AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazma hüququnda

Nərmin Məhərrəm Qızı Nəsrullayeva

Aytac Hamlet Qızı Məmmədova

Pərviz Abbas Oğlu Muradov

« Ağıllı şəhərlərdə təhlükəsizliyin təmin olunmasında blokçeyn texnologiyalarının tədqiqi» mövzusunda

MAGİSTR DİSSERTASİYA İŞİ

İxtisas: Kompüter mühəndisliyi

İxtisaslaşma: - Kompüter təhlükəsizliyi

Elmi rəhbər: **Əzimə Şahin qızı Abasova**

t.e.d., dos. **Yadigar Nəsib oğlu İmamverdiyev**

Bakı 2024

MÜNDƏRİCAT

GİRİŞ

Tədqiqatın aktuallığı. İnsan növünün yaşayış şəraitinin yaxşılaşdırılması bəşəriyyət yarananda bəri insanın əsas qayğılarından biri olmuşdur. Biz inkişaf etdikcə, həyatımızı asanlaşdırmağa yönəlmiş alət və texnikaların tətbiqinin sürətləndirilməsini nəzərə alsaq, bu təkmilləşdirmə ideyası getdikcə daha aydın görünür. Əsrlər boyu texnologiya bəşəriyyətin tərəqqisinin əsas amillərindən biri olmuşdur. Əslində, son rəqəmsal yeniliklər bizim fəaliyyət tərzimizi kökündən dəyişdirir və bizə əvvəllər heç kimin sahib olmadığı rahatlığı təklif edir. Bu yeniliklər gündəlik həyatımızın əsasını təşkil edir və ümumən həyatımızı dəyişir: iş rejimi, istehsal üsulu, istehlak üsulu, səyahət rejimi, qarşılıqlı əlaqə tərzi, ünsiyyət tərzi və s. Həqiqətən, texnoloji təsir təkcə insan növünün həyat tərzini dəyişdirmir, həm də onu ətraf mühiti fərqli şəkildə strukturlaşdırmağa sövq edir: yeni texnologiyalara uyğunlaşma baxımından düşünülmüş ərazi rəsmiləşdirmə forması. Hal-hazırda getdikcə daha çox ərazi rəqəmsal innovasiyalar baxımından ambisiyalara əsaslanan inkişaf strategiyalarını həyata keçirir. Bu, xüsusən də vətəndaşların və müəssisələrin ekoloji aspektlərə həssaslığını artırmaqla vətəndaşlara təklif olunan xidmətlərin idarə edilməsini, torpaqdan istifadənin planlaşdırılmasını, iqtisadi inkişafı və həyat keyfiyyətini kompleks şəkildə əhatə edir. Bunlar davamlılığa yönəlmiş istənilən inkişaf üçün vacibdir.

Şəhərin "ağıllı" olması şəhər əhalisinin artımı və sürətli urbanizasiyanın yaratdığı problemlərin aradan qaldırılması üçün strategiyaların bir hissəsidir. Bu ərazi kəşfiyyatının həyata keçirilməsi ümumiyyətlə ərazi maraqlı tərəfləri tərəfindən kütləvi məlumatların toplanması ilə özünü göstərir. Daha sonra daha yaxşı qərarlar qəbul etmək üçün bu məlumatlar emal oluna və bu müxtəlif aktorlar arasında paylaşıla bilər. Bu, əslində müxtəlif növ məlumatları əhatə edə bilər, lakin xüsusilə şəxsi məlumatlar və/və ya şirkət məlumatları və s. Bunlar sensorlar, digər əlaqəli obyekt sistemləri və ya əlaqə modulları vasitəsilə toplana bilər. Bununla belə, ümumilikdə ağıllı ərazilərin, xüsusən də ağıllı şəhərlərin inkişafı yalnız məlumatların idarə edilməsi ilə bağlı kritik

problemlər həll olunarsa effektiv ola bilər. Əks halda, qeyri-adekvat məlumatların idarə edilməsi böyük problemlərə, xüsusən də məlumatlara giriş üçün razılığın idarə edilməsi ilə əlaqəli rəqəmsal etimad probleminə səbəb ola bilər. Rəqəmsal texnologiyaya əsaslanan ərazilər müxtəlif aktorlar bir-birinə güvənməsə, effektiv fəaliyyət göstərə bilməz. Güvən əslində ağıllı şəhərin bütün komponentlərini birləşdirən əsas elementdir.

Blokçeyn, şifrələmə texnologiyasından istifadə edərək bağlanmış bloklarda qeydə alınan və saxlanılan əməliyyatların və ya hadisələrin paylanmış kitabıdır. Blokçeyndə bir uğursuzluq nöqtəsi, şəbəkədə məlumat paylanması səbəbindən normal funksiyaları kəsmir. Mərkəzləşdirilməmiş, izlənilə bilən və müdaxiləyə davamlıdır. O, mərkəzləşdirilmiş məlumat bazarının çatışmazlıqlarını aradan qaldıra, sistemin təhlükəsizliyini, istifadəçi davranışının izlənməsini və audit prosedurlarını təmin edə və ağıllı şəhərlər üçün güclü təminat verə bilər. Ağıllı şəhərlər kontekstində blokçeyn məlumat mübadiləsini təmin etmək, məlumatların bütövlüyünü təmin etmək və maraqlı tərəflər arasında etimadı gücləndirmək üçün təməl qat kimi xidmət edə bilər.

Blokçeynin kriptoqrafik xüsusiyyətləri məlumatların dəyişdirilməmiş və orijinal qalmasını təmin edərək, şəxsi identifikasiya, və kritik maliyyə əməliyyatları infrastruktur məlumatları kimi həssas məlumatların bütövlüyünü və təhlükəsizliyini gücləndirir. Ağıllı müqavilələr, blokçeynində yerləşdirilmiş proqramlaşdırıla bilən öz-özünə icra edilən müqavilələr müqavilələrin və xidmətlərin avtomatlaşdırılmış, şəffaf və dəyişməz icrasına imkan verir, bununla da bürokratiyanı azaldır və hesabatlılığı artırır. Blokçeyn əsaslı sistemlər vasitəsilə davamlılığı və resurs optimallaşdırılmasını təşviq edərək, resursların - enerji, su və ya tullantıların idarə edilməsi - səmərəli bölüşdürülməsi və izlənilməsinə nail olmaq olar. Blokçeynin mərkəzləşdirilməmiş arxitekturası tək uğursuzluq nöqtələrini aradan qaldırmaqla kiberhücumlara qarşı zəiflikləri azaldır və bununla da ağıllı şəhər sistemlərinin zərərli fəaliyyətlərə qarşı dayanıqlığını gücləndirir.

Bununla belə, ağıllı şəhərlərin təhlükəsizliyini təmin etmək üçün blokçeynin potensialı böyük olsa da, onun geniş şəkildə tətbiqində problemlər davam edir. Onun məlumatların idarə edilməsində inqilab etmək, təhlükəsizliyi artırmaq və ağıllı

şəhərlərin mürəkkəb çərçivələri daxilində şəffaf idarəçiliyi inkişaf etdirmək potensialı onu tədqiqat və tətbiq üçün perspektivli bir istiqamətə çevirir. Buna baxmayaraq, texnologiyanın imkanlarının nüanslı anlaşılması, mövcud problemlərin həlli üçün birgə səylərlə birlikdə təhlükəsiz və səmərəli ağıllı şəhərlərin gələcəyini formalaşdırmaqda blokçeynin bütün potensialını reallaşdırmaq üçün zəruridir.

Tədqiqatın elmi işlənmə dərəcəsi. Təhlükəsiz ağıllı şəhərlərdə blokçeyn texnologiyalarının istifadəsi ilə bağlı araşdırma nisbətən yeni və inkişaf etməkdədir. Blokçeyn kriptovalyutalar kontekstində əhəmiyyətli diqqət qazansa da, onun ağıllı şəhərlərdə tətbiqi hələ ilkin mərhələdədir. Buna görə də, bu tədqiqat təhlükəsiz ağıllı şəhərlər kontekstində blokçeynin potensial faydalarını, çətinliklərini və tətbiq strategiyalarını araşdıraraq sahəyə mühüm töhfə verir.

Tədqiqatın məqsədi. Bu dissertasiyanın məqsədi ağıllı şəhərlərin təhlükəsizliyinin təmin edilməsində blokçeyn texnologiyalarının istifadəsini araşdırmaq və qiymətləndirməkdir. Tədqiqat ağıllı şəhərlər daxilində məlumatların məxfiliyi, şəxsiyyətin idarə edilməsi, təhlükəsiz rabitə və əməliyyatların yoxlanılması kimi təhlükəsizliyi artırmaq üçün blokçeyn texnologiyasının effektiv şəkildə tətbiq oluna biləcəyi xüsusi sahələri müəyyən etmək məqsədi daşıyır.

Tədqiqatın vəzifələri. Tədqiqatın vəzifələri aşağıda qeyd olunmuşdur:

1. Blokçeyn texnologiyaları və onların ağıllı şəhərlərdə tətbiqi ilə bağlı mövcud bilik və tədqiqatları araşdırmaq üçün hərtərəfli ədəbiyyat araşdırmasının aparılması;
2. Ağıllı şəhərlərin üzləşdiyi xüsusi təhlükəsizliklə bağlı problemlərin və blokçeyn texnologiyasının bu problemlərin həllində təklif edə biləcəyi potensial faydaların müəyyən edilməsi və təhlili;
3. Ağıllı şəhərlərdə blokçeynin istifadəsi ilə bağlı maraqlı tərəflərin mövcud təcrübələrini və qavrayışlarını başa düşmək üçün nümunə araşdırmalarının araşdırılması;
4. Güclü təhlükəsizlik üçün blokçeyn texnologiyasının ağıllı şəhərlərin mövcud infrastrukturuna inteqrasiyasını əks etdirən konseptual çərçivə və ya modelin hazırlanması;

5. Simulyasiyalar və ya pilot tədqiqatlar vasitəsilə real dünyadakı ağıllı şəhər layihələrində blokçeyn texnologiyasının tətbiqinin mümkünlüyünün və effektivliyinin qiymətləndirilməsi;
6. Təhlükəsiz ağıllı şəhərlər kontekstində blokçeyn texnologiyasının potensial risklərinin və məhdudiyyətlərinin təhlili və onun səmərəli və təhlükəsiz həyata keçirilməsini təmin etmək üçün mexanizmlər və ya təlimatların təklif edilməsi.

Tədqiqatın nəzəri və metodoloji əsasları. Bu tədqiqatın nəzəri əsasını blokçeyn texnologiyası, ağıllı şəhərlər, təhlükəsizlik, informasiya sistemləri və şəhərsalma ilə bağlı nəzəriyyələr və konsepsiyalar təşkil edir. Tədqiqat ağıllı şəhərlərlə, o cümlədən şəhərsalma və idarəetmədə informasiya və kommunikasiya texnologiyalarının (İKT) inteqrasiyası ilə bağlı nəzəriyyə və konsepsiyalardan istifadə edəcək. Bu, müvafiq akademik jurnalların, konfrans materiallarının, kitabların, hesabatların və sənaye nəşrlərinin hərtərəfli ədəbiyyat icmalını əhatə edəcəkdir.

Metodoloji əsas baxımından bu tədqiqat qarışıq metodlardan istifadə edəcəkdir. Ağıllı şəhərlərdə blokçeyn tətbiqinin çətinlikləri və imkanları haqqında dərin fikirlər toplamaq üçün ədəbiyyata baxış, nümunə araşdırmaları və müsahibələr kimi keyfiyyətli metodlardan istifadə olunacaq. Bu keyfiyyətli üsullar təhlükəsiz ağıllı şəhərlərdə blokçeyndən istifadə ilə bağlı maraqlı tərəflərin qavrayışlarını, təcrübələrini və təcrübələrini zəngin şəkildə araşdırmağa imkan verəcək.

Tədqiqatın obyekti və predmeti. Tədqiqatın obyekti blokçeyn texnologiyalarının istifadəsi, xüsusilə təhlükəsiz ağıllı şəhərlərdə onların potensial tətbiqlərini araşdırmaqdır.

Tədqiqatın predmeti təhlükəsizlik və məlumatların idarə edilməsini artırmaq üçün blokçeyn texnologiyasının ağıllı şəhərlərin mövcud infrastrukturuna və proseslərinə inteqrasiyasıdır.

Tədqiqatın elmi yeniliyi. Bu tədqiqat ağıllı şəhərlərin təhlükəsizliyinin təmin edilməsində blokçeyn texnologiyalarının potensialının hərtərəfli araşdırılmasını təmin etməklə elmi biliyə töhfə verir. Əvvəlki tədqiqatlar blokçeynin texniki aspektlərinə və ya müxtəlif sektorlardakı xüsusi tətbiqlərə diqqət yetirsə də, bu tədqiqat təhlükəsiz ağıllı şəhərlər kontekstində blokçeynin çətinlikləri, faydaları və tətbiqi strategiyaları

haqqında hərtərəfli anlayışı təmin etmək məqsədi daşıyır. Bu tədqiqatın nəticələri blokçeynin qəbulunun nəzəri və praktiki nəticələrinə işıq salacaq və bu sahədə biliklərin inkişafına töhfə verəcək.

Tədqiqatın informasiya bazası. Tədqiqat məlumat bazası hərtərəfli təhlili təmin etmək üçün geniş mənbələri əhatə edəcəkdir. Akademik jurnallar və konfrans materialları blokçeyn texnologiyaları və onların ağıllı şəhərlərdə tətbiqi ilə bağlı elmi fikirlər və müasir tədqiqat nəticələri təqdim edəcək. Kitablar və hesabatlar təhlükəsiz ağıllı şəhərlər kontekstində blokçeynin nəzəri çərçivələri və praktiki nəticələri haqqında daha geniş anlayış təqdim edəcək. Bundan əlavə, sənaye nəşrləri ağıllı şəhər layihələrində blokçeyn tətbiqinin real dünya nümunələri və nümunələri təqdim edəcək. İlkin məlumatlar ağıllı şəhərlərdə blokçeyn texnologiyalarının inkişafı və tətbiqi ilə məşğul olan maraqlı tərəflərlə müsahibələr və sorğular vasitəsilə toplanacaq, eyni zamanda əvvəlki tədqiqatlar və qurulmuş ən yaxşı təcrübələr haqqında fikir əldə etmək üçün mövcud ədəbiyyatlar nəzərdən keçiriləcəkdir.

Tədqiqatın stukturu. Dissertasiya strukturu, giriş, üç (3) fəsil, doqquz (9) alt-fəsil, nəticə, istifadə olunmuş ədəbiyyatdan siyahısından, xülasələrdən (ingiliscə və rusca) və referatdan ibarət olmaqla, doxsan (90) səhifə təşkil etmişdir.

İlk fəsildə, təhlükəsizlik problemləri və onun ağıllı şəhərlərə təsirləri ilə yanaşı blokçeyn texnologiyasının konsepsiyasını, inkişafı və imkanlarını araşdırılır.

İkinci fəsildə, informasiya təhlükəsizliyi, imkanlar və tətbiqin cari vəziyyətinə diqqət yetirərək, ağıllı şəhərlərdə blokçeyn tətbiqlərini diqqətlə araşdırılır.

Üçüncü fəsildə, autentifikasiya, məxfiliyin qorunması və təklif olunan təhlükəsizlik proqramları kimi ağıllı şəhər infrastrukturunda blokçeyn tətbiqləri araşdırılır.

I FƏSİL. BLOKÇEYN TEXNOLOGİYASI VƏ ONUN TƏHLÜKƏSİZ AĞILLI ŞƏHƏRLƏRDƏ ROLU

1.1 Blokçeyn texnologiyasının konsepsiyası, inkişafı və imkan sahələri

Keçmişdə internet üzərindən ticarət istənilən elektron ödənişləri emal etmək üçün yalnız maliyyə institutları kimi etibarlı üçüncü tərəflərə etibar edirdi. Bununla belə, 2008-ci ildə Bitcoin-in tətbiqi bütün dünyada əməliyyatların necə işləndiyinə dair paradiqmanın dəyişməsinə səbəb oldu. Blokçeyn, avanqard kriptoqrafiyadan istifadə edərək milyonlarla kompüter arasında paylanmış açıq mənbəli verilənlər bazası kimi müəyyən edilir. Nəhayət, blokçeyn təhlükəsiz, mərkəzləşdirilməmiş, ictimai kitabdır və burada hər bir şəxs etibarlı üçüncü tərəfə ehtiyacı aradan qaldıraraq əməliyyat tarixinə tam şəkildə baxa bilər. Nümunə olaraq Bitcoin-dən istifadə edərək, indi blokçeyn texnologiyasının necə işlədiyinə dair ümumi məlumat verəcəyik. Zəncirdəki hər bir blok, şəbəkə iştirakçıları tərəfindən əməliyyatın baş verdiyini və saxtakarlıq olmadığını etiraf edir. Hər bir blok əvvəlki blokdan məlumat ehtiva edir, beləliklə, xronoloji ardıcıllıqla sıralanır, bloklar zənciri yaradır. Zəncirəyə blok əlavə etmək üçün həll bloka daxil olmaqla kriptoqrafik tapmacanı həll etmək lazımdır. Bu kriptoqrafik tapmacanı həll etmək üçün bütün madenciler şəbəkəsinə təxminən 10 dəqiqə vaxt lazımdır. Yeni əməliyyatlar kitaba əlavə edilməzdən əvvəl əksər istifadəçilər tərəfindən təsdiqlənməlidir. Bu əməliyyat təqribən bir saatlıq emal müddəti ilə nəticələnir ki, bu da cari maliyyə institutları ilə müqayisədə hələ də xeyli qısa müddətdir. Bununla belə, bu tapmacanın həlli xüsusi yaradılmış kompüterləri tələb edir və böyük miqdarda enerji sərf edir, buna görə də bu vəzifə adətən istifadəçilər tərəfindən tamamlanır. Istifadəçilər, birinci olmaq ümidi ilə kriptoqrafik tapmacaları həll edən blokçeyn şəbəkəsinin iştirakçılarıdır. Əgər istifadəçi tapmacanın həllində uğur qazanarsa, onlara 25 bitcoin veriləcək. Bu dəyər vaxtaşırı yarıya enir, çünki inflyasiyaya nəzarət etmək üçün maksimum 21 milyon bitcoin təyin edilib. Bu dizayn potensial olaraq şəbəkə istifadəçilərinin kriptoqrafik tapmacaları əldə etməkdən imtina etməsi ilə nəticələnə bilər, çünki bunun dəyəri çox yüksəkdir. Belə bir problemin öhdəsindən gəlmək üçün ödəyicinin özləri tapmacaya mükafat təyin etməsi, istifadəçiləri bu tapmaca üzərində

işləməyə həvəsləndirməsi mümkündür. Bu adətən 0,00000001 bitcoin olaraq hesablanacaqdır.

İşin sübutu bu sistemin əsas komponentidir. Zəncirə blok əlavə etmək qərarı səs çoxluğu olduğu üçün istifadəçilərin hansı növ səsə sahib olacağına qərar vermək vacib idi. Bir IP-bir səs sistemləri əvəzinə blokçeyn səsləri böyük mədən hovuzlarında hovuz operatoru və tətbiqə xüsusi inteqral sxemlər (ASICS kimi qısaldılmış) tərəfindən müəyyən edilir. Bu iş sübutu metodu səs çoxluğunun həmişə ən uzun zəncirdə olmasını təmin edir, çünki ona yatırılan hesablama gücünün əksəriyyətinə malikdir. Blokları istifadəçilərin sərvətinə mütənasib olaraq bölən sübut payı metodu ilə iş sübutunun əvəz edilməsi ilə bağlı təkliflər keçmişdə verilmişdir. Bu yeni metodun blokçeynlərin sürətini artıracağı, həmçinin hücum şansını 51% azaldacağı təklif edilir. Eyni zamanda, bu yeni üsul başlanğıcdan bəri redaktə edilməmiş blokçeyn texnologiyasına daxil edilməmişdir.

Blokçeynin əsas prinsipi bir zəncirdə bir-birinə bağlanmış məlumat blokları ətrafında fırlanır. Hər bir blokda bir sıra əməliyyatlar var və yoxlanıldıqdan sonra xronoloji ardıcıllıqla zəncirə əlavə olunur. Bu zəncir qovşaqlar və ya kompüterlər şəbəkəsi tərəfindən saxlanılır və hər bir iştirakçının kitab kitabının eyni nüsxəsinə malik olmasını təmin edir. Bu qeyri-mərkəzləşdirilmiş təbiət şəffaflığı və təhlükəsizliyi gücləndirərək, mərkəzi orqana ehtiyacı aradan qaldırır.

Blokçeynin texnologiyasının əsas xüsusiyyətlərindən biri onun mərkəzləşdirilməmiş olmasıdır. Məlumatların bir qurum tərəfindən saxlanıldığı və idarə edildiyi ənənəvi mərkəzləşdirilmiş sistemlərdən fərqli olaraq, blokçeyn əməliyyatları kollektiv şəkildə saxlayan və təsdiqləyən iştirakçılar şəbəkəsini təmin edir. Bu, banklar və ya dövlət orqanları kimi vasitəçilərə ehtiyacı aradan qaldırır və həmyaşıdlar arası əməliyyatlara imkan verir. Mərkəzsizləşdirmə həm də şəffaflığı artırır, çünki bütün iştirakçılar eyni məlumatlara çıxış əldə edir, beləliklə, fırıldaqçılıq və manipulyasiya riskini azaldır.

Digər mühüm aspekt şəffaflıqdır. Şəbəkənin hər bir iştirakçısı bütün blokçeynin surətinə malik olduğundan, əməliyyatlar hamı üçün görünür, yüksək səviyyədə şəffaflığı təmin edir və fırıldaqçılıq və ya manipulyasiya riskini azaldır. Blokçeynin

növbəti on ildə bir çox sənayeni əhatə edən əsas təməl texnologiya olacağı gözlənilir. Blokçeyn texnologiyasının xüsusiyyətlərinə görə istifadəçilərə verdiyi üstünlüklər aşağıdakılardır:

- ***Anonimlik*** - Anonimlik bu infrastrukturun əsas xüsusiyyətidir və onu həyata keçirmək üçün eyni şəxsləri və təşkilatları cəlb edir. Blokçeynlər istifadəçiləri yalnız kriptosisteminin vacib elementi olan açıq açarlar vasitəsilə tanımağa imkan verir. Bəzi istifadəçilərin hər bir əməliyyat üçün yeni açar yaratması ilə istifadəçilərin lazım olduğu qədər açıq açar yaratması tövsiyə olunur. Bu xüsusiyyət istənilən şəxsə və ya təşkilata hökumətin müdaxiləsi olmadan və son dərəcə aşağı əməliyyat xərcləri olmadan dünyanın istənilən yerinə istənilən məbləğdə pul əməliyyatı aparmağa imkan verir. Bu, bir çox transmilli şirkətləri texnologiyaya cəlb etdi, blokçeyn firmaları American Express, Deloitte və New York Stok Birjası kimi qlobal şirkətlərdən 1 milyard dollar investisiya aldı.
- ***Dəyişməzlik*** - Dəyişməzlik blokçeynin əsas xüsusiyyətidir və indiyə qədər onun uğurunun səbəblərindən biri kimi dəfələrlə müəyyən edilmişdir. Dizaynına görə, zəncirdə bir blokun dəyişdirilməsi hər bir sonrakı blokun dəyişdirilməsini əhatə edəcək, çünki hər blokda əvvəlki məlumat var. Bu, zəncirin genişləndiyi xətti sürət üçün qeyri-mümkündür, yeni bloklar təxminən hər on dəqiqədən bir buraxılır. Bu, geniş miqyasda bir güc kimi görünsə də, bu, həm də bir çatışmazlıq hesab edilə bilər, çünki bu, eyni zamanda, zəncirə girişi redaktə etməyin, məsələn, bir çarə və ya pulun geri qaytarılmasını həyata keçirmək mümkün olmayacaq deməkdir. Bununla belə, əksəriyyət hesab edir ki, bu, insanlara deyil, texnologiyanın arxasında duran riyaziyyata inamı yenidən müəyyənləşdirən sistemin aparıcı atributudur.
- ***Şəffaflıq*** - Blokçeynlər özəl və ya ictimai olaraq təsnif edilə bilər. Şəxsi və ictimai blokçeyn arasındakı yeganə fərq, icazəli blokçeyn kimi də adlandırılan özəl blokçeyn kontekstində şəbəkəyə girişin məhdudlaşdırılmasıdır (məsələn, kommersiya qurumu tərəfindən idarə olunan giriş məhdudlaşdırılmış platforma, özəl kapital izləmə aləti özəl kapital müqavilələri üçün və s.). Əksinə, ictimai blokçeynlər tamamilə şəffaf paylanmış kitabdır, şəbəkədəki bütün istifadəçilər baş

vermiş bütün əməliyyatları görə bilirlər. Bütün istifadəçilərin əvvəlki tranzaksiyaları görmək imkanı əsasən dəyişməzlik faktoru ilə bağlıdır, beləliklə, zənciri dəyişikliklərdən və saxtakarlıqdan qoruyur. Məxfiliyin olmamasının bəzi istifadəçilər üçün problem sayıla biləcəyi iddia edilsə də, sistemin şəffaflığı daha çox təqdir edilmişdir. Blokçeyn texnologiyasının, infrastrukturun bir çox tətbiqi təklif olunmaqla, pozucu texnologiyanın xüsusiyyətlərini göstərdiyi sübut edilmişdir. Blokçeyn texnologiyasının öz varlığı kimi yaşayıb-yaşamayacağı ilə bağlı texnologiya sahəsində xeyli müzakirələr aparılıb, bir çox ekspert onun pul dəyəri olmadan yaşaya bilməyəcəyinə inanır. Bununla belə, belə bir konsepsiyanın bir çox potensial istifadəsi ilə onun yalnız maliyyə sənayesində istifadə ediləcəyi ehtimalı azdır.

Blokçeynin texnologiyasının təkamülü müxtəlif funksiyaları təklif edən müxtəlif blokçeyn platformalarının meydana çıxması ilə davam edir. Məsələn, Ethereum, blokçeynin faydasını valyutadan kənarda genişləndirərək, mərkəzləşdirilməmiş tətbiqlər (DApps) və qeyri-işlənə bilən tokenlər (NFTs) konsepsiyasını təqdim etdi. Birlikdə işləmə qabiliyyəti və miqyaslılıq blokçeynin inkişafında mərkəz nöqtələri olaraq qalır. Fərqli blokçeynlərin problemsiz əlaqə saxlamasına imkan yaratmaq, daha çox əlaqəli ekosistemi inkişaf etdirmək üçün səylər davam edir. Yan zəncirlər, parçalanma və 2-ci səviyyə protokolları kimi həllər təhlükəsizliyə xələl gətirmədən əməliyyatın ötürülməsini təkmilləşdirməklə miqyaslılıq problemlərini həll etməyi hədəfləyir.

Bütün dünyada hökumətlər və tənzimləyici orqanlar innovasiya və mövcud qanunlara uyğunluq arasında tarazlıq yaratmaq, istehlakçıların müdafiəsini təmin etmək və sənaye artımını təşviq etmək üçün blokçeyn texnologiyasını tənzimləmək yollarını araşdırır. Blokçeyn texnologiyasının tətbiq olunduğu sahələr aşağıdakılardır:

- ***Ağıllı Müqavilələr*** - Ağıllı müqavilələrin müzakirəsi, ilk dəfə 1994-cü ildə Nik Szabo tərəfindən təqdim edilən blokçeynin meydana çıxmasından çox əvvəl mövcud idi, lakin bu, texnologiyanın bu günə qədər ən çox düşünülmüş istifadələrindən biridir. Ağıllı müqavilələr müqavilənin şərtlərini avtomatik yerinə yetirən kompüter proqramları və ya istifadəçi interfeysləri kompüter protokolları

ilə birləşdirildikdə yerinə yetirilən müqavilələr kimi müəyyən edilir. İndi hesab olunur ki, Szabonun yaradıcı ideyası qeyri-mərkəzləşdirilmiş kriptosistem vasitəsilə ağıllı müqavilələr aparmaqla reallığa çevrilə bilər, o, naməlum və etibarsız tərəflərə üçüncü tərəfə ehtiyac olmadan təhlükəsiz əməliyyatlar aparmağa imkan verir. Blokçeyn istifadə edərək yaradıla bilən potensial uyğun müqavilələrə evlilik müqavilələri və transmilli kredit proqramları daxildir. Ağıllı müqavilələrin istifadəsi ilə mümkün bazar baloncukları yaradan dəyişkənlik, həmçinin tənzimləmənin olmaması və müqavilələrin geri alınmazlığı kimi bir sıra risklər var. Bunun əksinə olaraq, ağıllı müqavilələrin çəkdiyi risklər ənənəvi ilə müqayisədə əhəmiyyətli dərəcədə azalır, çünki onlar avtonom, özünü təmin edir və mərkəzləşdirilməmişdir.

- ***Təchizat Zəncirinin İdarə Edilməsi*** **-** Tez-tez müəyyən edilir ki, tədarük zəncirləri istehlakçılar üçün qeyri-şəffafdır, məhsulların haradan gəldiyini və hara getdiyini müəyyən etmək getdikcə çətinləşir. Blokçeyn bu halda hər bir qovşaqda mövcud olan və tədarük zəncirində məhsulların izlənilməsinin rəsmi jurnalını yaradan şəffaf kitab kimi istifadə edilə bilər. Blokçeyn vasitəsilə SCM ideyası, qidada bakteriyaların baş verməsini izləmək üçün texnologiyadan istifadə edən və mənbəni dəqiq müəyyənləşdirə və geri çağırılmalı olan maddələrin sayını məhdudlaşdıra bilən Walmart tərəfindən konseptuallaşdırılmışdır. Qeyri-etik davranışa son qoymaq üçün almaz sənayesində də tətbiq edilmişdir.
- ***Səsvermə Sistemləri*** **-** Müasir konsepsiya maliyyə dairələrindən kənarda onlayn səsvermə sistemlərinə də genişləndirilə bilər, çünki məlumatların anonimləşdirilməsi istənilən səsvermə texnologiyası üçün zəruri olan şəxsi məlumatları qoruyur. Blokçeyndən səsvermə sistemlərində istifadə etməklə, hər bir səsin dəqiq qeydə alınması ilə daha çox şəffaflıq olacaq. Həmçinin təklif edilib ki, siyasətçilərin hakimiyyətə səs verməsi ilə yanaşı, siyasi qalmaqal baş verərsə, səslərin dəyişdirilməsi üçün də istifadə oluna bilər, nəticədə siyasətçi artıq səs çoxluğuna malik olmayacaq. Danimarkanın Liberal Alyansı siyasi partiyası tərəfindən 2014-cü ildə daxili seçkilər üçün blokçeyn səsvermə sistemindən istifadə edilib. 2018-ci ilin mart ayında Sierra Leone prezident seçkiləri prosesində

etimad və şəffaflığı təmin etmək üçün blokçeyndən istifadə edən dünyada ilk ölkə oldu. Agora adlı müstəqil bir fond tərəfindən izlənilən seçkidə verilən hər bir səs xüsusi icazəli blokçeyndə qeydə alınıb.

