BLOKÇEYN TEXNOLOGİYALARI

–MÜHAZİRƏLƏR–

İMAMVERDİYEV Y.N.

BAKI – 2025

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ
KİBERTƏHLÜKƏSİZLİK KAFEDRASI

Yadigar İmamverdiyev

BLOKÇEYN TEXNOLOGİYALARI
MÜHAZİRƏLƏR

BAKI – 2025

İmamverdiyev Y.N. «Blokçeyn texnologiyaları – mühazirələr»,
Bakı: AzTU nəşriyyatı, 2025, 124 s.

Kitabda kriptovalyuta və blokçeyn texnologiyalarının elmi-texniki məsələləri mühazirələr şəklində sistematik şərh olunur. Blokçeyn ekosisteminin əsas komponentləri, konsensus mexanizmləri, kriptoqrafik alqoritmlər və protokollar, rəqəmsal tokenlər və DeFi, ağıllı müqavilələr, NFT və Web3, blokçeynlərdə miqyaslanma və təhlükəsizlik problemləri əhatə olunur. Hər mühazirənin sonunda öyrənilən materialı möhkəmləndirmək üçün yoxlama sualları verilir.

Vəsait blokçeyn texnologiyalarının tətbiqi, tədqiqi və yaradılması sahəsində ixtisaslaşan tələbələr və mühəndislər üçün nəzərdə tutulmuşdur.

Üz qabığının dizaynı: Ayşən Qasımova (Qrup 641a1)

Mündəricat

Giriş

Təqdim olunan vəsait dünyada və ölkəmizdə böyük maraq doğuran kriptovalyuta və blokçeyn texnologiyalarına həsr olunub.

Blokçeyn texnologiyaları son onillikdə rəqəmsal transformasiyanın əsas sütunlarından birinə çevrilib. Əvvəlcə kriptovalyutalarla (xüsusilə Bitcoin) əlaqəli bir konsepsiya kimi meydana çıxsa da, bu texnologiya zamanla maliyyə, təchizat zənciri, səhiyyə, təhsil və dövlət xidmətləri kimi bir çox sektorda tətbiq imkanlarını nümayiş etdirib. Blokçeyn əsaslı sistemlərin təməlində şəffaflıq, dəyişilməzlik və mərkəziyətsizlik kimi prinsiplər dayanır ki, bu da onu verilənləri ənənəvi idarəetmə yanaşmalarından fərqləndirir.

Bu vəsait, SABAH-Kibertəhlükəsizlik ixtisaslaşmasında təhsil alan magistratura tələbələrinə 2023-cü ilin yaz semestrində oxunan mühazirələr əsasında hazırlanıb. Vəsaitin əsas məqsədi tələbələrə və tədqiqatçılara bu sahəyə dair sistemli biliklər vermək, texnologiyanın işləmə prinsiplərini, əsas komponentlərini və gələcək inkişaf potensialını aydın şəkildə izah etməkdir.

Qeyd edək ki, ölkəmizdə blokçeyn və kriptovalyutalar sahəsində 2017-ci ildən başlayaraq müxtəlif təşəbbüslər olub. Məlumata görə, ölkədə kriptovalyuta istifadəçilərinin sayı 120 min nəfərə çatıb və kriptovalyuta əməliyyatlarının həcmi 2023-cü ildə 4,4 milyard dollar olub. 2025-ci ilin yanvarında "Mobile Payment Solutions" MMC şirkəti (Portmanat brendi) “PortCoin” adlı kriptovalyuta yaratdığını açıqlayıb. 2025-ci ildə kriptovalyutalar və rəqəmsal aktivlər sahəsində tənzimlənmə mexanizmlərinin formalaşdırılması gözlənilir.

Rəqəmsal dünyada etibarlı, şəffaf və avtomatlaşdırılmış sistemlərə olan tələbat artdıqca, blokçeyn texnologiyaları da gündəlik həyatın ayrılmaz bir hissəsinə çevrilir. Ümid edirik ki, bu vəsait tələbələrə həm texnologiyanı öyrənməkdə, həm də gələcəkdə bu sahədə ixtisaslaşmaq üçün yaxşı bir təməl yaradacaq.

Mühazirə 1. Blokçeyn texnologiyalarına giriş

1.1. Blokçeyn anlayışı

Bitkoin blokçeyn (ing. blockchain) texnologiyası ilə işləyən ilk kriptovalyutadır və hazırda kriptovalyuta bazarının xeyli hissəsini tutur. Blokçeyn anlayışı da Bitkoin ilə əlaqədar meydana çıxıb.

