şəbəkə protokoluna uyğun olduqları müddətcə onlar heç bir tərəfin icazəsi olmadan icaraya verilib bazar hissələrinə görə rəqabətə qoşula bilər. Bu ənənəvi rəqəmsal platformalar üzərində proqram təminatı hazırlayan proqramçıların qarşılaşdığı müsadirə riskini azaldır.

İstedadların cəlb olunması baxımından mənbə kodu açıq olan layihələrdən fərqli olaraq kripto tokenlərə əsaslanan layihələr müsqətil şəxslərin zamanla layihələrə edilən qatqılarına əsaslanmamalıdır. Sistemin əsas tokenindən istifadə etməklə proqramçıların və investorların yatırımlarını stimullaşdırmaq olar. Bu cür yeni maliyyə mənbəsinin vasitəsi ilə şəbəkənin miqyasının artırıla bilinməsi üçün və fəaliyyətini təmin edə biləcək yeni şəxslərin cəlb olunmasıda istifadə olunur. Yoxlanış xərclərinin azaldılması nəticəsində bu cür model həmçinin daha kiçik miqyasda yoxlanışların aparılıb daha böyük miqyasda tətbiqinə imkan verir.

Əvvəlki paraqraflarda kredit və nəğd pulun fərqlərindən danışılmışdır və qeyd olunmuşdur ki nəğd pul sisteminin ilkin yüklənməyə ehtiyacı vardır, üstunlüyü isə alıcının borcunu ləğv etməməsi riskindən qaçmaq idi. Bundan əlavə nəğd pul sistemin daha iki üstünlüyü vardır. Birinci anonimlikdir. İstifadəçinin kredit kartı onun adı ilə bağlı olduğundan bank onun bütün xərclərini izləmək imkanına malikdir. Lakin, ödəniş nəğd pulla həyata keçdiyində bankın bundan xəbəri olmur. İkinci, nəğd pul oflayn tranzaksiyaların yerinə yetirilməsi imkanı yaradır beləki, üçüncü şəxsdən tranzaksiyanın təsdiqi barədə xəbərə ehtiyac qalmır.

Bitcoin tam olaraq bu iki xüsusiyyəti təklif etməsə də faydalı olmaq üçün onlara olduqca yaxındır. Anonimlik Bitcoində nəğd pul sistemindəki olduğu kimi deyildir. İstifadəçilər bitcoinlə ödəniş edən zaman öz həqiqi şəxsiyyətlərindən

istifadə etməyə ehtiyac deyildirlər. Lakin, ağıllı alqoritmlər istifadəçinin tranzaksiyalarını ictimai tranzaksiyalar kitabı əsasında bir-birləri ilə bağlayaraq istifadəçinin şəxsiyyətini müəyyən edə bilərlər. Bitcoin həmçinin avtonom rejimdə çalışmır.

Nəğd pullara kriptoqrafiyanın tətbiq edilməsi barədə erkən ideyalar 1983-cü ildə Devid Şaum tərəfindən irəli sürülmüşdü. Onun ideyasına belə bir misal üzərindən baxaq. Fərz edək ki, X şəxsi öz imzası olan vərəqləri paylayır və qeyd olunur ki, bu vərəqlərin daşıyıcıları onları X şəxsinə təqdim etməklə 1 dollara ala bilər. Əgər insanlar X şəxsinin sözünə güvənsələr onlar bu vərəqləri banknot kimi istfadə etməyə başlayacaqlar. Faktiki olaraq banknotlar kommersiya banklarının buraxdıqları borc öhdəlikləri olaraq mövcud olmuşdular. Yalnız yaxın keçmişdə hakimiyyət orqanları banklardan pul kütlələrini mərkəzləşdirmək və hüquqi olaraq almağı tələb etmişdilər.

Bu cür tranzaksiyaları rəqəmsal imzalar vasitəsilə də həyata keçirmək mümkündur. Lakin, bu zaman ikiqat xərc problemi yaranir. Bu problemin məğzi odur ki, istifadəçi müəyyən dəyər kəsb edən virtual valyuta göstəricisi olan məlumatı kopyalayaraq müxtəlif şəxslərə göndərə bilər.

Bu problemi aradan qaldırmağın yolu hər bir vərəqə unikal seriya nömrəsi verilməsidir. İstifadəçi bu cür vərəq əldə etdikdə imzanın həqiqiliyni yoxlayır və moderatordan vərəqdəki seriya nömrəsinin istifadə olunub olunmaması baradə məlumat alır. Moderator öz növbəsində istifadəçini məlumatlandırdıqdan sonra baş dəftərdə həmin seriya nömrəsinin artıq istifadə olunduğunu qeyd edir.

Real həyatda bu cür sistemi qurmaq olduqca çətin olardı. Lakin, rəqəmsal formada reallaşdırmaq olduqca sadədir. Bunun üçün sadəcə olaraq seriya nömrələrini oxuyan və yazan server yaratmaq lazımdır. Yeganə problem o idi ki, bu pullar artıq nəğd pullar deyildi buna görə də onların xərclənməsi barədə olan məlumatlar qeyd olunduğundan istifadəçilərin xərclərini izləmək olurdu. Burada Şaumun innovasiyası daxil olur. Onun fikrinə görə bütün sistemlər anonim olmalıdır. İstifadəçi vərəqdə seriya nömrəsini qeyd etdikdən sonra onu gizləyir.

Daha sonra moderator bu vərəqi imzalayır. Bu cür imzalama kriptoqrafiyada kor imzalama adlanır.

Bu təklif rəqəmsal pullar haqqında ilk ciddi təklif olmuşdu. İlkin olaraq bu sistem işləyirdi amma onun bank kimi hamının güvənəcəyi bir orqan tərəfindən idarə olunacaq mərkəzi servere ehtiyacı var idi. Bundan əlavə bütün tranzaksiyalar bu serverdən keçməli idi. Əgər server çökərsə bütün ödənişlər kəsilmiş olacaqlar. Bir neçə il sonra Şaum digər iki kriptoqraflar - Fiat və Naorla birgə oflayn elektron pul təklif elədilər. İlk baxışdan bu qeyri-mümkün görsənirdi. İstifadəçinin mərkəzi orqana qoşulmadan eyni bir pulu müxtəlif yerlərdə istifadə etmək imkanı olması məsələsi yaranırdı.

Bu təklifə görə, ikiqat xərclərlərin qarşısının alınmasına yox istifadəçinin şəbəkəyə yenidən qoşulması anında onların qeydə alınmasına fokuslanmaq lazımdır. Təyyarələrdə uçan zaman istifadəçilərin öz kredit kartlarından istifadə edə bilmək imkanları da bunun əsasındadır. Tranzaksiyanın emalı avia kompyaniya yenidən şəbəkəyə qoşulduqdan sonra baş verir. Əgər istifadəçinin kartına imtina olunubsa bu zaman istifadəçi avia kompaniyaya (və ya banka) borclu qalır. Ənənəvi iqtisadiyyat sistemı birinci səhvlərin və itkilərin qeyd olunması daha sonra itirilmiş məbləğin qaytarılması və ya cinayətkarın cəzalandırılması ideyası üzərində qurulub.

Şaum Fiat və Naorun ikiqat xərclərin qeydə alınması ideyası olduqca çətin kriqtoqrafiq tapşırıq idi. İstifadəçiyə verilən hər bir rəqəmsal pul onun şəxsiyyətini elə formada kodlaşdırır ki onun özündən başqa heç kim hətta bank belə kodu oxuya bilmir. Hər dəfə istifadəçi pul xərclədikdə pulu əldə edən şəxs ondan kodun istənilən alt çoxluğunu deşifrə eləməyini tələb edir və moderatorlar bunlar haqqında qeydlər aprarırlar. Bu deşifrələmə onların istifadəçinin şəxsiyyətini öyrənməsinə kifayət eləmir. Lakin, hər kimsə eyni pulu iki dəfə xərcləsə gec ya tez iki istifadəçi banka öz nişanları üçün getdikdə bank informasıyaları birləşdirərək həmin şəxsin kimliyini müəyyən edə bilər.

FƏSİL 2. KRİPTOQRAFİYA VƏ KRİPTOVALYUTA

2.1 Kriptoqrafik hash funksiyası

Kriptoqrafiyanın əsas anlayışlarından biri kriptoqrafik hash funksiyasıdır. Bu funksiya aşağıdakı üç xüsusiyyəti özündə saxlayan riyazi funksiyadır:

1. Təyin oblastı istənilən uzunluqlu sətir ola bilər.
2. Qiymətlər oblastı müəyyən qeyd olunmuş uzunluqlu simvolllar ardıcıllığı olmalıdır.
3. Hesablanması effektivdir - verilmiş daxil olunacaq sətir üçün sonlu zaman intervalında çıxış qiyməti almaq olur. Daha texniki şəkildə söyləsək n bitlik sətrin hesablanma vaxtı O(n)-ə bərabər olmalıdır.

Bu xüsusiyyətlər hash cədvəllər kimi verilənlərin strukturunun yaradılmasında istifadə olunan ümumi hash funksiyasını təyin edirlər. Hash funksiyaların kriptpqrafik təhlükəsiz olması üçün onlar əlavə üç xüsusiyyətə malik olmalıdırlar: toqquşmalara dayanıqlılıq, gizlilik, bulmacayönlülük. Qeyd etmək lazımdır ki kriptoqrafik hash funksiyası standart hash funksiyalardan biraz fərqlənir. Bulmacayönlülük xüsusiyyəti xüsusi halda hash funksiyalar üçün ümumi tələb deyildir lakin, kriptovalyutalar üçün xeyirlidir.

Toqquşmalara dayanıqlılıq. Kriptoqrafik hash funksiyalardan birinci istənilən onların toqquşmalara dayanıqlı olmasıdır. Toqquşmalar o zaman baş verir ki iki müxtəlif giriş veriləni daxil olunan zaman hash funksiya eyni bir nəticəni qaytarsın. H(x) funksiyası o zaman toqquşmalara dayanıqlı adlanır ki təyin oblastının istənilən iki fərqli qiymətlərində funksiyanın qiyməti bərabər olmasın.

Ixtiyari z,y üçün H(z)!=H(y)

Paraqrafın əvvəlində qeyd olunmuşdu ki, hash funksiyanın təyin oblastı istənilən uzunluqlu sətir qiymətlər oblastı isə müəyyən qeyd olunmuş uzunluqlu simvollar ardıcıllığıdan ibarətdir. Bu xüsiyyətlərdən aydın olur ki, hash funksiyanın təyin oblastı sonsuz çoxluq qiymətlər oblastı isə sonlu çoxluqdur.

Təyin oblastı qiymətlər oblastından böyük olduğundan Dirixle prinsipinə görə elə iki və ya daha çox giriş veriləni var ki onların daxil olunması zamanı toqquşmalar qaçılmazdır.

Qeyd etmək lazımdır ki Dirixle prinsipi aşağıdakı kimidir:

Əgər nk+1 sayda elementdən ibarət çoxluq k sayda altçoxluğa ayrılsa ən azı bir altçoxluqda n+1 sayda element olacaqdır (n,k ixtiyari natural ədəddirlər).