- ***MikroPayment*** **-** Blokçeyn texnologiyasının istifadəsi hazırda ekspert proqramçılar tərəfindən bütün internet brauzerlərinə və vebsaytlara daxil edilir. Bununla belə, bunun mikroödəmələrin ödənilməli olduğu "ölçülü internet"ə imkan verə biləcəyindən qorxurlar. Mikropayment çox kiçik ödəniş kimi müəyyən edilir və kriptovalyuta baxımından bu, 8-10 bitcoin olacaq. Mikroödənişlər ən çox musiqiçilər və rəssamlar üçün onlayn paylanan iş üçün qonorarların toplanması ilə bağlı axtarılır. Belə ödənişləri toplayan sənətçilərdən biri öz musiqisini satmaq üçün blokçeyndən istifadə edən Böyük Britaniyadan olan Imogen Heap-dir. Həmçinin mikroödəmələrin həyata keçirilməsinin spam poçtlarının baş verməsini azaldacağı da irəli sürülüb, çünki hər bir e-poçtda mikro ödəniş olacaq. Bitcoin mikroödəmələrdə getdikcə daha rəqabətli hala gəldi, lakin daha çox əsas təşkilatın bu sənayedə rəqabət aparmaq üçün əməliyyat xərclərini azaltmayacağına inanmaq üçün heç bir səbəb yoxdur.
- ***Əşyaların İnterneti*** **-** Blokçeyn texnologiyasının təklif olunan geniş istifadəsi, ağıllı cihazların bütün kommunikasiyalarının təhlükəsiz şəkildə saxlanıldığı Əşyaların İnternetini (IoT) əhatə edir. IBM və Samsung artıq IoT və blokçeyn texnologiyalarından istifadə edərək öz yuyucu vasitəni aşağı olduqda sifariş etmək üçün bir paltaryuyan maşın yaratdılar və bu, eksperiment kimi başlayan şeyin indi qlobal səviyyədə tanındığını göstərir. Blokçeyn IoT və ya ağıllı cihazların real vaxtda əməliyyatlar aparmasına və ünsiyyət qurmasına imkan verir və "mobil pul kisələri'nin sürətlə artması ilə ödənişlər mobil telefonlar vasitəsilə ödənilə bilər. IoT-də blokçeynin istifadəsi təklif olunan biri hesablaşma sistemidir. Milyonlarla ağıllı cihazın bir-biri ilə əlaqə saxlaması və əməliyyatlar aparması ilə bankların real vaxt rejimində trilyonlarla əməliyyatı emal etməsi mümkün deyil və bu şəraitdə blokçeyn işə düşəcək. Hələ ki, geniş tətbiq olunmasa da, potensial ümidvericidir.
- ***Xidmət Sistemləri*** **-** Blokçeyn texnologiyası səhiyyə sənayesində də araşdırılır. Blokçeynin təhlükəsiz və şəffaf təbiəti tibbi qeydlərin saxlanması və paylaşılması

üçün vahid və təhlükəsiz sistem yaratmaq üçün istifadə edilə bilər. Bu, xəstənin məxfiliyini artıra, tibbi səhvləri azalda və səhiyyə xidmətlərinin ümumi səmərəliliyini artıra bilər. Blokçeyn həmçinin müxtəlif səhiyyə təminatçıları arasında sağlamlıq məlumatlarının təhlükəsiz mübadiləsini asanlaşdıra bilər, problemsiz koordinasiyanı və qayğının davamlılığını təmin edə bilər. Blokçeyn xeyriyyəçilik sektorunda inqilab etmək potensialına malikdir. Blokçeyn istifadə edərək, donorlar töhfələrinin necə istifadə edildiyini və paylandığını görə bilərlər. Ağıllı müqavilələr vəsaitlərin bölüşdürülməsi, şəffaflığın və hesabatlılığın təmin edilməsi prosesini avtomatlaşdıra bilər. Bu, xeyriyyə təşkilatlarına ictimai inamı artıra və daha çox insanı ianə verməyə təşviq edə bilər. Rəqəmsal reklam sahəsində blokçeyn texnologiyası fırıldaqçılıq və şəffaflığın olmaması məsələlərini həll edə bilər. Reklamçılar tez-tez reklam fırıldaqçılığı, səhv hesabat göstəriciləri və reklamçılarla naşirlər arasında etibarın olmaması ilə bağlı problemlərlə üzləşirlər. Blokçeyn əsaslı həllər reklam yerləşdirmələrini izləmək üçün şəffaf və yoxlana bilən sistem təklif edə bilər, reklam verənlərin ödədiklərini almasını və reklamlarının nəzərdə tutulan auditoriyaya çatmasını təmin edir. Blokçeyn texnologiyası əqli mülkiyyət hüquqları və royaltilərin idarə edilməsi sahəsində də mühüm rol oynaya bilər. Blokçeynin dəyişməzliyi və izlənilməsi ilə mülkiyyət hüquqlarını, patentləri və müəllif hüquqlarını izləmək və idarə etmək daha asan olur.

Blokçeyn texnologiyası inkişaf etməyə davam etdikcə, onun müxtəlif sənaye sahələrində əhatə dairəsi və təsirinin genişlənəcəyi gözlənilir. Bununla belə, onun həyata keçirilməsinə ehtiyatla yanaşmaq və yarana biləcək hər hansı tənzimləyici, hüquqi və məxfilik problemlərini həll etmək vacibdir. Texnoloji innovatorlar, bizneslər, hökumətlər və tənzimləyici orqanlar arasında əməkdaşlıq blokçeyn texnologiyasının məsuliyyətli və geniş şəkildə tətbiqini təmin etmək üçün vacib olacaqdır. Maliyyə sistemlərinin və təchizat zəncirlərinin transformasiyasından tutmuş şəxsiyyət idarəçiliyi və səhiyyədə inqilabi dəyişikliklərə qədər blokçeyn sənayeləri yenidən formalaşdırmaq və daha şəffaf, təhlükəsiz və səmərəli rəqəmsal dünya yaratmaq gücünə malikdir. Bu texnologiyanı mənimsədikcə və onun imkanlarını

araşdırmağa davam etdikcə, etik nəticələri də nəzərə almaq və blokçeynin faydalarının hamı üçün əlçatan olmasını təmin etmək çox vacibdir.

1.2 Ağıllı şəhərlərdə təhlükəsizlik problemləri və imkanları

Son iki onillikdə "ağıllı şəhər" anlayışı getdikcə şəhərləşən dünyada güclü real tələbi və praktiki fonu səbəbindən həm akademik, həm də sənaye sahələrində artan diqqəti cəlb etmişdir. Ağıllı şəhərlərin inkişafı ilə ayaqlaşmaq üçün bir çox memarlıq dizayn edilmişdir. Bununla belə, bildiyimiz qədər vahid IoT arxitekturası yoxdur. Bu işin vurğusu ağıllı şəhərlərdə təhlükəsizlik və məxfilik məsələlərini ümumiləşdirmək olduğundan, burada təsvir edilən arxitektura tanınmış üç qatlı arxitekturaya və təklif olunan ümumi qəbul edilmiş arxitekturaya əsaslanır.

Tətbiq qatı, dəstək qatı və qavrama qatı adlanan təbəqələr arxitekturanın əsas təbəqəsidir. Qavrayış təbəqəsi əsasən real dünyadakı əşyalardan (məsələn, heterojen cihazlar, WSN-lər və sensorlar) məlumatların toplanması və əldə edilmiş məlumatın sonrakı emal üçün şəbəkə səviyyəsinə ötürülməsi üçün istifadə olunur. Şəbəkə səviyyəsi İnternet, WSN və rabitə şəbəkələri kimi əsas şəbəkələrdən asılı olan IoT arxitekturasının əsas təbəqəsidir. Bu təbəqənin məsuliyyəti qavrayış təbəqəsi tərəfindən toplanmış məlumatları ötürmək və ağıllı şeyləri, şəbəkə cihazlarını və serverləri birləşdirməkdir.

Şəkil 1.1 Ağıllı şəhər üçün IoT əsaslı memarlıq

Tətbiq qatı ilə çox yaxından işləyən dəstək qatı, ağıllı hesablama texnikaları (məsələn, bulud hesablamaları, kənar hesablamalar) vasitəsilə şaxələndirilmiş tətbiqlərin tələblərinə dəstək verir.

Tətbiq qatı, üst qat olaraq, istifadəçilərə fərdiləşdirilmiş tələblər əsasında ağıllı və praktik xidmətlər və ya proqramlar təqdim etmək üçün məsuliyyət daşıyır.

Ağıllı şəhərlərin qurulmasında məqsəd sakinlərə enerji, ətraf mühit, sənaye, yaşayış və xidmətlər kimi sakinlərin həyat standartları ilə sıx bağlı olan müxtəlif aspektlərdə fayda verməkdir. Ağıllı şəhərlərin ortaya çıxan ağıllı tətbiqləri aşağıdakı kimi təsnif olunur:

- ***Ağıllı Hökumət*** - Ağıllı hökumət ağıllı şəhərdə həlledici rol oynayır. Ağıllı hökumətin məqsədi informasiya texnologiyalarına əsaslanan məlumatları, institutları, prosesləri və fiziki infrastrukturları bir-biri ilə əlaqələndirməklə vətəndaşlara və icmalara daha yaxşı xidmət göstərməkdir. Bundan əlavə, ağıllı idarəetmə vətəndaşlara ictimai qərarların qəbulunda və şəhər planlaşdırılmasında iştirak etməyə imkan verir ki, bu da səmərəliliyi artıra və eyni zamanda məlumat şəffaflığını artıra bilər. Məsələn, e-hökumət fərdlərə konfrans mərkəzinə müraciət etmək, hesabların ödənilməsi və problemlərlə bağlı hesabat vermək kimi dövlət xidmətlərindən onlayn istifadə etməyə imkan verir.
- ***Ağıllı Nəqliyyat*** - Ağıllı nəqliyyatın məqsədi nəqliyyat sistemlərinin "daha ağıllı" istifadəsini təmin etməkdir. Xüsusilə, intellektual nəqliyyat şəbəkələri təhlükəsizliyi, sürəti və etibarlılığı artırmaqla əhaliyə daha yaxşı xidmət göstərə bilər. Nəqliyyat yönümlü mobil proqramlardan istifadə etməklə istehlakçılar ən qənaətcil və ən sürətli marşrutları taparkən öz cədvəllərini asanlıqla planlaşdıra bilərlər. Ağıllı nəqliyyat vasitələrinin digər ümumi tətbiqləri sürücünün pasportları, lisenziyanın tanınması sistemləri, avtomobil dayanacağı axtarışı və proqnozlaşdırılmasıdır.
- ***Ağıllı Mühit*** - Ağıllı mühit davamlı cəmiyyətin qurulması baxımından əhəmiyyətli dərəcədə töhfə verə bilər. Xüsusilə, texniki idarəetmə alətlərini qəbul etməklə, ağıllı şəhər enerji istehlakını, havanın keyfiyyətini, binaların struktur etibarlılığını

və nəqliyyat sıxlığını izləmək və çirklənmə və ya tullantıları səmərəli şəkildə həll etmək imkanına malikdir. İdeal olaraq, yeni ekoloji sensor şəbəkələri hətta gələcəkdə təbii fəlakətləri proqnozlaşdırmaq və aşkar etmək qabiliyyətinə malik ola bilər.

- ***Ağıllı Xidmətlər*** - Ağıllı xidmətlər vətəndaşlara bir çox aspektlərdə fayda verir. Məsələn, ağıllı səhiyyə proqramları daşınan cihazlar və tibbi sensorlar vasitəsilə insanların sağlamlıq vəziyyətini vaxtında izləyə bilər. Bundan əlavə, bəzi ağıllı xidmətlər məişət cihazlarının uzaqdan idarə olunması kimi rahat, ağıllı və enerjiyə qənaət edən yaşayış mühitləri yarada bilər. Nəhayət, sosial şəbəkələr, əyləncələr, ağıllı alış-veriş və digər ağıllı xidmətlər insanların gündəlik həyatının rahatlığını xeyli yaxşılaşdırıb.

Yuxarıda qeyd olunan ağıllı proqramlar ilə ənənəvi tətbiqlər arasındakı fərqləri anlamaq vacibdir. Bundan əlavə, hər hansı yeni təhlükəsizlik və ya məxfiliyin qorunması metodunu hazırlamazdan əvvəl ağıllı şəhərlərin xüsusiyyətləri nəzərə alınmalı və birləşdirilməlidir.

1) ***Heterojenlik*** - IoT əsaslı sistemlərdə yüksək heterojenlik ən fərqləndirici xüsusiyyətdir, yəni sistemlər müstəqildir, paylanır, saxlanılır və ya müxtəlif istifadəçilər tərəfindən istifadə olunur. Bu, həmçinin IoT qovşaqlarının, kommunikasiya protokollarının və texnologiyalarının, mobillik vasitələrinin, müxtəlif aparat performanslarına, platformalarına və s.-ə aiddir. Bildiyimiz qədər, ağıllı şəhərin vahid tərifi yoxdur və IoT arxitekturası ağıllı-aydınlara görə dəyişir. şəhər. Buna görə də ümumi təhlükəsizlik çərçivəsinin və xidmətinin olmaması digər böyük problemdir.
2) ***Resurs Məhdudiyyətləri*** - Əksər əşyaların cihazlarında məhdud resurs var ki, bu da təkcə məhdud yaddaş, batareya tutumu və emal imkanları deyil, həm də aşağı güclü radio standartlarına görə məhdud şəbəkə interfeysləri deməkdir. Daha konkret desək, daha ucuz, kiçik, lakin enerji çatışmazlığı olan quraşdırılmış qurğular ağıllı şəhərlərdə geniş şəkildə tətbiq olunur. Tipik olaraq, bu cihazların təsadüfi giriş yaddaşı və saxlama imkanları 8 və ya 16 bitlik mikro nəzarətçilərlə məhduddur. IEEE 802.15.4 radio ilə təchiz edilmiş simsiz şəbəkələr aşağı məlumat

sürətinə və çərçivə ölçülərinə səbəb olur (müvafiq olaraq 20-250 kb/s və 127 oktete qədər).

3) ***Hərəkətlilik*** - Şəhər mobilliyi müasir şəhərlərin inkişafı və tərəqqisi üçün mühüm mühərrik kimi qəbul edilmişdir. Ağıllı şəhərlərdə mobillik təkcə şəhərdaxili hərəkətə və malların bir yerdən digər təyinat yerinə çatdırılmasına deyil, həm də şəhərdaxili simsiz rabitə və nəqliyyat axınının real vaxt rejimində monitorinqi kimi texnologiyalar, eləcə də çevik reaksiyalar deməkdir. Bundan əlavə, ağıllı şəhərlərdə mobillik yaxşı inkişaf etmiş kommunikasiya infrastrukturu vasitəsilə fərdiləşdirilir.
4) ***Qoşulma və Miqyaslılıq*** - Bağlantı istənilən cihazın ağıllı dünyaya qoşulmasına imkan verir. Bu, uğurlu bir ağıllı şəhər üçün ən əsas xüsusiyyətdir və ağıllı şəhər planlarını irəli aparmaq üçün əsas hesab edilmişdir. Eyni zamanda, miqyaslılıq ağıllı şəhər ssenarilərində görünən bir xüsusiyyətdir. Ağıllı şəhərlər kiçikdən böyüyə sürətlə inkişaf edir ki, bu da həm məlumatların, həm də şəbəkə trafikinin sürətlə artmasına səbəb olur. Buna görə də ağıllı şəhər genişlənən sistemlər və mexanizmlər olmadan yaxşı işləyə bilməz.
5) ***İstifadəçilərin cəlb edilməsi*** - Ağıllı şəhərin tərifi təkcə qabaqcıl texnologiyalar və infrastrukturlardan ibarət deyil, insan faktorları (təhsil, yaradıcılıq və təhsil) də ağıllıların inkişafı üçün vacibdir, çünki ağıllı şəhərlərin qurulmasında əsas məqsəd sakinlərə xidmət göstərməkdir. Bundan əlavə, vətəndaşların iştirakı həmin ağıllı tətbiqlərin keyfiyyətini artıra bilər. Məsələn, onların tələblərinin və təhlükəsizliklə bağlı narahatlıqlarının ilkin anlaşılması mühafizə strategiyaları baxımından ən yaxşı nəticə ilə nəticələnəcək.

Son illərdə müxtəlif tətbiq ssenarilərində əhəmiyyətli problemlər aşkar edilmişdir. Məsələn, ağıllı şəbəkələrdəki ağıllı ölçmə infrastrukturu sakinlərin şəxsi həyatlarına, o cümlədən onların yaşayış vərdişlərinə və iş saatlarına nəzarət edə bilər. Eynilə, ağıllı evlər və səhiyyə kontekstində cihaz istehsalçıları və xidmət təminatçıları həssas məlumatlara giriş əldə edə bilərlər. Bundan əlavə, ağıllı mobillik proqramları tərəfindən toplanan böyük miqdarda trayektoriya məlumatı istifadəçinin yeri və hərəkət nümunələri haqqında nəticə çıxarmaq üçün istifadə edilə bilər. Bu problemlərə

əlavə olaraq, aşağıdakı maddələr sürətlə inkişaf edən ağıllı proqramlar tərəfindən yaradılan ən son problemlərdir.

- ***Botnet Fəaliyyətləri*** - Əşyaların İnterneti əsaslı Ağıllı Şəhərlərdə Bu yaxınlarda ortaya çıxan IoT botnetləri IoT sistemləri üçün ciddi təhlükələr törədir. Nümunəvi nümunə, cihazları (məsələn, IP kameralar, veb-kameralar, printerlər, DVR-lər və marşrutlaşdırıcılar) yoluxdura bilən, bir çox heterojen IoT cihazlarına infeksiya yaya bilən və nəhayət hədəf serverlərə qarşı DDoS-a səbəb ola bilən mirai botnetidir. Kompüterlər və ağıllı telefonlarla müqayisədə, IoT cihazları çox vaxt zəif təhlükəsizliklə və ya ümumiyyətlə heç olmasa dizayn edilir.
- ***Ağıllı Şəhərlərdə Sürücüsüz Avtomobillərin Təhdidləri*** - Yüksək texnologiyalı şirkətlər yol qəzalarını azaltmaq və daha təmiz və daha ağıllı bir cəmiyyət qurmaq məqsədi ilə avtonom nəqliyyat vasitələrinin (AVs) inkişafına milyardlarla dollar xərcləyiblər. Bununla belə, sürətlə böyüyən bu proqram əsas təhlükəsizlik problemi kimi qəbul edilir, çünki AV sındırıldıqdan sonra həm həyat təhlükəsizliyi, həm də məlumatların məxfiliyi təhlükə altına düşəcək. Xüsusilə, hakerlər əyləc basmaq, mühərriki söndürmək və sükanı idarə etmək kimi uzaqdan hücumlar həyata keçirmək üçün təhlükəsizlik səhvlərindən istifadə edə bilərlər. Bundan əlavə, özü idarə olunan avtomobilin kompüter sistemi tərəfindən toplanan kütləvi fərdi məlumatlar əhəmiyyətli məxfilik problemlərinə səbəb ola bilər.
- ***Ağıllı Şəhərlərdə Virtual Reallığın Məxfilik Problemləri*** - Texnologiyaya əsaslanan ağıllı şəhərlərdə virtual reallıq (VR) texnologiyası şəhər planlaşdırma şöbələri, səhiyyə xidməti təminatçıları və mühəndislik sənayesi sektoru kimi müxtəlif təşkilatlar və qurumlar tərəfindən mənimsənilib. Bununla belə, üçüncü tərəflərlə paylaşılan həssas məlumatlar, VR cihazları arasında şifrələnməmiş rabitə və sensorlar tərəfindən saxlanılan məlumatların hamısı məxfiliyin sızması təhlükəsi yaradır.

Doğrulama ağıllı sistemin müxtəlif təbəqələri üçün əsas tələbdir və şəxsiyyətləri sübut etmək və yalnız səlahiyyətli müştərilərin heterojen sistem üzrə xidmətlərə daxil ola bilməsini təmin etmək üçün lazımdır. Xüsusilə, ağıllı şəhərlərdə yerləşdirilən IoT cihazları şəbəkəni, digər qovşaqları və idarəetmə stansiyalarından gələn mesajları

autentifikasiya edə bilər. Bundan əlavə, ağıllı şəhərlərdə autentifikasiya məlumatlarının miqdarı sürətlə artdığından, real vaxt və dəqiq autentifikasiyanı təmin etmək üçün qabaqcıl texnologiyaların hazırlanması vacibdir. Məxfiliyin məqsədi məlumatın passiv hücumlardan və ya yanlış mənbəyə məruz qalmasının qarşısını almaqdır. IoT əsaslı tətbiqlərdə təcavüzkarların ünsiyyəti dinləmək və ya cihazlara daxil olmaq qabiliyyətinə malik olduğu güman edilir. Buna görə də, qovşaqlar arasında məlumat ötürülməsinin məxfiliyini qorumaq üçün etibarlı rabitə və saxlama sistemlərinin qurulması üçün şifrələmə əsaslı texnologiyalar geniş tətbiq olunur. Maraqlıdır ki, şəffaflıq və etibarlılıq identifikasiya və autentifikasiya üsullarının dizaynını çətinləşdirən iki amildir.

Ümumiyyətlə, əlçatanlıq o deməkdir ki, cihazlar və xidmətlər lazım olduqda əlçatan olmalıdır. Mövzumuza uyğun olaraq, ağıllı sistemlər və ya tətbiqlər hücuma məruz qaldıqda belə effektiv işləmə qabiliyyətinə malik olmalıdır. Üstəlik, bu qurğular hücumlara həssas olduğundan, ağıllı sistem hər hansı anormal vəziyyəti aşkar etməli və sistemə gələcək zərərləri dayandırmaq qabiliyyətinə malik olmalıdır. Dayanıqlıq, hücumlar və geniş miqyaslı fəlakətlər nəticəsində yaranan müxtəlif nasazlıqlara və uğursuzluqlara dözə bilən sistemin hücuma davamlılıq qabiliyyəti kimi qəbul edilir. Müdafiə mexanizmləri güclü möhkəmliyə və getdikcə daha ağıllı hücumların öhdəsindən gəlmək üçün adaptiv şəkildə öyrənməyə davam etmək qabiliyyətinə malik olmalıdır. Həm IoT cihazlarının, həm də cihazlar və bulud arasında mübadilə edilən məlumatların bütövlüyünü təmin etmək də vacibdir. Ümumi ağıllı tətbiqetmədə bir çox cihaz arasında məlumat mübadiləsi aparıldığı üçün, məlumat yaxşı qorunmursa, ötürülmə prosesi zamanı asanlıqla dəyişdirilir. Firewall və protokollar kimi bəzi üsullar IoT kommunikasiyalarında məlumat trafikini idarə edə bilər, lakin əksər IoT cihazlarının aşağı hesablama gücünə görə son nöqtələrdə bütövlüyü təmin edə bilməz.

Ağıllı şəhərdə yerləşdirilən cihazların və şəbəkələrin zəifliklərinə görə, ağıllı sistem yalnız iş şəraitinə nəzarət etmək və hər hansı anormal hadisələri vaxtında aşkar etmək imkanına malik olduqda təhlükəsiz hesab edilə bilər. Ənənəvi müdaxilənin aşkarlanması sistemi (IDS) üç yanaşmada geniş istifadə olunur: sui-istifadənin aşkarlanması, anomaliyaların aşkarlanması və spesifikasiyaya əsaslanan aşkarlama.

Bununla belə, heterojen və mürəkkəb ağıllı şəhər ekosistemində qlobal IDS həllinin sadə uyğunlaşması çevik deyil və qeyri-realdır. Bundan əlavə, sensorlar və cihazların əksəriyyəti resurs məhdud olduğundan, yüngül müdaxilənin aşkarlanması üsulları hazırlanmalıdır. Daxil olan təhdidləri əvvəlcədən proqnozlaşdırmaq və bilmək, hücumdan sonra aşkarlanmaq və bərpa etməkdən daha yaxşıdır. Eynilə, ağıllı şəbəkələrə yönəlmiş bir araşdırma göstərdi ki, bir çox zərərli hücumlar qorunub saxlanılır, bu o deməkdir ki, hücumu aşkar etdikdən sonra tədbirlər görmək çox gecdir və mövcud təhlükəsizlik mühafizəsi strategiyaları ağıllı şəbəkə üçün kifayət qədər qorunma təmin edə bilmir. Buna görə də, təhlükəsizlik vəziyyətindən xəbərdar olmaq və ağıllı tətbiqlərə müxtəlif hücumları avtomatik olaraq proqnozlaşdırmaq üçün intellektual IPS sistemlərinin hazırlanması böyük əhəmiyyət kəsb edir.

IoT, İnternet, ağıllıfon şəbəkələri, sosial şəbəkələr və sənaye şəbəkələri kimi müxtəlif şəbəkələrin bir-birinə bağlı və inteqrasiya olunduğu şəbəkələr şəbəkəsi kimi görünə bilər. Bu tip mürəkkəb mühitdə ən son problemlərin öhdəsindən gəlmək üçün yeni effektiv texnologiyalar tələb olunur. Məsələn, IoT-əsaslı infrastrukturlarda zərərli proqramların yayılması xüsusiyyətlərinin başa düşülməsi, simsiz sensor şəbəkələrində məlumatın yayılma nümunələrinin modelləşdirilməsi və effektiv qarşısının alınması strategiyalarının hazırlanması böyük əhəmiyyət kəsb edir. Ağıllı şəhərləri həyata keçirmək üçün inkişaf etməkdə olan bir texnologiya olaraq, duman əsaslı strukturlar yeni təhlükəsizlik problemləri təqdim edir, çünki paylanmış duman sistemlərinin əməliyyat mühitləri mərkəzləşdirilmiş buludlardan daha çox hücumlara qarşı həssasdır. Buludlarla müqayisədə duman sistemləri kiçikdir, nəticədə onların özlərini qorumaq imkanları məhduddur. Bundan əlavə, duman qovşaqları son istifadəçilərə yaxın olduğundan, şəxsi həssas məlumatlar kənardan çıxmazdan əvvəl istehlakçıların məxfiliyini qorumaq üçün qiymətli imkanlar təmin edir. Buna görə də, duman əsaslı ağıllı sistemlərdə ağıllı cihazların qorunmasına daha çox diqqət yetirilməlidir.

İstifadəçi mərkəzli ağıllı şəhərlərdə istehlakçılar istənilən vaxt məlumatları bir xidmət provayderindən istənilən digər xidmət təminatçısına silmək və ya köçürmək hüququna malik olmalıdırlar. Bundan əlavə, insanların təhlükəsizlik və məxfiliyə olan üstünlükləri nəzərə alınmalıdır, çünki münasibət və tələblər şəxsdən asılı olaraq dəyişə

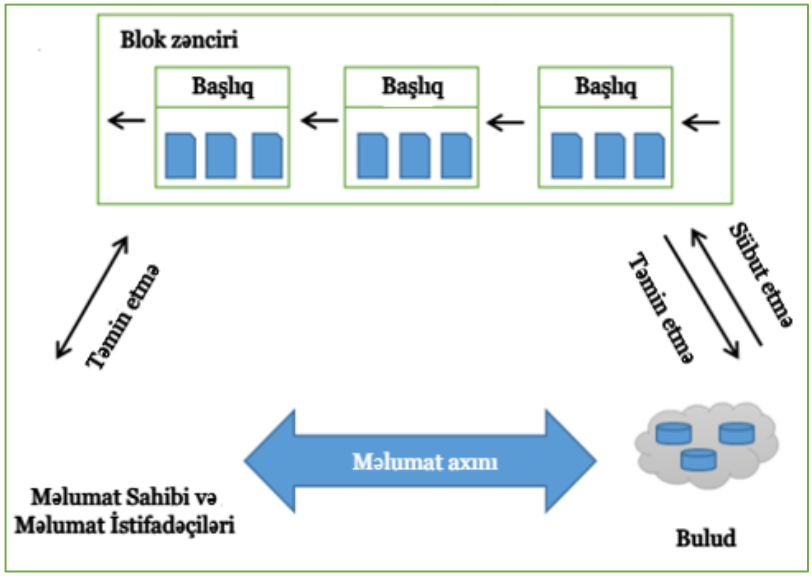
bilər. Üstəlik, konfiqurasiya edilə bilən məxfilik parametrlərinin sayının artması istifadəçilərin parametrlərini faktiki üstünlükləri ilə uyğunlaşdırmağı çətinləşdirir. Buna görə də, müxtəlif ağıllı tətbiqlərin həm təhlükəsizliyini, həm də rahatlığını artıra bilən istifadəçi dostu qoruyucu köməkçilərin inkişafı ümidvericidir.

1.3 Ağıllı şəhərin inkişafında blokçeyn texnologiyalarının rolu

Ağıllı sistemlər avtobuslar, evlər, parklar və ticarət mərkəzləri kimi bir çox sahədə istifadə olunur. İntellektual sistemlər insanların ehtiyaclarına uyğun yaradılmış texnologiyalardır. İnsanların ehtiyaclarını bilmək və onlara uyğun texnologiyalar istehsal etmək məlumatların toplanması və təhlili ilə mümkündür. Vətəndaşlara dövlət xidmətlərinin effektiv şəkildə göstərilməsinə və şəhər idarəçiliyinin təkmilləşdirilməsinə kömək etmək üçün toplanmış məlumatların toplandığı qədər təhlükəsiz saxlanılması böyük əhəmiyyət kəsb edir. Bu səbəbdən blokçeyn texnologiyası və ağıllı şəhər sistemləri birləşdirilir. Məlumatların icazəsiz dəyişdirilməsinə imkan verməyən blokçeyn texnologiyası təhlükəsizlik limitini daha yüksək dəyərlərə qaldırır. Ağıllı şəhər sistemlərində fərqli istifadə sahələrindən biri olan ağıllı şəhər sistemlərini istifadəyə yararlı hala gətirən cihaz sistemləridir. Zaman keçdikcə cihazların sayı və tətbiqlərin mürəkkəbliyi artır. Ağıllı şəhərlərdəki cihazlar və qovşaqlar çevik şəkildə şəbəkəyə qoşula və ya ayrıla bilər. Mərkəzləşdirilmiş sistemlərlə müqayisədə mərkəzləşdirilməmiş sistemlər cihazların sayının və tətbiqlərin mürəkkəbliyinin dəyişdiyi dinamik ssenarilər üçün daha uyğundur. Digər bir məqam isə şəhər rəhbərliyidir. Vətəndaşların iştirak, demokratiya və şəffaflıq istəyi güclüdür. Hökumət hökumət işləri, ətraf mühitlə bağlı məlumatlar və qərar qəbuletmə prosesi kimi şəhər hökuməti ilə bağlı məlumatları vətəndaşlara açıqlamalıdır. Şirkətlərdən həmçinin müştəri ilə bağlı məlumatların necə istifadə edildiyini açıqlaması tələb olunur. Blokçeyn bu problemlərin həllini təmin edir. Blokçeyn xüsusiyyətləri ağıllı şəhərlərdə bu çətinliklərin öhdəsindən gəlmək qabiliyyətinə malikdir.