Hər bir elektron ödəniş sistemi tranzaksiyaları haradasa saxlamalıdır. Bitkoində bütün informasiya bloklar zəncirində – blokçeyndə saxlanır.

Vikipediya blokçeyni tranzaksiyalar bloklarının zənciri kimi müəyyən edir. Lakin bu tərif Bitkoinin əsaslandığı bu texnologiyanın bütün mahiyyətini açmır.

Hər şeydən əvvəl, blokçeyn – paylanmış verilənlər bazasıdır, onun tam surətləri birranqlı şəbəkədə birləşmiş kompüterlərin (serverlərin) hər birində yerləşir.

Bu tərifə görə, blokçeyn tək bir kompüterdə mövcud ola bilməz.

P2P (peer-to-peer) şəbəkə adlandırılan birranqlı şəbəkə o deməkdir ki, ona birləşən bütün kompüterlər eyni hüquqa malikdirlər və mərkəzi (idarə edən) server yoxdur.

Buradan nəticə çıxarmaq olar ki, blokçeyn verilənlərin saxlanmasının mərkəzi olmayan sistemidir.

Verilənlərin təşkili texnologiyası kimi blokçeyn informasiyanın təhlükəsiz və tamlıqda saxlanmasını təmin edir. Yəni blokçeynə yazılmış tranzaksiyalarda hər hansı dəyişiklik etmək mümkün deyil – onları nə silmək, nə də düzəliş etmək mümkün olmur.

Bu çox vacib xassədir. Çünki, tranzaksiyalar maliyyə əməliyyatlarıdır və vahid etibarlı mərkəz (bank) yoxdur ki, bu tranzaksiyaların dəyişməzliyinə nəzarət etsin.

Bəs buna blokçeyndə necə nail olunur?

Blokçeynə bütün informasiya bloklar şəklində yazılır və bloklar öz aralarında blok başlığındakı heş qiyməti ilə "zəncirlənir".

Heş qiymət (heş-kod) *kriptoqrafik heş funksiyaların köməyi ilə hesablanır* və məlumatın tamlığına nəzarət etmək üçün istifadə edilir. Adətən, heş-funksiya müəyyən alqoritm şəklində reallaşdırılır və bu alqoritm ixtiyari uzunluqda məlumat üçün uzunluğu sabit olan *heş-kod* hesablayır. Heş-funksiyanın xassələri elədir ki, onun köməyi ilə alınan heş-kod məlumatla "möhkəm" bağlı olur. Məlumatın hətta bir bitini dəyişdikdə belə, heş-kodun bitlərinin ən azı yarısı dəyişir.

Bu dəyişiklik dərhal avtomatik aşkarlanır, çünki blokçeynin surətləri blokçeyn şəbəkəsindəki komputerlərin hər birində saxlanır.

Beləliklə, blokçeyn verilənlərin təşkilinin və saxlanmasının mərkəzi olmayan və kriptoqrafiyaya əsaslanan etibarlı üsuludur. Bundan əlavə, o bir-birinə inanmayan bütün iştirakçılar arasında konsensus əldə etməyə imkan verir.

1.2. Blokçeyn arxitekturasının əsas komponentləri

Blokçeyn arxitekturasının əsas komponentləri aşağıda qısa təsvir olunur.

Tranzaksiya (TX). Blokçeynin vəziyyətinin dəyişməsi ilə nəticələnən prosesdir. Blokçeyn platformasından asılı olaraq, tranzaksiya maliyyə dəyərinin transferi və ya ağıllı müqavilələr kimi ixtiyarı kodun yerinə yetirilməsi ola bilər.

Blok. Yaxın keçmişdə baş vermiş və hələlik təsdiqlənməmiş tranzaksiyaların çoxluğudur.

Hər bir blokda başlıq və tranzaksiyaların siyahısı olur. Başlıqda bir neçə məlumat, o cümlədən blokun sıra nömrəsi, başlığın heşi və əvvəlki blokun heşi olur. Bloklar JSON formatında ötürülür. Bitkoin blokunun strukturu barədə növbəti mühazirədə ətraflı məlumat veriləcək.

Blokçeyn. Bütün tranzaksiyaların/blokların saxlandığı paylanmış reyestrdir (verilənlər strukturudur).

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

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

Tam qovşaq. Bu qovşaqlar blokçeynin tam surətini saxlayırlar, lakin bloku mayninq etmirlər. Tam qovşaqlar tranzaksiyaları müvafiq blokçeynin konsensus qaydalarına görə validasiya edirlər, blokun qəbul və ya fork edilməsinə kömək edirlər. Bu, tam qovşaqların tranzaksiya və blok yaymaq imkanlarının olduğunu

nəzərdə tutur. Buna görə də, tam qovşaqlar blokçeynin təhlükəsizliyi üçün çox vacibdirlər.