Misal olaraq 256 bitlik çıxışa malik hash funksiyası götürək. 2^{256} + 1 sayda fərqli giriş verilənləri üçün hash funksiyanın qiymətlərini hesablayaq. Giriş verilənlərinin sayı mümkün çıxış qiymətlərinin sayından çox olduğundan bəzi çıxış qiymətləri eyni olacaqdır.

Yuxarıdakı misalda toqquşmanın olacağı dəqiqdir. Faktiki olaraq 2^{130} + 1 sayda giriş verilənləri üçün ən azı ikisinin toqquşma ehtimalı 99,8%-ə bərabərdir.

Növbəti toqquşmaları qeyd edən alqoritm bütün hash funksiyaları üçün keçərlidir. Lakin, problem ondadır ki onları qeyd etmək çox uzun vaxt alır. 256 bitlik çıxışa malik hash funksiya üçün ən pis halda 2^{256}+ 1 sayda orta halda isə 2^{128} sayda hesablama aparmaq lazımdır. Sözsüz ki bu ədədlər astronomik ədədlərdirlər. Əgər kompüter saniyədə 10 min qiymət hesablasa 2^{128} qiymətin yoxlanılmasına bir oktilion (10^{27}) il çəkəcəkdir. Başqa sözlə dünyada olan bütün kompüterlər kainatın yarandığı andan hesablamalar aparsalar belə toqquşmanın tapılması ehtimalı çox aşağıdır. Hətta Dünyanın növbəti iki saniyədə meteorit tərəfindən dağıdılması ehtimalından belə azdır.

Bu metodun praktiki olaraq əhəmiyyətinin olmadığı açıq-aşkar görsənir. Buna görədə hər bir konkret hash funksiyası üçün özəl metodun tapılması məqsədə uyğundur.

Misal olaraq növbəti hash funksiyaya baxaq:

$$H(x) = x \bmod 2^{256}$$

Bu funksiya hash funksiyaya qoyulan tələbləri ödəyir. Beləki, təyin oblastı istənilən uzunluqlu sətir, qiymətlər oblastı isə 256 bitlik simvollar ardıcıllığıdır və hesablanması olduqca effektivdir. Həmçinin toqquşmaları qeyd etmək üçün

effektiv axtarış metodu vardır. Bu funksiya sadəcə olaraq giriş verilənin son 256 bitini qaytarır. Deməli ixtiyari x üçün toqquşma arqumentin $x + 2^{256}$ qiymətində olacaqdır. Bu sadə misal praktikada istifadə oluna bilinməyəcək ümumi metoddan əlavə elə hash funksiyaların olduğunun göstəricisidir ki onlarda toqquşmaların qeyd olunması üçün effektiv metodlar var.

Praktikada istifadə olunan kriptoqrafik hash funksiyalar sadəcə funksiyalardır hansı ki toqquşmaların tapılması olduqca çətindir. Bəzi hallarda köhnə MD5 hash funksiyasında uzun illərdən sonra toqquşma qeydə alınmışdır. Buna görə də bu funksiya köhnəlmiş hesab olunur və praktiki olaraq istifadə olunmur.

Gizlilik. Hash funksiyalardan tələb olunan ikinci xüsusiyyət gizlilikdir. Bu xüsusiyyət ondan ibarətdir ki, əgər y=H(x) funksiyasının çıxış qiyməti verilibsə ona uyğun giriş verilənini müəyyən etmək olmur. Problem ondadır ki bu xüsiyyət qeyd olunduğu kimi həqiqi deyil.

Hash funksiya gizli sayılır: gizli kəmmiyyət olan r yüksək minimum entropiyası olan ehtimal paylanmasından seçiləndə H(r || x)-ə görə x dəyişəninin qiymətini müəyyən etmək olmur. (|| konkatensiya əməliyatıdır)

İnformasiya teoriyasında minimal entropiya nəticənin nə qədər proqnozlaşdırıla bilinməsi ölçüsüdur. Yüksək minimum entropiya isə intiutiv olaraq paylanmanın çox geniş olması ideyasını əks etdirir. Konkret olaraq bu o deməkdir ki, əgər r 256 bitlik sətirdən bərabər seçilsə onda istənilən konkret sətirin seçilmə ehtimlı $1/2^{256}$-a bərabərdir. Bu ədəd isə sonsuz kiçik ədəddir.

Bulmacayönlülük. Hash funksiyalardan tələb olunan üçüncü xüsusiyyət onların bulmacayönlü olmasıdır. Bu xüsusiyyət digərlərindən biraz mürəkkəbdir.

H hash funksiyası o zaman bulmacayönlü adlanır ki, əgər k yüksək minimum entropiya paylanmasından seçilibsə ixtiyarı n bitlik giriş veriləni üçün 2^n zamandan az vaxtda H(k // x)=y ödəyən x tapmaq mümkün olmasın.

Praktikada mütəlif hash funksiyalar istfadə olunur. Bitcoinin istifadə elədiyi hash funkisya isə məhz SHA-256 funksiyasıdır.

Əvvəl qeyd etmişdik ki hash funkisyaların təyin oblastı istənilən uzunluqlu

sətirlər çoxluğu olmalıdır. Qeyd olunuş uzunluqlu giriş verilənləri üçün hash funksiya qura bildiyimizdən elə bir ümumi çevirmə metodu var ki bu funksiyasını təyin oblastı istənilən uzunluqlu sətirlər çoxluğu olan hash funksiyaya çevirir. Bu çevirmə Merkl-Damqard çevirməsi adlanır. SHA-256 bu çevirmədən istifadə edir. Ümumi terminalogiyada qeyd olunmuş uzuluqlu toqquşmalara qarşı dayanıqlı olan baza hash funksiyası sıxılma funksiyası adlanır. İsbat olunmuşdur ki əgər əsas sıxılma funksiyası toqquşmalara dayanıqlıdırsa onda ümumi hash funksiyası da toqquşmalara dayanıqlıdır.

Merkl-Damqar çevirməsi olduqca sadədir. Fərz edəki ki sıxılma funksiyası m uzunluqlu girişə və n-dən kiçik çıxışa malik bir funksiyadır. Girişi istənilən uzunluqlu olan hash funksiyanın giriş verilənləri m-n uzunluqlu bloklara bölünür. Konstruksiya növbəti qayda ilə çalışır. Hər bir blok giriş ilə birgə sıxılma funksiyasına ötürülür. Bu zaman girişin uzunluğu (m-n)+n=m olur hansı ki sıxılma funksiyasının girişinin uzunluğudur. Birinci blok üçün hansı ki əvvəlki blokun girişi yoxdur inisalizasiya vektoru istifadə olunur. Hər dəfə hash funksiyası çağırılanda bu metoddan istifadə olunur. Son blokun nəticəsi hash funksiyanın nəticəsi olur.

SHA-256 768 bitlik girişə və 256 bitlik çıxışa malik sıxılma funksiyasından istifadə edir.

2.2 Hash göstəricilər və verilənlərin strukturu

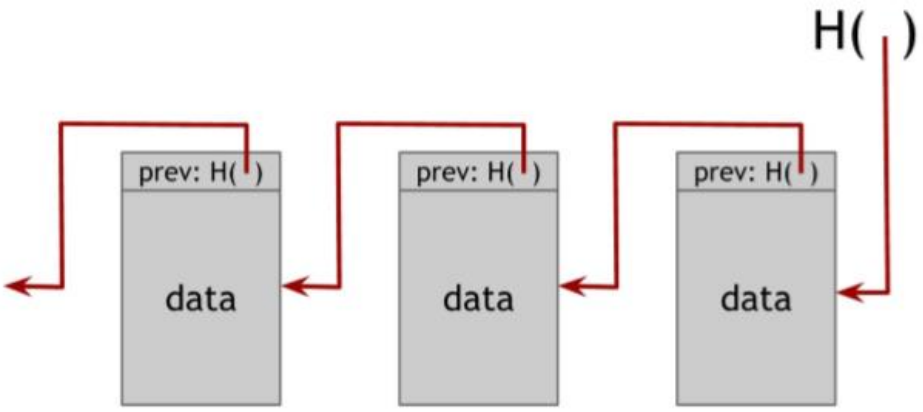
Hash göstəricililər irəlidə bəhs olunacaq sistemlərdə olduqca faydalı olan verilən strukturudur. Hash göstərici sadəcə hansısa informasıyanın kriptoqrafik hashi ilə birgə saxlandığı yerə göstəricidir. Adi göstərici istifadəciyə informasiyanı əldə etmək imkanı verirsə hash göstərici eyni zamanda informasiyanın dəyişib dəyişməməsi barədə də məlumant verir.

Hash göstəricilər ilə istənilən tip verilənlərlər strukturu qurmaq mümkündur. İntiutiv olaraq tanış verilənlər strukturu olan əlaqəli siyahı və ya binar axtarış ağacları götürüb onları hash göstəricilər ilə realizə etmək olar.

Blokçeyn. Aşağıdakı fiqurda hash göstərici istifadə olumuş əlaqəli siyahı əks olunmuşdur. Bu verilənlər strukturunu Blokçeyn adlandıraq.

Regulyar əlaqəli siyahılarda bloklar seriyasında hər bir blok müəyyən informasiyaya və əvvəlki blokun göstəricisinə malikdirlərsə Blokçeyndə bu göstəricilər hash göstəricilər ilə əvəz olunur. Beləliklə, hər bir blok əvvəlki blokun informasıyasının harada olmasından əlavə bu dəyərin rezumesi özündə saxlayır. Bu da öz növbəsində dəyərin dəyişib dəyişməməsini izləmək imkanı yaradır. Biz sadəcə ən sonuncu bloka işarə edən və siyahın başlığı olan hash göstəricini qeyd edirik.

Blokçeyn



Şəkil 2.1

Blokçeyndən istifadə variantlarından biri jurnaldır. Yəni elə bir strukturdur olmalıdır ki, özündə böyük həcmli informasiya saxlasın və yeni məlumatları jurnalın sonuna əlavə etməyə imkan versin. Əgər kimsə jurnalda olan əvvəlki məlumatları dəyişməyə çalışsa onu qeyd etmək mümkün olsun.

Blokçeynin nəyə görə bu strukturda olmasını başa düşmək üçün belə bir suala baxmaq lazımdır. Kimsə zəncirin ortasındakı məlumatlara müdaxilə etsə nə baş verəcək? Xüsusi halda həmin şəxsin məqsədi bunu elə yerinə yetirməkdir ki, hash göstərcini ağlında saxlayan istifadəçi falsifikasiyanı qeydə ala bilməsin. Bu məqsədinə çatmaq üçün həmin şəxs k blokunda dəyişiklik edir. k blokunda

məlumatlar dəyişdiyindən k+1-dakı hash yenilənməli olacaq. Qeyd etmək lazımdır ki, hash funksiya toqquşmalara dayanıqlı olduğundan statik olaraq yeni hash-in kontentin dəyişməsi ilə uyğun olmayacağına zəmanət verilib. Buna görə də k blokundankı məlumatla k+1 blokunun hash göstəricisi arasında uyğunsuzluq olacaqdır. Bloka müdaxilə edən şəxs işinə davam edərək növbəti blokun hash-inin dəyişməsini gizlətməyə çalışa bilər, amma bu strategiya siyahının başına gəib çatdıqda uğursuzluqla nəticələnəcəkdir. Xüsusi halda istifadəçi siyahının başında olan hash göstəricini özündə saxlayırsa həmin şəxs onu dəyişə bilməz. O özünü göstərməmiş heç bir blokda dəyişiklik edə bilməz.