Blokçeyn sistemləri adətən mərkəzi üçüncü tərəf olmadan “peer-to-peer” işləyir. Sistemdə hər bir qovşaq real dünya kimliyini gizli saxlayaraq ictimai təxəllüs ünvanı

ilə əlaqələndirilir. Daxili psevdonimləşdirmə istifadəçilərin şəxsiyyətlərinin məxfi saxlanmalı olduğu istifadə halları üçün uyğundur. Blokçeyn texnologiyası hər kəsə bütün əməliyyat qeydlərinə daxil olmaq imkanı verir və onları şəffaf edir. Konsensus alqoritmləri blokçeynəyə daxil edilməzdən əvvəl razılığa gəlmək üçün bütün mərkəzləşdirilməmiş qovşaqlar tərəfindən icra edilir. Beləliklə, blokçeyn sistemində qərarlar bütün qovşaqlar tərəfindən "peer-to-peer" qaydasında qəbul edilir və onu demokratikləşdirir. Blokçeyn sistemində bütün əməliyyatlar rəqəmsal imzadan istifadə etməklə imzalanır. İstənilən kiçik dəyişiklik fərqli bir hash yaradır və dərhal aşkar edilə bilər ki, bu da paylaşılan kitabı dəyişməz edir. Bu yaxşı xüsusiyyətlərə görə, blokçeyn texnologiyasının ağıllı şəhərlərə tətbiqi məlumatların bütövlüyünü təmin edə bilər. O, həmçinin yerli və milli hökumət sistemlərindəki şirkətləri, məktəbləri, xəstəxanaları, universitetləri və fərdləri məlumatları paylaşmağa və ortaq qərarların qəbulunu təşviq etməyə, şəffaf şəhər idarəçiliyini təmin etməyə və etibarlı, şəffaf, demokratik ağıllı şəhərin həyata keçirilməsini və yerləşdirilməsini təşviq edə bilər. Bununla belə, təşviqlərin olmaması təşkilatlar və fərdlər arasında məlumat mübadiləsinə mənfi təsir göstərir, biznesin inamını və hökumətə inamını azaldır. Qrafik 1.2-də ağıllı sistemlərdə blokçeynin əlaqəsini göstərir.



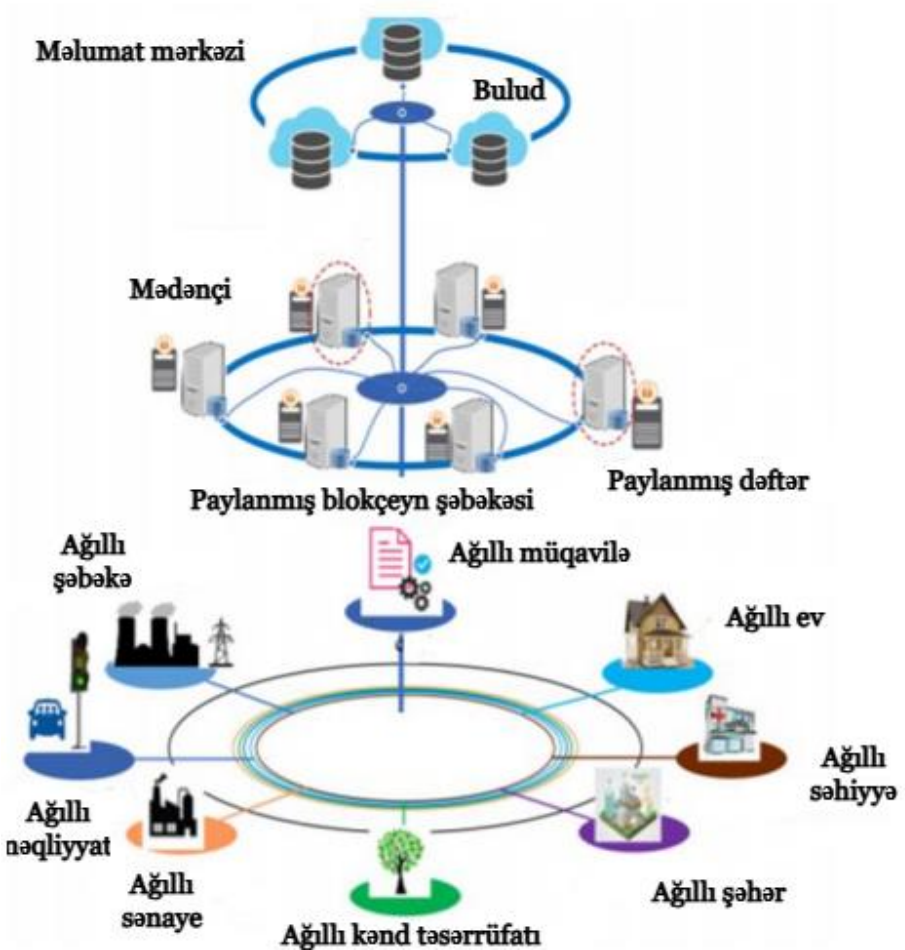
Şəkil 1.2 Ağıllı şəhərdə mərkəzləşdirilməmiş idarəetmə arxitekturası

Blokçeyn texnologiyası ağıllı şəhərləri əhəmiyyətli dərəcədə təkmilləşdirir. Ağıllı şəhərlərdə ağıllı vətəndaş, ağıllı sağlamlıq, ağıllı şəbəkə, ağıllı nəqliyyat, təchizat

zəncirinin idarə edilməsi, ağıllı biznes, ağıllı ev, ağıllı hökumət, ağıllı təhsil və digər sahələr var. Ağıllı vətəndaşlıq xidməti bu nümunələrdən biridir. Vətəndaşlar ağıllı şəhərlərin mərkəzidir. Vətəndaşların şəxsi məlumatlarının təhlili fərdiləşdirilmiş xidmətlərin göstərilməsi, texnoloji inkişafın və iqtisadi artımın sürətləndirilməsi, gələcək bazar tendensiyalarının proqnozlaşdırılması və şirkətlərin qərar qəbul etmə prosesinin optimallaşdırılması kimi bir çox üstünlüklərə malikdir. Son illərdə şəhər əhalisinin sürətli artımı ilə vətəndaşların şəxsi məlumatları eksponent olaraq artır. Hazırda bu məlumatlar bəzi sosial media platformaları vasitəsilə toplanır, saxlanılır və təhlil edilir. Bu mərkəzləşdirilmiş üsul vətəndaşlara şəxsi məlumatlarının necə istifadə edildiyi barədə az məlumat verir. Blokçeyn vətəndaşlara şəxsi məlumatlarını toplamaq, saxlamaq və onlara girişi idarə etmək imkanı verən perspektivli texnologiyadır. Məlumat saxlama sistemlərində blokçeynin şəffaflıq, təhlükəsizlik və dəyişməz xüsusiyyətləri blokçeyni bu proses üçün ideal seçim edir. Başqa bir misal, fərdi məlumatlara girişə nəzarət, kimin məlumat əldə edə biləcəyini müəyyən etmək üçün icazələr təyin etmək məqsədi daşıyır. Cəmiyyətimizdə vətəndaşların şəxsi məlumatlarının necə istifadə edildiyi barədə məlumatı azdır. Bununla belə, vətəndaşlar şəxsi məlumatlarının harada saxlandığına və onların məlumatlarına kimin daxil ola biləcəyinə nəzarət etmək istəyirlər. Şəhər əhalisinin sürətlə artması ilə bütün vətəndaşların şəxsi məlumatlarına mərkəzi giriş-nəzarət serveri əsasında giriş nəzarətini idarə etmək çətinləşir. Blokçeyn texnologiyasından istifadə etməklə fərdi məlumatlara giriş nəzarəti hazırlanır.

Son illərdə məlumatlar cəmiyyətimizdə və iqtisadiyyatımızda dəyərli aktivə çevrilir. Buna görə də, məlumat mübadiləsi bazarları daha populyarlaşır. Məlumat mübadiləsi bazarlarında məlumat sahibləri məlumatlarını istehlakçılara paylaşa və ya sata bilərlər. Bununla belə, cari məlumat mübadiləsi bazarları mərkəzləşdirilmişdir, burada bütün iştirakçılar səlahiyyətli üçüncü tərəfə etibar etməlidirlər. Mərkəzləşdirilmiş bazarlarda məlumat sahiblərindən və müştərilərdən səlahiyyətli üçüncü tərəfə bəzi idarəetmə haqqı ödəmələri tələb olunur. Bu köçürmə həm də təhlükəli mühit yarada bilər. Bu çətinlikləri aradan qaldırmaq üçün blokçeyn texnologiyası məlumat sahibləri və müştərilər tərəfindən birgə mərkəzləşdirilməmiş

məlumat mübadiləsi bazarı yaratmaq üçün istifadə edilə bilər. Məlumat sahibləri və məlumat istehlakçıları arasında əməliyyat qeydləri blokçeynində qeyd olunur. Ağıllı müqavilələr məlumatların müəllif hüquqları və şəxsi məlumatların istifadəsi kimi məlumat mübadiləsi qaydalarını təmin etmək üçün istifadə olunur. Blokçeyn və ağıllı müqavilələr bəzi tədqiqatçılar tərəfindən vətəndaşların fəaliyyətini inkişaf etdirmək və təkmilləşdirmək üçün istifadə edilə bilər. Blokçeyn texnologiyası iradə layihəsini saxtalaşdırmaya davamlı, təhlükəsiz və şəffaf saxlamaq, eyni zamanda əməliyyat sürətini artırmaq üçün istifadə olunur. Blokçeyn əsaslı ağıllı müqavilə sistemindən istifadə etməklə benefisiarlar öz hüquqları uğrunda mübarizə çətinliyindən azad ola bilərlər. Blokçeyn texnologiyasının şəffaflığı hökumətə vəsiyyətnamələrin işlənməsinə nəzarət etməyə imkan verir.



Şəkil 1.3 Paylanmış blokçeyn əsaslı ağıllı şəhər şəbəkəsi arxitekturası

Sağlamlıq vətəndaşların xoşbəxt həyatının əsasıdır. Vətəndaşlar tibbi texnologiyanın inkişafından böyük fayda əldə edirlər. Lakin dünya əhalisinin sürətli

urbanizasiyası səbəbindən ənənəvi səhiyyə xidmətləri vətəndaşların tələbatını ödəmək üçün kifayət etmir. Artan tələb və məhdud resurslar arasındakı ziddiyyət ənənəvi səhiyyə xidmətlərinin ağıllı, səmərəli və davamlı səhiyyə xidmətlərinə çevrilməsini zəruri edir. Ağıllı səhiyyə xidmətlərinin həyata keçirilməsi daşınan cihazlar, ağıllı xəstəxanalar, ağıllı təcili yardım və ağıllı təcili yardım sistemləri kimi bir çox komponentlə bağlıdır. Xəstə məlumatları xəstələrin effektiv müalicəsi üçün çox vacibdir. Ağıllı səhiyyədə müxtəlif xəstəxanalar arasında xəstə məlumatlarının mübadiləsi tibb bacılarına və həkimlərə xəstənin vəziyyətini mühakimə etməyə və hətta uzaq yerlərdə belə xəstənin sağlamlığı ilə bağlı real vaxtda qərarlar qəbul etməyə kömək edə bilər. Ağıllı səhiyyədə blokçeyn tətbiqinin bir çox üstünlükləri var. Tibbi məlumatlar blokçeynində təhlükəsiz və dəyişməz şəkildə saxlanıla bilər. Xəstələr tibbi məlumatlarının istifadəsinə nəzarət edə və məlumatlarına girişi çevik şəkildə idarə edə bilərlər.

İnformasiya kommunikasiyası və texnologiyasının inkişafı ilə ağıllı avtomobillər son illərdə çox diqqət çəkib. İntellektual nəqliyyatın məqsədi sürücülər və sərnişinlər üçün rahatlıq və rahatlığı təmin etmək, nəqliyyatın hərəkətini və səyahət səmərəliliyini artırmaq və nəqliyyat vasitələrinin yol təhlükəsizliyini artırmaqdır. Ağıllı nəqliyyatda bir avtomobil adətən yol kənarındakı bölmələr və ətrafdakı nəqliyyat vasitələri ilə əlaqə saxlamaq üçün bir neçə şəbəkə interfeysinə malikdir. Blokçeyn texnologiyasının paylanmış təbiəti ağıllı nəqliyyatın möhkəmliyini artıra və nəqliyyat vasitələrinin kommunikasiya idarəçiliyini və məlumat mübadiləsini təkmilləşdirə bilər. Blokçeynin köməyi ilə mərkəzləşdirilməmiş, etibarlı ağıllı nəqliyyat sistemi yaradıla bilər. Elektrikli nəqliyyat vasitələri və şarj stansiyaları bir çox ölkədə yaşıl nəqliyyat sistemlərinin inkişafı üçün istifadə olunur. Blokçeyn və ağıllı müqavilələr elektrik nəqliyyat vasitələri və şarj stansiyaları arasında mərkəzləşdirilməmiş və şəffaf elektrik ticarətini asanlaşdırmaq üçün istifadə edilə bilər. Elektrikli nəqliyyat vasitələrinin tələbat məlumatları və şarj stansiyalarının qiymətləri və yerləşmə məlumatları ümumiyyətlə blokçeyndə saxlanılır, bunun əsasında hər bir elektrik avtomobili ən uyğun doldurma stansiyasını seçə bilər.

Ağıllı qurğular müəyyən xidmətləri təmin etmək üçün bir-biri ilə əlaqə saxlamalıdır. Mərkəzləşdirilməmiş bir texnologiya olaraq, blokçeyn cihazlar arasında əlaqəni təşviq edir və ağıllı evdəki hər bir cihaza birbaşa digər cihazlardan məlumat tələb etməyə imkan verir. Ağıllı ev sahibi cihazlar arasında rabitəni idarə etmək üçün xüsusi blokçeyn strukturundan istifadə edir. Yerli qurğular arasındakı əlaqə tarixçələri blokçeyndə əməliyyatlar kimi qeyd olunur. Ağıllı evin sahibi cihazlar arasında rabitəni idarə edə bilir. Cihaz sahibi tərəfindən icazə verilən cihazlar yalnız paylaşılan açardan istifadə edərək bir-biri ilə əlaqə saxlaya bilər. Enerji istehlakı kartlar və ya mobil cihazlarla ödənilir. Bununla belə, gələcək ağıllı ev sistemləri insan müdaxiləsi olmadan avtomatik ödənişə yönəlmiş texnologiyalarla inkişaf edir. Blokçeyn və ağıllı müqavilələr avtomatik ödəniş üçün bir vasitədir.

İnformasiya kommunikasiyası və texnologiyalarının inkişafı ilə nəqliyyat sektoru böyük təsirə məruz qalmış və intellektual nəqliyyat sistemləri formalaşmışdır. Ağıllı Nəqliyyat Sistemi (ITS) ağıllı nəqliyyat vasitələrini işə salmaq üçün internetə çıxışı və bir-biri ilə əlaqəni təmin edir. Ağıllı nəqliyyatın məqsədi sürücülər və sərnişinlər üçün nəqliyyatda rahat istifadəni, səmərəliliyi və təhlükəsizliyi artırmaqdır. Blokçeyn texnologiyası sayəsində mərkəzləşdirilməmiş, təhlükəsiz, şəffaf və davamlı ağıllı nəqliyyat sistemləri yaradılır. Məsələn, Danimarkada blokçeyn texnologiyası nəqliyyat vasitələrinin və nəqliyyat vasitələrinin sahiblərinin qeydiyyatı və bu qeydlərin idarə olunması və monitorinqində istifadə olunur. Ağıllı şəhərlərdə süni intellektin inkişafı ilə avtonom avtomobil texnologiyasının geniş yayılacağı gözlənilir. Avtonom bir avtomobilin işləməsi üçün naviqasiya sistemi, yol məlumatı, yanacaq mövcudluğu, sürücülük vəsiqəsi məlumatı, yol vergiləri, sürət yoxlamaları, dayanacaq yerləri kimi ətraf mühit məlumatları tələb olunur. Bu məlumatların ötürülməsi blokçeyn texnologiyası ilə təhlükəsiz şəkildə həyata keçirilə bilər. Eyni zamanda, avtonom nəqliyyat vasitəsinin hərəkəti və sürücünün yol hərəkəti qaydalarına əməl etməsi kimi istifadəçi davranışı ilə bağlı məlumatlar da qeydə alına bilər.

Dünyada kömür, neft və təbii qaz kimi qalıq yanacaqlar ümumiyyətlə enerji mənbəyi kimi istifadə olunur. Bu yanacaqların həddindən artıq istehlakı ətraf mühitin çirklənməsinə və istixana qazı emissiyalarının artmasına səbəb olur. Ətraf mühitin

qorunması və onun davamlılığının təmin edilməsi məqsədilə bərpa olunan enerji mənbələrindən (günəş enerjisi, külək enerjisi və s.) istifadə genişləndirilməlidir. Bu kontekstdə səmərəli, təhlükəsiz, qənaətcil və davamlı elektrik şəbəkəsi sistemini təmin etmək üçün ağıllı şəbəkə sistemi tövsiyə olunur. Qeyri-mərkəzləşdirilmiş elektrik şəbəkəsi sistemi çox sayda istehlakçı və istehsalçının idarə edilməsi üçün çox vacibdir. Blokçeyn texnologiyası elektrik enerjisi ilə bağlı məlumatların saxlandığı kitabçanı saxlamaqla mərkəzləşdirilməmiş, şəffaf və etibarlı elektrik ticarəti bazarının həyata keçirilməsini dəstəkləyir.

Blokçeyn texnologiyasının ətraf mühitin qorunması potensialı BMT və digər təşkilatlar tərəfindən müxtəlif layihələr vasitəsilə sınaqdan keçirilmişdir. Məsələn, blokçeyn Ümumdünya Vəhşi Təbiət Fondu (WWF) üçün hazırlanmış qeyri-qanuni ton balığı ovunu aradan qaldırmaq üçün bir vasitə olmuşdur. O, CarbonX adlı platformada istixana qazı emissiyalarının azaldılmasını kriptovalyutaya çevirmək üçün istifadə edilib. BMT-nin Ətraf Mühit Proqramı (UNEP), Danimarka Texniki Universiteti və Danimarka Xarici İşlər Nazirliyi arasında əməkdaşlıq hesab edir ki, blokçeyn texnologiyasına əsaslanan iqlim fəaliyyəti şəffaflıq, iqlimin maliyyələşdirilməsi və təmiz enerji bazarları sahələrində iqlim fəaliyyətini sürətləndirə bilər. Blokçeyn texnologiyası cəmiyyətlərin iqlimə təsirlərini azaltmaq üçün necə hərəkət etdiyini göstərmək üçün şəffaf və etibarlı bir yol təqdim edir.

Ağıllı şəhərlərin əsas məqsədi öz vətəndaşlarının həyat keyfiyyətini və rifahını yüksəltmək olmalıdır. Blokçeyn texnologiyası bu məqsədlə ictimai təhlükəsizlik və ictimai sağlamlıqda rol oynayır. İctimai təhlükəsizlik nöqteyi-nəzərindən bir nümunə, hər hansı bir polis idarəsi tərəfindən qeydə alınan bütün cinayət məlumatlarına real vaxt rejimində çıxışı təmin edən Bostonda qurulmuş blokçeyn texnologiyasıdır. Blokçeyn texnologiyası şəffaf, yoxlanıla bilən, etibarlı, qeyri-mərkəzləşdirilmiş, məlumatların saxlanması və qorunması kimi xüsusiyyətlərə malikdir, bu da onu ictimai sağlamlığın qorunmasında effektiv vasitəyə çevirir. Xəstəliyin yayıldığı ərazilərin aşkarlanması, xəstəlik simptomlarının və dəyişikliklərinin monitorinqi, Covid-19 pandemiyasının monitorinqində tibbi dərman və avadanlıqların tədarükü kimi bir çox sahədə faydalar təmin etmişdir. Xəstələrin şəxsi məlumatlarını ehtiva edən

məlumatların saxlanması və qorunması blokçeyn texnologiyası ilə xəstənin təhlükəsizliyinə mənfi təsir göstərmədən mümkündür. Bu texnologiyanın ictimai səhiyyədə istifadəsinin genişləndirilməsi epidemiyaya sürətli reaksiya verməyə imkan verəcək. Birgə səylə TYMLEZ, Cyberprint, Compumatika və Traxion kimi texnologiya şirkətləri koronavirusa qarşı blokçeyn texnologiyasından istifadə edərək hökumət, səhiyyə işçiləri və xəstəxanalarla şəffaf şəkildə məlumat mübadiləsi sistemi qurdular və tibbi məhsulların tədarük zəncirini blokçeyn platformasına köçürdülər. daha şəffaf və açıq şəkildə.

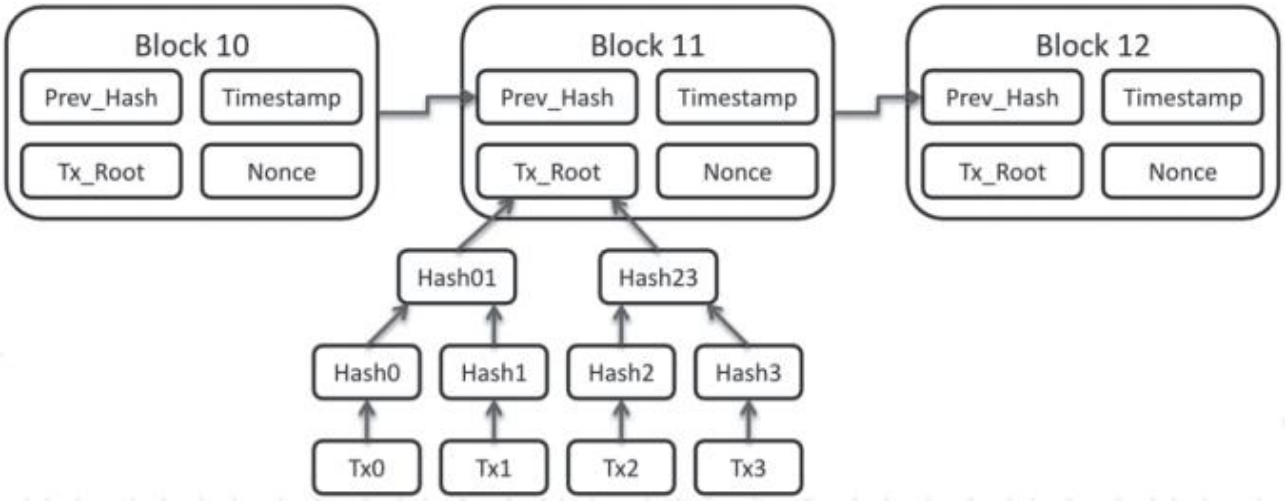
Cənubi Koreyada ictimai sağlamlığın qorunması üçün COVID-19 epidemiyası ilə mübarizə aparmaq üçün blokçeyn texnologiyası ilə əlaqə izləməni dəstəkləyən şəxsiyyət idarəetmə sistemi yaradılıb. Cənubi Koreyanın turizm məkanı olan Jeju adasına gələn ziyarətçilərdən ağıllıfon tətbiqini yükləmələri və daxil olduqları yerlərdə QR kodları skan etmək üçün istifadə etmələri xahiş olunur. İstifadəçilər proqramı telefonlarına quraşdırdıqda, onların şəxsiyyətləri ictimai blokçeyn şəbəkəsi vasitəsilə təsdiqlənir. Daha sonra proqramda rəqəmsal barmaq izinin autentifikasiyası həyata keçirilir və PİN kodu təyin edilir. Beləliklə, şəxsiyyət məlumatları xüsusi blokçeyn sistemində qeyd olunur. İstifadəçinin şəxsi məlumatları istifadə etdikləri biznes və xidmətlərin qeydlərindən ayrı saxlanılır. İstifadəçi məlumatları işlərin məxfi qalmasını təmin edəcək.

Epidemiya dövründə rəqəmsal infrastrukturun ictimai səhiyyənin idarə olunması baxımından bir çox sahədə böyük əhəmiyyət kəsb etdiyi müşahidə edilir. Gələcək epidemiyalara effektiv şəkildə hazırlaşmaq və lazımi şəraiti təmin etmək üçün ağıllı şəhərlər rəqəmsal infrastrukturunu gücləndirməlidir. Rəqəmsal infrastrukturların hazırkı və gələcək strukturunun gücləndirilməsinə blokçeyn texnologiyasının bu prosesə inteqrasiyası ilə nail olunacaq.

II FƏSİL. AĞILLI ŞƏHƏRLƏRDƏ BLOKÇEYN TEXNOLOGİYALARININ TƏTBİQLƏRİNİN TƏDQİQİ

2.1. Blokçeyn texnologiyalarının informasiya təhlükəsizliyində rolu

Blokçeyn texnologiyası tətbiq edildikdən sonra diqqət onun təmin etdiyi informasiya təhlükəsizliyi xüsusiyyətlərinin yerinə yetirilməsinə yönəldilir. Məlumatların bütövlüyünə diqqət yetirərək, blokçeyn kitabçası dəyişməzdir. Blokdakı hər bir əməliyyat onun göndəricisi tərəfindən kriptoqrafik olaraq imzalanır, blokçeyndəki hər blok kriptoqrafik olaraq onun istifadəçisi tərəfindən imzalanır, hər blokda dərhal əvvəlki blokun hashı var və blokçeyn şəbəkəsindəki bütün iştirakçılar zəncir haqqında konsensusa nail olurlar. Blokçeyndə bir əməliyyatı dəyişdirmək üçün təcavüzkar hər bir sonrakı bloku müvafiq olaraq dəyişdirməli, həmin blokun və sonrakı blokların konsensus problemini həll etməli və şəbəkə iştirakçılarının 50%-dən çoxunu yeni zənciri qəbul etməyə inandırmalıdır. Bu məqsədə çatmaq üçün tələb olunan heşinq xassələri və hesablama və elektrik enerjisinin miqdarı səbəbindən bu vəziyyət qeyri-mümkündür. Merkle ağacı, blokçeyn texnologiyalarında heşinqin əsas istifadəsidir. Merkle ağacı blokdakı bütün əməliyyatları vahid barmaq izində ümumiləşdirir və blokdakı bütün əməliyyatların dəyişdirilmədən daxil edildiyini yoxlamağa imkan verir.



Şəkil 2.1 Merkle ağacı

Merkle ağacı yalnız əməliyyatları bloklamaq üçün deyil, bəzən də kitab vəziyyətinə də tətbiq olunur. Qeyri-inkar etmə, bütövlüklə sıx bağlı olan digər

informasiya təhlükəsizliyi xüsusiyyətidir. Blokçeyndəki hər bir əməliyyat göndərən tərəfindən kriptoqrafik olaraq imzalandığından və zəncir dəyişməz olduğundan, göndərən heç vaxt əməliyyatı sifariş etdiyini inkar edə bilməz.

Mövcudluq baxımından blokçeyn şəbəkəsinin paylanmış xarakteri onu yüksək dərəcədə əlçatan edir. Bundan əlavə, ictimai blokçeyn şəbəkələrindəki əməliyyatlar adətən göndəriciyə onların emalı və saxlanma istehlakına bərabər olan xərc tələb edir. Bu xərc əməliyyatı ehtiva edən blokun istifadəçisi üçün mükafatla nəticələnir. Bundan əlavə, o, "Xidmətdən İmtina (DoS)" hücumlarından qoruyur, çünki hücum potensial təcavüzkar üçün sərf olunan resurslara mütənasib xərc tələb edir. Məsələn, Ethereum MainNet-də bu xərc qaz konseptində öz əksini tapıb. Qaz əməliyyatın hesablama və saxlama xərclərini əks etdirir. Mövcudluq konsepsiyası "anti-SPoF (anti-Single Point of Failure)" konsepsiyası ilə əlaqələndirilir. SPoF-nin qarşısının alınması, kritik tətbiqlərə gəldikdə və yüksək əlçatanlıq dərəcəsi təklif etməli olan və hətta o qədər də kritik olmayan tətbiqlərə gəldikdə məcburi tələbdir. Bu uğursuzluq nöqtəsi təsadüfən və ya qəsdən təcavüzkar tərəfindən istismar edilərsə, bütün ekosistem dağılır, ona görə də bu problemdən qaçmaq üçün blokçeyn kimi davamlı infrastrukturlardan istifadə etmək maraqlıdır. Məxfiliyə gəlincə, bu anlayışı məxfiliklə qarışdırmamaq vacibdir, baxmayaraq ki, onlar adətən əl-ələ verirlər. Ümumiyyətlə, ictimai blokçeyn şəbəkələri əməliyyatları hesablara bağlayır. Bu hesablar ictimai-özəl açar cütü ilə təmsil olunur və onlarla əlaqəli vəziyyətə malik ola bilər, lakin onlar adətən müəssisə və ya fiziki şəxslə əlaqələndirilmir. Yalnız müvafiq şəxsi açara malik olan şəxs kriptoqrafik imza vasitəsilə hesabın adından əməliyyata başlaya bilər, lakin açar cütünün arxasında olan şəxsin kimliyi məlum deyil. Beləliklə, bu psevdoanonimlik sayəsində yüksək dərəcədə məxfilik təklif olunur. Əlbəttə ki, blokçeyn üçün şəxsiyyət idarəetmə çərçivələri var, lakin bu çərçivələr klassik blokçeyn şəbəkəsinin nüvəsinin bir hissəsi deyil. Blokçeyn texnologiyalarının güclü tərəflərindən biri əməliyyatların şəffaflığıdır, bu konsepsiya ümumiyyətlə məxfiliklə ziddiyyət təşkil edir (şifrələmə kimi başa düşülür). Buna görə də, xüsusi blokçeyn texnologiyaları və özəl şəbəkələr istisna olmaqla, blokçeyn şifrələmə imkanlarını təmin etmir və bu, tətbiq olunarsa, tətbiq səviyyəsində həyata keçirilməlidir. Digər tərəfdən, icazə adətən icazəsiz blokçeyn şəbəkələrində tətbiq

səviyyəsinə buraxılır, halbuki icazə verilən blokçeyn şəbəkələrində texnologiyanın əsas hissəsinin bir hissəsi ola bilər. Bir sözlə, belə nəticəyə gələ bilərik ki, blokçeyn son dərəcə təhlükəsiz və davamlı texnologiyadır, lakin ümumilikdə məxfiliyi (şifrələmə kimi başa düşülür) əsas məqsədləri sırasına daxil etmir.