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

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

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

1.3. Blokçeyn arxitekturasının modelləri

Blokçeynin müxtəlif arxitektura modelləri var. Ən sadə yanaşmada arxitektura adətən üç qatdan ibarətdir: 1) Konsensus qatı; 2) Verilənlər qatı; 3) Tətbiq qatı. Bu qatların funksiyalarını belədir:

1) **Konsensus qatı:** konsensus mexanizminin işlədiyi və tranzaksiyaların yoxlanıldığı qatdır. Bu qat şəbəkənin təhlükəsizliyini təmin etmək üçün çox vacibdir.
2) **Verilənlər qatı:** tranzaksiya, blok və ağıllı müqavilə məlumatlarının blokçeyn şəbəkəsi üzərindən əlçatan olmasını və yoxlanılmasını təmin edən qatdır.
3) **Tətbiq qatı:** Ağıllı müqavilələrin və blokçeyn tətbiqlərinin icrasını təmin edən qatdır; İstifadəçilərə ağıllı müqavilələr və mərkəziyətsiz tətbiqlərlə qarşılıqlı əlaqə qura biləcəkləri interfeys təqdim edir.

Blokçeyn şəbəkəsinin infrastruktur qatlarını təsvir edən **L0, L1, L2 və L3** modeli daha geniş yayılıb. Bu qatlar fərqli funksiyaları yerinə yetirir və şəbəkənin

miqyaslanma**,** təhlükəsizlik**,** emal sürəti və istifadəçi təcrübəsi kimi əsas məsələlərini həll etmək üçün nəzərdə tutulub.

Layer 0 (L0) – əsas infrastruktur qatı. Müxtəlif blokçeyn şəbəkələrini və ya L1-ləri birləşdirən və əlaqələndirən şəbəkə infrastrukturu və protokol qatıdır. Vəzifəsi qovşaqlar arasında rabitəni və məlumat ötürülməsini təşkil etmək, fərqli L1-lərin əlaqəsini təmin etmək, multizəncir sistemlər yaratmaqdır.

Layer 1 (L1) – əsas blokçeyn qatı. Əsas blokçeyn infrastrukturudur – Konsensus, ağıllı müqavilələrin icrası, tranzaksiyaların emalı və təhlükəsizlik bu qatda təmin olunur. Bitcoin, Ethereum, Solana, BNB Chain

Layer 2 (L2) – miqyaslama həlləri qatı. Layer 1 şəbəkəsinin yüklənməsini azaltmaq üçün onun üzərində qurulmuş texnologiyalardır. Əsas vəzifəsi daha sürətli və ucuz tranzaksiyalar aparmaq, əsas şəbəkəyə əlavə yük yükləmədən funksionallığı artırmaqdır. Bu qatda olan texnologiyalara nümunə kimi Rollup-lar (Optimistik və ZK-Rollup-lar), Plasma, Validium göstərmək olar.

Layer 3 (L3) – tətbiq və inteqrasiya qatı. Layer 2 üzərində çalışan, istifadəçi yönümlü tətbiqləri və protokolları əhatə edən qatdır. DeFi, NFT, oyunlar, sosial tətbiqlər kimi spesifik xidmətləri təklif edə bilər. Bəzən interoperabilik və xidmət yönümlü middleware-lər də bura daxil edilir.

1.4. Blokçeynin növləri

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

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

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

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

- *açıq blokçeyn* (ing. public blockchain) – tamamilə açıq blokçeyndir, tranzaksiyalar azad şəkildə həyata keçirilir və onlara heç kim nəzarət etmir, hər bir kəs konsensus prosedurunda iştirak edə bilər;

- *konsorsium blokçeyni* (ing. consortium blockchains) – konsensus proseduruna seçilmiş qovşaqlar nəzarət edir;
- *özəl blokçeyn* (ing. fully private blockchain) – mərkəzi orqan bütün tranzaksiyaları izləyir və nəzarət edir.

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

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

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

1.5. Kriptobirjalar

Kriptovalyuta infrastrukturunun əsas komponentlərindən biri də kriptovalyuta birjalarıdır (kriptobirjalardır). Kriptobirjanın qiyməti əsasən tələb və təklif amili ilə müəyyən olunur. Bitkoinə tələbin artması ilə paralel olaraq 2011-ci ildə onların mübadiləsi üçün onlayn birjalar yaranmağa başladı. Bu birjalar xüsusiyyətinə görə əsasən 2 yerə bölünür:

1) Kriptovalyutanın real valyutaya mübadilə edildiyi birjalar;

2) Kriptovalyutaların digər kriptovalyutalara mübadilə edildiyi birjalar.