Nəticədə kimsə zəncirə müdaxilə etməyə çalışsa o zəncirin əvvəlinə qədər bütün hash göstəriciləri dəyişməli olacaqdır və ən sonda kontrol punktu ilə qarşılaşmalı olacaq, çünki o siyahının başına müdaxilə edə bilməz. Aydın olur ki, sadəcə başlıq hash göstəricini yadda saxlamaqla bütün siyahının hash açılışını yadda saxlamaq olur. Beləliklə, özündə istənilən sayda blok saxlayan blok zənciri qurmaq olar. Siyahının başında olan xüsusi blok mənşə bloku adlanır. (Şəkil 2.2)

Aşağıdakı Javascript dilində yazılmış kod nümunəsi Blokçeynin əsas xüsusiyyətlərini özündə əks etdirir.

```
const SHA256 = require('crypto-js/sha256')
class Block{
        constructor(index,timestamp, data, previousHash = ' '){
            this.index=index;
            this.timestamp=timestamp;
            this.data=data;
            this.previousHash=previousHash;
            this.hash=this.calculateHash();
                }
        calculateHash(){
            return SHA256(this.index + this.previousHash + this.timestamp +
```

```
            JSON.stringify(this.data)
        }
}
class Blockchain{
    constructor(){
        this.chain = [this.createGenesisBlock()];
    }
    createGenesisBlock(){
        return new Block(0, ’01/01/2018’, ‘Genesis block’. ‘0’);
    }
    getLatestBlock(){
        return this.chain[this.chain.length-1];
    }
    addBlock(newBlock){
        newBlock.previousHash = this.getLatestBlock().hash;
        newBlock.hash = newBlock.calculateHash();
        this.chain.push(newBlock);
    }
}
```

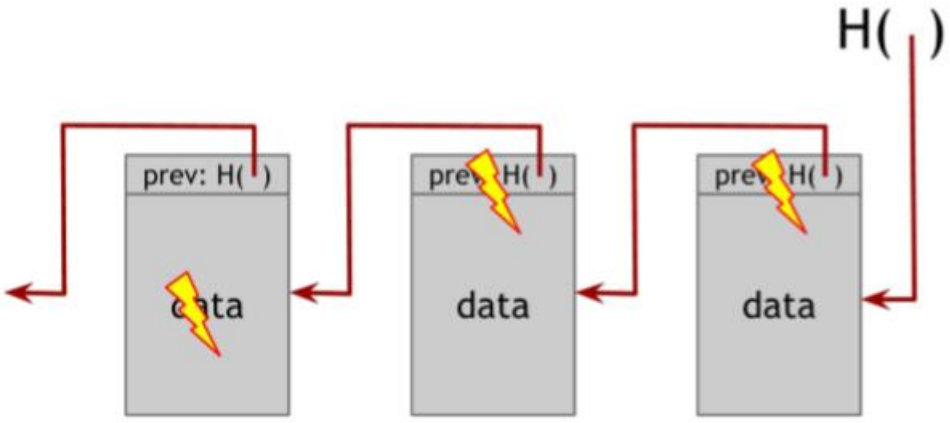
Blokçeyn konstruksiyası qeyd etdiyimiz Merkl-Damqard konstruksiyası ilə çox oxşardır. Eyni təhlükəsizlik arqumenti hər ikisində də tətbiq olunur.

Merkel ağacları. Hash göstəricilər ilə qurula bilən digər faydalı verilənlər strukturu hash göstəricili binar ağaclarıdır. Bu ağaclara başqa adla Merkel ağacları da deyilir. Fərz edək ki özündə məlumat saxlayan bir neçə blok vardır. Bu bloklar ağacın yarpaqlarını özündə saxlayırlar. Bu verilənlər blokları iki-iki qruplaşdırılır. Daha sonra hər bir cüt üçün iki hash göstəriciyə malik verilənlər strukturu yaradılır.

Bu verilənlər strukturu ağacın ikinci səviyyəsini yaradır. Sonra onlar cüt-cüt

qruplaşdırılaraq hashlarını özündə saxlayan yeni verilən strukturu yaradılır. Proses bu qayda ilə bir blok alınana qədər davam olunur. Həmin blok ağacın kökü olur. Əvvəlki kimi yalnız ağacın kökündəki hash-i yadda saxlamaqla hash göstəricilərdən keçməklə ağacın istənilən yarpağına getmək olur. Kimsə yarpaqlarda dəyişiklik etməyə çalışsa avtomatik olaraq olan blokun hash-i dəyişdiyindən üst səviyyədəki blokun hash göstəricisi ilə eyni olmayacaq. Bu bizə məlumatların dəyişilməməsindən əmin olmağa imkan verir. Həmin şəxs üst səviyyədəki blokun hash göstəricisini dəyişməyə çalışsa bu zaman ondan üst səviyyədəki blokda da dəyişiklik olacaqdır. Bu cür davam edən şəxs nəticədə ağacın kökünə gəlib çıxacaqdır. Kökdəki hash-i dəyişdirə bilmədiyindən isə ağacın istənilən blokuna müdaxilə uğursuzluqla nəticələnəcəkdir.

Müdaxilə olunmuş Blokçeyn



Şəkil 2.2

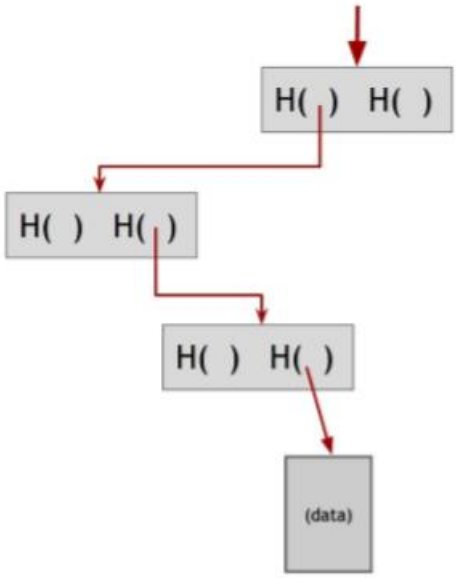
Merkel ağacıın Blokçeyndən digər bir üstünlüyü isə ondan ibarətdir ki, hər hansısa blokdakı məlumatdan istifadə etmək üçün uyğun təpələrdən keçərək məlumatın yerləşdiyi bloka ağacın qalan hissəsini inkar eləməklə çatmak mümkündur.

Əgər ağacda n təpə varsa bu zaman log(n) obyekt göstərilməlidir. Hər addımda övlad blokun hash-ini hesablamaq tələb olunur. Hesablama təxminən log(n) qədər

vaxt alır. Buna görə də Merkel ağacında çox böyük sayda blok olsa belə hər hansısa bloka olduqca qısa zaman anında müraciət etmək olar. Beləliklə, müraciətin zamanı təpələrin sayının loqarifmi ilə hesablanır.

Nizamlanmış Merkel ağacı elə ağaca deyilir ki, aşağı blokları hər hansısa nizamlama funksiyasına görə nizamlanmış olsun. Bu funksiya əlifba, leksiki, ədəd və ya digər xüsusiyyətə görə nizamlama aparan funksiya ola bilər.

Merkel ağacı



Şəkil 2.3

Nizamlanmış Merkel ağacı hər hansısa obyektin ağaca daxil olub olmamasını loqarifmik zamanda yoxlamaq imaknı verir. Başqa sözlə konkret blokun ağacda olub olmamasını isbat etmək mümkündur. Bunun üçün sadəcə həmin blokdan əvvəlki və sonrakı bloklara yolu göstərmək lazımdır. Əgər bu iki blok ardıcıl olarlarsa bu əldə olan blokun ağaca daxil olmamasının isbatıdır. Daxil olsa idi həmin iki blokun arasında olmalı idi.

Hash göstəricilərin binar ağaclarda və əlaqəli siyahılarda istifadəsindən bəhs edərkən onu da qeyd etmək lazımdır ki, bir qayda olaraq hash göstəriciləri istənilən

verilənlərin strukturunda dövr olmayana qədər istifadə etmək olar. Əgər verilənlərin strukturunda dövr varsa bu zaman bütün hash-ları tapmaq alınmayacaqdır. Bunun səbəbi isə əks hesablama aparmaq üçün dövrün sonunun olmamasıdır.

FƏSİL 3. MƏRKƏZLƏŞDİRİLMİŞ VƏ MƏRKƏZLƏŞDİRİLMƏMİŞ PROQRAMLAR, BLOCKCHAİN TEXNOLOGİYASININ TEXNİKİ SƏVİYYƏDƏ ARAŞDIRILMASI

3.1 Mərkəzləşdirilməmiş şəbəkə və Mərkəzləşdirilməmiş verlilənlər

Proqram bu və ya digər məqsədlər üçün müəyyən proqramlaşdırılma dilində yazılmış əmrlər ardıcıllığıdır. Dünyada hal-hazırda milyonlarla proqram təminatı vardır. Onların əksər hissəsi mərkəzləşdirilmiş klient-server modelini realizə edir. Bir çox proqramlar paylanmış modeli və çox az bir qismi olan ən yeni proqramlar isə mərkəzləşdirilməmiş modeli realizə edir.

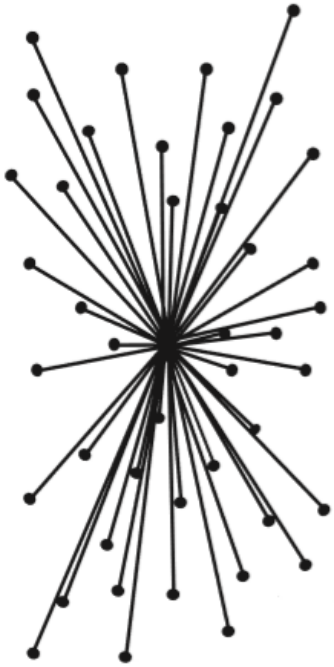
Müasir günümüzdə mərkəzləşdirilmiş model ən çox yayılmış model sayılır. Mərkəzləşdirilmiş sistemlər ayrı-ayrı blokların işlərini idarə edir və bütün informasiya yeganə mərkəzdən keçir. Ayrı-ayrı stansiyalarının işi birbaşa mərkəzin informasıyanı qəbul edib-göndərmək potensialından asılıdır. Facebook, Amazon, Google və digər hegemon xidmətlər internetdə bu model əsasında realizə olunublar.