Blokçeyn texnologiyalarının ən innovativ tətbiqlərindən biri onu təhlükəsiz saxlama və bərpa sistemləri ilə istifadə etməkdir. Yedəkləmə və bərpa sistemi adətən aşağıdakı xüsusiyyətlərə malikdir:

- ***Davamlı/Avtomatik məlumat ehtiyat nüsxəsi:*** O, fayllarınıza etdiyiniz dəyişikliklərin eyni vaxtda saxlama yerinə kopyalanmasını təmin edir. Bu, məlumat itkisi halında hətta ən son dəyişiklikləri bərpa etməyə imkan verir, beləliklə, bərpa nöqtəsi məqsədinizi azaldır.
- ***Artan ehtiyat nüsxə:*** Bu, tam faylın deyil, yalnız dəyişikliklərin kopyalandığı ehtiyat nüsxə növüdür. Bu, məlumatların surətini çıxarmaq üçün sərf olunan vaxtı azaldır və işinizi ləngitmir.
- ***Ani bərpa:*** Bu xüsusiyyət proqramın dayanma müddətini azaltmaq üçün ehtiyat nüsxə şəklinin müvəqqəti olaraq ikinci yaddaşda işləməsinə imkan verir.
- ***Məlumatların təkmilləşdirilməsi:*** Məlumat ehtiyat nüsxə saxlama yerinə ötürüldükdə o, dublikat məlumat qeyd bloklarını aradan qaldırır. Bu, şəbəkə yükünü və tələb olunan saxlama yerini azaldır.
- ***Səhvsiz nüsxə:*** Məlumatın ehtiyat nüsxəsi proqramının xüsusiyyətləri həmçinin mənbədən kopyalanan və ehtiyat nüsxə serverində saxlanılan verilənlərin eyni olmasını və uyğunsuzluğunu və xətaları ehtiva etməməsini təmin edir.

Ümumi təyinatlı sistemlər nöqteyi-nəzərindən, blokçeynin həll edəcəyi gözlənilən əsas problem müdaxilə hücumlarından olan nəzarət məlumatlarıdır, məlumatların tamlığı ilə birbaşa bağlıdır. "Əksər Əşyaların İnterneti" sistemləri proqram təminatı vasitəsilə idarə olunur, ona görə də cihazların proqram təminatının yenilənməsinin bütövlüyünü və həqiqiliyini təmin etmək, diqqətlə həll edilməli olan mürəkkəb və kritik bir məsələdir. Buna görə də, yeniləmələrin yüksək mövcudluğu bir tələbdir. Mikro proqram təminatının təkmilləşdirilməsi üçün mövcud olan həllərin əksəriyyəti istehsalçının proqram təminatının paylanması prosesini öz məhsullarının

təchizatçılarına həvalə etdiyi müştəri-server modelindən asılıdır. Mərkəzi müştəri-server arxitekturasının çatışmazlıqları "Vahid Uğursuzluq Nöqtəsi (SPoF)" olur və server mövcud olmadıqda IoT cihazları resurslara (yeniləmələrə) daxil ola bilmir. İki yanaşma var: əl və avtomatik. Bir tərəfdən, əl ilə yeniləmə prosesində, cihaz sahibi proqram təminatı yeniləmə prosesinə başlamalıdır. Ümumiyyətlə, bu cür yeniləmə məhdud bant genişliyi olan cihazlar tərəfindən qəbul edilir və ya birbaşa sahibi bunu bu şəkildə etməyə qərar verir. Bununla belə, cihazın sahibi bütün əməliyyatları əl ilə yerinə yetirməli olduğu üçün mikroproqramı əl ilə yeniləmə mexanizmi o qədər də səmərəli deyil. Bundan əlavə, proqram təminatının yenilənməsi prosesi zamanı insan səhvinin baş verməsi və ya yeniləmə üçün resursların olmaması səbəbindən cihazların köhnəlməsi ehtimalı yüksəkdir.

Digər tərəfdən, bu gün avtomatik yeniləmənin qəbul edilməsi daha cazibədar görünür. Beləliklə, IoT cihazının istehsalçısı cihaz sahibinin aktiv iştirakı olmadan proqram təminatının yenilənməsinə başlaya bilər. Mövcud proqram təminatının avtomatik yenilənməsi prosesi müştəri-server arxitekturasından istifadə edir, burada provayderin repozitoriyası server, IoT cihazı isə müştəri tərəfinə çevrilir. Ümumiyyətlə, proqram təminatının serverdən müştəriyə çatdırılmasının iki yolu var: PUSH və PULL üsulları. Bu iki üsul arasındakı fərqlər layihənin proqram təminatının təkmilləşdirilməsi prosesinin təşəbbüskarındadır. PUSH metodunda cihaz istehsalçısı proqram təminatının ikili faylını paylayaraq mikroproqram yeniləmə prosesinə başlayır. PULL metodunda isə, digər tərəfdən, proqram təminatının serverə endirilməsi üçün ikili sorğu göndərərək proqram təminatının yenilənməsi prosesini başlatan IoT cihazıdır.

Paylanmış yaddaş tələb edən əvvəlkilər kimi istifadə hallarını tapdığımızda, faylların harada saxlanacağını və onlara kimin daxil ola biləcəyini həll etmək lazımdır. Blokçeyn texnologiyası saxlama həlləri təklif etmir və faylları blokçeynində saxlamaq tövsiyə edilmir. Mümkün bir həll, mərkəzləşdirilməmiş P2P fayl saxlama sistemləri kimi paylanmış saxlama sistemlərinin istifadəsidir. Bu cür yaddaşdan istifadə edərkən fayllar müxtəlif həmyaşıdlarda təkrarlanan parçalara bölünür. Arxivə giriş tələb edən həmyaşıd eyni anda bir neçə həmyaşıdda qismən yerləşən bu arxivin hissələrini

toplayır. Performans P2P BitTorrent şəbəkəsininkinə bənzəyir və fayllar hash və ya barmaq izi ilə indekslənir. Bu cür saxlamanın həyata keçirilməsi üçün əsas həll yolu IPFS-dən istifadə etməkdir. IPFS, faylları hissələrə bölən və onları tələb edən həmyaşıdlarda təkrarlayan paylanmış faylların saxlanmasına imkan verən mərkəzləşdirilməmiş hipermedia P2P protokoludur. Fayl endirildikdə, eyni anda müxtəlif mənbələrdən parçalar toplanır. Hər bir fayl öz hash və ya barmaq izi vasitəsilə müəyyən edilir və əldə edilir. IPFS, blokçeynə əsaslanan paylanmış saxlama şəbəkəsi olan Filecoin-in əsasını təşkil edir. Bu şəbəkə əsasən IPFS-ni məlumatların saxlanması üçün xüsusi blokçeyn şəbəkəsinə inteqrasiya edir, burada qovşaqlar göstərilən saxlama xidmətinə görə ödəniş kimi ayələr alır (və müştərilər onları ödəyir). Məxfilik və giriş nəzarətinə gəldikdə, IPFS protokoluna heç bir şifrələmə mexanizmi və ya giriş nəzarəti daxil deyil. Üçüncü tərəflərə açıqlanmasının qarşısını almaq üçün arxivi paylaşmazdan əvvəl hər bir faylı şifrələmək müştəri və ya DApp-dan asılıdır, bu da çox yönlü və qarşılıqlı işləyə bilən həll yolu deyil. Qısacası, IPFS müəyyən dərəcədə möhkəmlik, bütövlük və çox yüksək əlçatanlıq ilə böyük faylların paylanmış və mərkəzləşdirilməmiş saxlanmasını təmin edir. Blokçeyndə yalnız bir neçə bayt tutan faylların hashini saxlamaqla hər iki sistem əlaqələndirilir və faylın bütövlüyünə zəmanət verilir.

“Məzmun Çatdırılma Şəbəkəsi (CDN)” eyni məlumat dəstinin müxtəlif nüsxələrini ehtiva edən üst-üstə düşmüş kompüterlər şəbəkəsindən ibarətdir. Onun yaradılmasının məqsədi, məlumatların mövcudluğunu və çıxışını mümkün qədər yaxşılaşdırmaq üçün xidmətdə mövcud olan bant genişliyini maksimuma çatdırmaqdır. Müştəri məlumatların nüsxələrindən birinə daxil olur. Məlumat replikalarını təmin etməklə və xidməti təmin edən qovşağı yaxınlaşdırmaqla, cavab müddəti yaxşılaşdırılmalı və xidmət kəsilməsinin qarşısı alınmalıdır. Uyğun olmayan CDN vəziyyəti şəbəkəni cavablarında uğursuzluğa düçar edərsə, fərqli müşahidəçi məsləhətləşən eyni xidmət üçün fərqli məlumatlara malik ola bilər. İlk növbədə hansı komponentin uğursuz olduğu və hansı məlumatın etibarlı olması ilə bağlı konsensus işi asanlaşdıracaq. Blokçeynin ortaya çıxmasından və “Distribution Ledger Technologies-in” tərifindən əvvəl “DdoS” kimi hədəflənmiş hücumlara daha çox

müqavimət göstərməyə imkan verən əməkdaşlıq şəbəkələri tapmaq artıq mümkün idi. Lakin iştirakçını öz hesablama gücünü bu şəbəkələrə təklif etməyə həvəsləndirmək çətin idi. Yeni əməkdaşlar cəlb etmək qabiliyyətinin olmaması şəbəkənin böyüməsini çox çətinləşdirdi və müdafiə sistemlərinin gücünü sarsıtdı. Blokçeyn, paylanmış sistemin yeni konsepsiyası olaraq, təhlükəsizlik sisteminin təkmilləşdirilməsində iştirak edən iştirakçılara mükafat verməyə imkan verir. Kibertəhlükəsizlikdə tətbiqinə əlavə olaraq, CDN-lərin verilənlər bazası və DNS xidmətləri kimi digər məqsədlərlə ya özəl, ya da birgə şəkildə yerləşdirilməsini tapmaq da mümkündür. Lakin onlar multimedia fayllarının mübadiləsi və ya proqram təminatının paylanması kimi digər müxtəlif xidmətləri də təklif edə bilərlər. Qeyd edildiyi kimi, xidmətlərin paylanması mərkəzləşdirilmiş xidmət tərəfindən təqdim olunan problemin həlli kimi düşünülür. Blokçeynin paylanmış təbiəti bu xidmətləri mərkəzləşdirməyə imkan verir. Əldə edilən xüsusiyyətlər hər iki yanaşma üçün ümumidir, onlardan ən vacibi və qarşı tərəfi aşağıda verilmişdir.

- Hər bir fərdi serverin yükü azalır, lakin sistemin serverlərinin sayı artır.
- Şəbəkə trafiki paylanır, lakin məlumat sinxronlaşdırılmalıdır.
- Daha yüksək texniki xidmət xərcləri müqabilində gecikmə azalır və bant genişliyi artır.

Bir sözlə, CDN-lərin istifadəsi bəzi üstünlüklər əlavə edir, eyni zamanda arxitekturanın mürəkkəbliyini artırır. Kopyalama güzgülərinin təklif edilməsi və müştəriyə daha yaxından giriş ehtiyacından təsirlənən bir neçə aspekt var. Xidmətin yüksək əlçatanlığını təmin etmək üçün orijinal serverdə əvəzedicilər olmalıdır. Digər tərəfdən, verilən məlumatların ardıcıllığını təmin etmək lazımdır. Nəzəri cəhətdən hər zaman eyni məlumata malik olan bir sıra coğrafi cəhətdən paylanmış maşınlar olduğundan, sinxronizasiya problemləri yarana bilər. Bundan əlavə, şəbəkədəki bütün qovşaqları tapmaq, məlumatları daxildə sinxronlaşdırmaq və xaricdə daha yaxşı müştəri xidməti göstərmək üçün daimi daxili marşrutlaşdırma xidməti olmalıdır. Bundan əlavə, bütün bu mexanizmlər xidmətin keyfiyyətini yaxşılaşdıran, lakin hesablama və saxlama zamanı əlavə xərc yaradan istifadəçi girişlərinin və serverdən istifadənin qeydinə əsaslanır.

Blokçeyn üçün başqa bir maraqlı istifadə halı təhlükə kəşfiyyatıdır. Təhdid kəşfiyyatı prosesləri şirkət ekosisteminə uyğunlaşdırılmalıdır ki, onu düzgün şəkildə inteqrasiya etsin. Bu günlərdə təhdid intellektinə aid məsələlərdən biri şirkətlərin adətən eyni təhlükələri tədqiq etmək üçün çox vaxt sərf etməsi, digərlərinin isə diqqətdən kənarda qalmasıdır. Nəticədə, müxtəlif maraqlı tərəflər arasında məlumat mübadiləsi aparmaq üçün çox vacib olan yeni tendensiyalar yaranır. Bu prinsipə əməl edərək, müxtəlif şirkətlər bir-birinin xeyrinə təhdidlər haqqında məlumat paylaşa bilirlər. Nəhayət, paylaşılan məlumatların paylanmış kitabçası təhlükə kəşfiyyatı fəlsəfəsinin əsas məqsədidir. Təhdidlərin idarə edilməsi ekosistemində mərkəzsizləşdirmə heç də yeni deyil. Əvvəlki işlər, təhdid kəşfiyyatından istifadə hallarına tətbiq edilən mərkəzsizləşdirmə strategiyalarını öyrənir. Digərləri, təhlükə kəşfiyyatı həllini həyata keçirmək üçün ortaq bir infrastruktur təklif edirlər. Mərkəzsizləşdirmə ilə, məlumatların və məlumatların paylaşılan konsepsiyalarının vahid görünüşü, blokçeyn ağla gəlir. Fərqli tərəflər arasında sinxronizasiya, daha əvvəl də qeyd edildiyi kimi, həmyaşıd yönümlü arxitekturasına görə təbii olaraq blokçeyn tərəfindən edilən vacib bir tələbdir.

Təhdid kəşfiyyatından istifadə halları üçün blokçeyn tətbiqini müzakirə edərkən, "Ağıllı Müqavilələr"də yaxşı bir aktivdir. Aydınlıq üçün, "Ağıllı Müqavilə" şəbəkədəki qovşaqlar arasında paylaşılan və deterministik çıxışla hamısı tərəfindən icra edilə bilən kompüter proqramıdır. Bu kod parçası bizə yoxlanıla bilən xüsusi hərəkətləri yoxlamağa, tətbiq etməyə və ya yerinə yetirməyə imkan verir ki, hər kəs sistemin məntiqi axınını bilsin. Başqa sözlə, hər kəs sistemin işləməsindən xəbərdardır və ona əməl etmək məcburiyyətindədir. Bundan əlavə, konsensus bütün qovşaqlar arasında sinxronizasiyanı təmin edən bir mexanizm kimi təqdim olunur. Yuxarıda qeyd olunan "Ağıllı Müqavilələr" yalnız məlumat mübadiləsinə yönəlmiş ənənəvi paylanmış arxitekturalardan uzaq yüksək səviyyəli hesablamalara imkan verir. Bundan əlavə, biz nə vaxtsa daha fəlsəfi düşünə bilərik və deyə bilərik ki, blokçeyn daha futuristik bir həlldir, çünki o, bizə heç kim tərəfindən idarə olunmayan, lakin hər kəs tərəfindən yoxlana bilən şəbəkələr yaratmağa imkan verir. Digər tərəfdən, digər ümumi kibertəhlükəsizlik həllərinə gəldikdə, blokçeyn ənənəvi sistemlərə bəzi əlavə dəyər

əlavə edə bilər. Məsələn, çox maraqlı bir istifadə halı paylanmış müdaxilə aşkarlama sistemləridir. Bununla belə, bu paylanmış müdaxilənin aşkarlanması sistemləri müəlliflərin bu sistemlərə təsir edən zəiflikləri öyrəndiyi yerdə göstərildiyi kimi tam təhlükəsiz olmaqdan uzaqdır. Blokçeyn, üçüncü tərəflərə etibar etmək ehtiyacından qaçaraq, göstərildiyi kimi paylanmış müdaxilə aşkarlama sistemi kimi işləyə bilər. Əsasən fərqli cihazlardan fərqli qeydləri blokçeyn infrastrukturunda saxlanılanlarla müqayisə etməkdən ibarət olan "log müqayisəsi" adlandırdığımız şeyi etməklə sənaye mühitlərində bəzi sıfır günlük hücumları aşkar etmək də çox faydalı ola bilər. Təcavüzkar bir sistemə daxil olduqda, onun adətən etdiyi ilk işlərdən biri onun mövcudluğunun hər bir sübutunu silməkdir, ona görə də o, adətən onu müəyyən bir hadisə ilə əlaqələndirə biləcək hər jurnalı silməyə çalışır. Etibarlı saxtakarlığa qarşı infrastruktura malik olmaqla, biz demək olar ki, real vaxt rejimində sistemin pozulduğunu və ya sistemdəki qeydləri "dizayn üzrə" dəyişməz olan blokçeyndə saxlanılanlarla müqayisə etmədən aşkar edə bilərik. Qeyd etmək lazımdır ki, blokçeyn diskdə çox sürətlə böyüyür, lakin məsələn, log hashləri kimi sadə məlumatları saxlamaqla biz bu problemin öhdəsindən asanlıqla gələ bilərik.

Fəaliyyətləri izləməkdənsə, yalnız təmiz təhdid ağıllısına diqqət yetirməklə yanaşı, giriş sistemlərini təkmilləşdirmək üçün blokçeyn tətbiq edən bəzi tədqiqatlar var. İlk nümunələrdən biri, Romadakı La Sapienza Universitetinin və Sauthempton Universitetinin bəzi üzvləri tərəfindən yazılmış, məlumatların bütövlüyünü və sabitliyini təmin edən paylanmış verilənlər bazası əsasında Avropa Sunfish layihəsinin həllini tapmağa çalışır, təhlil edir. Nokia Bell Labs, qeydləri idarə etmək üçün ictimai bloklar əvəzinə özəl və icazəli blokçeynlərdən istifadə etməyi təklif edən kiçik bir hesabat dərc etdi, bu halda, banklarla əlaqəli məlumatlara diqqət yetirdi. Əvvəlki paraqrafda qeyd edildiyi kimi, qeydlərin saxlanması problemli ola bilər. Nəticədə, hashlərlə işləmək daha müdrikdir, çünki blokçeynlə disk istifadəsinə həddindən artıq təsir etmədən məlumatların bütövlüyünü əldə etmək həmişə mümkündür.

2.2. Ağıllı şəhərlərdə blokçeyn texnologiyalarının potensial imkanları

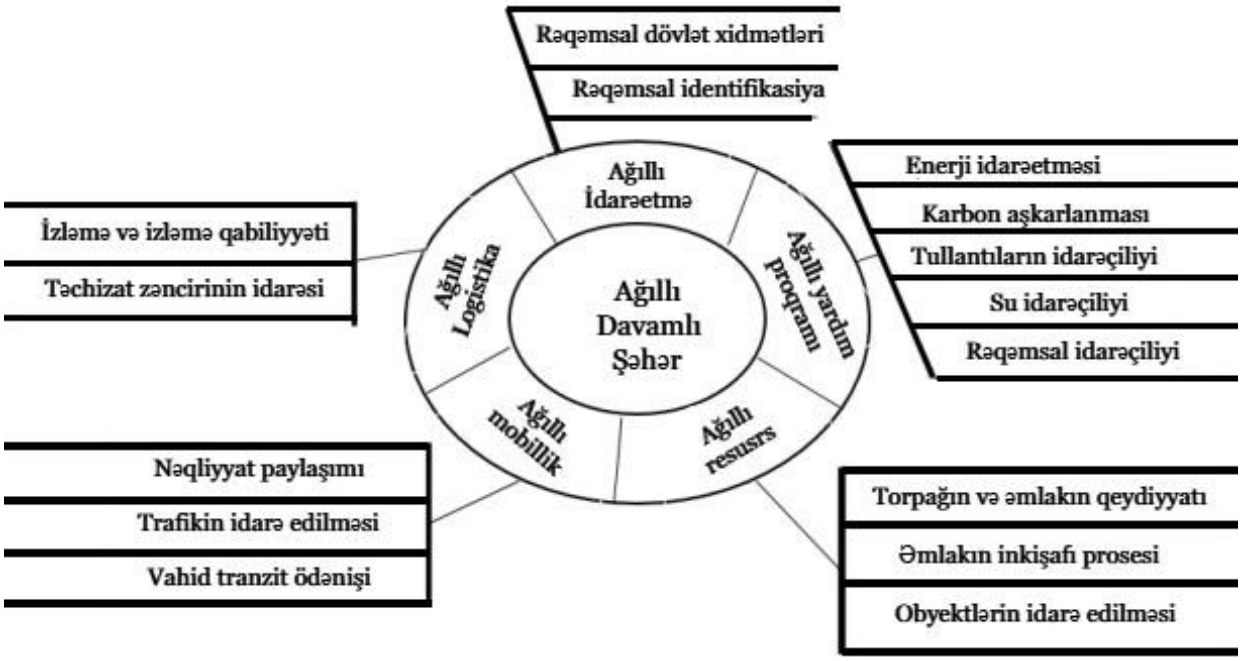
Blokçeyn perspektivli bir texnologiyadır və bu yaxınlarda müxtəlif sənaye sahələrinin böyük diqqətini cəlb edir. İlk dəfə 2008-ci ildə kriptovalyuta kimi təqdim edilən bitkoin sayəsində bu söz səs-küyə çevrilib. Blokçeyn, bank işi, səhiyyə, istehsalat və digər sənayelər kimi hər bir sektora və sənayeyə təsir edəcək növbəti texnoloji nailiyyətlərdən biri kimi qəbul edilir. Blokçeyn ümumiyyətlə qlobal həmyaşıd şəbəkəsinin konsensusuna əsaslanan istifadəçilər şəbəkəsində paylanmış kitab texnologiyası (DLT) kimi tanınır. Rəqəmsal kitab dəftəri bloklara şifrələnir və onu əvvəlki bloka zəncirləyir və daim böyüyən blokçeyn yaradır.

Ənənəvi olaraq bir çox əməliyyatlar və tətbiqlər mərkəzi sistem vasitəsilə həyata keçirilir. Mərkəzləşdirilmiş sistem tez-tez bir nöqtədən məlumat toplamaq, saxlamaq və təhlil etmək üçün tənqid olunur. Üstəlik, satıcı ilə alıcı arasında aparılan əməliyyatlarda, əməliyyatların aparılmasında vasitəçilik etmək üçün etibarlı vasitəçiyə ehtiyac duyulacaq ki, bu da prosesi ləngitəcək və əlavə xərclər yaradacaq. Beləliklə, o, innovativ rəqəmsal əməliyyatların ənənəvi korporativ aktivləri əvəz etdiyi vasitəçiləri aradan qaldırır. İnformasiya bir-birinə bağlı şəbəkə vasitəsilə müxtəlif coğrafiyalara, qurumlara və ölkələrə paylanır. Nəticə qeyri-müəyyənliyi aradan qaldıran daha şəffaf və etibarlı əməliyyat qeydidir. Dəyişməzlik blokçeyn texnologiyasının ən böyük xüsusiyyətlərindən biri olaraq görülür və bu onu bir çox sektorda üstünlük təşkil edir. Hər blokda (unikal kriptoqrafik nömrə) əvvəlki blokun hashı (kriptoqrafik imza) olduğundan, əməliyyat bloka zəncirləndikdən sonra onu dəyişdirmək, dəyişdirmək və ya silmək mümkün deyil. Buna görə də, bu bloklar zəncirə əlavə edildikdən sonra, yüksək etibarlılığı təmin edərək dəyişdirilə bilməz. Nəticədə, blokçeyn ağıllı müqaviləni dəstəkləmək üçün istifadə edilə bilər, çünki blokçeyn müqavilənin danışıqlarını və ya icrasını yerinə yetirmək və icra etmək qabiliyyətinə malikdir. Ağıllı müqavilə razılaşma haqqında məlumatdan ibarətdir və yalnız şərtlər və şərtlər şəbəkədəki bütün qovşaqlar tərəfindən yoxlanıldıqda və mərkəzi nəzarət olmadan konsensus protokolu ilə həyata keçirildikdə yerinə yetirilir. Qrafik 2.2-də göstərildiyi

kimi ağıllı şəhər çərçivəsində blokçeyn tətbiqinin beş əsas potensial sahəsinin olduğunu ortaya qoydu.

Qrafik 2.2

Ağıllı davamlı şəhər-blokçeyn (SSRİ) inteqrasiya çərçivəsi



Blokçeyn texnologiyası hökumətlərə ağıllı şəhəri idarə etməyə kömək edə bilər. O, ictimai xidmətlərin göstərilməsi və istismarını yaxşılaşdırmaq potensialına malikdir. Blokçeyn texnologiyasından istifadə edərək, gəlirlər, xərclər, müqavilələr və digərləri kimi dövlət qeydləri qeydə alına və bir-biri ilə əlaqələndirilə bilər. Bu, korrupsiyanın qarşısını almaqla şəffaflığı gücləndirir. Bundan əlavə, seçici saxtakarlığını aradan qaldırmaq üçün mərkəzləşdirilməmiş səsvermə platforması yaradıla bilər. Hər bir vətəndaşın şəxsiyyəti ağıllı şəhər şəbəkəsində təhlükəsiz şəkildə saxlanıla bilər. Vətəndaşın şəxsiyyəti və milli şəxsiyyət, doğum və ölüm qeydləri, pasportlar, sağlamlıq və iş qeydləri kimi məlumatları blokçeynlə əlaqələndirilə bilər ki, bu kimliklərdən istifadə zamanı saxtakarlığı azaltsın. Şəxsiyyət şəxsi məlumatların etibarlı şəkildə saxlanmasına, əlaqələndirilməsinə, paylaşılmasına və müvafiq qurumlar tərəfindən istifadəsinə imkan verə bilər. Məlumat və qeydlər şəbəkə daxilində şifrələnir və qorunur. Beləliklə, sürətli aşkarlama və sənədləşdirmə ilə yorucu prosesləri və sənədləşmə işlərini aradan qaldırır.

Blokçeynin getdikcə daha çox istifadə edildiyi sahələrdən biri mobillikdir. Paylaşma iqtisadiyyatının və birgə istehlakın böyüməsi, blokçeynin unikal güclü tərəflərindən istifadə edən inam problemləri kimi problemləri ortaya çıxardı. Məsələn, paylaşma iqtisadiyyatında ridesharing ümumi istifadə halına gəldi. Nəqliyyat vasitələri və vətəndaş məlumatlarını blokçeyn şəbəkələrində saxlayaraq, vətəndaşların təsdiqlənmiş rəqəmsal şəxsiyyətdən istifadə edərək paylaşılan nəqliyyat vasitələrinin məlumatlarına daxil ola bilməsi üçün etibar şəbəkəsi yaradır. Sürücülərin və müştərilərin şəxsiyyətləri, həmçinin gəzinti paylaşımı xidmətlərinə müraciət edərkən asanlıqla yoxlanıla bilər. Bundan əlavə, ağıllı şəhərdə bilet almaq üçün daha səmərəli sistemlər (məsələn, avtobuslar, qatarlar, velosipedlər) lazımdır. Blokçeyn rəqəmsal biletlərin alınması və rəqəmsal tokenlərdən istifadə edərək əməliyyatların asanlaşdırılması üçün vahid platforma təqdim edir. Blokçeyn, qeydləri saxlamaq və ağıllı şəhərdə istifadə edilən müxtəlif ictimai nəqliyyat növləri üçün əməliyyatları asanlaşdırmaq üçün vahid platforma kimi istifadə edilə bilər. Bu vahid platformanın vahidliyi prosesi asanlaşdıracaq və çoxsaylı bilet maşınlarına və ya masalarına baş çəkmək çətinliyini aradan qaldıracaq.

Bundan əlavə, şəhərsalmaçı rəqəmsal nişanlardan istifadə edərək ortaq gəzinti və ya ictimai nəqliyyatda istifadə etdikləri üçün vətəndaşları mükafatlandıra bilər və qeydlər blokçeynində saxlanıla bilər. Bu təşviqlər dəyişməz qeydlərə əsaslanan blokçeyn texnologiyasından istifadə edərək effektiv şəkildə paylana bilər. Trafik məlumatları IoT sensorları və blokçeyn ilə inteqrasiya oluna bilər. Şəhər planlayıcısı real vaxt həllini təmin edərək, trafik vəziyyətini izləmək və idarə etmək üçün real vaxt trafik məlumatlarına daxil ola bilər. Şəhərdə tıxac problemi xüsusilə pik saatlarda və ya mövsümlərdə həll edilə bilər. Blokçeyni ağıllı mobillik sahəsinə inteqrasiya etməklə, yollarda və nəqliyyatda daha az avtomobil səmərəli şəkildə idarə oluna bilər. Beləliklə, davamlılığa töhfə verən qalıq yanacaq emissiyalarını və havanın çirklənməsini azaldır.

Blokçeyn, ağıllı müqavilələrin yaranması səbəbindən torpaq, əmlak və mənzillərin qeydiyyatını və əməliyyatlarını asanlaşdıra bilər. Beləliklə, ənənəvi ağ-qara razılaşması aralıq razılaşma ilə əvəz olunur. Zəif aktiv əməliyyatları, ikiqat

qeydiyyat və saxtakarlıq məsələləri aradan qaldırıla bilər. O, həmçinin mülkiyyət sənədi, dizayn, tikinti və texniki xidmət mərhələlərini əhatə edən daşınmaz əmlakın inkişafı prosesinə kömək edir. Bütün çertyojlar, təsdiqlər, hesabatlar və qeydlər blokçeyn vasitəsilə çəkilə və saxlanıla bilər. Beləliklə, o, aktivin bütün həyat dövrü ərzində dəyişməz görünüş təmin etməklə uçotun aparılmasında dəqiqliyi və şəffaf sistemi təmin edir. O, potensial olaraq binaların qrafikə uyğun vaxtında təmir edilməsinə kömək edə bilər, çünki blokçeynində saxlanılan qeydlər gələcəkdə obyektin idarə edilməsi üçün asanlıqla əldə edilə bilər.