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

Hazırda kriptovalyutaların alqı-satqısı ilə məşğul olan yüzlərlə kirptovalyuta birjası mövcuddur, onlardan populyarlığına və dövriyyəsinə görə ən məşhurları: Binance (Şanxay), Bitfinex (Honkonq), Coinbase, Livecoin, Poloniex, Btc-e, Bittrex, BtcChina, Kraken və s.

Mərkəziyətsiz birjalar. Mərkəziyətsiz birjalar (DEX, decentralized exchange) – paylanmış reyestr əsasında işləyən, öz serverlərində istifadəçilərin vəsaitlərini və fərdi məlumatlarını saxlamayan və yalnız istifadəçilərin aktivlərin alqı və ya satqısı sifarişləri üzrə axtraış platforması kimi çıxış edən birjadır. Belə platformalarda alqı-satqı iştirakçılar arasında hər hansı maliyyə vasitəçisi olmadan birbaşa (peer-to-peer) baş verir.

Lakin hazırda özlərini mərkəziyətsiz adlandıran birjaların əksəriyyəti yuxarıdakı tərifi tam ödəmir: istifadəçilərin aktivlərin alqı və ya satqı sifarişləri və satışlar barəsində verilənləri saxlamaq üçün onlar öz serverlərindən istifadə edirlər, lakin bu zaman gizli açarlar istifadəçinin özündə saxlanır.

Hazırda tam işləyən 200-dən çox mərkəziyətsiz birja var, onlardan bəziləri aşağıda göstərilir:

- IDEX – Ethereum-da mərkəziyətsiz birja, alqı-satqı real zamanda edilə bilər və birbaşa aparat pulqabından alqı-satqı imkanı vardır;
- Waves Dex – çoxplatformalı mərkəziyətsiz birjadır (Waves layihəsi), kriptovalyutaları fiat pullara dəyişmək imkanı var. Layihənin nümayəndələri iddia edirlər ki, bu platformadakı alqı-satqının həcmi bütün mərkəziyətsiz birjalardakı ticarətin ümumi həcminin 25 %-ni təşkil edir;
- Bancor Network – avtomatik qiymət yaranması olan mərkəziyətsiz birja;
- Switcheo Network – NEO blokçeyni əsasında mərkəziyətsiz multiçeyn birja.

Özünü yoxlamaq üçün suallar

1. Blokçeyn nədir?
2. Birranqlı şəbəkə nədir?
3. Blokçeyndə bloklar nəyin vasitəsilə zəncirlənir?
4. Blokçeyndə hansı kriptoqrafik vasitə istifadə edilir?
5. Blokçeyndə blok anlayışını izah edin.
6. Tranzaksiya nədir?
7. Mayninq nədir?
8. Tam qovşaq nədir?
9. Sadə qovşaq nədir?
10. Bitkoin blokçeynində blokun yekun təsdiqi necə həyata keçirilir?

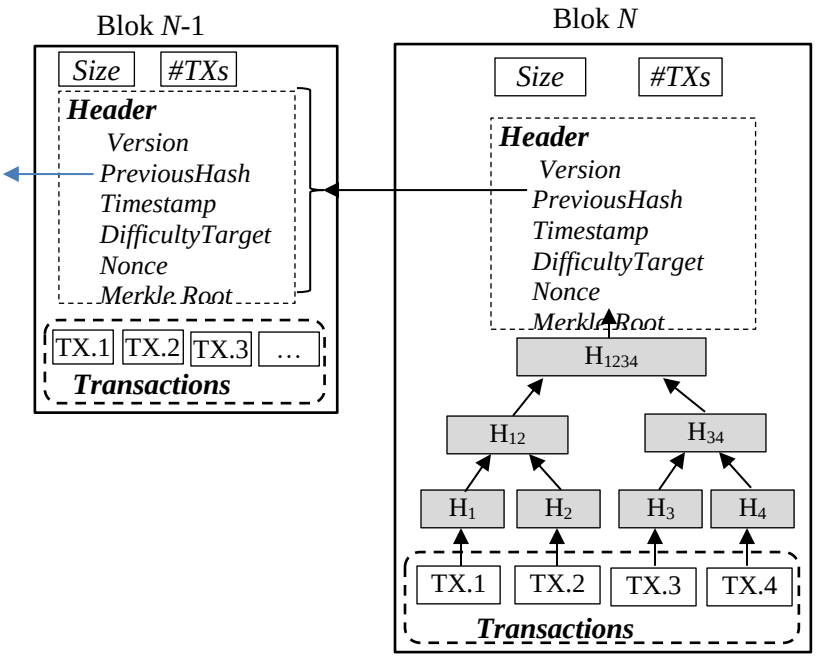
11. Konsesnsus protokolu nədir?
12. Blokçeynin hansı növləri var?
13. Ekskluziv blokçeyn nədir?
14. İnkluziv blokçeyn nədir?
15. Hibrid blokçeyn nədir?
16. Hibrid blokçeynin əsas xüsusiyyətləri nələrdir?
17. Mərkəziyətsiz birjalar nədir?
18. Kriptobirjaların xüsusiyyətləri hansılardır?