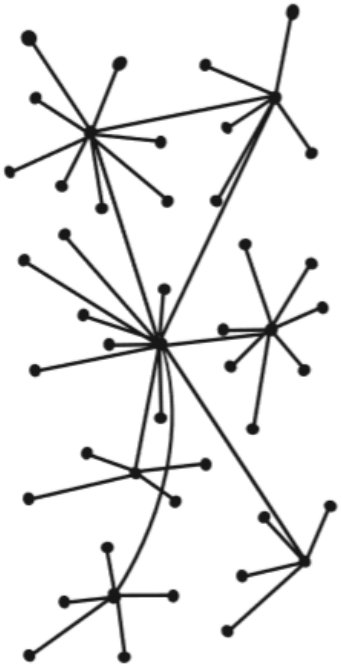
Müasir günümüzdə mərkəzləşdirilmiş model ən çox yayılmış model sayılır. Mərkəzləşdirilmiş sistemlər ayrı-ayrı blokların işlərini idarə edir və bütün informasiya yeganə mərkəzdən keçir. Ayrı-ayrı stansiyalarının işi birbaşa mərkəzin informasıyanı qəbul edib-göndərmək potensialından asılıdır. Facebook, Amazon, Google və digər hegemon xidmətlər internetdə bu model əsasında realizə olunublar.

Bəs sistem eyni zamanda həm paylanmış həm də mərkəzləşdirilməmiş ola bilər

mi? Bəli bu mümkündür. Bu cür sistemə misal olaraq Bitcoin sistemini misal göstərmək olar. Bitcoin sistemi tranzaksiyalar jurnalı, bloklar zənciri çoxlu sayda kompüterdə saxlanılan paylanmış sistemdir. Bitcoin həm də mərkəzləşdirilməmiş sistemdir. Çünki sistemin hər hansısa düymü öz fəaliyyətini dayandırsa belə sistem öz fəaliyyətini davam etdirəcək. Beləliklə, hansısa pirinq texnologiyası ilə birgə Blokçeyndən istifadə edən istənilən sistem eyni zamanda həm paylanmış həm də mərkəzləşdirilməmiş ola bilər. Qeyd etmək lazımdır ki mərkəzləşdirilmiş sistemlər də həm də paylanmış ola bilərlər.

Mərkəşləşdirilmiş **Mərkəzləşdirilməmiş** **Paylanmış**





Şəkil 3.1 Şəkil 3.2 Şəkil 3.3

Mərkəzləşdirilməmiş sistemlərin tədqiqat sahəsi aktiv şəkildə formalaşdırılır və onun inkişaf etdirilməsində müxtəlif modellərlə eksperiment aparan çoxlu sayda mütəxəssis iştirak edir. Fərqli mütəxəssislər mərkəzləşdirilməmiş sistemlərin nə olması barədə fərqli təsəvvürə malikdirlər.

İlkin mərhələlərdə Dünya toru demək olar ki, praktiki əhəmiyyət daşımırdı və vahid mərkəzə malik deyildi. HTTP protokolu planetdə bütün internetə çıxışı olan cihazları birləşdirir. Öz işində HTTP protokolu çoxsaylı güvənli serverlərə söykənir. Bundan əlavə HTTPS protokolu güvənli serverlərə və sertifikasiya mərkəzlərinə daha bir səviyyə əlavə edir. İnsanlar başqalarının da qoşulub məlumat saxlaya biləcəyi öz şəxsi serverlərini quraşdırmaq və işlətmək imkanı əldə etdilər. Daha sonra server proqramları yaranmağa başlandı. Bununla da yaxşı tanınan verilənlərin mərkəzləşdirilmiş idarə arxitekturası yarandı.

Dünya torunun inkişaf mərhələlərin birində Brem Koen tərəfindən BitTorrent protokolu yaradıldı. Bu protokol internetdən böyük həcmli məlumatların yüklənməsi üçün yaradılmışdı. Problem onda idi ki, böyük həcmli məlumatların yüklənməsi çox uzun vaxt alırdı. Dünya torunun sürətlə böyüməsi ilə məlumatların da həcmi böyüyürdü. BitTorrent problemi yükləyicilərdən paylayıcılara çevirərək həll etdi. Əgər istifadəçiyə hər hansısa məlumat lazımdırsa, onu bir yox bir neçə mənbədən yükləyə bilər. Məlumat nə qədər populyardırsa, bir o qədər də çox istifadəçi onu yükləmişdir və uyğun olaraq paylamışdır. Mənbələr nə qədər çox olarsa yüklənmə sürəti də bir o qədər çox olar. Siderlər (faylları ilkin yayan və ya onları bütünlüklə yükəyən şəxslər) mükafat olaraq daha yüksək sürətlə yüklənmə qazanırdılar. Liçerlər (şəbəkədən daha çox istifadə edib amma az resurs göndərən şəxslər) isə əksinə yükləmə sürətinin məhdudlaşdırılması ilə cəzalandırılırdılar. Başqa sözlə verilənlərin ötürülməsi sistemi sən-mənə, mən-sənə prinsipi əsasında təşkil olunmuşdu. Bu metod böyük həcmli mediafaylların paylanmasında öz effektivliyini sübut etmişdir. Sırf bu səbəb asılı olaraq BitToreent protokolu inkişaf etməyə davam edir.

Mərkəzləşdirilməmiş verilənlər ən vacib anlayışlardan biridir. Müasir günümüzdə insanlar öz məlumatlarını iri şirkətlərə güvənirlər və həvəslə onları pulsuz xidmət qarşılığında dəyişirlər. İnsanlar həmçinin öz məlumatlarının saxlanması üçün müəyyən qədər ödəniş də edirlər. Onlar inanırlar ki həmin şirkətlər bu məlumatları başqa məqsədlər üçün istifadə etməyəcəklər. Lakin

Edvard Snouden sübut etdi ki, bu cür şirkətlər istifadəçilərin məlumatlarının gizlilik hüquqlarını pozurlar. Əmək əsasında olan iqtisadiyyatdan informasiya əsasında olan iqtisaqiyyata keçid informasiyaların dəyərinin artmasının bariz nümunəsidir. Belə olduğu halda informasiyaların təhükəsizliyi və gizliliyi ön plana gəlir.

Uzun illərdir ki, informasiyaların mərkəzləşdirilməmiş formada gizlilik və təhlükəsizlik məsələsi mütəxəssislər tərəfindən araşdırılır və bunun üçün bir neçə variant təklif olunmuşdur.

Varinat 1. Məlumatların Blokçeyn bloklar zənciri vasitəsi ilə saxlanılması.

Bu variant ən hiyləsiz variant hesab olunur. Blokçeyn məlumatların mərkəzləşdirilməmiş formada saxlanılması problemini həll edir. Hər bir blokun replikasiyası bütün serverlərdə yerləşir və heç kəs bu bloklarda dəyişiklik edə bilməz. Məlumatların bütün serverlərdə saxlanılması və onun istifadəçin özündən başqa heç kim başa düşməsin bilməsin deyə verilənlərin şifrələnməsi üçün SHA-256 alqoritmindən istifadə olunur. Lakin, Bitcoin bloklar zənciri böyük həcmli informasiyaların emalı üçün nəzərdə tutulmayıb. Onların əsas istifadə məqsədi tranzaksiyalar jurnalının saxlanmasıdır. Blokların yüklənməsi bir neçə gün çəkə bilər, pis miqyaslaşma və blokların şişməsi isə proqramçılar üçün ciddi və həll olunmaz problemə dönə bilər. İstifadəçilər məlumatlarını bloklar zəncirinə köçürməklə Bitcoin maynerlərini həmin məlumatları pulsuz saxlamağa vadar edirlər. Belə olduğu halda maynerlərin xərclərini gəlirlərini aşdığından şəbəkəni dəstəkləmək istəkləri də azalır.

Fərz edək ki, maynerlərin məlumatları saxlamaq üçün xərcləri istifadəçilər tərəfindən hər hansısa vəsait forması ilə qarşılana bilər bu zaman bloklar zəncirin həcmi inanılmaz ölçülərə çatacaqdır. Digər tərəfdən bəşəriyyət bir neçə petabaytın sadə ölçü vahidi kimi görsənəcəyi dövrə döğru irəliləyir. Beləliklə, verilənlərin mərkəzləşdirilməmiş formada bloklar zəncirində saxlanılmasının məqəsədə uyğun olmadığı aydın olur.

Varinat 2. Verilənlərin paylanmış Hash cədvəllərdə saxlanılması.

Paylanmış hash cədvəllər (PHC) son on ildir ki öz məşhurluğunu itirlər. Onlar verilənlərin sürətlərindən əlavə onların axtarışını və etibarlığını təmin edən indeksasiya funksiyalarının sürətlərini də paylayırlar. Napster və Gnutella kimi ilkin fayl mübadiləsi proqramları PHC-in müxtəlif dərəcədə məzkəzləşdirilməmiş şəxsi versiyalarını istifadə edirdilər. Bəziləri bütün verilənlərin yerdəyişməsini izləmək üçün mərkəzləşdirilmiş trekerlərdən, bəziləri isə bütün verilənlərin ötürüldüyü və yalnız bir imtina nöqtəsini təmsil edən mərləzləşdirilmiş mənbələrdən istifadə edirdilər.

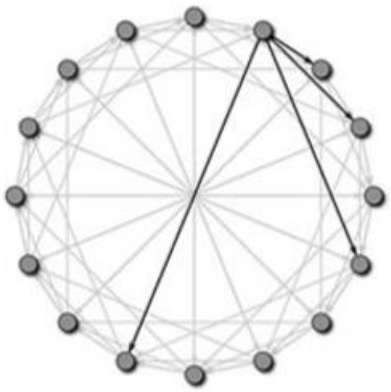
PHC-nin ilk işləyən realizasiyası əvvəlki paraqrafda bəhs edilən BitTorrent protokolu olmuşdur. Bu protokoldan hal hazırda 300 milyon istifadəçi istifadə edir. Verilənlərin mərkəzləşdirilməmiş formada saxlanmasına baxmayaraq BitTorrent hələ də şəbəkənin monitorinqini aparan mərkəzləşdirilmiş trekerlərdən asılıdır. Bu səbəbdən də BitTorrent protokolunun bu qədər etibarlı olmağına baxmayaraq o hər hansı imtina nöqtəsinə malikdir.

BitTorrent verilənlərin mərkəzləşdirilməmiş formada saxlanmasını təklif etmir. O sadəcə paylanmış verilənlərə mən-sənə, sən-mənə prinsipi əsasında yüksək sürətlə girişi təmin edir. Bu o da deməkdir ki, bu protokolun paylanmış hash cədvəllərində mərkəzləşdirilməmiş proqramların verilənlərinin saxlanması məqsədə uyğun deyil. BitTorrentin məlumat saxlamaq üçün istifadəsində problem odur ki, məlumatları çoxlu sayda qovşaqlarda saxlamaq stimulu yoxdur. Şəbəkə elə formalaşdırılıb ki, ən yüksək prioritet ən çox tələb olunan fayla verilir. İnsanlar bir-birinin məlumatlarının replikasiyalarının şəbəkədə uzun müdddət saxlanmasında maraqlı olmalıdırlar. Digər tərəfdən istifadəçilər Amazon Web Services kimi yaxşı reputasiyalı mərkəzi serverdən istifadə edəndə əmin olurlar ki məlumatları itməyəcək. Razılaşmaya əsasən onlar heç nədən asılı olmadan istifadəçilərin məlumatlarını saxlamalıdırlar.