Blokçeyn texnologiyasının ağıllı xidmətlərə, xüsusən də enerji idarəetmə sisteminə kömək edə biləcəyi bir neçə üsul var. Blokçeyn enerji istifadəsini və tələbini dəqiq qeyd etməyə kömək edəcək. Ticarət platformasına çatmaq üçün müxtəlif cihaz və avadanlıqlar şəbəkələr vasitəsilə enerji akkumulyatoruna və mobil telefon vasitəsilə proqrama qoşulur. Bununla istifadəçi akkumulyatorlarda yığılan enerjinin miqdarına baxa və ticarət platformasında satış məzənnəsini yoxlaya bilər. Faktiki enerji istehlakı haqqında məlumat şəffaf şəkildə izlənilə bilər. İstehlakçılar üçün qida ehtiyaclarından xəbərdar olmaq asandır. O, həmçinin istifadəçini öz istifadə və istehlak nümunələri barədə xəbərdar edir. Öz növbəsində istifadəçi buna uyğun reaksiya verə bilər. Eynilə, şəhərin müxtəlif hissələri üçün su istifadəsini tənzimləmək üçün blokçeyn texnologiyasından istifadə etməklə su istehlakı izlənilə bilər. Üstəlik, enerji əməliyyatları blokçeyn texnologiyasının və "Əşyaların İnternetinin (IoT)" birləşməsi ilə həyata keçirilə bilər. Məsələn, damında günəş panelləri olan evlər artıq enerjini eyni yoldakı qonşulara sata bilər. İstifadəçi enerji satmaq qərarına gəldikdə, əməliyyat baş verir və əməliyyat blokçeyn kitabçasında qeyd olunur. Beləliklə, o, vasitəçilərə ehtiyac olmadan istehlakçılar və alıcılar arasında əməliyyat və ödənişlərə icazə verərək mərkəzləşdirilməmiş enerji bazarı yaradır. O, həmçinin məişət texnikası, nəqliyyat vasitələri və avadanlıqların karbon izini izləmək üçün istifadə edilə bilər. Həm təchizatçılar, həm də istehlakçılar hər bir məhsulun ətraf mühitə təsirini başa düşə bilərlər. Blokçeyn əsaslı tətbiqdəki qeydlər dəyişdirilə bilmədiyi üçün bu, toplanacaq karbon vergisinin miqdarını müəyyən etmək üçün istifadə edilə bilər. Böyük karbon izi olan bir məhsulun alınması baha başa gəlirsə, bu, alıcıları onu almaqdan

çəkindirəcək. Beləliklə, bazarda məhsullara tələbatı azaldır. Nəticədə, şirkət tələbatı artırmaq üçün karbon izlərini azaltmaq üçün tədarük zəncirlərini yenidən quracaq. Effektiv tullantıların idarə edilməsini və proqnozlaşdırılan modelləşdirməni asanlaşdırmaq üçün blokçeyn IoT sensorları və süni intellektlə inteqrasiya oluna bilər. IoT tullantıların yığılmasını aşkar edir və tullantıların toplanması operatorlarına tullantıları təmizləmək və atmaq üçün xəbərdarlıq edir. Bu məlumat blokçeyn tərəfindən saxlanıla və istifadəçilər və maraqlı tərəflərlə paylaşıla bilər. Tullantıların istehsal səviyyəsi izlənilə və tullantıların idarə olunması strategiyaları yaradıla bilər. Tullantıların səviyyəsini asanlıqla və real vaxt rejimində izləməklə o, tullantıların toplanması cədvəllərini və toplanması üçün optimal marşrutları optimallaşdırmağa kömək edir. O, həmçinin tullantı toplayan maşınlara yanacaqdan maksimum istifadə etməyə kömək edir.

Blokçeyn vətəndaşları havanın keyfiyyəti indeksi haqqında məlumatlandırmaq və ya monitorinq məqsədləri üçün çirkləndirici səviyyələri ölçmək üçün IoT sensorları ilə inteqrasiya edə bilər. Bu, sağlam ətraf mühitin qorunmasına və problem daha da pisləşmədən çirklənmə ilə mübarizə üçün daha effektiv üsulların tapılmasına kömək edir. Nəticədə, smart kommunal sahəsində blokçeyn tətbiqləri CO_2 emissiyalarının azaldılmasına və davamlılığın təmin edilməsinə töhfə verəcək həllər təmin edə bilər. Məlumatların şəffaflığı və mərkəzləşdirilməmiş təbiətinə görə izləmə və monitorinqdə faydalıdır. Beləliklə, təsirin qiymətləndirilməsi və qiymətləndirmənin təqibi daha asan olacaq və beləliklə, daha sürətli nəticələr və strategiyalar təklif oluna bilər.

Ölçəklənəbilərlilik, ağıllı şəhərlərdə tam potensialını açmaq üçün blokçeyn üçün kritik bir məsələ olaraq qalır. Tranzaksiyaların işlənməsi sürəti və tutumunda mövcud məhdudiyyətlər geniş yayılmağa mane olur. Parçalanma, ikinci səviyyəli həllər və konsensus mexanizmlərindəki irəliləyişlər kimi yeniliklər bu genişlənmə problemlərini həll etməyi hədəfləyir. Şəhər mühitində yaradılan böyük həcmli məlumatların yerləşdirilməsi üçün miqyaslılığa nail olmaq üçün səylər lazımdır.

Qarşılıqlı işləmək başqa bir əsas maneədir. Fərqli protokol və standartlara malik çoxsaylı blokçeyn platformalarının mövcudluğu harmonik ekosistemin yaradılmasında problem yaradır. Bu platformalar arasında qarşılıqlı əlaqənin təmin edilməsi müxtəlif

şəhər sistemləri arasında fasiləsiz məlumat mübadiləsi və əməkdaşlıq üçün vacibdir. Fərqli blokçeynlərin effektiv ünsiyyət qurmasına və daha vahid ağıllı şəhər infrastrukturunu təşviq etməyə imkan vermək üçün standartlaşdırma səyləri davam edir. Tənzimləyici mühit blokçeyn texnologiyasının ağıllı şəhərlərə inteqrasiyasında həlledici rol oynayır. Qaydalarda aydınlıq hüquqi və etik standartlara uyğunluğu təmin edir və innovasiyalar üçün əlverişli mühiti gücləndirir. Hökumətlər məlumatların qorunması, məxfilik və ağıllı müqavilələrin qanuniliyi ilə bağlı narahatlıqları həll edərək blokçeyn tətbiqi üçün aydın qaydalar yaratmalıdırlar. Tənzimləyicilər, sənaye maraqlı tərəfləri və texnoloji yenilikçilər arasında birgə səylər balanslaşdırılmış və dəstəkləyici çərçivələr yaratmaq üçün vacibdir. Ağıllı şəhərlərdə blokçeyn inteqrasiyasının uğuru əsasən vətəndaşların qəbulundan və iştirakından asılıdır. Blokçeyn texnologiyasının faydaları, funksiyaları və potensial təsiri haqqında ictimaiyyəti maarifləndirmək çox vacibdir. Məlumat sahibliyi, məxfilik və təhlükəsizlik tədbirləri ilə bağlı şəffaf ünsiyyət vətəndaşlar arasında inam yaratmaq üçün vacibdir. İcmaların qərar qəbul etmə proseslərinə cəlb edilməsi və nəzərəçarpacaq faydaların nümayiş etdirilməsi ağıllı şəhər təşəbbüslərində daha çox qəbul və iştiraka təkan verəcək. Dünyanın bir çox şəhərləri blokçeyn texnologiyasını birləşdirən pilot layihələri və real dünya tətbiqlərini işə salıb. Məsələn, Dubayın blokçeyn Strategiyası 2020-ci ilə qədər bütün dövlət əməliyyatlarını blokçeynəyə keçirməyi, müxtəlif sektorlar üzrə səmərəliliyi və şəffaflığı artırmağı hədəfləmişdir. Bundan əlavə, Sinqapurun Ubin Layihəsi maliyyə sistemlərində texnologiyanın potensialını nümayiş etdirərək banklararası ödənişlər üçün blokçeynin istifadəsini araşdırır.

Şəhər şəhərlərində daim artan əhali mövcud infrastruktur və resurslara böyük yük qoymuşdur. Rəqəmsal transformasiya şəhərlərin infrastrukturunun sakinlərin artan ehtiyaclarına cavab verməsini təmin etmək üçün əlverişli yoldur. Ağıllı şəhəri inkişaf edən texnologiyalarla birləşdirmək yaşayış standartlarını artırır, lakin kiberhücum təhdidlərini nəzərə almamaq olmaz. Kibertəhlükəsizlik ağıllı şəhərin inkişafından əvvəl həll edilməli olan əsas təhlükədir. Çoxlu sayda cihaz və maşınların bir-birinə qoşulması ənənəvi kibertəhlükəsizlik həllərinin həll edə bilmədiyi bir sıra yeni təhlükəsizlik problemlərini ortaya qoyur. Beləliklə, həm dövlət qurumları, həm də

xidmət təminatçıları həqiqətən ağıllı şəhərləri inkişaf etdirməkdən çəkinirlər. Bununla belə, ağıllı şəhər şəhəri kiber təhlükələrdən qorumaq üçün mərkəzləşdirilməmiş blokçeyndən istifadə edə bilər. Bu fəzilətdən əlavə, bu texnologiyanın davamlı inkişafa təsiri ekoloji, iqtisadi və sosial kimi müxtəlif aspektlərdən hiss olunur. Blokçeyn texnologiyası Dayanıqlı İnkişaf Məqsədləri (SDGs) ilə güclü uyğunluğa malikdir və onun tətbiqi ağıllı şəhər çərçivəsində Dayanıqlı İnkişaf Məqsədlərinə nail olmağa töhfə verə bilər.

2.3. Ağıllı şəhərlərdə blokçeynlərin tətbiqi vəziyyətinin analizi

Əvvəlcə Bitcoin kimi kriptovalyutaların əsasını təşkil edən texnologiya kimi inkişaf etdirilən blokçeynlər, ağıllı şəhərlər də daxil olmaqla müxtəlif domenlərdə rəqəmsal valyutalardan kənar tətbiqləri tapmaq üçün təkamül etdi. Ağıllı şəhərlər resursların idarə edilməsini optimallaşdırmaq, həyat keyfiyyətini yaxşılaşdırmaq və şəhər xidmətlərinin səmərəliliyini artırmaq üçün innovativ texnologiyalardan istifadə edən şəhər əraziləridir. Paylanmış kitab texnologiyası olaraq, blokçeynlər ağıllı şəhər ekosistemləri daxilində məlumat təhlükəsizliyi, etibar, şəffaflıq və qarşılıqlı fəaliyyətlə bağlı problemləri həll etmək potensialına malikdir.

Etibarlı məlumat mübadiləsi Avropa Blokçeyn Xidmət İnfrastrukturu (EBSI) layihəsində təklif olunan ilk istifadə hallarından biridir. Dövlət sektorunda məlumat mübadiləsi hökumət idarələri arasında şaquli şəkildə idarə olunur və bu, üfüqi əlaqənin olmamasına səbəb olur. Bununla belə, blokçeyn sistemləri paylanmış konsensus mexanizmləri ilə təsdiqlənmiş həmyaşıdlar arası ünsiyyətə imkan verir. 2007-ci il kiberhücumlarından sonra Estoniya hökumət depolarında saxlanılan məlumatların bütövlüyünü təmin etmək üçün blokçeyn texnologiyasının istifadə imkanlarını araşdırdı. Nəticədə, Estoniya hökuməti dövlət idarələri arasında məlumatların yayılması üçün Açarsız İmza İnfrastruktur (KSI) texnologiyasını tətbiq etdi. Fayl dəyişikliyi və məlumat dəyişməz və tam şəffaf olduqda KSI-də blokçeynə yeni hash dəyəri əlavə olunur. Təqdim olunan icazəli blokçeyn pilotu müdafiə departamentinin filialları və müttəfiq hökumətlər arasında sənədlərin paylaşılmasını təmin etmək üçün

FlureeDB (blokçeyn əsaslı qrafik verilənlər bazası) istifadə edir. FlureeDB yüksək ölçülə bilən, məlumat şifrələməsindən istifadə edən, semantik məlumatların standart formatlaşdırılmasını və üzərində saxlanılan dəyişilməz məlumatları təklif edən həmyaşıd arxitekturaya malikdir.

Bir çox təhsil şirkətləri sertifikatlarının asanlıqla saxtalaşdırılması faktını həll etmək üçün çalışırlar. Buna görə də, təkmilləşdirilmiş şəffaflıq və həqiqiliyin təsdiqlənməsi təhsil sertifikatları üçün vacibdir. Burada biz təhsil sahəsində ən son üç blokçeyn pilotunu və layihələrini təsvir edirik.

- EBSI-dən diplomdan istifadə nümunəsi.
- Maltada akademik etimadnamələr üçün Blokcerts layihəsi.
- Avropa İttifaqı tərəfindən birgə maliyyələşdirilən EBSILUX layihəsi Lüksemburqda diplomdan istifadə nümunəsini həyata keçirir.

Diplomdan istifadə nümunəsi EBSI layihəsində təklif olunan ilk istifadə nümunələrindən biridir. Bu layihə vətəndaşlara təhsil etimadnamələrini idarə edərkən nəzarəti geri qaytarır. Bundan əlavə, bu layihə yoxlama xərclərini və vaxtını azaldır və etibar və orijinallığı artırır. Blokcertsblokçeyn əsaslı sertifikatların yaradılmasına, verilməsinə, baxılmasına və yoxlanılmasına imkan verən MIT-nin açıq standart layihəsidir. Bu sertifikatlar kriptoqrafik olaraq imzalanmışdır, müdaxiləyə qarşı davamlıdır və paylaşıla bilər. EBSILUX layihəsi Lüksemburqda məktəblər, universitetlər, tələbələr və işəgötürənlər arasında şəffaflığı və etimadı təmin etmək üçün akademik sertifikat qeydlərindən istifadəni təşviq edən diplomdan istifadə nümunəsini həyata keçirir.

Mərkəzləşdirilməmiş rəqəmsal şəxsiyyət əlavə giriş və parollar olmadan müxtəlif elektron xidmətlərə etibarlı, təhlükəsiz və asan giriş imkanı verir. Rəqəmsal identifikasiya sahəsində təkmilləşdirilmiş beş blokçeyn layihəsi aşağıdakılardır:

- EBSI-dən Self-Suveren Identity istifadə nümunəsi.
- uPort mərkəzləşdirilməmiş şəxsiyyət.
- İsveçrədə Zug ID.
- Lüksemburqda ESSIF layihəsi.

- NGI eSSIF-LAB.

Self-Suveren Identity istifadə halı EBSI layihəsində təklif olunan ilk istifadə hallarından biridir. Bundan əvvəl, uPort layihəsi 2015-ci ildə ConsenSys-də başlamışdır. Hazırda uPort inkişaf edib və iki yeni layihəyə - Serto və Veramoya bölünüb, hər ikisi mərkəzləşdirilməmiş şəxsiyyət və məlumatlara insan mərkəzli nəzarət missiyasını həyata keçirir. Zug ID layihəsi uPort layihəsindən istifadə etdi və Ethereum blokçeynində mərkəzləşdirilməmiş şəxsiyyət platforması hazırladı. Mərkəzləşdirilməmiş şəxsiyyət və eZug tətbiqi ilə Zuq sakinləri Zug şəhərinin onlayn xidmətlərindən rəqəmsal olaraq, xüsusən də çöldə olduqda və mobil cihazlardan istifadə edərkən istifadə edə bilərlər. Məsələn, blokçeyn əsaslı identifikatoru olan hər kəs 2019-cu ilin noyabr ayından e-velosiped götürə bilir. ESSIF ümumi və qarşılıqlı fəaliyyət göstərə bilən Self-Suveren Identity (SSI) çərçivəsini həyata keçirməyi hədəfləyir. eSSIF-Lab AB tərəfindən maliyyələşdirilən layihədir və yeni nəsil, açıq və etibarlı rəqəmsal şəxsiyyət həlli kimi öz-özünə Suveren Kimliklərin (SSI) geniş şəkildə mənimsənilməsini inkişaf etdirməyi hədəfləyir.

Notarius dövlət hökuməti tərəfindən təyin edilmiş və müəyyən bir hərəkəti və ya əməli təsdiq edə bilən vəzifəli şəxsdir. Notarial qaydada məlumatın həqiqiliyini yoxlamaq lazımdır. Dövlət sektorunda təkmilləşdirilmiş dörd notariat layihəsi aşağıdakılardır:

- EBSI layihəsindən notariat təsdiqi.
- Braziliyada mülki tərəfdaşlığın notarial təsdiqi.
- Vyanada açıq məlumatların notarial təsdiqi.
- Şanxayın blokçeynlə işləyən notariat platforması.

EBSI-nin notarial təsdiqindən istifadə halı həqiqiliyin yoxlanılması, məsuliyyətin, izlənilmənin, auditin aparılmasının və saxtakarlığın qorunmasının təmin edilməsi üçündür. Growth Tech, blokçeyn texnologiyasından istifadə edərək, Braziliyada notarial qaydada təsdiq edilmiş mülki tərəfdaşlığı sınaqdan keçirmək üçün Notarius kitabçası platformasından istifadə etdi. Vyana şəhəri dövlət idarəçiliyi məlumatlarının təhlükəsizliyini təmin etmək üçün blokçeyn üzrə notariat xidmətindən istifadə edir. Artıq 4000-ə yaxın açıq məlumat resursu notarial qaydada təsdiqlənir və dərc olunur.

Həll data.gv.at saytındakı bütün açıq hökumət məlumatlarına şamil ediləcək və bütün Avstriyada istifadə olunacaq. Şanxay Xuhui Notarius tərəfindən idarə olunan Hui Cun platforması notariat funksiyalarını həyata keçirən blokçeyn əsaslı məlumat saxlama protokoludur. Qırx (40) firma 2020-ci ilin yanvarında istifadəyə verildiyi vaxtdan bəri Şanxayın blokçeynlə işləyən notariat platformasından 3000-dən çox işi idarə etmək üçün istifadə edib.

Dünyada pensiya sistemləri aşağı mobillikdən, şəffaflıq və nəzarətin olmamasından əziyyət çəkir. Blokçeyn texnologiyası gələcək nəsil pensiya sistemlərinin inkişafı üçün perspektivli istiqamətlər təqdim edir. Bir neçə blokçeyn əsaslı pensiya layihələri aşağıda təsvir edilmişdir:

- BMT Pensiya Fondu Blokçeyndə üz tanıma sistemini qəbul edir.
- Hollandiyada APG və PGGM-dən blokçeyn üzrə yeni pensiya idarəçiliyi tətbiqi.
- Kanada maliyyə firması BMO Capital Markets-dən blokçeyn üzrə müəllimlərin pensiya planı.

BMT-nin pensiya fondu pensiya uyğunluğunun illik yenidən sertifikatlaşdırılması üçün blokçeyndə üz tanımadan istifadə edir. Bununla belə, üz identifikasiyası ilə bağlı alqoritmik meyllərlə bağlı bəzi narahatlıqlar var və daha yaxşı uyğunlaşma üçün bunlar həll edilməlidir. İki böyük Hollandiyalı pensiya inzibatçısı, APG və PGGM, pensiya idarəçiliyinin blokçeyn prototipinin birinci mərhələsini uğurla başa vurdu. Birinci mərhələ uğurlu oldu və APG yeni pensiya fondunu işə salmaqla texnologiyanı daha da sınaqdan keçirməyi planlaşdırdığını açıqladı. APG hesab edir ki, bu prototipin davamlı inkişafı daha az xərclə daha çevik, sadə və şəffaf pensiya idarəetmə sistemi yaradacaq. Pensiya fondunun investoru olan Ontario Müəllimlər, pensiya planlarını idarə etmək üçün blokçeyn pilotu üçün Monreal Bankı ilə əməkdaşlıq etdi. Pilot əməliyyat - Qiymətli Kağızlar üçün ənənəvi Kanada Depozitarisi (CDS) kimi sifariş edilmiş və blokçeyn vasitəsilə uğurla paralelləşdirilmişdir. Əməliyyata emitent kimi Bank of Monreal və alıcı kimi Ontario Müəllimləri daxil idi.

Torpaq mülkiyyətində aydınlığın olmaması iqtisadi fəaliyyətləri sıxışdırır. Blokçeynində torpaq mülkiyyəti reyestrləri haqqında dörd prototip aşağıda təsvir edilmişdir:

- Gürcüstanda Exonum torpaq mülkiyyət reyestrinin pilotu.
- Ruanda Hökumətinin torpaq reyestri üçün Ubutaka blokçeyn layihəsi.
- Medici Torpaq İdarəsi tərəfindən Liberiyada blokçeyn üzrə torpaq idarəçiliyi üzrə pilot.
- İsveçdə əmlak əməliyyatları üçün blokçeyn pilotu.

Exonum Land mülkiyyət hüququ Gürcüstanda ilk dəfə 2016-cı ildə istifadəyə verilmiş uğurlu pilotdur. Bu pilot blokçeynində 1,5 milyondan çox torpaq mülkiyyətini qeydə alıb. Bu həll yolu ilə Gürcüstan Respublikasının Dövlət Reyestrinin Milli Agentliyi (NAPR) Gürcüstan vətəndaşlarına kriptoqrafik sübutlarla dəstəklənən aktivlərinin rəqəmsal sertifikatlarını təqdim etdi. Medici torpaq idarəsi, Ubutaka adlı blokçeyn platformasında torpaq əməliyyatlarını qeyd edən layihəni sınaqdan keçirmək üçün Ruanda hökuməti ilə əməkdaşlıq etdi. Ubutaka blokçeyn Ruandanın mövcud torpaq reyestrinin infrastrukturu ilə inteqrasiya olunacaq. Medici Land Governance (MLG) Overstock.com-un blokçeyn törəmə şirkətidir. MLG-nin Liberiyada torpaq idarəsi üçün daha bir pilotu var. İsveç blokçeyn startapı ChromaWay telekommunikasiya provayderi Telia, Kairos Future məsləhət qrupu və iki bank, SBAB və Landshypotek ilə sıx əməkdaşlıqda əmlak əməliyyatları üçün blokçeynini uğurla sınaqdan keçirdi.

Blokçeyndən istifadə edərək hökumət tenderləri üçün təhlükəsiz və şəffaf çərçivə təklif olunur. Bu iş əsasən təhlükəsizlik, məxfilik, şəffaflıq və iş sürətinin yaxşılaşdırılmasına yönəlib. Dövlət satınalma prosesləri üçün istifadə olunan iki blokçeyn layihəsi aşağıdakılardır:

- Belçikada Digipolis-dən Smart Satınalma Aləti layihəsi.
- Cənubi Koreyada dövlət satınalmaları üçün Seul rayonu blokçeyn əsaslı sistem.

Gigipolis Belçikanın Antverpen şəhəri üçün İT sistemləri və xidmətlərinin təmin edilməsinə cavabdehdir. Digipolis, təkliflər üçün sorğuların dərcini və satıcılardan tenderlərin təqdim edilməsini birləşdirən blokçeyn əsaslı proqram hazırladı. Cənubi

Koreyanın Seul rayonu blokçeyn əsaslı təklif qiymətləndirmə sistemini uğurla tətbiq etdiklərini açıqladı. Yeni blokçeyn sistemi ictimai tenderlərə cavabların qiymətləndirilməsinin şəffaflığını və etibarlılığını artırmaq məqsədi daşıyır. Siam Commercial Bank-ın fintech törəmə şirkəti olan Accenture və Digital Ventures birlikdə Taylandda rəqəmsal satınalma prosesi üçün unikal blokçeyn həllini hazırlayıb və istifadəyə verib. Bu həll şirkətlərin mal almaq və satmaq, ödəniş etmək və qəbul etmək və maliyyələşdirmə üsullarını asanlaşdırır.

Blokçeyn texnologiyası ticarətlə bağlı ofis prosedurlarını daha etibarlı, şəffaf, hesabatlı və səmərəli etməklə, gəmiçilik və liman sənayesinə əhəmiyyətli dərəcədə təsir göstərmişdir. Malların daşınmasının mürəkkəbliyini, sənaye standartlarını və tənzimləyici gözləntilərə cavab verməsini nəzərə alaraq, malların daşınması ilə məşğul olan müəssisələr oyunu dəyişən bu texnologiyadan yararlanmağa hazır olmalıdırlar. Burada müvəffəqiyyətli layihələr aşağıdakılardır:

- Sloveniyanın Koper limanında CargoX blokçeyn Sənəd Transferi.
- Maersk və IBM-dən TradeLens.
- Maqta Gateway və Abu Dhabi Ports törəmə şirkətindən Silsal.
- Hollandiya bankı ABN AMRO, Rotterdam Limanı və Samsung SDS-dən DELIVER blokçeyn ticarət təşəbbüsü.

CargoX platforması etibarlı rəqəmsal mühitdə orijinal və məxfi ticarət sənədlərinin ötürülməsinə imkan verir. Qəbul edənlər həmişə orijinal mənbəni təsdiq edə və sənədlərinin sahibliyini sübut edə bilərlər. Maersk və IBM gəmiçilik sənayesi üçün TradeLens blokçeyn texnologiya həllini sınaqdan keçirib. TradeLens, qlobal göndərmə əməliyyatında iştirak edən bütün iştirakçılara real vaxt rejimində daşınma hadisələrini təhlükəsiz və problemsiz şəkildə mübadilə etməyə imkan verən sənədsiz ticarət və tədarük zəncirinin tam görünməsini təmin edir. Maqta Gateway və Abu Dhabi Ports törəmə şirkətindən Silsal ticarət icması arasında maraqlı tərəflər arasında qüsursuz və təhlükəsiz əlaqə təmin etmək üçün blokçeyn texnologiyasını və unikal rəqəmsal istifadəçi şəxsiyyətlərini birləşdirir. Hollandiyanın ABN AMRO bankı daşıma konteynerlərini izləmək və dərhal maliyyələşdirmək üçün Rotterdam Limanı və Samsung SDS ilə blokçeyn ticarət təşəbbüsü olan DELIVER ilə əməkdaşlıq etdi.

Uğurlu pilot sınaqdan sonra bu üç firma təsdiq edir ki, DELIVER fiziki sənədlərə və ya uzun yoxlama yoxlamalarına ehtiyac olmadan bütün göndərmə prosesini təhlükəsiz idarə edə bilər.

Maliyyə sektorunda rəqəmsal aktivlərin tətbiqi sürətlə inkişaf edir. Rəqəmsal aktivlər üçün real vəziyyət ən görkəmli tətbiq sahələrindən biridir. Maliyyə sektorundakı layihələr aşağıdakılardır:

- Vanguard-dan aktivlə təmin edilmiş qiymətli kağızların (ABS) buraxılması üçün Blokçeyn pilotu.
- Infosys-dən blokçeyndə Finacle Trade Connect.
- R3-dən blokçeyndə Marco Polo ticarət maliyyələşdirmə platforması.

Texnologiya provayderi Symbiont ilə tərəfdaşlıqda Vanguard investisiya idarəetmə şirkəti aktivlə təmin edilmiş qiymətli kağızların (ABS) buraxılışını rəqəmsallaşdırmaq üçün nəzərdə tutulmuş blokçeyn pilotunu tamamladı. O, ABŞ-ın böyük ABS emitenti BNY Mellon, Citi və State Street ilə sıx əməkdaşlıqda başdan-başa əməliyyat axınlarını təkrarlamaqla blokçeyndə ABS hesablaşmasının bütün həyat dövrünü uğurla modelləşdirdi. Blokçeyn proqram şirkəti R3, ticarət maliyyəsi texnoloji provayderi TradeIX və bir qrup böyük bank Marco Polo ticarət maliyyə platformasını blokçeynində uğurla sınaqdan keçirdi. Bu həll hazırda ticarət maliyyəsinin üç sahəsini əhatə edir: riskin azaldılması, kreditor borclarının maliyyələşdirilməsi və debitor borclarının maliyyələşdirilməsi.

Blokçeyn məlumatların etibarlı, saxtakarlığa qarşı qalmasını və hüquq-mühafizə orqanları üçün son dərəcə vacib olan sübutlar zəncirinin qorunmasını təmin edir. Hüquq-mühafizə sahəsində istifadə olunan perspektivli blokçeyn layihələri aşağıdakılardır:

- Çində İnternet Məhkəmələrində Blokçeyn Sübutları.
- Çin, İsveçrə və Fransada blokçeyn üzrə şirkətin qeydiyyatı.
- Uyğunluğun yoxlanılması üçün WeCanComply blokçeyn platforması.

Blokçeyn texnologiyası saxta sübutların yaradılması və saxlanması üçün Çin İnternet Məhkəmələrində tətbiq edilmişdir. Bu proses ənənəvi üsullardan daha sürətli və daha sərfəli olur. Çin məhkəməsi ilk dəfə 2018-ci ilin iyununda Hangzhou Huatai

Media Culture Media ilə Shenzhen Daotong Technology Development işində blokçeyn sübutlarını qəbul etdi. Quançjou ştatının Huanqpu şəhərində Çin yerli hökuməti blokçeyn üzrə şirkətin qeydiyyatı layihəsi üzrə uğurlu pilot sınaq keçirib. İndi abituriyentlər "bir forma, bir kolleksiya, bir kliklə əməliyyat" sistemindən istifadə edərək, şirkəti qeydiyyatdan keçirmək üçün vahid platformadan istifadə edə bilərlər. IBM İsveçrə və Fransada oxşar bir növü uğurla başa vurdu. Bir neçə İsveçrə bankı özəl kastodian banklara və xarici aktiv menecerlərinə uyğunluq sənədlərini mübadilə etməyə imkan verən WeCanComply blokçeyn platformasına qoşulub.

Bərpa olunan enerji mənbələri olduqca etibarsızdır və etibarsız enerji artıqlığı və enerji tələbləri yaradır. Buna görə də, blokçeyn texnologiyası bərpa olunan enerji inteqrasiyasının həyata keçirilməsi, ticarət platformaları və enerji izafilərinin və tələblərinin düzgün idarə edilməsi üçün populyarlaşır. Sınaqdan keçirilmiş üç perspektivli layihələr aşağıdakılardır:

- Hollandiyanın Rotterdam limanında mərkəzləşdirilməmiş enerji şəbəkəsi layihəsi.
- Hindistanda peer-to-peer damüstü günəş ticarəti pilotu işə salındı.
- Brooklyn Microgrid layihəsi günəş enerjisini izləmək və izləmək üçün blokçeyndən istifadə edir.

Distro, Hollandiyanın Rotterdam limanında Microgrid elektrik ticarət platforması bərpa olunan enerji təchizatı və tələbini koordinasiya etmək üçün süni intellekt və blokçeyn texnologiyasından istifadə edir. Hindistan Ağıllı Şəbəkə Forumu (ISGF) Avstraliyalı texnoloji qabaqcıl Power Ledger ilə Uttar Pradeşdə blokçeyn peer-to-peer ticarət pilotunu işə saldı. Bu pilot layihə təchizatçıların qonşu ev təsərrüfatları ilə blokçeyn platformasında ağıllı müqavilələr vasitəsilə damda günəş enerjisi ticarətinin mümkünlüyünü nümayiş etdirəcək. Brooklyn Microgrid layihəsi qonşuların günəş enerjisini alqı-satqı və izləyə bilməsi üçün damdakı günəş panellərini birləşdirir.

Blokçeyn texnologiyası müxtəlif tətbiq sahələrində getdikcə populyarlaşır və tətbiq oluna bildiyi yerlərdə, yerləşdirilmiş proqramların sayı artan blokçeyn platformalarında əsas ictimai xidmət təşəbbüsləri mövcuddur. Bununla paralel olaraq, daha çox ölkə öz blokçeyn strategiyalarını, vizyonunu və 2030-cu ilə qədər vizyona yönəlmiş yol xəritələrini inkişaf etdirməyə başlayacaqdır.