Mühazirə 2. Bitkoin blokçeyni

2.1. Bitcoin blokçeyninin strukturu

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

- *Version* – versiya nömrəsi (konsensus protokolunun yenilənməsini izləmək üçün istifadə edilir);
- *PreviousHash* – zəncirdə bilavasitə əvvəl gələn blokun heşi;
- *Timestamp* – blokun yaradılması tarixi;
- *Difficulty Target* – hədəf qiyməti, mayninq prosesində bu qiymətdən kiçik olan heş axtarılır;
- *Nonce* – mayninq alqoritmində istifadə edilən sayğac; (Kriptoqrafiyada nonce – “number used once” baxılan kontekstdə yalnız bir dəfə istifadə edilən ədədi bildirir.)
- *Merkle Root* – bloka daxil olan bütün tranzaksiyaların heşləri əsasında yaradılan binar ağacdır.



Şəkil 1. Bitcoin blokçeyninin strukturu

Bitkoin blokunun strukturu. Bitkoin protokolunun spesifikasiyasında blokun strukturu aşağıdakı cədvəldəki kimi müəyyən edilir (Yuxarıdakı şəkildə bits əvəzinə *DifficultyTarget* göstərilib.)

Ölçüsü (baytla)	Verilənlərin adı	Tipi	İzahı
4	version	int32_t	Blokun versiyası
32	*prev_block*	char[32]	Əvvəlki blokun heşi
32	*merkle_root*	char[32]	Blokdakı tranzaksiyaların heşlərindən hesablanmış Merkl kökü
4	timestamp	uint32_t	Blokun yaradılması zamanı və tarixinin UNIX zaman nişanı
4	*bits*	uint32_t	Blok üçün istifadə edilən çətinlik hədəfi (*Difficulty Target*)
4	*nonce*	uint32_t	Blokun generasiyasında istifadə edilən təsadüfi ədəd
?	*txn_count*	var_int	Blokdakı tranzaksiyaların sayı
?	*txns*	tx[]	Blokdakı tranzaksiyaların "tx" komandası şəklində siyahısı

İlk altı parametr (*txn_count* və *txns*-dən başqa hamısı) blokun başlığını əmələ gətirir. Məhz başlığın heşinə *blokun heşi* deyilir, yəni tranzaksiyaların özləri blokun heşinin hesablanmasında bilavasitə iştirak etmirlər. Bunun əvəzində onları xüsusi struktura – *Merkl ağacına* daxil edirlər.

Əslində, *bits* parametrində iki ədəd yazılır: birinci bayt **exponent**, qalan 3 bayt **mantissa** adlanır.

Bits parametrindən Target aşağıdakı düsturla alınır:

$$Target = mantissa * 2\text{^}(8 * exponent - 3).$$

2.2. Bitkoin tranzaksiyaları

Öz mahiyyətinə görə, blokçeyn əsaslı kriptovalyutalar rəqəmsal imzaların zəncirindən ibarətdir və pul vəsaitlərinin sistemdə yolunu əks etdirir. Bu kontekstdə əsas anlayış tranzaksiyadır. Faktiki olaraq, tranzaksiya – blokun ünvanı olan minimal elementidir, blok isə öz növbəsində blokçeynin ünvanlı elementidir (ing. transaction, lat. transactio – müqavilə, razılaşma).

Tranzaksiyaların iki növü var:

- "Standart" tranzaksiyalar – sistemin istifadəçilərindən vəsaitlərin ötürülməsini kodlaşdırır,
- "Generasiya edən" tranzaksiyalar blokun generasiyası üçün mükafat olaraq mədənçiyə yeni hasil edilmiş bitkoinlər verilir.

Tranzaksiyaların strukturu. Şərti olaraq, tranzaksiyada iki sahə var – Input və Output. Əyanilik üçün şəkil 3-də göstərilmiş misala baxaq.

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

Şəkil 3. Bitkoin şəbəkəsində tranzaksiyaya misal

Baxılan tranzaksiya f5d8ee3… tranzaksiyasından bitkoinləri istifadə edir və onları 40437170… ünvanına göndərir.