Məlumatların PHC-lərdə mərkəzləşdirilməmiş formada saxlanmasından və məlumatların sürətli ötürülməsindən əlavə onların qorunulmasının qarantiyası lazımdır. Buna görə də istifadəçilərin məlumatları bu və ya digər formada

saxlaması üçün stimul lazımdır. Bundan əlavə məlumatların istinadlarının həqiqilikdən əmin olmaq lazımdır. Qeyd etmək lazımdır ki, bu idea yeni deyil. Bu ideyanı realizasiya edən sistem isə Ümümdünya Fayl Sistemi (İnterplanetary File System İPFS) adlanır. İPFS açıq proekt olub, hal-hazırda alfa versiya mərhələsindədir. Bu layihənin əsas məqsədi verilənlərin şəbəkədə mərkəzləşdirilməmiş formada limitsiz müddətdə saxlanılmasına imkan yaratmaqdır. Başqa sözlə istinadların heç vaxt öz həqiqiliyini itirməyəcək və verilənləri vahid mərkəzsiz idarə edən şəbəkə yaratmaqdır. İstifadəçilər İPFS klientini yükləməklə istənilən məlumatları yükləmək və əvəzində bu məlumatlara baxmağa imkan yaradan hash əldə edirlər.

Chord



Şəkil 3.4

İP ünvanlar əsasında olan Ümümdünya torundan fərqli olaraq İPFS kontent ünvanlanan sistemdir. Əgər İP ünvanlar əsasında olan sistemdə DNS server öz fəaliyyətini dayandırsa onun bütün məlumatları əlçatmaz olacaq. Kontent ünvanlanan sistem isə daha effektiv ünvanlanma formasına malikdir çünki məlumatların əlçatanlığı yeganə bir serverdən asılı deyildir. İstifadəçiyə hansısa məlumat lazım olduqda sistemin məlumatın sürətinin yerləşdiyi ən yaxın qovşaqa marşrut yaratması nəticəsində kontent ünvanlanan sistemdə həmin məlumat İP ünvanlanan sistemdən daha tez yüklənir.

Məlumatların saxlanılması üçün İPFS PHC-lərdən istifadə edir. Sistem məşhur Kademlia PHC-nin realizasiyası əsasındadır. Bundan əlavə bəzi idealları Chord

PHC və BitTorrent PHC-dən almışdır. İstifadəçi məlumatları İPFS-ə yükələyəndə onlar müəyyən sayda qovşaqlara köçürülür. Bunun səbəbi isə hər hansısa qovşaq sıradan çıxdıqda məlumatlar digər qovşaqlarda əlçatan olsun. BitTorrentdə olduğu kimi məlumatlar nə qədər çox tələb olunarlarsa hər yüklənmədə yeni sürət yaradılması hesabına onların saxlanma etibarlılığı da bir o qədər çox olar. Chord-un əsas özəlliyi böyük akortlar daxilində bir-birinə yaxın yerləşən dünyadakı bütün qovşaqlarda PHC-lərin axtarış sürətlərini artıran akortlar yaradılan PHC çevrələridir. Yəni, Yer kürəsini ardıcıl böyüyən akortlar seriyası kimi təsvir etmək olar.

İndi Amazon və Google kimi mərkəzləşmiş xidmətlərin dünyanın hər yerində istifadəçilərin seçiminə uyğun məlumatlar mərkəzləri vardır amma adətən bu mərkəzlər avtomatik seçilir. Bütün dünyada paylanmış çoxlu sayda məlumatlar mərkəzi olmasına baxmayaraq məlumatların yüksək sürətlə ötürülməsi mərkəzləşdirilməmiş sistem altında birləşdirilən bir neçə qovşaq olduqda mümkündur.

PHC strukturunu formalaşdırmaq və istifadəçilərə istədikləri məlumatları tapmaq imkanı vermək üçün İPFS bir-biri ilə bağlı qovşaqlar seriyası olan merkleDAG adlanan sadə və çevik verilənlər strukturundan istifadə edir. Başqa sözlə buna istiqamətlənmiş dövrsüz qraf demək olar. MerkleDAG-a əlaqəli siyahı və ya ağac kimi baxmaq olar. PHC-ə yeni məlumat əlavə olunanda sistem SHA-256 şifrələməsi ilə açıq və qapalı açar cütü generasiya edir. İPFS-də bütün məlumatlar ictimaiyyətə açıq olduğundan istifadəçilərin özləri şifrələmənin qayğısına qalmalıdırlar. Məlumatlara baxışa icazə verən qapalı açar sahibliyi məlumatın bu və ya digər istifadəçiyə aid olmasının isbatıdır.

3.2 Blokçeyn mədənçiliyini ekosistemi

Bitcoin, Ethereum, Litecoin kimi işin yoxlanılması sistemlərində sistem üzvləri trazaksiyaların yoxlanılması və digər düyünlərə ötürülməsindən əlavə əlavə hesablamalar tələb olunan blokların yaradılması və Blokçeyn zəncirinin sonuna

bağlanması ilə məşğuldurlar. Bu prosesə başqa adla Blokçeyn mədənçiliyi də deyilir. Hesablama baxımından bahalı olan məsələlərin həll olunub mükafat qazanılması Blokçeyn mədənçiləri arasında bir növ yaraşın yaranmasına səbəb olmuşdur.

Bitcoin mədənçiliyi şəbəkəni iki əsas faktorla: yeni bitcoinlərin yaranması və tranzaksiyaların təsdiqi ilə təmin edir. Mədənçilər düzgün tranzaksiyaları izləyir və onları yeni blokda birləşdirirlər.

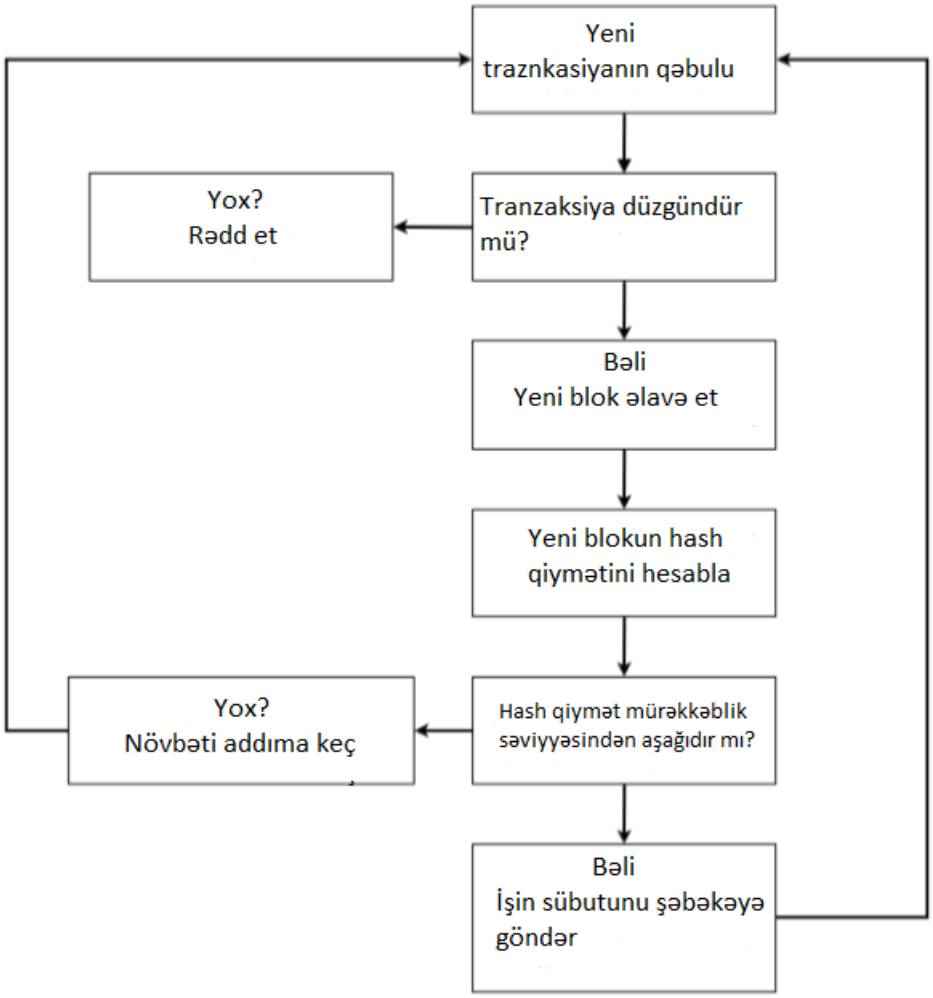
Mədənçilər nöqteyi-nəzərindən blokların müəyyən dəyəri vardır. Bloklardan olan baytlar çətin hesablama problemlərinə cavab tapılmasının bazasını təşkil edir. Mədənçilər problemlərə digər mədənçilərdən daha tez həll tapmaq ümidilə milyonlarla cəhd edirlər. Həll tapılanda isə şəbəkəyə bu barədə cəld məlumat verirlər. Əgər bu şəbəkə tərəfindən təsdiqlənərsə bu zaman mədənçi tranzaksiyaya qoyulan vergi qədər yeni bitcoin əldə edir. Hesablama gücü çox olan maşının şəbəkədəki digər maşınlarla müqayisədə məsələləri hamısından tez həll edib mükafat qazanma ehtimalı daha çoxdur. Hər dəfə mədənçi yeni blokun yaranmasını təsdiqlədikdən sonra əvvəlcədən təyin olunmuş kripqrafik mükafat tokenini öz hesabına əlavə edə bilir. Bu mükafat istifadəçilər tərəfindən tranzaksiyaların emalı zamanı prioritetin artırılması üçün əlavə olunan dəyərlə birlikdə mədənçilərin fəaliyyətləri üçün daha böyük stimul yaradır. Beləliklə, mədənçilər tranzaksiyaların yerinə yetirilməsi ilə bağlı bir-birlərilə yarışa çıxırlar. Şəbəkənin təhlükəsizliyinin qorunması və dəstəklənməsi məqsədilə mədənçilərin yeni resurslar ayırması üçün mükafat olaraq sistemin əsas tokenindən istifadə olunur. Bu, aralıq vasitəçilər olmadan trazaksiyaları yerinə yetirmək üçün şəbəkənin dəstəklənməsi üçün çoxlu sayda mədənçilərin cəlb olunması məqsədi ilə izah olunur. Qeyd etmək lazımdır ki, mədənçilik proseslərinin əsas məqsədi şəbəkədə tranzaksiyaların yoxlanılması deyildir. Əsas məqsəd şəbəkənin kiber hücumlara qarşı dayanıqlılığının təmin olunmasıdır beləki, Blokçeyn zəncirinə əlavə olunan hər bir yeni blok onun kənardan müdaxiləsinin daha çətin olmasını təmin edir. Beləliklə, şəbəkənin həqiqi vəziyyəti haqqında konsensus zamanla da