III FƏSİL. BLOKÇEYN TEXNOLOGİYALARININ AĞILLI ŞƏHƏR İNFRASTRUKTURUNDA TƏTBİQLƏRİNİN TƏDQİQİ

3.1. Ağıllı şəhərlərdə autentifikasiya və avtorizasiya üçün blokçeynlərin tətbiqi

Əşyaların İnternetinin (IoT) yaranması şəhər həyatının müxtəlif aspektlərini avtomatlaşdıran və optimallaşdıran bir-biri ilə əlaqəli qurğular və sensorlar ilə xarakterizə olunan ağıllı şəhərlərin inkişafına yol açdı. Bununla belə, bu cihazlar arasında təhlükəsiz və etibarlı rabitənin təmin edilməsi mühüm problem olaraq qalır. Blokçeyn texnologiyası, mərkəzləşdirilməmiş və müdaxiləyə davamlı təbiəti ilə ağıllı şəhərlərdə autentifikasiya və avtorizasiya tapşırıqları üçün perspektivli həll yolu kimi ortaya çıxdı. Əşyaların İnterneti (IoT) termini 1999-cu ildə istifadə olunduğundan bəri bir çox təriflər verilmişdir. Tipik IoT arxitekturası müxtəlif İnformasiya və Kommunikasiya Texnologiyalarından (İKT) istifadə edərək şəbəkə üzərindən qoşulan və buludda resurs tutumlu əməliyyatları yerinə yetirən "əşyalar" kimi yaradılmış cihazlardan ibarətdir. Unikal identifikasiya İnternetə qoşulma qabiliyyəti ilə yanaşı, əşyaların əsas xüsusiyyətlərindən biridir. Unikal identifikasiya ya Şəbəkə İnterfeys Kartına (NIC) təyin edilmiş MACID və ya şəbəkə tərəfindən qoşulmuş hər bir fərdi cihaza təyin edilmiş IP ünvanı ola bilər. IoT memarlığı ağıllı səhiyyədən sənaye IoT və ağıllı şəhərlərə qədər dəyişən bir çox tətbiqdə istifadə olunur. Bu IoT şəbəkələrini insanlar və proseslərlə birləşdirmək Hər Şeyin İnternetini (IoE) yaradır. Çox mürəkkəb bir mühit olan Səhiyyə Kiber-Fiziki Sistemində (H-CPS) bir çox IoT şəbəkələri təchizat zəncirlərində, tibb mərkəzlərində, qayğı mərkəzlərində və s. istifadə olunur. Sağlamlıq Sığortasının Daşınması və Hesabatlılığı Aktına (HIPPA) əsasən, bu cür həssas səhiyyə məlumatları yüksək məlumat məxfiliyi və təhlükəsizliyi ilə idarə edilməlidir. Qoşulmuş cihazların sayı gündən-günə artdığından, daha yüksək hesablama və güc tələbləri hesabına möhkəm təhlükəsizlik mexanizmlərinin tətbiqi IoE mühitləri üçün mümkün həll yolu deyil. Bu cür möhkəm təhlükəsizlik sistemlərinin olmaması təcavüzkarların sistemlərə uzaqdan icazəsiz giriş əldə etmələri üçün qapılar açmışdır.

IoT arxitekturası TCP/IP kimi rabitə protokolu yığınından müstəqildir və aşağı bant genişliyi IoT tələblərinə cavab verə bilən bir çox yüngül protokollarla təchiz edilmişdir. IoT-dəki şeylər sensor məlumatların toplanması və onların əşyalarla müqayisədə bir az daha yüksək hesablama və saxlama qabiliyyəti olan bir lövhəli kompüterlər (SBC) olan son cihazlara ötürülməsindən məsuldur. Bu ekoloji məlumatların toplanması və ötürülməsi IoT arxitekturasının əsas problemlərindən biridir və müxtəlif orta proqram texnologiyaları tərəfindən asanlaşdırılır. Edge Məlumat Mərkəzlərindən (EDC) ibarət olan kənar təbəqə real vaxt rejimində məlumat emal bölmələri kimi çıxış edəcək və təcili məlumatların işlənməsini təmin edəcək. Hərbi və sənaye IoT daxil olmaqla bir sıra tətbiqlər EDC-lərin inteqrasiya olunmuş IoT arxitekturasından istifadə etməklə həyata keçirilə bilər. Məlumatların toplanması və təhlükəsiz ötürülməsi kritik tətbiqlərdə həyata keçirilən bu cür arxitekturaların mühüm aspektləridir. Həm simmetrik, həm də asimmetrik kriptoqrafiya üsullarını əhatə edən bir çox təhlükəsizlik alqoritmləri mövcuddur. Rabitə və mərkəzi qurum zamanı həyata keçirilən kriptoqrafiya əməliyyatları, paylanmış iştirakçılar arasında konsensusa nail olmaq üçün mərkəzi orqanın tələblərini həll edə bilən blokçeyndən istifadə etməklə əvəz edilə bilər. Blokçeyn arxitekturasında mərkəzi qurum mövcud deyil və paylanmış kitabı təmin etmək və şəbəkədəki qovşaqlar arasında konsensus saxlamaq üçün konsensus alqoritmi istifadə olunur. Bəzi geniş istifadə olunan blokçeyn konsensus alqoritmləri Proof-of-Work (PoW), Proof-of-Stake (PoS) və Proof-of-Activity (PoA)dır. Lakin mövcud alqoritmlər yüksək hesablama imkanları və IoT arxitekturalarında mövcud olmayan resurslar tələb edir.

Bir ölçü hamıya uyğun olmadığı üçün müxtəlif tətbiqlər üçün müxtəlif konsensus protokolları təklif olunur. Ən çox istifadə edilən konsensus protokolu təklif olunan heşchash CPU dəyəri funksiyasına əsaslanan İş Proof-of-Work (PoW) alqoritmidir. Bu konsensus protokolunda, şəbəkədəki müxtəlif qovşaqlar bir kriptoqrafiya hash funksiyasını həll etmək üçün doğru nonce tapmaq üçün yarışır. Doğru olmayanı tapan qovşaq, həvəsləndiricilərin veriləcəyi yeni blok əlavə etmək imkanı əldə edəcək. PoW kriptovalyutalarda geniş istifadə olunur; lakin yüksək hesablama tələbləri onu resurs məhdud IoT mühitləri üçün uyğun etmir.

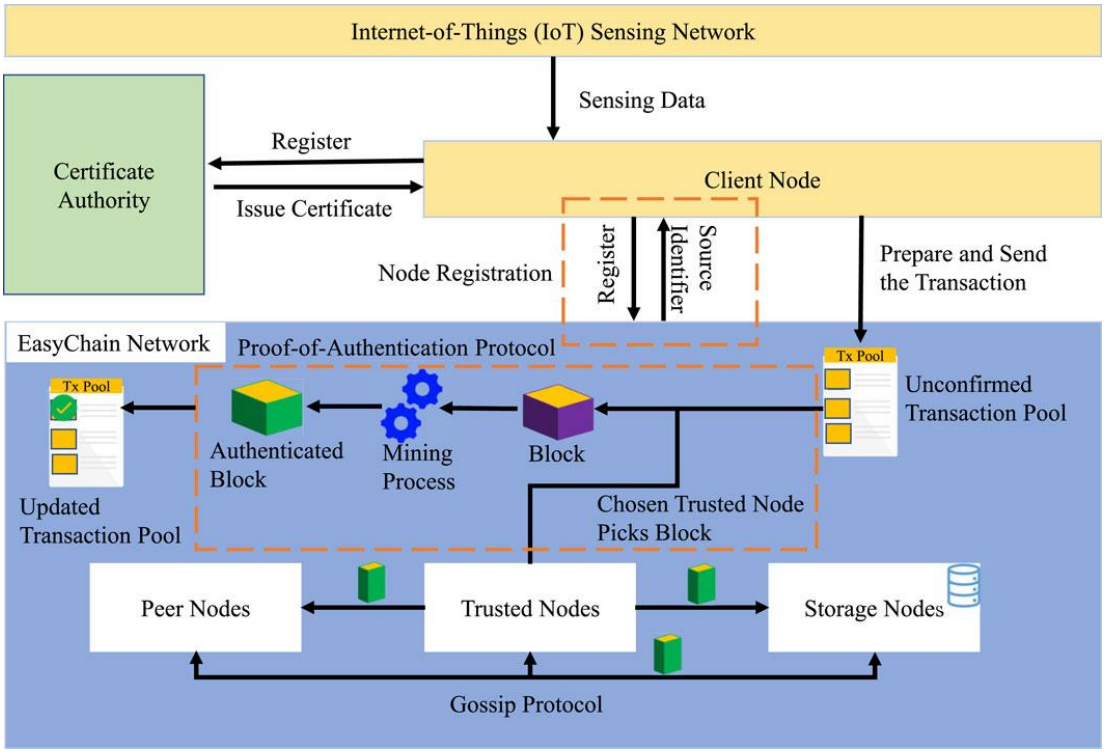
Proof-of-Stake (PoS) PoW kimi hesablama qabiliyyəti əvəzinə istifadəçini seçmək üçün parametrlər kimi əsasən payın miqdarını istifadə edən PoW-un yanında başqa məşhur konsensus mexanizmidir. Bu, yüksək hesablama tələblərinə ehtiyacı aradan qaldırır və şəbəkənin ötürmə qabiliyyətini artırır. Bununla belə, PoW kimi, PoS kriptovalyuta şəbəkələrində daha populyardır, lakin pay anlayışı IoT sistemləri üçün aktual deyil. BitShares layihəsində PoS-in bir variantı olan Delegated Proof-of-Stake (DPoS) təklif olunur. DPOS-da istifadəçi səsləri ilə müəyyən sayda şahid və ya blok istehsalçısı seçilir. DPOS PoW və PoS-dan daha sürətli olsa da, daha mərkəzləşdirilmişdir və pul aspektlərindən asılılıq onu IoT sistemləri üçün yaxşı namizəd etmir. Proof-of-Morportance (PoI), qazanan qovşağın pul qoyuluşları ilə birlikdə düzgün şəkildə təsdiqlənmiş əməliyyatların sayı kimi çoxsaylı amillərdən istifadə etməklə hesablanmış reputasiya əsasında seçildiyi PoS variantıdır.

Proof-of-Elapsed Time (PoET) Hyperledger Fabric-də Intel tərəfindən təklif olunan başqa bir konsensus protokoludur. Təsadüfi gözləmə vaxtı dəyərləri Etibarlı İcra Mühiti (TEE) vasitəsilə hər bir düyün üçün təyin ediləcək. Daha yüksək ötürmə qabiliyyətini təmin etsə də və xüsusi şəbəkələr üçün nəzərdə tutulsa da, mexanizm şəbəkəni mərkəzləşdirir və Software Guard Extensions (SGX) kimi Intel alətlərindən çox asılıdır.

Proof-of-Activity (PoA) PoW və PoS birləşməsidir. İlk addımda madenciler mürəkkəb kriptoqrafiya tapmacasını yerinə yetirəcəklər və yalnız başlıq məlumatı və mədən mükafatı ünvanı olan boş şablon bloku yaradacaqlar və onun heç bir əməliyyatı yoxdur. Sonrakı mərhələdə bloku yoxlamaq və şəbəkəyə əlavə etmək üçün təsdiqləyiciləri tapmaq üçün PoS mexanizmi tətbiq olunur. Etibarlı blok əlavə edildikdən sonra əməliyyatlar yeni yaradılmış bloka qeyd olunacaq. PoA yüksək enerji sərfiyyatına və gecikmə müddətinə malikdir, bu da onu IoT sistemləri üçün əlverişli həll etmir. PoW yerinə yetirən kreditə əsaslanan PoW mexanizmi təklif olunur və tapmacanın çətinliyi düyünün dürüstlüyünə əsaslanaraq dinamik olaraq dəyişir.

Bloklar blokçeynə əlavə edildikdən sonra o, saxlama qovşaqlarına ötürülür. Təcrübəli tibb bacısı və ya həkim saxlama qovşaqlarından məlumat əldə edə bilər. Bu, həkimin çox aşağı gecikmə ilə xəstənin həyati funksiyalarını uzaqdan izləməsini

asanlaşdırır. Blokların autentifikasiyası və yüksək trafiklə blokçeynə əlavə edilməsi üçün təxminən 400 millisaniyə vaxt tələb olunur. Bu, aşağı gecikmə müddəti olan əməliyyatları təmin edir və həkimin xəstə məlumatlarına daxil olmasını asanlaşdırır. Xəstə təcili yardım maşını ilə xəstəxanaya aparılarkən həkim xəstənin həyati vəziyyətini qiymətləndirə bilər və həkim buna uyğun müalicə strategiyası hazırlaya bilər. Təklif olunan EasyChain mexanizmi üç mərhələyə bölünə bilər: Müştəri qovşaqlarının ilkin qeydiyyatı, Tranzaksiyaların yaradılması və işlənməsi və xəstə məlumatlarına təhlükəsiz girişi təmin etmək üçün Sağlam girişə nəzarət mexanizmi. Təklif olunan EasyChain-in proqram arxitekturası Şəkil 3.1-də göstərilmişdir.



Şəkil 3.1 Təklif olunan EasyChain-in proqram təminatı arxitekturası

İlkin addım zamanı hər bir müştəri qovşağı EasyChain şəbəkəsində qeydiyyata alınır. Şəbəkənin hər bir qovşağına unikal özəl və ictimai RSA kriptoqrafiya açarları verilir. Təyin edilmiş açıq açar $P_{\upsilon}KN$ və şəxsi açar $P_{\gamma}KN$ müştəri qovşağının təhlükəsiz fayl yerində saxlanılır. Müştəri nodu MACID və mənbə ID (SID) adlı təsadüfi yaradılan unikal ID göndərəcək. Şəbəkədəki hər bir iştirakçı qovşaq tərəfindən qovşaq siyahısı saxlanılır ki, bu da yeni qovşaqlar üçün həmyaşıdların kəşfinə kömək edir.

Bütün mövcud qovşaqlar yeni qovşaq məlumatı ilə yeniləndikdən sonra, bu qovşaq siyahısının mövcud qovşaqdan bir nüsxəsi də yeni qovşaq tərəfindən digər mövcud qovşaqların aşkar edilməsi üçün yeni əlavə edilmiş qovşağa kopyalanacaq. Bununla yanaşı, zəncir məlumatı da başlanğıc/qeydiyyat mərhələsində yeni N düyün'də kopyalanır. Şəbəkəyə yeni düyün qeydiyyatının ətraflı addımları Alqoritm 3.1-də göstərilmişdir.

Cədvəl 3.1 "EasyChain" Şəbəkəsinə Yeni Qovşaqların Qeydiyyatı

Ardıcıllıq	***Python Alqoritmi***
Daxiletmə	Hər düyün MACID, Mənbə ID-si və öz təyin edilmiş Şəxsi (PγK) və Açıq açarları (PυK) ilə əlaqəli öz şəxsiyyətinə malik olacaq. Müştəri proqramının işlədiyi port nömrəsi ($Port_{num}$).
Çıxış	Bütün şəbəkə qovşaqlarında qovşaq siyahısı yeni əlavə edilmiş qovşaqlarla yenilənəcək.
1	şəbəkəyə daxil olan hər yeni N düyün üçün
2	Bu düyün üçün təsadüfi və unikal olan unikal mənbə ID (SID) yaradılır.
3	RSA Açıq açar (PυKN) və Şəxsi Açarlar (PγKN) yaradılır və bu düyün üçün təyin edilir.
4	Şəxsi Açar yaradıldı PγKN ← rsa.generateNewKey(ictimai eksponent, açar ölçüsü)
5	Açıq Açar yaradıldı PυKN ← PγKN.getPublicKey()
6	RSA Şəxsi PγKN və ictimai PυKN açarları müştəri düyün təhlükəsiz saxlama yerində saxlanılır.
7	Açıq açar faylı ← writePublicKey(PυKN, fayl adı)
8	Şəxsi açar faylı ← writePrivateKey(PγKN, fayl adı)
9	Yeni düyün qeydə alınıb və bütün şəbəkə qovşaqlarına yayımlanır
10	registerAndBroadcastNode(Portnum, MACID, SID, PυKN)
11	Mövcud Düyün Siyahısında hər Ni düyün üçün edin
12	Ni düyün siyahısı yeni düyün məlumatı ilə yenilənir
13	NodeListi.append(NodeN(Portnum, MACID,SID,PυKN))
14	son
15	NodeListN ← getNodeListOfExistingNodes()
16	Consensus-u işə salın və ən uzun məqbul zənciri yeni N düyünə köçürmək
17	Node N ChainN üçün Zəncir ← getLongestAcceptedChain()
18	SID-i qaytarmaq
19	son

Müştəri qovşağı şəbəkədə qeydiyyatdan keçdikdən sonra o, əməliyyatlar yarada və məlumatı şəbəkə daxilində paylaşa bilər. Kənar müştəri qovşağından yaradılan

əməliyyat SHA-256 hashing alqoritmindən istifadə edilərək heşlənəcək və kənar müştəri qovşağının şəxsi açarından istifadə edərək rəqəmsal imza yaratmaq üçün istifadə olunacaq. Yaradılan rəqəmsal imza daha sonra MACID ilə birlikdə əməliyyat məlumatlarına əlavə olunacaq. Rəqəmsal imza, Doğrulamanın təsdiqlənməsi alqoritminin əsas autentifikasiya addımı kimi istifadə olunur, MACID isə ikinci dərəcəli autentifikasiya üçündir. Əməliyyat kənar müştəri qovşağı tərəfindən yaradıldıqdan sonra o, bütün şəbəkəyə yayımlanacaq və təsdiqlənməmiş əməliyyatlar hovuzuna əlavə olunacaq. Şəbəkədəki etibarlı qovşaqlar təsdiqlənməmiş tranzaksiya hovuzundan hələ təsdiq edilməmiş əməliyyatları götürəcək. Etibarlı qovşaq daha sonra eyni heşinq alqoritmi (SHA-256) və rəqəmsal imzadan əldə edilən əməliyyat qovşağının açıq açarından istifadə edərək əməliyyat məlumatlarının hashını hesablayır. Sonra mesajın bütövlüyünü və nüfuzsuzluğunu yoxlamaq üçün hər iki hash müqayisə edilir. Bu, tranzaksiya məlumatlarının əsl qovşaqdan gəldiyini və zərərli qurumların heç birinin şəbəkə üzərindən əlaqə qurarkən məlumatları dəyişdirə bilməməsini təmin edir. Əgər heşlər uyğun gəlirsə, o zaman etibarlı qovşaq kənar cihazdan göndərilən MACID-i müqayisə edərək əməliyyatda ikinci dərəcəli autentifikasiya həyata keçirir. MACID yoxlaması uğurlu olduqda, etibarlı qovşaq tərəfindən yaradılan təsadüfi bir dəyər olan təsadüfi identifikasiya sübutu bloka əlavə edilir və bütün şəbəkədə dərc olunur. Təklif olunan PoAh əsaslı EasyChain, yalnız təsdiqlənmiş müştərilərin iştirak edə və məlumat paylaşa biləcəyi özəl şəbəkələr üçün nəzərdə tutulmuşdur. HIPPA-ya görə, fərdlərin sağlamlıq məlumatlarına maksimum təhlükəsizlik və məxfilik verilməlidir. Bu cür möhkəm nəzarət giriş metodologiyasını həyata keçirmək üçün xəstə haqqında hər hansı məlumat təqdim edilməzdən əvvəl sorğu edəni müəyyən etmək üçün RSA açarlarından istifadə edilir. Şəbəkədəki qovşaqlar, zəncir məlumatları ilə yanaşı, müraciət edənin giriş icazəsi verilmiş bütün açıq açarlarına malik olan Girişə Nəzarət Siyahısını (ACL) saxlayır. Yaradılan əməliyyatın vaxt möhürü də təkrar hücumların qarşısını almaq üçün sorğuya əlavə olunur. Yaratma əməliyyatının və blokların yaradılmasının ətraflı addımları Alqoritm 3.2-də göstərilmişdir.

Cədvəl 3.2 "EasyChain" Tranzaksiya Generasiyası

Ardıcıllıq	***Python Alqoritmi***
Giriş	Şəbəkədəki bütün kənar qovşaqların təyin olunmuş Şəxsi (PγKe) və Açıq düymələri (PυKe) olacaq.
Çıxış	Yeni blok yaradılır və zəncirə əlavə edilir.
1	ti vaxt intervalı üçün edin
2	Tranzaksiya Trx kənar müştəri qovşağı (e) tərəfindən yaradılır, o cümlədən işlənmiş məlumat məlumatları, yəni.
3	Trx ← Transaction yaradın(yəni)
4	Metadata Trx əməliyyatına əlavə edildi
5	Trx ← Trx.append(Metadata)
6	SHA-256 alqoritmi hash hesablamaq üçün istifadə olunur.
7	Rəqəmsal İmza kənar qovşağın şəxsi açarından istifadə etməklə yaradılır.
8	İşarə ← PγKe(SHA − 256(Trx))
9	E kənar müştəri qovşağının MAC ünvanı əməliyyata əlavə edilir və blok yaradılır.
10	Blok olun ← Trx+.appendHeader(Dsign, MAC)
11	Hazırlanmış Blok Be bütün şəbəkədə yayımlanır
12	Yaradılmış əməliyyat daha sonra konsensus addımları üçün etibarlı qovşaq tərəfindən seçilməzdən əvvəl təsdiqlənməmiş hovuza əlavə edilir.
13	Etibar dəyəri həddi (θ) əsasında etibarlı qovşaq (V) etibarlı qovşaq siyahısından <Siyahı>qovşaqlarından seçilir.
14	İlkin autentifikasiya mənbə müştəri qovşağının açıq açarı ilə rəqəmsal imza üzərində seçilmiş etibarlı düyün V tərəfindən həyata keçirilir.
15	DecryptedMessageHash(MDdec) ← Şifrəni aç(Dsign, PυKe)
16	ComputedMessageHash(MDcom) ← SHA − 256(receivedtransaction(Trx+))
17	əgər MDdec = = MDcom onda
18	İkinci dərəcəli autentifikasiya əməliyyat aparan qovşağın MACID-də həyata keçirilir.
19	əgər Be.MACID = = NodeListOfVerifyingNode.getMACID(Be.SID) olarsa, onda
20	Random Proof-of-Authentication yaradılmır və qovşaqlar şəbəkəsinə yayımlanmadan əvvəl bloka əlavə edilir.
21	başqa
22	bloku keç
23	bitərsə
24	son

Təklif olunan EasyChain-də məlumat əldə etmək üçün ətraflı addımlar Alqoritm 3.3-də göstərilmişdir.

Cədvəl 3.3 "EasyChain" üçün təklif olunan Girişə Nəzarət Alqoritmi

Ardıcıllıq	***Python Alqoritmi***
Giriş	PKI sistemi sorğuçuya öz açıq açarı PυKd və özəl açarı PγKd ilə təyin edir
1	Müraciət edən sorğunun yaradıldığı vaxt damğası TS ilə birlikdə sorğu əməliyyatı yaradır
2	TXreq.append(dataRequestInformation,TS)
3	Reqhash ← SHA-256(TXreq)
4	DigitalSignrequester ← Reqhash.encrypt(PγKd)
5	TX+req ← TXreq.append(DigitalSignrequester)
6	Yaradılmış sorğunu şəbəkəyə dərc edin
7	Requester.publish(TX+req)
8	Hər Məlumat Sorğusu üçün
9	Təyin edilmiş unikal identifikator əsasında sorğu edənin ictimai məlumatını əldə edir
10	PυKd ← getPublicKey(requesterID)
11	Açıq açarı qovşaqlarda Girişə Nəzarət Siyahısına (ACL) qarşı yoxlayın
12	ACL-də PυKd olarsa
13	SHA-256 alqoritmi sorğunun hashını hesablamaq üçün istifadə olunur
14	ComputedHash ← SHA-256(TXreqdat)
15	Əlavə edilmiş rəqəmsal işarə sorğuçunun PυKd açıq açarından istifadə etməklə deşifrə edilir
16	SentHash ← DigitalSignrequester.Decrypt(PυKd)
17	SentHash və ComputedHash-ı müqayisə edin
18	əgər ComputedHash = = SentHash onda
19	Vaxt damğasının δT həddi daxilində olub olmadığını yoxlayın
20	TS ≥ TS-δt və ya TS ≤ TS+δt olarsa
21	Saxlama qovşaqlarından tələb olunan məlumatları əldə edin
22	Reqdata ← retrieve(TXhash)
23	Əldə edilmiş məlumatları sorğuçuya göndərin
24	NetworkNode.publish(Reqdata)
25	başqa
26	Sorğudan imtina edin
27	bitərsə
28	başqa
29	Sorğudan imtina edin
30	bitərsə
31	başqa
32	Sorğudan imtina edin
33	bitərsə
34	son

Şəxsi şəbəkədən məlumat tələb etmək üçün sorğuçu düyün bütün məlumatlarla əməliyyat yaradır. Sorğunun şəxsi açarından istifadə edən rəqəmsal imza hesablanır və onu şəxsi blokçeynə göndərməzdən əvvəl sorğu əməliyyatına əlavə edilir. Giriş sorğuları şəbəkə qovşaqlarından biri tərəfindən götürülür və sorğu edənin açıq açarı sorğuçuya təyin edilmiş unikal ID əsasında götürülür. Alınan açıq açar daha sonra qovşaqlarda həyata keçirilən Girişə Nəzarət Siyahısı (ACL) ilə müqayisə edilir. Sorğunun girişi təsdiqləndikdən sonra, rəqiblərin zərərli sorğularının qarşısını almaq üçün göndərilən rəqəmsal imza əsasında sorğuçu təsdiqlənir. Rəqəmsal imza təsdiqlənərsə, yalnız tələb olunan məlumatlar götürülür və sorğuçuya geri göndərilir. Digər hallarda, sorğular ləğv ediləcək və bununla da möhkəm girişə nəzarət mexanizmi təmin ediləcək.

PoW konsensus alqoritmi vəziyyətində əməliyyatlar təsdiq edildikdən sonra kriptoqrafik tərs hash hesablanır. Hesablama tamamlandıqdan sonra təsdiqlənmiş blok yerli blokçeyn kitabçasına əlavə etmək üçün cihazlar şəbəkəsinə yayımlanır. PoS vəziyyətində, pay əvvəlcə istifadəçi tərəfindən qoyulur. Paya əsasən, istifadəçilər bloku minalamaq üçün təsadüfi seçilir. Blok qazma tamamlandıqdan sonra şəbəkəyə yayımlanır. Bu proseslər yüksək resurslardan, bəzi hallarda isə hashın hesablanması üçün Qrafik Emalı Birliklərindən (GPU) istifadə edir. Bu yüksək performanslı prosessorlar IoT cihazında mövcud deyil.

PoAh məhdud resurslu, aşağı gücə malik, aşağı performanslı IoT cihazları üçün hazırlanmışdır. Şəbəkə məhdud sayda etibarlı qovşaqlarla işə salınır. Etibarlı qovşaqlar etibar dəyəri sıfırdan yüksək olan şəbəkəyə daxil edilmiş təhlükəsiz qurğular hesab olunur. “tr > 0”, Şəbəkədəki cihazların qalan hissəsi “tr = 0” sıfır etibar dəyəri təyin edilmiş müştəri qovşaqlarıdır. Tranzaksiya bloku autentifikasiya edildikdə, etibar dəyəri ‘1’ dəyəri ilə artır və saxta blok təsdiqlənərsə, etibar dəyəri ‘1’ azalır. Müştəri qovşaqlarının etibar dəyərini qazanmaq üçün təsdiqlənmiş bloku müəyyən etmək şansı var. Müştəri nodu etibarlı qovşaq tərəfindən təsdiqlənmiş bloku müəyyən etdikdə, etibar dəyəri ‘tr = 0,5’ artır. Müştəri qovşağı həmçinin ‘tr = 1’ etibar dəyərini qazanmaq üçün etibarlı qovşaq tərəfindən təsdiqlənmiş saxta bloku müəyyən edə bilər. Etibarlı qovşağın etibar dəyəri ‘tr < eşikdən aşağı düşərsə, th’, cihaz etibarlı qovşaq statusunu

itirə bilər. PoAh tətbiqində “5” həddi nəzərə alınır və etibarlı qovşaqlara “10” etibar dəyəri təyin edilir.

Cədvəl 3.4 Təklif olunan PoAh konsensus alqoritmində etibar dəyərinin idarə edilməsi

Ardıcıllıq	***Python Alqoritmi***
Daxiletmə	10 dəyəri olan etibarlı qovşaqların və 0 dəyəri olan digər şəbəkə qovşaqlarının etibar dəyərini işə salın.
Nəticə	Düyünlərin yenilənmiş etibar dəyəri.
1	th həddindən böyük olan trN etibar dəyəri ilə seçilmiş etibarlı düyün Nsel üçün. et
2	Əgər Doğrulanmış blok o zaman
3	Doğrulanmış blok şəbəkəyə yayımlanır;
4	əgər trclient etibar dəyərinə malik Müştəri düyün Nclient saxta blok tapırsa
5	trclient + +; {Müştəri qovşaqlarının etibar dəyəri 1 dəyərlə artır
6	trN − −; {Güvənli qovşaq etibar dəyərini 1 azaltmaqla cəzalandırıldı}
7	Etibarlı düyün statusu yeni trN th eşikdən az olarsa ləğv edilir;
8	başqa
9	əgər trclient etibar dəyərinə malik Müştəri nodu Nclient blok təsdiqini həyata keçirirsə
10	trclient + 0,5; {Müştəri qovşaqlarının etibar dəyəri 0,5 artır}
11	trN + +; {Seçilmiş etibarlı düyün etibar dəyəri 1 artır}
12	başqa
13	trN + +; {Yalnız seçilmiş etibarlı düyün etibar dəyəri 1 artır}
14	bitərsə
15	başqa
16	trN − −; {Seçilmiş etibarlı qovşaq mövcud deyil}
17	Etibarlı qovşaq statusu yeni trN th eşikdən az olarsa ləğv edilir;
18	bitərsə
19	Yeni etibarlı düyün və GOTO seçin (Addım − 1);
20	son

Müştəri düyünü blok yaratmaq üçün əməliyyatları və mənbə açıq açarını toplayır. Daha sonra şəbəkədə yayımlanır. Etibarlı qovşaq bloku qəbul edir və blokdakı imzanın təsdiqlənməsi üçün mənbə ictimai açarını, y-ni alır. Doğrulama prosesi imzanın yoxlanılması üçün açıq və özəl açarla asimmetrik kriptoqrafiyadan istifadə edir. Şəxsi açarı təcavüzkar asanlıqla əldə edə bilməz. İmza yoxlanıldıqdan sonra etibarlı qovşaq MAC ünvanını autentifikasiyanın ikinci mərhələsi üçün qiymətləndirir. Blok etibarlı

qovşaq tərəfindən təsdiqləndikdən sonra, başqalarının onu yerli blokçeyn kitablarına əlavə etdiyi PoAh identifikatoru əlavə edərək bloku yenidən şəbəkəyə yayımlayır.