Alan tərəf bu tranzaksiyadan olan bitkoinləri istifadə etmək istədikdə, sadəcə, öz tranzaksiyasının Input sahəsində bu tranzaksiyanı göstərir.

Input sahəsi – digər tranzaksiyanın konkret Output sahəsinə istinad edir (tranzaksiyada bir neçə müstəqil Output sahəsi ola bilər). Input sahəsində göstərilmiş tranzaksiyadan olan bütün bitkoinlər toplanır və bu cəm baxılan tranzaksiyada tam istifadə edilməlidir. **Previous tx** əvvəlki tranzaksiyaya istinaddır, **Index** sahəsi isə bu tranzaksiyanın məhz hansı Output-unun istifadə edildiyini göstərir.

scriptSig sahəsi iki hissədən – açıq açar və imzadan ibarətdir. Göstərilmiş açarın heşi əvvəlki tranzaksiyada göstərilmiş alan tərəfin heşinə uyğun olmalıdır. Açıq açar tranzaksiyada göstərilən imzanın yoxlanması üçündür. İmza verilmiş tranzaksiyanın bəzi sahələrinin əsasında generasiya edilir. Beləliklə, açıq açar imza ilə birlikdə təsdiq edir ki, tranzaksiya əvvəlki tranzaksiyada göstərilən həqiqi alan tərəfindən yaradılmışdır. Qeyd etmək lazımdır ki, imza heç zaman tranzaksiyaya bütövlükdə tətbiq edilmir və istifadəçilər tranzaksiyanın hansı hissələrinin imzalandığını göstərə bilərlər (əlbəttə, scriptSig sahəsindən başqa).

Output sahəsi – Output sahəsində bitkoinlərin göndərilməsi üçün təlimatlar olur. **Value** sahəsi bu outputa istinad edildikdə onda olacaq Satoshi miqdarını göstərir (1 BTC=100 000 000 Satoshi).

scriptPubKey bitkoinləri bu tranzaksiyadan digərinə keçirmək üçün "Doğru" qiyməti verməli olan skriptdir. Skripti yoxlamaq üçün scriptSig və scriptPubKey sahələri birləşdirilir (konkatenasiya) edilir, sonra skript yerinə yetirilir. Qeyd etmək lazımdır ki, skript komandalar stekidir, burada bir komandanın çıxış verilənləri digər komandanın girişinə daxil olur. Belə skript sistemi sayəsində göndərən bitkoinlərin verilməsi üçün müxtəlif tipli şərtlər yarada bilər. Məsələn, elə Output yaratmaq olar ki, bu tranzaksiyadan bitkoinləri istənilən istifadəçi ala bilsin. Həmçinin elə skript yaratmaq olar ki, onun yerinə yetirilməsi üçün açar əvəzinə parol istifadə edilsin.

Tranzaksiyada heç də həmişə yalnız bir Input və Output olmur. Tranzaksiyada bir neçə Input (bir neçə tranzaksiyaya istinad edilir) və bir neçə Output (bitkoinlər bir neçə şəxsə göndərilir) ola bilər, həm də hər bir Output üçün özünün unikal skripti ola və digər çıxışlardan asılı olmadan yerinə yetirilə bilər. Həmçinin tranzaksiyada onun nə zaman icra oluna biləcəyini göstərən zaman məhdudiyyətləri də ola bilər.

Tranzaksiyaların emalı. Tranzaksiya şəbəkəyə daxil olduqda əvvəlcə bütün əlyetər Bitkoin qovşaqları tərəfindən yoxlanır və təsdiqlənir. Yoxlamadan uğurla keçdikdən sonra o, *mempul* adlanan yaddaş sahəsində növbəyə durur (ing. memory pool – yaddaş hovuzu) və mədənçinin onu növbəti bloka daxil etməsinə qədər burada gözləməyə məcburdur. Beləliklə, mempul – bütün gözləyən tranzaksiyaların saxlandığı yaddaş sahəsidir.

Mempul BIP 35-in hissəsidir və *yüngül pulqabılara* tranzaksiyalar etməyə imkan verir. Eyni zamanda , mempul Bitkoin şəbəkəsinin aktual problemlərindən biridir. Tranzaksiyalar ondan nə qədər sürətlə keçirsə, istifadəçilər şəbəkənin işindən bir o qədər razı qalırlar. Əgər yeni blokların yaradılması sürəti tranzaksiyaların mempula əlavə edilməsi sürətindən aşağıdırsa, onda böyük tıxac yarana bilər, onun nəticəsində tranzaksiyalar ölçüsündən və tranzaksiya haqqından asılı olaraq saatlarla (hətta sutkalarla) öz təsdiqlənmələrini gözləyə bilərlər.