da güclənir. Sistemin həqiqi vəziyyətini pozmaq istəyən bir şəxs bunun üçün çox böyük miqdarda resurs sərf etməlidir. Şəbəkə öz həqiqi vəziyyətini ən uzun Blokçeyn zənciri ilə müəyyən etdiyindən hər hansısa bir blokun dəyişdirilməsi və əsas zəncirin həmin həmin blokla birləşdirilməsi mümkün olmadığıdan onun vəziyyətini dəyişmək uğursuz olacaqdır. İşin yoxlanılması sistemlərində şəbəkənin təhlükəsizliyi hesablamaların aparılması üçün nəzərdə tutulmuş çətinlik dərəcəsi ilə düz mütənasibdir. Şəbəkənin əsas tokenindən nə qədər çox istifadə olunarsa onun dəyəri bir o qədər də çox olar və dəstəklənməsi üçün mədənçilərin qoşulmasına əlverişli şərait yaradar. Şəbəkəyə qoşulmuş mədənçilər isə növbəsində sistemin təhlükəsizliyini və effektivliyini artırmış olarlar. Eyni zamanda bunun tərsi də doğrudur. Əgər şəbəkənin əsas tokeninin bazar dəyəri aşağı düşməyə başlarsa bu zaman mədənçilər üçün şəbəkənin dəstəklənməsi maddi baxımdan əlverişli olmazdır. Qazanc əldə edə bilməyən mədənçilər sistemin dəstəklənməsindən imtina edərək ekosistemi tərk edə bilərlər. Belə bir vəziyyətdə Blokçeyn zənciri öz təhlükəsizliyini təmin edə bilmədiyi üçün bütün iştirakçıların ekosistemi tərk etməsinə gətirib çıxara bilər. Əgər mədənçilik prosesi digər məqsədlər üçün əlverişlidirsə bu zaman mədənçilik prosesin dəyəri aşağı olacaqdır. Lakin, əldə olunmuş nəticəni sataraq qazanc əldə edə bilərlər. Qazanc əldə edə bilən mədənçilər üçün sistemin dəstəklənməsi və təhlükəsizliyinin təmin olumnası maddi baxımdan onların öz maraq dairələrində qala bilər. Şəbəkənin həqiqi vəziyyətinə gəlib çatması prosesi mərhələsi bazarın dizaynının formalaşmasında vacib rol oynayir. Konkret tranzaksiyaların təhlükəsizlik dərəcəsindən asılı olaraq istifadəçilər öz tranzaksiyalarının yerləşdiyi blokdan sonra bir neçə blokun hazırlanmasını gözləməli olurlar. Bu o deməkdir ki, Blokçeyn zəncirinin həqiqi vəziyyətinin alınması üçün bir neçə tranzaksiyanın optimal formada yeni bloka əlavə olunması müəyyən intervallarla yerinə yetirilir. Qeyd etmək lazımdır ki müxtəlif tip tranzaksiyaların icrası üçün yeganə Blokçeyn sistemi uyğun olmaya bilər. Bu baxımdan istifadəçinin məqsədindən asılı olaraq müxtəlif Blokçeyn sistemlərindən öz fəaliyyətlərini davam etdirir. Tranzaksiyaların ölçüləri və onlarla

bağlı olan atributalardan, təhüləsizlik dərəcəsindən, məxfilikdən asılı olaraq müxtəlif sektorlar müxtəlif Blokçeyn sistemlərindən istifadə edə bilərlər.

Şəbəkəyə transilyasiya edilən hər bir tranzaksiya ikiqat xərclərin qarşısının alınması üçün yoxlanılmalıdır. Mədənçidə əlçatan balansı təsdiqləmək üçün bütün zəncirin yoxlanılmış sürəti olmalıdır.

Mədənçilik prosesi



Şəkil 3.5

Hər hansısa müəyyən Bitcoin klienti yüklədikdən sonra klient şəbəkədən hər bir bloku yoxlamaqla Bitcoin zəncirini yükləməyə başlayır və Blokçeyn replikasiya olunaraq lokal şəkildə saxlanılır.

Blokçeynin lokal sürəti sistemin işə düşdüyü vaxtdan etibarən olan bütün tranzaksiyaları özündə saxlayır. Bu kitabça hər bir tranzaksiyanın xərclər balansını

yoxlamaq üçün istifadə olunur və saxlanılır. Əgər tranzaksiya həqiqi deyilsə bu zaman ondan imtina olunur.

İkinci yoxlanış isə rəqəmsal imzanın yoxlanılmasını tələb edir. Tranzaksiyanın tamlığını yoxlamaq üçün kriqtoqrafik alqoritmlərdən istifadə edərək mədənçi tranzaksiyaya yapışdırılmış imzanı yoxlaya bilər. Tranzaskiya üzərində istənilən modifikasiya yalnış imzaya gətirib çıxaracaq və beləliklə, mədənçi emal olunacaq tranzaksiyanın qapalı açarın əsl versiyasına sahib olan şəxs tərəfindən göndərildiyini təsdiqləyə bilər. Həqiqi tranzaksiyalar siyahısından istifadə edərək mədənçi yeni blok yaradır və onu çətin hesablama tapşırıqları üçün əsas kimi götürür.

Əvvəldə izah olunmuş hash müəyyən verilənlər yığımına tətbiq olunan riyazi funksiyanın nəticəsi kimi təsvir olundu. Bizim baxdığımız halda isə verilənlər özündə həqiqi tranzaksiyalar yığını olan yeni bloku ifadə edir. Verilənlərə hash funksiya tətbiq olunanda o müəyyən bir nəticə qaytarır. Əgər veriləndəki hər hansı bayt dəyişilsə və yenidən hash funksiya tətbiq olunsa nəticə radikal olaraq fərqlənər.

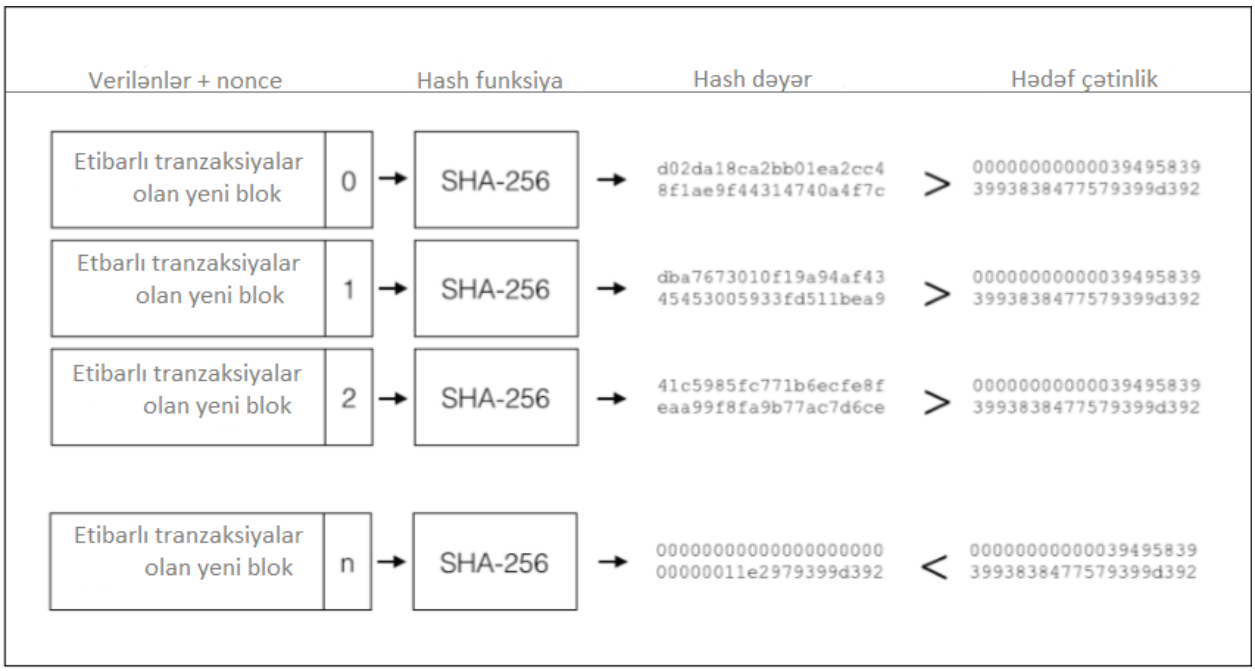
Mədənçilik özünə hash nəticələrin alınması üçün hash funksiyaları daxil edir. Əgər hash məqsədə uyğun olarsa bu zaman o həll sayılır, əks halda verilənlərə nonce dəyişəni əlavə olunmaqla yenidən hash funksiyaya göndərilir. Bu proses həll tapılana qədər davam edir.

Həll tapıldıqdan sonra şəbəkəyə yeni blok formasında transilyasiya olunur. Şəbəkədəki digər qovşaqlar hash-i hesablamaqla işin sübutunu yoxlaya bilərlər. Əgər iş qəbul olunsa yeni blok Blokçeynə əlavə olunur. Həll ilə razılaşan qovşaqlar daha sonra yeni blokdan qarşılıqlı şəkildə şəbəkədəki digər qovşaqlarla birgə istifadə edirlər. Nəticə etibarilə yeni Bitcoin-lər və tranzasiyalardan gəlirlər qələbə qazanmış mədənçiyə verilir.

Hash nəticələrin hesablanması olduqca bahalıdır. İşi sübut etmək üçün hash funksiyası həqiqi hash-in tapılmasına qədər çoxlu sayda yerinə yetirilir. Buna görə də iş çətin hesabi tapşırığın hesablanma kimi təsvir olunur. Əvvəl qeyd etdiyimiz

kimi Bitcoin SHA-256 hash funksiyasından istifadə edir. Bu təhlükəsiz kriptoqrafik hash funksiyası proqram təminatı və ya daha çox effektivlik üçün aparat təminatı vasitəsi ilə hesablana bilər.

Hash dəyər hesablanması prosesi



Şəkil 3.6

Xüsusi halda mədənçilər hədəf dəyərdən daha kiçik hash dəyər tapmağa çalışırlar. Onlar uduşlu hash tapmaq üçün saniyədə milyonlarla hash hesablayacaqlar. Verilənlər yığımında istənilən kiçik dəyişiklik hash dəyərin dəyişməsinə səbəb olduğundan yığıma nonce dəyişəni əlavə olunur. Hər təkrarda nonce dəyişəni inkrement olunur. İnkrement olunduqdan sonraki hash əvvəlki hash-dan tamamilə fərqli olur. Bu, mədənçiyə yayınlanan çətinlik dərəcəsindən daha aşağı olan hash dəyər tapmaq üçün başqa bir şans verir.

Növbəti şəkildə həqiqi tranzaksiyalardan və nonce dəyişənindən ibarət olan blokun qeyd olunmuş çətinlik dərəcəsindən aşağı olan hash dəyərin tapılması əks olunmuşdur.

Şəkildən görünür ki, eyni verilənlər inkrement olunaraq hash-in yenidən hesablanması üçün istifadə olunur. Brute force yanaşmasından istifadə edərək mədənçilər n-i tapmaq üçün milyonlarla cəhd eləyirlər.

Mükafatlar üçün rəqabət artdıqca hesablanması çətin olan problemlərin həllinin

tapılması dərəcəsi də artır. Həll tapmaq istəyən mədənçilərin sayının çoxalması hər 10 dəqiqədə orta dərəcənin yeni bir blokun gözlənilən dərəcəsindən az olmasına gətirib çıxarır.