Cədvəl 3.5 PoAh konsensus alqoritminin proseduru

Ardıcıllıq	***Python Alqoritmi***
Giriş	SHA − 256 hash bütün qovşaqlarda istifadə olunur. Hər bir iştirakçının şəxsi (PrK) və açıq açarları (PuK) var.
Çıxış	Kitaba əlavə edilən Doğrulanmış Bloklar.
1	(Trx+) → bloklar; {Birdən çox əməliyyat bloklar yaratmaq üçün birləşdirilir.}
2	(SPrK)(blok) → yayım; {Blok şəxsi açarla imzalanıb və şəbəkəyə yayımlanır.}
3	(VPuK)(blok) → MAC yoxlanılması; {Etibarlı qovşaqlar mənbə açıq açarı ilə bloku təsdiqləyir}
4	Əgər təsdiq edilibsə
5	blok‖PoAh(D) → yayım; {Autentifikasiya edilmiş blok etibarlı düyün imzası ilə şəbəkəyə yayımlanır}
6	H(blok) → Blokları zəncirə əlavə edin; {Blokun etibarlı düyün imzası varsa, onlar bloka əlavə edirlər.}
7	başqa
8	bloku atın; {Blok orijinal deyilsə, ləğv edilir.}
9	bitərsə
10	GOTO (Addım − 1) növbəti blok üçün

Təklif olunan EasyChain Python proqramlaşdırma dilindən istifadə etməklə həyata keçirilir. Dörd qovşağı olan IoT Sistemi, aralarında bir qovşaq doğrulama qovşağı kimi fəaliyyət göstərmək üçün həddən artıq etibar dəyəri verilmişdir. Eksperimental quraşdırma üçün bütün qovşaqlar 4 GB LPDDR4-3200 SDRAM ilə 1,8 GHz tezlikdə Broadcom BCM2711 dördnüvəli Cortex-A72 (ARM v8) 64 bit SoC əsasında hazırlanmış Raspberry Pi 4 Model B istifadə edərək həyata keçirilir. Düyünün hesablama imkanlarını ölçmək üçün OpenSSL qovşağın kriptoqrafik performansını ölçmək üçün etalon testləri həyata keçirmək üçün istifadə olunur. Sınaq üçün MD5, SHA-256 və SHA3-256 daxil olmaqla bir sıra həzm alqoritmləri seçilir. Simulyasiyanın qiymətləndirilməsi üçün istifadə olunan məlumat ölçüsü kiçik olduğundan, 32 GB SD Kartı olan qovşaqlardan biri yaddaş qovşağı kimi çıxış edir.

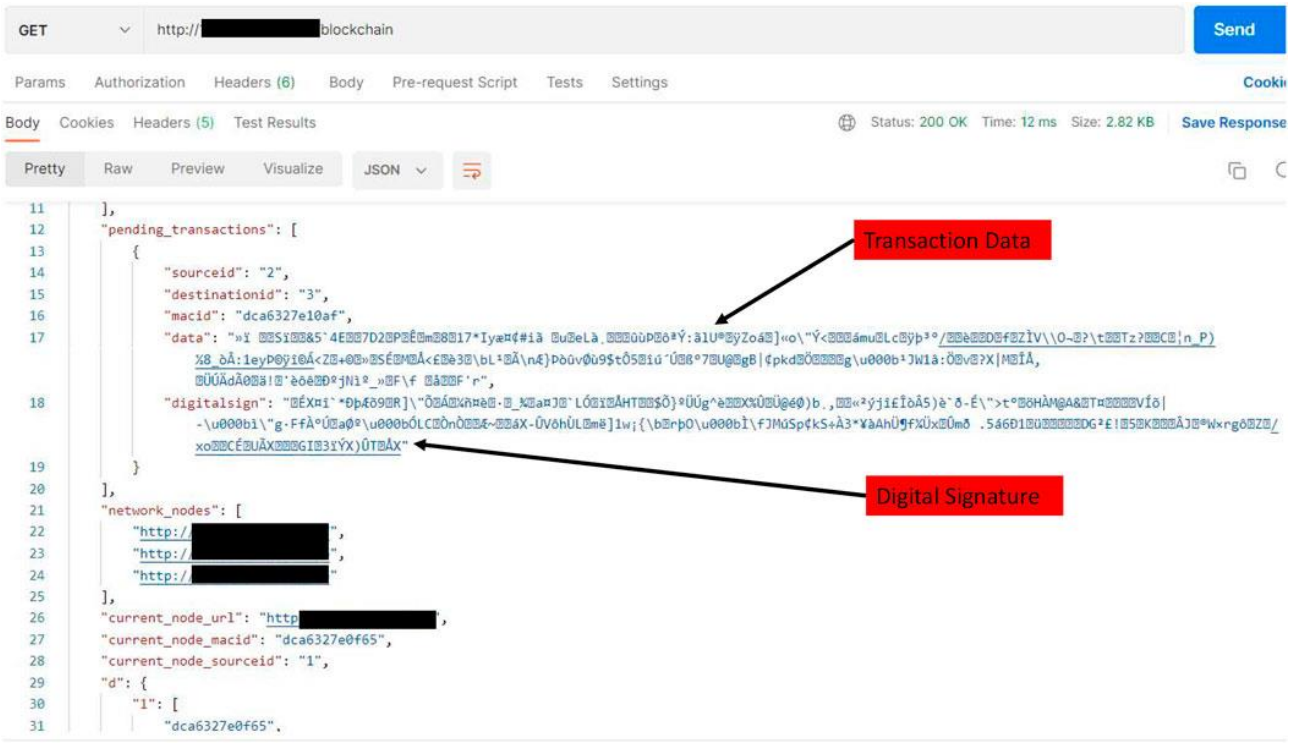
hazırkı eksperimental quruluşda. Real vaxt proqramlarında böyük həcmdə yaddaş tələb olunarsa, SSD USB 3.0 portu vasitəsilə Raspberry Pi 4 qovşağına qoşula bilər. Planetlərarası Fayl Sistemi (IPFS) istifadə edərək zəncirdənkənar saxlama da məlumatların saxlanması üçün həll yolu kimi həyata keçirilə bilər. RSA ictimai kriptoqrafiya sistemi EasyChain-də şifrələmə, rəqəmsal imzalar və imzaların yoxlanılması üçün istifadə olunur.

Şəkil 3.2-də digər zəncir məlumatları ilə birlikdə mühasibat kitabının strukturunu göstərir. Blokçeyn kitabçası gözləyən əməliyyatlar, qeydiyyatdan keçmiş şəbəkə qovşaqları və PoAh ikincili identifikasiyası üçün MAC ünvanı kimi müvafiq məlumatlarla birlikdə zəncirə əlavə edilən minalanmış bloklardan ibarətdir.

Şəkil 3.2 Tətbiq olunan EasyChain üçün genezis blokunu göstərən kitab strukturu

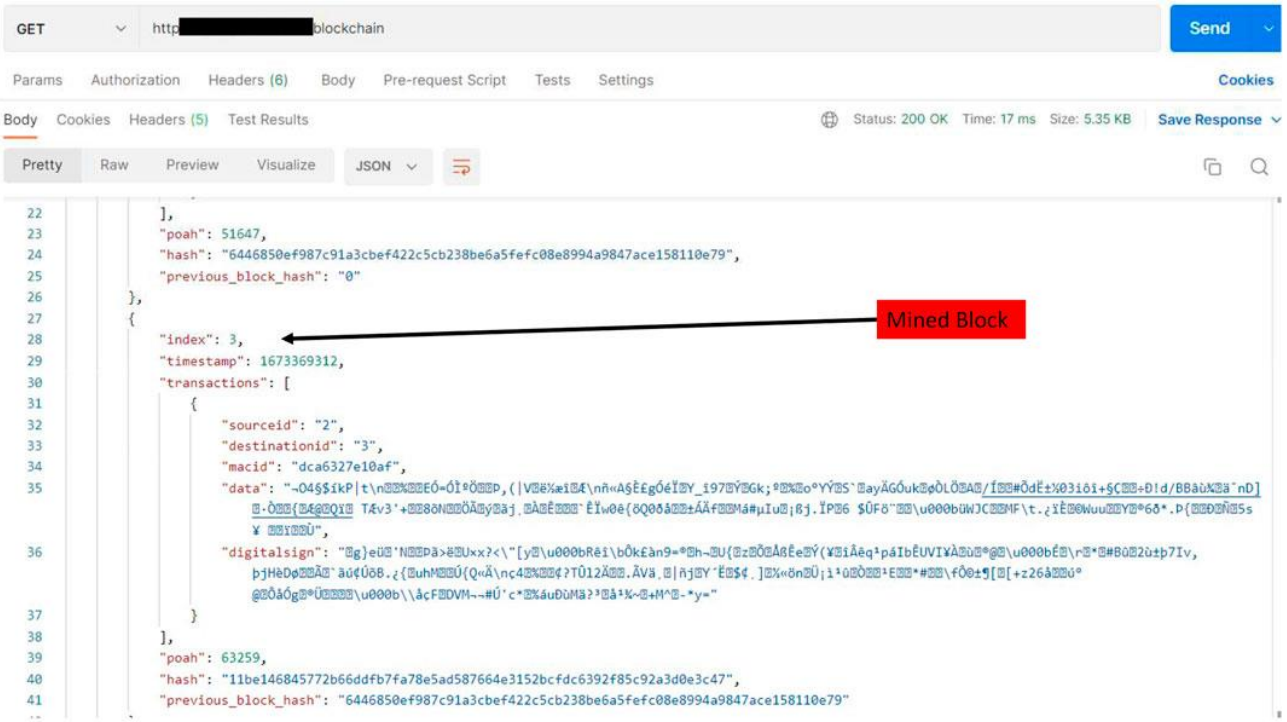
Müştəri qovşağından əməliyyatların həyata keçirilməsi üçün xəstənin şəxsiyyəti, Bədən istiliyi, tənəffüs dərəcəsi, doymuş oksigen səviyyəsi (SpO2) və qan təzyiqi kimi vacib məlumatlardan ibarət nümunə monitorinq məlumatları istifadə olunur. Xəstə məlumatlarını göndərməzdən əvvəl əməliyyat şəxsi açarla imzalanır və yayım

əməliyyatı hər bir şəbəkə qovşağında təsdiqlənməmiş əməliyyat hovuzuna əlavə olunacaq. Əlavə edilmiş təsdiqlənməmiş əməliyyatı Şəkil 3.3-də görmək olar.



Şəkil 3.3 Əməliyyat EasyChain-də təsdiqlənməmiş tranzaksiya hovuzuna əlavə edilir

Şəbəkədəki etibarlı qovşaqlardan biri təsdiqlənməmiş tranzaksiya hovuzundan əməliyyatları götürəcək və PoAh konsensusunu həyata keçirəcək. Konsensus əldə edildikdən sonra o, hər bir həmyaşıd qovşağında zəncirdə yeni blok kimi əlavə olunacaq və müvafiq əməliyyat təsdiqlənməmiş hovuzdan təmizlənəcək. Təsdiqlənmiş blok Şəkil 3.4-də göstərilmişdir.



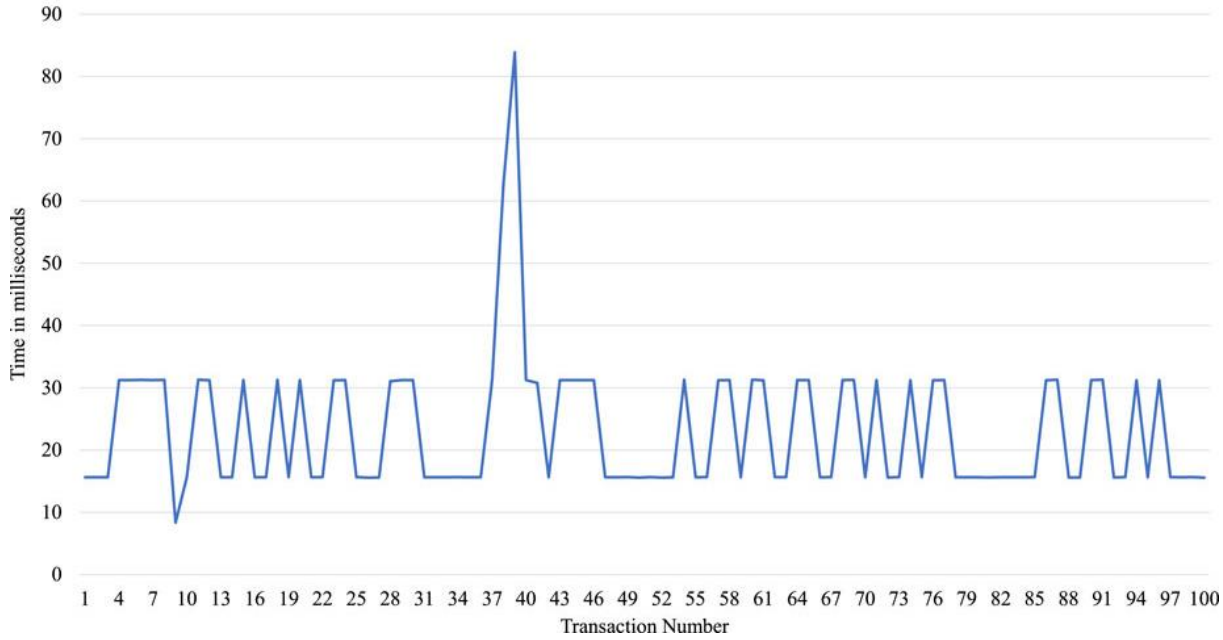
Şəkil 3.4 Etibarlı düyün tərəfindən təklif olunan PoAh konsensusunu yerinə yetirdikdən sonra zəncirə əlavə edilmiş blok

Tətbiq olunan EasyChain-in performansını qiymətləndirmək üçün əməliyyat vaxtı və blok yaratma vaxtları təhlil edilir. Əməliyyatın etibarlı qovşağa çatması üçün çəkilən vaxtı və konsensus mexanizmini yerinə yetirmək və yeni blok əlavə etmək üçün etibarlı qovşaq tərəfindən sərf olunan vaxtı qeyd etmək üçün vaxt möhürləri blokların işlənməsinin bir çox yoxlama nöqtələrində yaradılır.

Vaxt möhürü “tcp” müştəri qovşağının sensor elementlərdən məlumatları topladığı və əməliyyat hazırladığı vaxtdır, vaxt damğası “ttr” isə müştəri əməliyyatının etibarlı node çatması üçün çəkilən vaxtdır. Müştərinin əməliyyat vaxtı “δct” bu zaman damğalarından hesablanır.

$$\delta_{ct}=t_{tr}-t_{cp} \quad (1)$$

Tətbiq olunan EasyChain-də müştəri qovşağından cəmi 100 əməliyyat həyata keçirilir və ölçülmüş əməliyyat vaxtlarını Şəkil 3.5-də görmək olar.

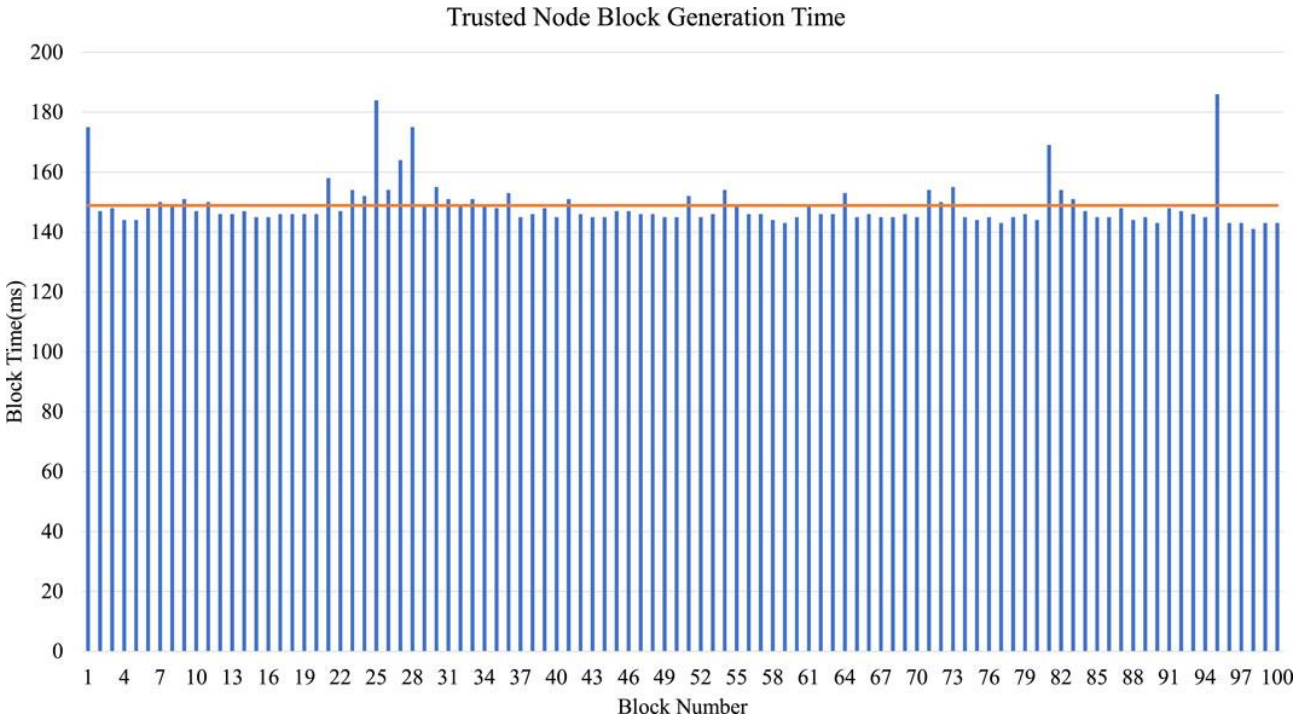


Şəkil 3.5 Müştəri qovşağının tranzaksiyanı etibarlı düyün göndərməsi üçün vaxt

Eynilə, blok yaratma vaxtı, tranzaksiya etibarlı qovşağa çatdıqda qeydə alınan vaxt ttr və ttm PoAh konsensusunu yerinə yetirdikdən sonra blokun minalandığı vaxtdan ölçülür.

$$\delta_{tb}=t_{tm}-t_{tr} \quad (2)$$

Hesablanmış blok yaratma vaxtlarını Şəkil 3.6-da görmək olar. Minimum, Maksimum və Orta vaxtlar hesablanmış və Cədvəl 3.1-də göstərilmişdir. Müştəri qovşağı üçün minimum, maksimum və orta əməliyyat müddətlərinin 8,34 ms, 83,87 və müvafiq olaraq 23,09 ms olduğunu görə bilərik. Eynilə, etibarlı qovşaqların minimum, maksimum və orta blok vaxtları müvafiq olaraq 141 ms, 186 ms və 148.9 ms-dir.



Şəkil 3.6 Yeni blok yaratmaq üçün etibarlı qovşaq üçün tələb olunan vaxt

Cədvəl 3.6 Tətbiq olunan EasyChain-də əməliyyat və bloklama vaxtı

Müddət	***Müştəri qovşağı***	***Etibarlı qovşaq***
Minimum vaxt (ms)	8.34	141
Maksimum vaxt (ms)	83.87	186
Orta vaxt (ms)	23.09	148.89

PoAh konsensus alqoritmi yalnız qovşaqlar tərəfindən göndərilən əməliyyatları təsdiqləyən PoW və PoS kimi digər konsensus alqoritmlərindən fərqli olaraq məlumatları ötürən cihazları təsdiqləyir. PoAh resurs məhdud IoT mühitləri üçün uyğun olan əhəmiyyətli dərəcədə daha az enerji və resurslardan istifadə edir. PoAh-da blokda sensorlar tərəfindən toplanan xəstə məlumatı, xəstə üzərindəki cihazın şəxsiyyəti və blok yaradılan zaman damğası var. Bütün qovşaqlar IPv4 istifadə edərək simli və ya simsiz interfeys vasitəsilə eyni şəbəkəyə qoşulur. MAC ünvanı blok yaradılması zamanı cihazların identifikasiyası kimi istifadə olunur. Blok etibarlı qovşaqlar tərəfindən təsdiq edildikdən sonra o, etibarlı qovşaq və yerli blokçeyn kitabçasına əlavə edilmiş digər qovşaqların imzası ilə şəbəkəyə yayımlanır. PoAh-ın

miqyaslana bilən və IoE üçün uyğun olduğunu təsdiqləmək üçün kağızda aşağıdakı iddialar irəli sürülür.

3.2. Ağıllı şəhərlərdə gizliliyin qorunması üçün blokçeynlərin tətbiqləri

Ağıllı şəhərlər səmərəli və davamlı şəhər xidmətləri təmin etmək üçün sensorlar, Əşyaların İnterneti (IoT) cihazları və istifadəçi tərəfindən yaradılan məlumatlar kimi müxtəlif məlumat mənbələrindən istifadə edir. Bununla belə, bu cür məlumatların toplanması və təhlili fərdlər və onların davranışları haqqında həssas məlumatların toplanması ilə bağlı kritik məxfilik riskləri yaradır. İcazəsiz giriş, məlumatların pozulması və şəxsi məlumatların sui-istifadəsi ağıllı şəhər təşəbbüsləri ilə əlaqəli məxfilik problemləri arasındadır. Ağıllı şəhərlərdə məxfiliyin qorunması üçün blokçeynlərin bəzi əsas tətbiqləri bunlardır:

1. ***Şəxsiyyətin İdarə Edilməsi:*** Blokçeynlər ağıllı şəhər ekosistemində fərdlərin şəxsiyyətini idarə etmək üçün təhlükəsiz platforma kimi xidmət edə bilər. Mərkəzləşdirilməmiş şəxsiyyət idarəçiliyini təmin etməklə, blokçeynlər məlumatların məxfiliyini təmin edir və şəxsiyyət oğurluğu riskini azaldır. Blokçeyn texnologiyası üzərində qurulmuş ağıllı müqavilələr istifadəçilərə şəxsi məlumatlarına nəzarəti təmin etməklə avtorizasiya proseslərini asanlaşdıra və məlumatların məxfiliyini artıra bilər.
2. ***Təhlükəsiz Məlumat Paylaşımı:*** Ağıllı şəhər mühitlərində dövlət qurumları, xidmət təminatçıları və vətəndaşlar kimi müxtəlif qurumlar məlumatları təhlükəsiz şəkildə paylaşmalıdırlar. Blokçeynlər mərkəzləşdirilməmiş saxlama və girişə nəzarət mexanizmlərini təmin etməklə şəffaf və təhlükəsiz məlumat mübadiləsini təmin edir. Ağıllı müqavilələr məlumat mübadiləsi müqavilələrini tətbiq etmək və məxfi məlumatların yalnız səlahiyyətli tərəflər üçün əlçatan olmasını təmin etmək üçün istifadə edilə bilər, beləliklə, məxfilik qorunur.
3. ***Razılığın İdarə Edilməsi:*** Məxfiliyin qorunması məlumatların toplanması və istifadəsi üçün şəxslərdən məlumatlı razılığın alınmasına əsaslanır. Blokçeyn əsaslı həllər, hesabatlılığı və məxfiliyin qorunmasını təmin edərək, şəxslərin razılığının şəffaf və yoxlana bilən qeydini təmin edə bilər. Ağıllı müqavilələrdən istifadə

etməklə razılığın idarə edilməsi prosesləri avtomatlaşdırıla və fərdlər tərəfindən idarə oluna bilər ki, bu da onlara öz şəxsi məlumatları ilə bağlı əsaslandırılmış qərarlar qəbul etmək imkanı verir.

4. ***Təhlükəsiz IoT Bağlantısı:*** Ağıllı şəhər mühitlərində IoT cihazlarının yayılması onların kiberhücumlara qarşı həssaslığı səbəbindən məxfilik və təhlükəsizlik problemləri yaradır. Blokçeyn texnologiyası cihazın autentifikasiyası və təhlükəsiz rabitə üçün mərkəzləşdirilməmiş infrastruktur təmin etməklə IoT təhlükəsizliyini artıra bilər. Məlumatları şifrələmək və blokçeynində saxlamaqla IoT cihazları ilə bağlı məxfilik riskləri azaldıla bilər.

Barselona vətəndaşların iştirakına və məlumatlara əsaslanan idarəetməyə sadiqliyi ilə məşhurdur. Şəhər, vətəndaşların məxfiliyini təmin edərkən öz məlumatlarına nəzarət etmək imkanı verən blokçeyn əsaslı aşağıdakı proqramları həyata keçirib?

- ***Razılığın İdarə Edilməsi:*** "MyData" layihəsi vasitəsilə Barselona vətəndaşlara məlumatların toplanması və istifadəsi üçün açıq razılıq verməyə imkan verir. Blokçeyn texnologiyası fərdlərin razılığının dəyişməz və yoxlana bilən qeydini təmin edir, onlara şəxsi məlumatlarına nəzarət imkanı verir və məxfiliyini qoruyur.
- ***Təhlükəsiz IoT Bağlantısı:*** Barselona IoT cihazlarının təhlükəsizliyini və məxfiliyini artırmaq üçün blokçeyn texnologiyasından istifadə edir. Cihazın identifikasiyası və kommunikasiyası üçün blokçeyndən istifadə etməklə şəhər IoT cihazları ilə bağlı məxfilik risklərini azaldır və bununla da vətəndaşların məxfiliyini qoruyur.

Sinqapur vətəndaşların məxfiliyini qoruyarkən təhlükəsiz və səmərəli məlumat infrastrukturu qurmağı qarşısına məqsəd qoyan "Smart Nation Təşəbbüsünün" bir hissəsi kimi aşağıdakı blokçeyn texnologiyasını mənimsəmişdir:

- ***Təhlükəsiz Məlumat Paylaşımı:*** Sinqapur hökuməti dövlət qurumları və özəl qurumlar arasında təhlükəsiz və yoxlanıla bilən məlumat mübadiləsini təmin etmək

üçün blokçeyn əsaslı məlumat platformalarını araşdırır. Blokçeyn texnologiyası verilənlərə giriş üzərində nəzarəti təmin etməklə və məlumat mübadiləsi müqavilələrini tətbiq etməklə məlumatların məxfiliyini təmin edir.

- ***Şəxsiyyətin İdarə Edilməsi:*** Sinqapur məxfilik və təhlükəsizliyi artırmaq üçün "SingPass" adlı blokçeyn əsaslı rəqəmsal şəxsiyyət sistemini inkişaf etdirir. SingPass vasitəsilə fərdlər şəxsi məlumatlarının paylaşılmasına nəzarət etməklə, məxfiliyin qorunmasını təmin etməklə müxtəlif dövlət xidmətlərinə təhlükəsiz şəkildə daxil ola bilərlər.

Cənubi Koreyada ağıllı şəhər layihəsi olan "Songdo" məxfiliyin qorunması və məlumat təhlükəsizliyini artırmaq üçün aşağıdakı blokçeyn texnologiyasından istifadə edir:

- ***Səhiyyə Məlumatlarının İdarə Edilməsi:*** "Songdo" səhiyyə məlumatlarını idarə etmək üçün blokçeyn əsaslı sistem tətbiq etmişdir. Sistem xəstələrə sağlamlıq qeydlərinə nəzarət etməyə və onların həssas tibbi məlumatlarına kimin daxil ola biləcəyinə qərar verməyə imkan verir. Bu, məxfiliyi təmin edir və mərkəzi vasitəçilərə ehtiyacı aradan qaldıraraq məlumatların pozulması riskini azaldır.
- ***Enerji Ticarəti üçün Ağıllı Müqavilələr:*** "Songdo" sakinlər arasında həmyaşıdlar arasında enerji ticarətini asanlaşdırmaq üçün blokçeyn smart müqavilələrindən istifadə edir. Blokçeyn texnologiyası vasitəsilə təhlükəsiz və şəffaf əməliyyatlar mərkəzi orqana ehtiyac olmadan həyata keçirilə bilər. Bu qeyri-mərkəzləşdirmə daha səmərəli və dayanıqlı enerji ekosistemini inkişaf etdirərək məxfilik və məlumatların bütövlüyünü təmin edir.
- *Məlumatların Monetizasiyası:* "Songdo"da fərdlərin şəxsi məlumatlarını təhlükəsiz şəkildə pula çevirmək imkanı var. Blokçeyn texnologiyasından istifadə etməklə vətəndaşlar məlumatlarını biznes və ya tədqiqatçılarla paylaşmağı seçə, eyni zamanda onun istifadəsi üzərində nəzarəti saxlaya bilərlər. Bu, fərdlərə məxfiliklərini qoruyarkən məlumatlarının dəyərindən faydalanmaq imkanı verir.

Blokçeyn texnologiyasından istifadə etməklə, bu şəhərlər fərdi məlumatların yalnız səlahiyyətli şəxslərlə paylaşılmasını təmin edərək, fərdlərə şəxsi məlumatlarına daha çox nəzarət etməyə imkan verib. Bu, təkcə məxfiliyi qorumur, həm də şəxsiyyət oğurluğu, məlumatların pozulması və şəxsi məlumatlardan sui-istifadə riskini azaldır. Bundan əlavə, ağıllı şəhərlərdə blokçeynin istifadəsi şəffaflığı, hesabatlılığı və etimadı təşviq edir, çünki texnologiya əməliyyatların və qarşılıqlı əlaqələrin dəyişməz və yoxlanıla bilən qeydlərini təmin edir. Bu, maraqlı tərəflər arasında məlumat bütövlüyü və etibarlı məlumat mübadiləsi mədəniyyətini inkişaf etdirir. Bu çətinliklərə baxmayaraq, məxfiliyin qorunması və məlumatların təhlükəsizliyində blokçeyn texnologiyasının potensialını nəzərdən qaçırmaq olmaz. Şəhərlər daha ağıllı və daha çox əlaqəli mühitlərə çevrilməyə davam etdikcə, məxfiliyi qorumaq üçün innovativ həllər tapmaq vacib məsələyə çevrilir. Blokçeyn, fərdlərə yeni texnologiyaların və xidmətlərin üstünlüklərindən yararlanmaqla yanaşı, öz məlumatları üzərində nəzarəti saxlamağa imkan verən perspektivli bir həll təklif edir.

3.3. Ağıllı şəhər təhlükəsizliyi üçün blokçeynlərin tətbiqi üzrə təkliflər

Ağıllı şəhərlər konsepsiyası şəhər həyatının müxtəlif aspektlərini inkişaf etdirmək üçün texnologiyanı birləşdirir. Təhlükəsizlik bu rəqəmsal əlaqəli mühitlərdə vətəndaşların təhlükəsizliyinin və məxfiliyinin təmin edilməsində mühüm sütun kimi dayanır. Mərkəzləşdirilməmiş və dəyişməz bir kitab sistemi kimi ortaya çıxan blokçeynlər, unikal xüsusiyyətləri ilə ağıllı şəhər təhlükəsizliyini gücləndirmək üçün potensial həllər təklif edir.