Məsələn, 2017-ci ilin mayında Bitkoin şəbəkəsi çox ciddi problemlə üzləşmişdi. Mempul-da təsdiqlənməmiş tranzaksiyaların sayı 200 minə çatmışdı, emal edilməmiş verilənlərin həcmi isə 120 Mb-dan çox idi. Nəzərə alsaq ki, Bitkoin şəbəkəsində 1 blokun həcmi 1 Mb-dır və blokun yaradılması 10 dəqiqə çəkir, onda 120 blokdan ibarət növbə bir neçə sutka gecikmişdi, çünki təsdiqlənməmiş yeni tranzaksiyalar da növbəyə daim qoşulurlar.

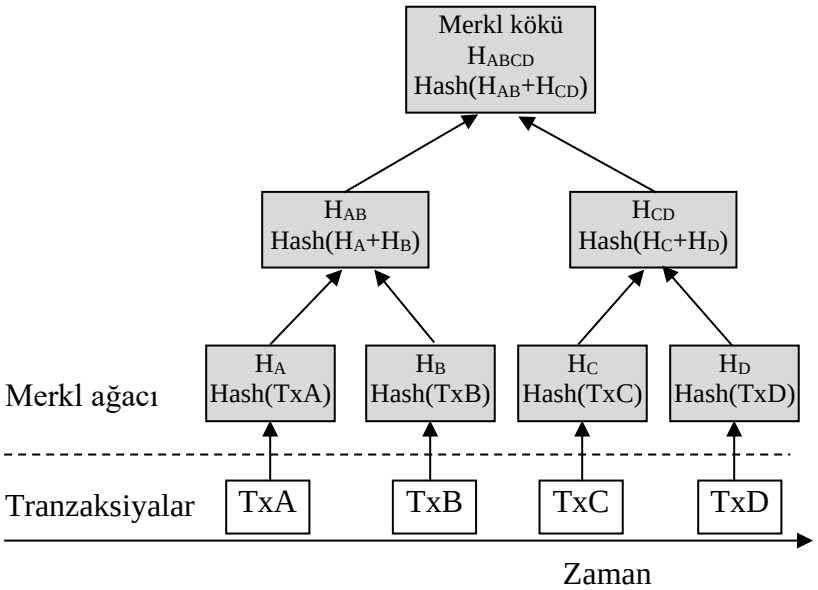
2.3. Merkl ağacı

Bitkoin şəbəkəsində qovşaqlar bərabərhüquqlu və anonimdirlər, onlar bir-birinə etibar etməyə bilərlər. İnamın olmadığı vəziyyətdə verilənlərin verifikasiyası

problemi meydana çıxır: blokda düzgün tranzaksiyaların yazılmasını necə yoxlamaq olar? Hər blokun yoxlanmasına böyük zaman və hesablama resursları sərf etmək lazım gələrdi. Merkl ağacları bu problemi həll etməyə və prosesi asanlaşdırmağa imkan verir.

Merkl ağaclarının konsepsiyası 1979-cu ildə Ralf Merkl (Ralph Charles Merkle) tərəfindən patentləşdirilmişdi.

Merkl ağacı böyük ölçüdə verilənləri toplamaq və təsdiq etmək üçün istifadə olunan verilənlər strukturudur. Merkl ağacına "Binar heş ağacı" da deyirlər. Merkl ağacı kriptoqrafik heş funksiyasının nəticələrindən ibarətdir. Bitkoin sistemində Merkl ağacı tranzaksiyaları blokda toplamaq üçün istifadə olunur. Tranzaksiyaların heş cütləri birləşərək ağacın düyününü əmələ gətirir. Bu proses "Merkl kökü"-nə qədər davam edir. Şəkil 2-də alqoritm təsvir edilmişdir.



Şəkil 2. Merkl ağacında düyünlərin hesablanması

Fərz edək ki, TxA, TxB, TxC, TxD tranzaksiyaları var. Merkl ağacında kriptoqrafik heş funksiya kimi ikiqat SHA-256 (ing. double-SHA-256) tətbiq edilir. Bu tranzaksiyaların ikiqat heş qiymətlərini H_A, H_B, H_C, H_D kimi işarə edək. H_A, H_B, H_C və H_D Merkl ağacının yarpaqlarında yerləşir.

$$H_A = SHA256(SHA256(TxA))$$

Ardıcıl yarpaq düyün cütləri birləşərək ikiqat heşlənir və ağaçdakı valideyn düyünü əmələ gətirir. Yarpaq düyünlərdə yerləşən heş qiymətlər 32 bayt olduğuna görə valideyn düyün 64 bayt olur.