Bunu kompensasiya eləmək üçün hər 2016 blokdan sonra çətinlik dərəcəsi hesablanır və düzəlişlər olunur. İstənilən çətinlik dərəcəsinin alınması üçün hesablamada traznaksiyaların son 2 həftəsi də nəzərə alınır. Əgər orta göstərici 10 dəqiqəlik ortalamadan kiçikdirsə bu zaman çətinlik artırılır və əksinə əgər o, böyükdürsə bu zaman çətinlik azaldılır.

Mədənçilər çətinlik göstəricilərdən istifadə edərək bir bitcoin-in əldə edilməsi üçün tələb oluna biləcək hesablama gücünü proqnoz edə bilərlər.

İlkin vaxtlarda hash-lərin hesablanması üçün standart prosessorlardan istifadə olunurdu. Birinci Bitcoin klientinə prosessordan mədənçilik üçün istifadə etmək imkanı verən funksiya əlavə olunmuşdu. Bitcoinin ilk günlərində bir prosessordan istifadə edərək mükafat almaq olduqca asan idi. Lakin, mədənçilərin sayı artdıqca prosessor tez bir şəkildə köhnəlmiş sayıldı.

Rəqabət artıqca proqram təminatı qrafik prosessorlardan istifadəyə adaptasiya olunduruldu. Qrafik prosessorlar adi prosessorlardan fərqli olaraq riyazi hesablamaları daha sürətli aparmağa optimizasiya olunmuşdurlar. Onlar çətin qrafiki proqramların və rendering-in hesalanma sürətinin artırılması üçün nəzərdə tutulublar. Onların optimizasiya hash funksiyaların hesablanması üçün çətin riyazi hesablamalar aparmağa imkan verir.

Operatorlar mədənçilik qrafik prosessorlara nəzarət edirlər. Bir kompüterə bir neçə videokart birləşdirmək mümkündür. Bu isə öz növbəsində çoxlu istiliyin ayrılmasına səbəb olur. Cihazların maksimal performasını saxlamaq üçün kondisionerlər daim soyutmalıdırlar.

GPU-lar tətbiqat üçün standart kimi qəbul olunduqdan sonra kompüter çipləri hazırlayan şirkətlər hash hesablamalar aparacaq xüsusi mikroçiplər hazırlamağa başladılar. Bu bir saniyədə hesablana biləcək hash-lərin sayını nəzərə çarpacaq dərəcədə artırdı.

Hash hesablamalar aparılması üçün ilkin olaraq Field-Programmable Gate Arrays (FPGAs) yaradılmışdı. Bunlar proqramçıya aparat səviyyəsində instruksiyaları kodlaşdırmağa imkan verən xüsusi inteqrə olunmuş çiplər idilər. Bu çiplər az enerji sərf eləməklə sürətli hash hesablamalar aparmaq imkanı verirdilər.

Xüsusi inteqral mikrosxemlərin (ASİC) yaradılması ilə bitcoin mədənçiliyi daha da asanlaşdı. Bu çiplər bir saniyədə milyardlarla hash hesablama imkanı verir.

Aparatların performans-güc cədvəli Cədvəl 3.1

Aparat	Performans (hash/saniyə)	Güc (Vt)
CPU	1-50 milyon	150-300
GPU	100-800 milyon	500-1000
FPGA	100-800 milyon	5-40
ASİC	10 000-1 000 000 milyon	200-600

Cədvəldən görünür ki, ASİC aparatından istifadə enerjiyə nə qədər qənaət edir. Buna görə də adi prosessorlar, qrafik proessorlar və FPGA prosessorların çoxu ASİC aparat təminatı ilə əvəz olunur. Rəqabət baxımından ASİC-dən başqa aparat təminatından istifadə etmək sərfəli sayılmır.

Maksimal performansa nail olmaq üçün və aparatlara qoyulan tələblərdən dolayı onları dəstəkləmək və lazımi şəraitdə saxlamaq vacibdir.

Ən nəzərə çarpan tələbat soyutma sisteminin olmasıdır. Aparatların sabit temperaturda işləyə bilməsini təmin etmək üçün soyutma sistemindən istifadə olunur. Mədənçilik sistemi qurulan zaman soyutma sisteminin xərclərinin də hesabatı verilməlidir.

Aparatların və soyutma sisteminin istifadə elədiyi elektrik enerjisinin qiyməti hesablanıb nizamlanmalıdır. Təmiz və stabil elektrik aparatların zədələnməməsi üçün vacib faktorlardan biridir. Elektrik zirvələri və yüksək yüklənmə işin qırılmasına səbəb ola bilər.

Aparatların daim monitorinqi aparılmalıdır. Dayanış vaxtı nəzərə parçan

dərəcədə investisiya itkisinə səbəb ola bilər. Bunun üçün də adətən aparatların dəskətlənməsi və moniorinqirini aparan işçi heyəti tələb olunur.

Bir ASİC mədənçinin yeni blokdan mükafat alması üçün işin sübutunu tapmaq çətin məsələ ola bilər. Bu xüsusən də şəbəkədə individual işləyən mədənçilər üçün doğrudur. Bitcoin əldə etmək şansını artırmaq üçün hovuz adlanan strategiya mövcuddur.

Mədənçilik operatorları öz kollektiv güclərini vahid mədənçilik hovuzu altında birləşdirə bilərlər. Qrup şəklində işin sübutunu tapmaq şansı daha çox olur. Mükafat əldə olunduqdan sonra hovuz qazancı görülən iş əsasında mədənçilər arasında bölür.

Mədənçilik hovuzları bütöv bloku tək emal etməsi çətin olan az enerji tələbatı ilə işləyən mədənçilər üçün əlverişlidir. Hovuzlarda iş aksiyalarla ölçülür. Hər bir sübut göstərənə bir aksiya verilir. Mədənçilik hovuzlarında işin sübutu ən asan çətinlik dərəcəsi əsasında qəbul olunur. Ən sadə çətinlik dərəcəsində hesabi tapşırığın həllinin tapılmasında nonce dəyişəninin qiymətini daha böyük diapozonda götürmək olar. Sədə çətinlik dərəcəsində yaradılan işin sübutu ayrı-ayrı mədənçilərin işlədiklərini sübut etmələri əsasındadır. Axır-əvvəl aksiyalar çətinlik dərəcəsi ilə uyğun olduqda hovuz mükafat qazanır və təqdim olunmuş aksiyalar əsasında bölünür.

Mədənçilik vergiləri bir qayda olaraq ödəniş metodundan asılı olaraq 0.5-3.0% arası dəyişir. Ödəniş metodlarına əsaslanaraq hovuzun operatoru aksiya haqqında yalan məlumat verən mədənçi tərəfindən risklə qarşılaşa bilər. Bir qayda olaraq risk nə qədər çox olarsa ödəniş dəbir o qədər çox olur.

Hesabatda adətən raunddan istifadə olunur. Raund dedikdə emal olunan cari blok başa düşülur. Blok emalı bitdikdən sonra raund bağlanır və yeni raound başlanır.

Mədənçilik operatoru tərəfindən ödəniş müxtəlif metodlar əsasındadır. Bəzi metodlar daha cəld ödənişlər üçün optimillaşdırıldığı halda digərləri isə yeni aksiyalar üçün stimul yaradır. Saxtakarlıqların qarşısının alınması üçün də müxtəlif

metodlar tətbiq olunur. Hovuz operatorları tam komissiya ilə yanaşı mədənçilərin öz hovuzlarına qoşulmaqları üçün xüsusi metodlardan istifadə edirlər.

Lakin, praktika göstərmişdir ki, bu cür mədənçilik bir-başa düyünlərin yerləşdiyi çoğrafi mövqelərdən asılıdır. Əvvəldə qeyd etdiyimiz kimi düyünlərdə tranzaksiyaların emalı çox böyük enerji tələb edir. Burdan belə bir nəticəyə gəlmək olar ki, enerji təminatının dəyərinin yüksək olduğu ölkələrdə bu bazarın inkişaf etməsi olduqca çətindir.

Ödəniş formaları Cədvəl 3.2

Ödəniş	Təsvir
Ardıcıl	Mükafat mədənçilərə aksiyalara uyğun olaraq proporsional ödənir.
Səhm payı	Mədənçilər təqdim olunan hər aksiyaya uyğun ödəniş əldə edirlər. Ödənilən məbləğ cari çətinlik dərəcəsindən asılıdır. Hovuzun operatoru riskə getmiş olur. Hovuzun tələb etdiyi vergi ən yüksək olur.
Hesab	Təqdim olunan aksiyanın vaxtından asılı olan ardıcıl mükafatlandırma. Daha sonra aksiyaların vaxt reytinqi üzrə qiyməti qalxır.

Mümkün mənfəətlərin hesablanması üçün əlçatan aparat təminatı ilə mürəkkəblik dərəcəsinin müqayisəsi aparılmalıdır. Aşağıdakı düsturdan istifadə edərək mədənçilikdən qazanılan mükafatı hesablamaq olar.

$$B=(h * 86\,400 * r) / (2^{32} * d) \qquad (4.1)$$

Burada,

B - orta hesabla bir gündə qazanılan mükafat

h - vahid zaman anında hesablanan hash-lərin sayı

r - bir blokdan qazanılan mükafat

d - çətinlik dərəcəsi

86 400 - bir gündə saniyələrin sayı

Bu düsturda mənfəət yalnız hash-lərin hesablanması sürəti və çətinlik dərəcəsi

əsasında hesablanır. Praktikada isə mənfəətin hesablanması zamanı daha dəqiq qiymət almaq üçün aparatlar üçün çəkilən xərclər, elektirk enerjisi tarifləri, işçi personalın maaşı və texniki təminat xərcləri də nəzərə alınır.

Blokçeyn texnologiyasının imkanlarını daha da genişləndirən layihələrdən biri də Ethereum layihəsidir. Ehtereum layihəsinin ağ məqaləsinin çap olunması və layihənin həyata keçirilməsi Blokçeyn texnologiyasını da yeni nəsil yaratdı. Mahiyyəti üzrə bu texnologiya Blokçeyn mühitində proqram təminatlarını icra etmək üçün yaradılmış virtual maşındır. Ethereum platformasının ən güclü tərəfi isə ağıllı müqavilələr konsepsiyasının daxil olunmasıdır. Ağıllı müqavilələr Ethereum açıq registerində saxlanılan və konkret blokun adresi ilə bağlı olan kiçik proqram təminatlarıdırlar. Ethereum ağıllı müqavilələri Blokçeyn şəbəkəsində icra olunması üçün C++. Javascript və Python dillərindən törənmiş Solidity dilində hazırlanırlar. Ağıllı müqavilələr kompilyasiya olunaraq bytecode-a çevrilib Blokçeyndə saxlanılır və Ethereum virtual maşını (EVM) tərəfindən icra olunur. Praktiki olaraq ağıllı müqavilələr vasitəsi ilə standart proqram təminatları kimi istənilən hesablama tapşırıqlarını yerinə yetirmək olar. Lakin, blockhain texnoligiyasının mərkəzləşdirilməmiş struktura malik olması və Ehtereum konsensus protokolu bu cür proqram təminatlarının hazırlanması zamanı bir sıra məhdudiyyətlər qoyur. Ağıllı müqavilələr üç hissədən ibarətdirlər:

1. Proqramın kodu hansı ki müqavilənin məntiqi əsasını özündə əks etdirir.

2. Mesajlar çoxluğu hansı ki müqavilə bu mesajları qəbul edəndən sora proqram təminatını işə salır.

3. Metodlar çoxluğu hansk ki müqvilə məntiqinə əsasən müəyyən bir nəticə əldə etmək imkanı verir.

Blokçeyndə yaradılmiş ağıllı müqavilə dəyişməzdir. Bu o deməkdir ki, bir dəfə Blokçeynə yazılmış ağıllı müqavilə sistemin təbiətinə görə bir daha dəyişdirilə bilməz. Ağıllı müqavilələr biznes proseslərinin avtomatlaşdırılaraq blokchain şəbəkəsində aparılmasına imkan verir.