Əhəmiyyətli bir təklif, ağıllı şəhərlərdə kritik infrastrukturu təmin etmək üçün blokçeynin mərkəzləşdirilməmiş təbiətindən istifadə etməyi əhatə edir. Ənənəvi mərkəzləşdirilmiş sistemlər tək nöqtəli uğursuzluqlara və kiberhücumlara həssasdır. Blokçeynin paylanmış dəftər sistemi nəzarəti mərkəzsizləşdirir, zəiflikləri azaldır və elektrik şəbəkələri, su sistemləri və nəqliyyat şəbəkələri kimi əsas xidmətlərin dayanıqlığını artırır. Həmçinin, blokçeynlə işləyən şəxsiyyət idarəçiliyi vətəndaşın autentifikasiyasında və məlumatların məxfiliyində inqilab edə bilər. Kriptoqrafik üsullar və qeyri-mərkəzləşdirilmiş şəxsiyyət yoxlaması vasitəsilə fərdlər şəxsi

məlumatlarına nəzarəti davam etdirərkən xidmətlərə təhlükəsiz şəkildə daxil ola bilərlər. Bu təklif təkcə vətəndaş məlumatlarını qorumur, həm də şəxsiyyət oğurluğu və saxtakarlığı azaldır.

Blokçeyn texnologiyasının ayrılmaz tərəfi olan ağıllı müqavilələr müqavilələrin icrasında avtomatlaşdırma və şəffaflıq təklif edir. Ağıllı şəhər təhlükəsizlik protokollarında ağıllı müqavilələrin tətbiqi fövqəladə hallara cavab sistemlərini rasionallaşdıra, böhranlar zamanı resursların bölüşdürülməsini optimallaşdıra və idarəetmədə şəffaflığı təmin edə bilər. Bundan əlavə, bu müqavilələr təhlükəsizlik protokollarına uyğunluğu avtomatlaşdıra, insan səhvlərini azalda və ümumi sistemin səmərəliliyini artıra bilər.

Blokçeynin saxtakarlığa davamlı təbiəti, həmçinin məlumatların bütövlüyü və kibertəhlükəsizliyində inqilab edə bilər. Məlumatları blokçeynə lövbərləməklə, ağıllı şəhərlər icazəsiz girişin və ya manipulyasiyanın qarşısını alaraq həssas məlumatları qoruya bilər. Bu təklif Ağıllı şəhər əməliyyatları üçün mühüm əhəmiyyət kəsb edən bir-birinə bağlı cihazlar üçün etibarlı ekosistem yaratmaqla, IoT cihazlarının və şəbəkələrinin təhlükəsizliyini təmin edir.

Ağıllı şəhər mühitində müxtəlif sistemlər və maraqlı tərəflər arasında qarşılıqlı fəaliyyət mühüm əhəmiyyət kəsb edir. Blokçeynin təhlükəsiz, qarşılıqlı fəaliyyət göstərə bilən platformalar yaratmaq potensialı, vahid və təhlükəsiz infrastrukturu təmin edərək, müxtəlif şəhər komponentləri arasında problemsiz rabitə və məlumat mübadiləsini asanlaşdıra bilər.

Bununla belə, blokçeyn vəd versə də, problemlər davam edir. Ölçüləbilənlirlik, enerji istehlakı, tənzimləyici çərçivələr və inteqrasiya mürəkkəbliyi onun ağıllı şəhər təhlükəsizliyi üçün geniş şəkildə qəbul edilməsində maneələr yaradır. Bu çətinliklərin öhdəsindən gəlmək hökumətlərdən, sənayelərdən və texnoloji yenilikçilərdən ağıllı şəhər mühitləri üçün uyğunlaşdırılmış genişlənən, enerjiyə qənaət edən və qanunvericiliyə uyğun blokçeyn həlləri hazırlamaq üçün birgə səylər tələb edir.

Ölçüləbilənlirlik əhəmiyyətli bir problem olaraq qalır. Ağıllı şəhərlər mürəkkəblik və ölçü baxımından böyüdükcə blokçeyn şəbəkələrinin artan əməliyyat həcmlərini idarə etmək qabiliyyəti mühüm əhəmiyyət kəsb edir. Mövcud blokçeyn

arxitekturaları geniş miqyaslı şəhər mühitlərinin tələb etdiyi miqyasda mübarizə aparır. Bu məhdudiyyəti aradan qaldırmaq üçün parçalanma, 2-ci səviyyə protokolları və konsensus mexanizmlərində irəliləyişlər kimi həllər araşdırılır.

Enerji istehlakı başqa bir kritik problemdir. Proof of Work (PoW) kimi konsensus mexanizmləri üçün tələb olunan hesablama gücü ətraf mühitlə bağlı narahatlıqları artırır. Proof of Stake (PoS) və ya Proof of Authority (PoA) kimi daha enerjiyə qənaət edən konsensus modellərinə keçid ağıllı şəhərlərdə davamlı blokçeyn tətbiqi üçün vacib olur.

Tənzimləyici çərçivələr həm çətinliklər, həm də imkanlar yaradır. Blokçeyn texnologiyasını əhatə edən tənzimləyici mənzərə bütün dünyada fərqli mövqelərlə inkişaf edir. İnnovasiyaları təşviq etmək və mövcud qaydalara uyğunluğu təmin etmək arasında tarazlığın yaradılması çox vacibdir. Ağıllı şəhər blokçeyn tətbiqləri üçün xüsusi olaraq hazırlanmış tənzimləyici aydınlıq və çərçivələr geniş tətbiqi təşviq etmək üçün vacib olacaq.

Təhsil və maarifləndirmə blokçeyn texnologiyasının qəbul edilməsində və anlaşılmasında mühüm rol oynayır. Maraqlı tərəflər ağıllı şəhər təhlükəsizliyində blokçeyn tətbiqi ilə bağlı faydalar, risklər və ən yaxşı təcrübələr haqqında məlumatlandırılmalıdırlar. Təlim proqramları və seminarlar şəhər rəsmilərinə, tərtibatçılara və vətəndaşlara blokçeyn texnologiyasını effektiv şəkildə mənimsəmək imkanı verə bilər.

Aşağıdakı cədvəl ağıllı şəhər təhlükəsizliyini gücləndirmək üçün blokçeyn texnologiyasından istifadə edən əsas təklifləri əks etdirir:

Cədvəl 3.7 Ağıllı şəhərlərdə blokçeyn texnologiyalarının tətbiqi ilə əlaqəli təkliflər

Təklif	***Təsvir***
Mərkəzləşdirilməmiş İnfrastruktur Təhlükəsizliyi	Mərkəzləşdirilməmiş nəzarət vasitəsilə elektrik şəbəkələri, su sistemləri və nəqliyyat şəbəkələri kimi kritik infrastrukturun təhlükəsizliyini təmin etmək.
Blokçeyn Şəxsiyyət İdarəetməsi	Mərkəzləşdirilməmiş platformada kriptoqrafik şəxsiyyətin yoxlanılması vasitəsilə vətəndaşın autentifikasiyası və məlumat məxfiliyinin artırılması.

Ağıllı Müqavilə Avtomatlaşdırılması	Sadələşdirilmiş fövqəladə hallara cavab, resurs bölgüsü və şəffaf idarəetmə üçün razılaşmaların avtomatlaşdırılması.
Məlumatların bütövlüyü və kibertəhlükəsizlik	Məlumatların müdaxiləyə davamlı blokçeynlərə bərkidilməsi ilə həssas məlumatların və IoT cihazlarının təhlükəsizliyini təmin etmək.
Qarşılıqlı işləyə bilən həllər	Şəhər komponentləri arasında qüsursuz əlaqə və məlumat mübadiləsi üçün təhlükəsiz, qarşılıqlı fəaliyyət göstərən platformaların yaradılması.

Bu təkliflər blokçeyn texnologiyasının potensialından istifadə etməklə ağıllı şəhər təhlükəsizliyini gücləndirmək üçün əlverişli strategiyalar təqdim edir. Ölçüləbilənlirlik, enerji səmərəliliyi və normativlərə uyğunluq kimi problemlərin həlli bu təkliflərin effektiv şəkildə həyata keçirilməsində mühüm rol oynayacaqdır. Müxtəlif sektorlardan olan maraqlı tərəflərin birgə səyləri həyati əhəmiyyət kəsb edir. Hökumətlər, texnoloji şirkətlər, şəhər planlaşdırıcıları və kibertəhlükəsizlik mütəxəssisləri ağıllı şəhər təhlükəsizliyi üçün standartlaşdırılmış, qarşılıqlı fəaliyyət göstərə bilən blokçeyn həllərini layihələndirmək və həyata keçirmək üçün əməkdaşlıq etməlidirlər. Açıq mənbəli protokolların və çərçivələrin yaradılması təşəbbüsləri müxtəlif ağıllı şəhər komponentləri arasında uyğunluq və təhlükəsizliyi təmin etməklə əməkdaşlığı və yeniliyi təşviq edə bilər.

NƏTİCƏ

Təhlükəsiz ağıllı şəhərlərdə blokçeyn texnologiyalarından istifadənin tədqiqi innovasiya, təhlükəsizlik və səmərəliliyi birləşdirən çoxşaxəli mənzərə təqdim edir. Bu kəşfiyyat təbii olaraq təhlükəsiz, səmərəli və mərkəzləşdirilməmiş sistemləri inkişaf etdirmək üçün inkişaf etməkdə olan texnologiyaların və şəhər infrastrukturunun birləşməsini araşdırır. Blokçeyn və ağıllı şəhərlərin kəsişməsi idarəetmə, təhlükəsizlik və vətəndaşların cəlb edilməsi mənzərəsini yenidən formalaşdırarkən müxtəlif şəhər problemlərinin həlli üçün perspektivli çərçivə təklif edir. Blokçeynin ağıllı şəhərlərə inteqrasiyasının potensial tətbiqlərini, çətinliklərini və nəticələrini araşdıraraq, onun transformasiya potensialı və uğurlu tətbiqi üçün vacib olan mülahizələr haqqında hərtərəfli anlayış ortaya çıxır. Ağıllı şəhərlər kontekstində blokçeyn məlumatların, əməliyyatların və xidmətlərin idarə edilməsində inqilab edə bilər. Mərkəzləşdirilməmiş təbiəti sayəsində blokçeyn tək uğursuzluq nöqtələrini azaldır, kritik infrastrukturun və məlumatların saxlanmasının təhlükəsizliyini gücləndirir. Blokçeynin əsas xüsusiyyəti olan ağıllı müqavilələr, razılaşmaları avtomatlaşdırır və icra edir, prosesləri sadələşdirir və vasitəçiləri azaldır, beləliklə, ağıllı şəhərlərdə resursların bölüşdürülməsini optimallaşdırır və əməliyyat səmərəliliyini artırır.

Dissertasiyanın birinci fəsilində, ağıllı şəhərlərdə təhlükəsizlik problemləri və imkanlarını daha dərindən araşdırır, möhkəm və təhlükəsiz texnologiyalara ehtiyacı vurğulanır. Həmçinin blokçeyn texnologiyasının bu problemlərin həllində və ağıllı şəhərlərin inkişafına töhfə verməsində oynaya biləcəyi mühüm rolu vurğulanır.

Dissertasiyanın ikinci fəsilində, keçərək plan ağıllı şəhərlər kontekstində blokçeyn texnologiyalarının müxtəlif tətbiqlərini araşdırılır. Xüsusi olaraq məlumatların bütövlüyünü və məxfiliyini necə təmin edə biləcəyini araşdırılaraq, məlumat təhlükəsizliyində blokçeynin roluna diqqət yetirir. Bundan əlavə, plan blokçeynin ağıllı şəhərlərə gətirdiyi potensial imkanları, məsələn, tranzaksiyaların sadələşdirilməsi və şəffaflığın artırılmasını araşdırılır.

Dissertasiyanın üçüncü fəsilində, diqqəti ağıllı şəhər infrastrukturunda blokçeyn texnologiyalarının tətbiqinə yönəldir. Plan, ağıllı şəhərlərdə autentifikasiya və

avtorizasiya məqsədləri üçün blokçeynlərin necə istifadə oluna biləcəyini araşdırılır. Bundan əlavə, təhlükəsiz və etimada əsaslanan ağıllı şəhərlərin təmin edilməsinin vacib aspekti olan məxfiliyin qorunması üçün blokçeyn texnologiyasının potensialını araşdırılır. Bu fəsildə, ağıllı şəhər təhlükəsizliyini artırmaq üçün blokçeynlərin tətbiqi üçün düşündürücü təkliflərlə yekunlaşır. Ümumiyyətlə, bu plan təhlükəsiz ağıllı şəhərlər sahəsində blokçeyn texnologiyasının müxtəlif aspektlərinin hərtərəfli araşdırılmasını təmin edir. O, blokçeynin təhlükəsizlik problemlərini həll etmək və ağıllı şəhərlərin səmərəliliyini artırmaq üçün gətirdiyi böyük potensialı vurğulanır. İnformasiya təhlükəsizliyi, ağıllı şəhər infrastrukturu və məxfiliyin qorunması sahəsində blokçeyn tətbiqlərinin hərtərəfli təhlilini təqdim etməklə, bu plan təhlükəsiz və davamlı ağıllı şəhərlər üçün blokçeyn texnologiyasından istifadə etməkdə maraqlı olan tədqiqatçılar, siyasətçilər və sənaye mütəxəssisləri üçün dəyərli mənbə rolunu oynayır.

Bundan əlavə, blokçeynin ağıllı şəhərlərdə inteqrasiyası enerji, nəqliyyat, səhiyyə və idarəetmə də daxil olmaqla müxtəlif sektorları əhatə etmək üçün inzibati funksiyalardan kənara çıxır. Enerji idarəçiliyində blokçeyn həmyaşıdlar arası enerji ticarətini asanlaşdırır, bərpa olunan enerji təşəbbüslərini təşviq edərkən səmərəli paylama və istifadəyə imkan verir. Nəqliyyatda o, təhlükəsiz və şəffaf mobillik həllərinə imkan verir, marşrutları optimallaşdırır və müxtəlif nəqliyyat növləri arasında qarşılıqlı əlaqəni artırır. Həmçinin, blokçeynin səhiyyədəki rolu həssas xəstə məlumatlarının bütövlüyünü və təhlükəsizliyini təmin edir, səhiyyə təminatçıları arasında qarşılıqlı əlaqəni asanlaşdırır və səhiyyə xidmətlərini təkmilləşdirir.

Bununla belə, potensial faydalar arasında blokçeynin ağıllı şəhərlərdə inteqrasiyası nəzərə alınmalı olan bir sıra problemlərlə qarşılaşır. Blokçeyn şəbəkələrinin hesablama intensivliyi və saxlama tələbləri səbəbindən miqyaslılıq əhəmiyyətli bir narahatlıq olaraq qalır. Bundan əlavə, müxtəlif blokçeyn platformaları müstəqil fəaliyyət göstərdikcə sistemlər arasında problemsiz məlumat mübadiləsinə mane olan qarşılıqlı fəaliyyət problemləri yaranır. Bundan əlavə, tənzimləyici çərçivələr, məxfiliklə bağlı narahatlıqlar və maraqlı tərəflər arasında konsensusa ehtiyac geniş miqyasda qəbul edilməsinə əhəmiyyətli maneələr yaradır.

Təhlükəsiz ağıllı şəhərlərdə blokçeyn tətbiqinin nəticələri texnoloji irəliləyişləri üstələyir, sosial, iqtisadi və idarəetmə paradiqmalarına təsir göstərir. Blokçeyn tərəfindən dəstəklənən gücləndirilmiş şəffaflıq və hesabatlılıq vətəndaşların dövlət qurumlarına və idarəetmə sistemlərinə inamını artıra bilər. Qeyri-mərkəzləşdirmə güc dinamikasını dəyişdirərək, qərarların qəbulu proseslərində vətəndaşların daha çox iştirakını və inklüzivliyini təmin edir. İqtisadi baxımdan, blokçeynin səmərəliliyinin artırılması və xərclərin azaldılması həm dövlət, həm də özəl sektora fayda gətirərək, resurs bölgüsünü optimallaşdıra bilər.

Nəticə etibarilə, təhlükəsiz ağıllı şəhərlərdə blokçeyn texnologiyalarının tədqiqi böyük potensial və mürəkkəb problemlərlə xarakterizə olunan transformativ səyahəti əhatə edir. Onun inteqrasiyası təhlükəsizlik, səmərəlilik və vətəndaş mərkəzli xidmətləri gücləndirərək şəhər sistemlərində inqilab etmək qabiliyyətinə malikdir. Bununla belə, uğurlu icra texniki, tənzimləyici və ictimai mülahizələri nəzərə alan vahid yanaşma tələb edir. Siyasətçilər, texnoloqlar və vətəndaşlar arasında birgə səylər, təhlükəsiz, səmərəli və inklüziv şəhərlərin qurulmasında blokçeynin tam potensialından istifadə etmək üçün mütləqdir.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISI

1. “Ağıllı şəhər” (Smart City) və “Ağıllı kənd” (Smart Village) konsepsiyasının hazırlanması haqqında Azərbaycan Respublikası Prezidentinin Sərəncamı, 2021.
2. “Azərbaycan Respublikasının işğaldan azad edilmiş ərazilərinə Böyük Qayıdışa dair I Dövlət Proqramı”nın təsdiq edilməsi haqqında Azərbaycan Respublikası Prezidentinin Sərəncamı, 2021.
3. Qasımlı V., Hüseyn R., Hüseynov R., Həsənov R., Cəfərov C., Bayramova A., “Yaşıl İqtisadiyyat”. Azərbaycan Respublikası İqtisadi İslahatların Təhlili və Kommunikasiya Mərkəzi, 2022.
4. İmamverdiyev Y. “Big Data və fərdi məlumatların təhlükəsizliyi,” “Big data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı, pp. 109-113, 2016.
5. Duman, B., & Özsoy, K., Endüstri 4.0 Perspektifinde Akıllı Tarım. 4th International Congress on 3D Printing (Additive Manufacturing) Technologies and Digital Industry, 11-14 April 2019, 540-555, Antalya.
6. Gülseçen S., Özdemir Ş., Çelik S., Uğraş T. & Özcan M., Dijital Dünyadan Yansımalar Bilgide ve Vatandaşlıkta Değişim, XVIII. Türkiye’de İnternet Konferansı Bildiri Kitapçığı, 223-227, 2013.
7. Örselli, E. & Dinçer, S., Akıllı Kentleri Anlamak: Konya ve Barcelona Üzerinden Bir Değerlendirme. Uluslararası Yönetim Akademisi Dergisi., 2019, 2(1), 90-110. DOI: 10.33712/mana.547086
8. Gönen, E., İnternetin Yeni Çağı: Blockchain, Fintechtime, 2018, Sayı 8, s.36-71.
9. Tekin Bilbil, E., Yerel Yönetimler ve Blokzincir Teknolojisi: Bir Yönetişim Tasarısı/Stratejisi Önerisi, Kent Akademisi, Volume, 2019, 12 (39), Issue 3, Pages, 475-487.
10. Yıldırım, H., Açık ve Uzaktan Öğrenmede Blokzincir Teknolojisinin Kullanımı. Açıköğretim Uygulamaları ve Araştırmaları Dergisi (AUAd), 2018, 4(3), 142-153.

11. Karaköse, İmparator S. Erciyes Üniversitesi, S.B.E. Yayımlanmamış Y.L. Tezi, Elektronik Ödemelerde Blok Zinciri Sistematiği ve Uygulamaları. Kayseri: Erciyes, 2017.
12. Makrushin D. and Dashchenko V., Fooling the 'Smart City', Technical Report, Kaspersky Lab, pp. 1-22, Sep. 2016.
13. Claycomb W. R. and Nicoll A., Insider Threats to Cloud Computing: Directions for New Research Challenges, in 36th Annual Computer Soft. and Appl. Conf., pp. 387-394, 2012.
14. Christidis K. and Devetsikiotis M., Blockchains and Smart Contracts for the IoTs, IEEE Access, Special section on the plethora of Research in IoT, pp. 2292-2303, 2016.
15. Jindal, A.; Kumar, N.; Singh, M. A unified framework for big data acquisition, storage, and analytics for demand response management in smart cities. Future Gener. Comput. Syst. 2020, 108, 921-934.
16. Lu, H.-P.; Chen, C.-S.; Yu, H. Technology roadmap for building a smart city: An exploring study on methodology. Future Gener. Comput. Syst. 2019, 97, 727-742.
17. Hassani, H.; Huang, X.; Silva, E.S. Fusing Big Data, Blockchain and Cryptocurrency: Their Individual and Combined Importance in the Digital Economy; Palgrave Pivot: London, UK, 2019; ISBN 978-3-030-31390-6.
18. Chourabi, H.; Nam, T.; Walker, S.; Gil-Garcia, J.R.; Mellouli, S.; Nahon, K.; Pardo, T.A.; Scholl, H.J. Understanding smart cities: An integrative framework. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4-7 January 2012; pp. 2289-2297.
19. Carli, R.; Dotoli, M.; Pellegrino, R.; Ranieri, L. Measuring and managing the smartness of cities: A framework for classifying performance indicators. In Proceedings of the 2013 IEEE International Conference on Systems, Man, and Cybernetics, Manchester, UK, 13-16 October 2013; pp. 1288-1293.
20. Treiblmaier, H. Combining blockchain technology and the physical internet to achieve triple bottom line sustainability: A comprehensive research agenda for modern logistics and supply chain management. Logistics 2019, 3, 10.

21. Salah, K.; Rehman, M.H.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and open research challenges. IEEE Access 2019, 7, 10127-10149.
22. Saghiri A.M., Blockchain Architecture. In: Kim S., Deka G. (eds) Advanced Applications of Blockchain Technology. Studies in Big Data, vol 60. Springer, 2020, Singapore. https://doi.org/10.1007/978-981-13-8775-3_8
23. Zamfiroiu, Alin., Rotuna, Carmen., et al., Smart City Ecosystem Using Blockchain Technology. Informatica Economica, 23(4), 41-50, 2019.
24. Shwe, H.Y., Jet, T.K., Chong, P.H.J.: An IoT-oriented data storage framework in smart city applications. In: 2016 International Conference on Information and Communication Technology Convergence (ICTC), pp. 106-8, 2016.
25. Fanning, K., Centers, D.P.: Blockchain and its coming impact on financial services. J. Corp. Account. Finance 27(5), 53-57, 2016.
26. Chourabi, H., et al.: Understanding smart cities: an integrative framework. In: 2012 45th Hawaii International Conference on System Sciences, pp. 2289-97. IEEE, 2012.
27. Toh, C.K.: Security for smart cities. IET Smart Cities 2(2), 95-104, 2020.
28. Chen, D., Wawrzynski, P., Lv, Z.: Cyber security in smart cities: a review of deep learning-based applications and case studies. Sustain. Cities Soc. 66, 102655. Elsevier, 2021.
29. Zheng, D., et al.: Smart grid power trading based on consortium blockchain in Internet of Things. In: International Conference on Algorithms and Architectures for Parallel Processing, pp. 453-459. Springer, Cham, 2018.
30. Wan, J., et al.: A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Trans. Ind. Inf. 15(6), 3652-3660, 2019.
31. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J., “Blockchain contract: Securing a blockchain applied to smart contracts”, in 2016 IEEE International Conference in Consumer Electronics (ICCE), pp. 467-468.
32. Guo, M., Liu, Y., Yu, H., Hu, B., Sang, Z., “An overview of smart city in China”, China Communications, 2016, vol.13, issue.5.

33. Christidis K. and Devetsikiotis M., “Blockchains and Smart Contracts for the IoTs”, IEEE Access, Special section on the plethora of Research in IoT, 2016, pp. 2292-2303.
34. Lombardi P., Giordano S., Farouh H., and Yousef W., “Modelling the Smart City Performance”, Innovation: The European Journal of Social Science Research25: 2, 2019, 137 - 149.
35. Gori P, Parcu PL, Stasi ML, Smart Cities and Sharing Economy, vol 96, Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS, 2015.
36. Dobrovnik, M.; Herold, D.M.; Fürst, E.; Kummer, S. Blockchain for and in Logistics: What to Adopt and Where to Start. Logistics 2018, 2, 18.
37. Orecchini F, Santiangeli A, Zuccari F, Pieroni A and Suppa T, Blockchain Technology in Smart City: A New Opportunity for Smart Environment and Smart Mobility. Int. Conf. on Intelligent Computing & Optimization (Springer, Cham) pp 346-354, 2018.
38. Karmakar A and Sahib U, Smart Dubai: Accelerating Innovation and Leapfrogging EDemocracy: In E-Democracy for Smart Cities, 2017. (Singapore: Springer pp 197-257)
39. Pieroni A, Scarpato N, Di Nunzio L, Fallucchi F and Raso M, Smarter city: smart energy grid based on blockchain technology. Int J Adv Sci Eng Inf Technol 8 (1) 298-306, 2018.
40. Грингард Сэмюэл. Интернет вещей: Будущее уже здесь. - М.: Альпина Диджитал, 2015. - 426 с.
41. Изделия и услуги, интегрирующие информационные технологии и Интернет вещей. Дартмут: Центр цифровых стратегий при Бизнес-школе Така в Дартмуте, 2014.
42. Кириллова Е.А., Павлюк А.В. Гражданско-правовые аспекты оптимизации трансграничного наследования бизнеса // Проблемы экономики и юридической практики. 2017. № 6. С. 135-140.
43. Шваб К. Четвертая промышленная революция. М.: Эксмо, 2016. 208 с.

EXPLORİNG THE USE OF BLOCKCHAİN TECHNOLOGİES İN SECURE SMART CİTİES

SUMMARY

Relevance of the study. The study addresses the pressing need for secure infrastructure in smart cities by exploring how blockchain's decentralized, immutable nature can significantly enhance security measures.

Research goals and objectives. This research aims to assess the viability of integrating blockchain technology into smart city frameworks to bolster security measures. Objectives include analyzing existing implementations, identifying challenges, and proposing effective integration strategies.

Used research methods. Employing a mixed-methods approach, the study will leverage qualitative methods like literature review and case studies, alongside quantitative methods such as data analysis and surveys.

Research database. Utilizing a diverse database comprising scholarly articles, case studies of smart city projects, technical documentation on blockchain platforms, and relevant statistical data will inform the research.

Limitations of the study. Limitations may arise due to the dynamic nature of technology, potential biases in case study selection, and constraints related to accessing real-time data from ongoing smart city initiatives.

Results of the study. Anticipated outcomes include an in-depth understanding of the benefits and challenges of implementing blockchain in smart cities, along with proposed frameworks or recommendations to enhance security while integrating this technology.

Keywords: Blockchain, Smart Cities, Security, Decentralization, Integration, Viability, Challenges, Strategies.

ИЗУЧЕНИЕ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ БЛОКЧЕЙН В БЕЗОПАСНЫХ УМНЫХ ГОРОДАХ

РЕЗЮМЕ

Актуальность исследования. В исследовании рассматривается острая потребность в безопасной инфраструктуре в умных городах, изучая, как децентрализованный, неизменный характер блокчейна может значительно повысить меры безопасности.

Цели и задачи исследования. Это исследование направлено на оценку жизнеспособности интеграции технологии блокчейн в структуру умного города для усиления мер безопасности. В задачи входит анализ существующих реализаций, выявление проблем и предложение эффективных стратегий интеграции.

Использованные методы исследования. Используя смешанный подход, исследование будет использовать качественные методы, такие как обзор литературы и тематические исследования, наряду с количественными методами, такими как анализ данных и опросы.

База данных исследований. Для исследования будет использована разнообразная база данных, включающая научные статьи, тематические исследования проектов «умного города», техническую документацию по платформам блокчейна и соответствующие статистические данные.

Ограничения исследования. Ограничения могут возникнуть из-за динамического характера технологий, потенциальных ошибок при выборе тематических исследований и ограничений, связанных с доступом к данным в реальном времени из текущих инициатив «умного города».

Результаты исследования. Ожидаемые результаты включают глубокое понимание преимуществ и проблем внедрения блокчейна в умных городах, а также предлагаемые структуры или рекомендации по повышению безопасности при интеграции этой технологии.

Ключевые слова: блокчейн, умные города, безопасность, децентрализация, интеграция, жизнеспособность, проблемы, стратегии.

ABREVİATURALAR LİSTİ

ABS	Təmin Edilmiş Qiymətli Kağızlar
ACL	Girişə Nəzarət Siyahısı
APG və PGGM	Bütün Pensiya Qrupu
CDN	Məzmun Çatdırılma Şəbəkəsi
CDS	Qiymətli Kağızlar üçün Ənənəvi Kanada Depozitarisi
DApps	Mərkəzləşdirilməmiş Tətbiqlər
DLT	Paylanmış Kitab Texnologiyası
DPoS	Əməliyyatların işlənməsi və blokçeynində yeni blokların yaradılması üçün kriptovalyuta konsensus mexanizmi
EBSI	Avropa Blokçeyn Xidmət İnfrastrukturu
EBSI	Avropa Blokçeyn Xidmətləri
EDC	Kənar Məlumat Mərkəzləri
GPU	Qrafik Emalı Birlikləri
H_CPS	Səhiyyə Kiber Fiziki Sistemi
HIPPA	Sağlamlıq Sığortasının Daşınması və Hesabatlılığı Aktı
IDS	Ənənəvi Müdaxilənin Aşkarlanması Sistemi
IoT	Əşyaların İnterneti
IPFS	Planetlərarası Fayl Sistemi
ISGF	Hindistan Ağıllı Şəbəkə Forumu
ITS	Ağıllı Nəqliyyat Sistemi
İKT	İnformasiya və Kommunikasiya Texnologiyaları
KSI	Açarsız İmza İnfrastruktur
NAPR	Gürcüstan Respublikasının Dövlət Reyestrinin Milli Agentliyi
NFTs	Qeyri İşlənə Bilən Tokenlər
NIC	Şəbəkə İnterfeys Kartı

PoA	İş sübutu (PoW) və Stake sübutu (PoS) mexanizmini birləşdirir
PoET	Şəbəkədə blokçeyn hüquqları və ya blok qalibləri haqqında qərar vermək üçün icazəli blokçeyn şəbəkələrində tez istifadə olunan konsensus mexanizmi
PoS	Stake Sübutu
PoW	İş Sübutu
SBC	Bir Lövhəli Kompüterlər
SGX	Proqram Təminatının Mühafizəsi Uzantıları
SPoF	Vahid Uğursuzluq Nöqtəsi
SSI	Özü Müstəqil Şəxsiyyət
TEE	Etibarlı İcra Mühiti
UNEP	BMT'nin Ətraf Mühit Proqramı
VR	Virtual Reallıq
WWF	Ümumdünya Vəhşi Təbiət Fondu