NƏTİCƏ

Blokçeyn texnologiyası nə qədər güclü olsa da onun gələcəyi haqda nəsə söyləmək olduqca mürəkkəbdir. Blokçeyn sistemlərinin daim fəaliyyətdə olması üçün mədənçilər öz işlərini dayandırmamalıdırlar. Lakin nəzərə alsaq ki bitcoin vasaitlərin sayı 21 000 000 BTC ilə məhdudlanır bu gələcəkdə mədənçilərin bu sektordan soyumasına gətirib çıxara bilər. Gəlir əldə edə bilməyən mədənçilər öz fəaliyyətlərini dayandıraraq sistemi çökdürə bilərlər. İqtisadiyyatçılar bitcoin-ə qoyulan suallara cavab tapmaqda çətinlik çəkirlər. Bəziləri bu sistemin gələcəkdə hətta müasir bank sistemini çökdürəcəyini proqnozlaşdırırlar. Digərləri isə bitcoini qabarcıq adlandırırlar. Bitcoin texnologiyası dövlətləri də qarışıq vəziyyətə salmışdır. Müxtəlif dövlətlər bitcoin-lə necə rəftar etməli olduqları barədə qarışıq fikirlər içindədirlər. Bir sıra dövlətlər bitcoin-dən istifadəni və mədənçiliyi qadağan etdikləri halda digərləri bu sistemi dəstəkləmək üçün addımlar atırlar.

Dissertasiyanın birinci fəslində aparılmış anazlizlər və müqayisələr cari rəqəmsal mübadilə sistemlərində informasiya təhlükəsizliyi riskini izah etmişdir. İnformasiyanın müəyyən bir dəyər aldığı dövrdə isə bu cür risklərin olması maddi və mənəvi baxımdan iqtisadi sistemler istifadəçilərinə zərər yetirə bilər. Bunun qarışısının alınması məqsədi ilə Blokçeyn texnologiyasının mümkün tətbiq olunma variantları göstərilmiş və analiz edilmişdir. Eyni zamanda bir çox imkanları olan yeni iqtisadi proseslərin icra olunması modelinin yarada biləcəyi problemlər və onların həlləri araşdırılmışdır. Bazarın effektiv fəaliyyət göstərə bilməsi üçün yeni Blokçeyn sisteminin bütün üzvləri sistemdə yerinə yetirilən tranzaksiyaların həqiqiliyini yoxlamaq imkanı alırlar.

Təşkilatların və müəssislələrin bu texnologiyalar üzərində müxtəlif təcrübələr aparmaqları onların bu sahədə nə qədər maraqlı olduqlarının göstəricisidir. Sistemin mərkəzi idarəetməsinin olmaması yeni innovativ layihələrinin sistem üzərində qurulmasına imkan verir. Bazarlara yeni üzvlərin daxil olması imkanı isə monopoliyanın aradan qalxmasına və rəqabətin güclənməsi üçün şərait yaradır. Yeni üzvlər şəbəkənin imkanlarını daha da genişləndirərək istifadəçilər üçün yeni

xidmətlərin yaranmasını vədd edir.

Blokçeyn texnoligasının tətbiqi ilə banklar və aralıq vasitəçilər bir sıra çoxlu resurs tələb edən əməliyyatların xərclərini azaltmaq imkanı əldə edirlər. Şəbəkə yoxlanış xərclərinin azaldılması bu cür qurumların qənaət etdiklərini resursları başqa istiqamətlərin inkişaf etdirilməsinə sərf edə bilərlər. Bu texnologiyanın tətbiqi eyni zamanda müxtəlif yeni peşələrin yaranması üçün imkan yaradır.

Dissertasiyanın üçüncü fəsildə bəhs edilən Blokçeyn mədənçiliyi isə öz növbəsində Blokçeyn mədənçiliyi deyilən yeni bir bazar yaradır. Bu bazarda şəbəkə üzvləri sistemin fəaliyyətini dəstəkləmək vasitəsi ilə qazanc əldə edib sistemə qatqılarını artırmaq üçün yeni resurslar daxil edə bilərlər.

Blokçeyn texnologiyasının geniş tətbiq olunması nəticəsində proqram təminatlarının hazırlanması bazarında da yeni bir sahə yaranır. Bu sahə mərkəzləşdirilməmiş proqram təminatı hazırlanması sahəsidir. Lakin, bu sahənin yeni olması yeni ixtisaslaşmış kadrların yetişdirilməsi üçün kifayət qədər resursun olmaması problemlemi ilə üzləşir. Blokchain şəbəkələrinin mənbə kodunun açıq olması dünyanın bütün mütəxəssisləri tərəfindən dəstəklənməsinə imkan verir. İndividual proqram təminatı mütəxəsisləri bu kodları götürüb onlar üzərində öz bildikləri yenilikləri əlavə edərək sistemdəki səhvlərin aradan qaldırılmasına kömək edə bilərlər.

Bir çox iqtisadiyyatçılar gələcək üçün əsas perspektiv kimi Blokçeyn texnologiyasını görürlər. Bu texnologiyadan nəyinki ticarət sistemində, eyni zamanda müxtəlif idarəetmə sistemlərində də tətbiq etmək mümkündur.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISIError! Bookmark not defined.

1. Andreas M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies
2. Richard Caetano, Learning Bitcoin
3. Melanie Swan, Blockchain. Blueprint for a new Economy
4. Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Bitcoin and Cryptocurrency Technologies
5. Kaye Scholer, An İntroduction to Bitcoin and Blockchain Technology
6. Siraj Raval, Decentralized Applications, Harnessing Bitcoin's Blockchain Technology
7. W. Feller, An introduction to probability theory and its applications,1957
8. R.C. Merkle, Protocols for public key cryptosystems, In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society,
9. Michael Crosby, Nachiappan, Pradhan Pattanayak, BlockChain Technology Beyond Bitcoin
10. Andreas M. Antonopoulos, The Internet of Money
11. Agrawal, A., J. Gans, and A. Goldfarb (2016): The simple economics of machine intelligence, Harvard Business Review, 17.
12. Athey, S., C. Catalini, and C. Tucker (2017): The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, National Bureau of Economic Research Working Paper.
13. Beck, R., J. S. Czepluch, N. Lollike, and S. Malone (2016): Blockchain-the Gateway to Trust-Free Cryptographic Transactions., in ECIS, p. ResearchPaper153.
14. Bekkers, R., C. Catalini, A. Martinelli, C. Righi, and T. Simcoe (2019): Disclosure rules and declared essential patents, Discussion paper, National Bureau of Economic Research.
15. Böhme, R., N. Christin, B. Edelman, and T. Moore (2015): Bitcoin:

Economics, technology, and governance, The Journal of Economic Perspectives, 29(2), 213–238.

16. Halaburda, H., and M. Sarvary (2016): Beyond bitcoin: The economics of digital currencies. Springer.
17. Iansiti, M., and K. R. Lakhani (2017): The Truth About Blockchain, Harvard Business Review, 95(1), 118-127.
18. Mann, S., J. Nolan, and B. Wellman (2002): Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments., Surveillance & society, 1(3), 331-355.
19. Roth, A. E., and A. Ockenfels (2002): Last-minute bidding and the rules for ending second-price auctions: Evidence from eBay and Amazon auctions on the Internet, The American Economic Review, 92(4), 1093–1103.
20. Tucker, C., and C. Catalini (2018): What Blockchain Cant Do, Harvard Business Review.
21. Von Hippel, E., and G. Von Krogh (2003): Open source software and the private-collective innovation model: Issues for organization science, Organization science, 14(2), 209-223.
22. Wright, A., and P. De Filippi (2015): Decentralized blockchain technology and the rise of lex cryptographia, .
23. Walport, M. (2016): Distributed ledger technology: beyond block chain, UK Government Office for Science.
24. Roth, A. E. (2002): The economist as engineer: Game theory, experimentation, and computation as tools for design economics, Econometrica, 70(4), 1341-1378.
25. Lerner, J., and J. Tirole (2002): Some simple economics of open source, The journal of industrial economics, 50(2), 197-234.
26. Henderson, R. M., and K. B. Clark (1990): Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms, Administrative science quarterly, pp. 9-30.

ABSTRACT

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world. The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology and revolution in this space has just begun. This white paper describes blockchain technology and some compelling specific applications in both financial and non-financial sector. We then look at the challenges ahead and business opportunities in this fundamental technology that is all set to revolutionize our digital world. Understanding the real economic problems that the technology should aim at solving is a first step towards identifying the marketing beachheads for the technology. The branding of any blockchain can be categorized under an economic framework pointing to the types that have the potentials of being sustainable and disruptive. Selection of appropriate beachheads, verticals, services etc. should aim to pro mote the exchange of real goods and services, and/or the utilization the accounting/data advantage of the technology.

РЕЗЮМЕ

Блокчейн - это, по сути, распределенная база данных записей или публичный регистр всех транзакций или цифровых событий, которые были выполнены и переданы участвующим сторонам. Каждая транзакция в публичной книге проверяется консенсусом большинства участников системы. И после ввода информация никогда не может быть стерта. Блокчейн содержит определенную и проверяемую запись каждой когда-либо сделанной транзакции. Биткойн, децентрализованная одноранговая цифровая валюта, является наиболее популярным примером использования технологии цепочки блоков. Сам по себе биткойн цифровой валюты является весьма спорным, но основная технология блокчейна сработала безупречно и нашла широкое применение как в финансовом, так и в нефинансовом мире. Основная гипотеза состоит в том, что блокчейн устанавливает систему создания распределенного консенсуса в цифровом онлайн-мире. Это позволяет участвующим организациям точно знать, что произошло цифровое событие, создав неопровержимые записи в публичной книге. Это открывает двери для развития демократической открытой и масштабируемой цифровой экономики из централизованной. В этой прорывной технологии есть огромные возможности, и революция в этом пространстве только началась. В этом техническом документе описывается технология блокчейна и некоторые важные приложения как в финансовом, так и в нефинансовом секторе. Затем мы рассмотрим проблемы и возможности для бизнеса в этой фундаментальной технологии, которая готова революционизировать наш цифровой мир. Понимание реальных экономических проблем, на решение которых должна быть направлена технология, является первым шагом к определению маркетинговых плацдармов для этой технологии. Брендинг любого блокчейна можно классифицировать в соответствии с экономической структурой, указывая на типы, которые могут быть устойчивыми и

разрушительными. Выбор подходящих плацдармов, вертикалей, услуг и т. Д. Должен быть направлен на содействие обмену реальными товарами и услугами и / или использование преимуществ технологии в области бухгалтерского учета / данных.