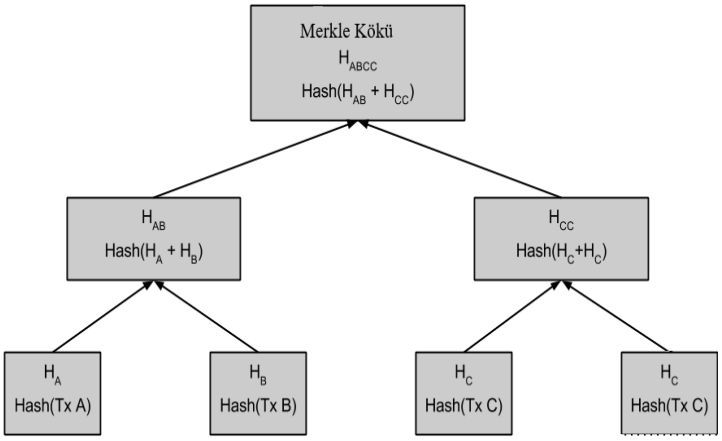
$$H_{AB} = SHA256(SHA256(H_A + H_B))$$

Ağacın qurulması aşağıdakı qaydada aparılır:

1. Bloka yerləşdirilmiş tranzaksiyaların heşləri hesablanır: Hash(TxA), Hash(TxB), Hash(TxC) və s.
2. Tranzaksiya heşlərinin cəmlərindən heşlər hesablanır, məsələn, Hash(H_A + H_B). Merkl ağacı binar ağacdır, buna görə hər bir iterasiyada elementlərin sayı cüt olmalıdır. Buna görə blokda tək sayda tranzaksiya varsa, axırıncı tranzaksiya özü ilə toplanır və heşi hesablanır: Hash(H_C + H_C).
3. Sonra heşlərin cəmindən heşlər yenidən hesablanır. Proses bir heş – ağacın kökü (ing. Merkle root) alınana kimi təkrarlanır. O, blokun tamlığının kriptoqrafik isbatıdır (yəni bütün tranzaksiyaların göstərilən ardıcıllıqda yerləşdiyinin). Kökün qiyməti blokun başlığında yerləşdirilir.

Göstərilən üsulu istənilən sayda tranzaksiyaya tətbiq etmək olar. Bir Bitkoin blokuna yüzlərlə, bəzi hallarda isə mindən artıq tranzaksiya daxil ola bilər.

Əgər yarpaq düyündəki tranzaksiyaların sayı tək sayda olarsa, şəkil 3-də təsvir olunan kimi, son düyün təkrar istifadə olunur.



Şəkil 3. Merkl ağacında tranzaksiyalar tək olduğu halda düyünlərin hesablanması

Qeyd olunan sxemlərdə Merkl kökü ağacda ən böyük qiymət kimi görünsə də, sadəcə, 32 baytdır.

Merkl ağacı verilmiş verilənlər hissəsinin MerkleRoot-a daxil olmasını digər hissələr olmadan yoxlamağa imkan verir.

2.4. Merkl ağaclarının istifadəsi

Fayl sistemləri Merkl ağaclarından informasiyada səhvin olmasını yoxlamaq üçün, paylanmış verilənlər bazaları isə yazıları sinxronlaşdırmaq üçün istifadə edirlər. Blokçeynlərdə isə Merkl ağacları ödəmələrin sadələşdirilmiş verifikasiyanı (ing. Simplified Payment Verification, SPV) həyata keçirməyə imkan verir.

Ümumiyyətlə, Bitkoin qovşaqlarının aşağıdakı növləri var:

- **Tam qovşaq** – blokçeyndə bütün bloklar zəncirini və tranzaksiyalar zəncirini aşağıya doğru (zamana görə) Genezis bloka qədər saxlayır.
- **SPV-qovşaqlar** – yalnız blokların başlığını yükləyirlər, blokda olan tranzaksiyaları yükləmirlər. SPV-qovşaq bütün blokların zəncirini yoxlayır və bu zənciri verilmiş tranzaksiya ilə əlaqələndirir (Merkl kökünün köməyi ilə). SPV-qovşaqlar seçməklə yoxlamaq üçün müəyyən tranzaksiyaları alırlar.

SPV-kliyentləri "yüngül müştərilər" adlandırırlar (çünki bütün bloku yox, yalnız onun başlığını saxlayırlar), onlar tranzaksiya haqqında məlumatı yoxlamaq üçün bütün heşləri hesablamırlar, yalnız Merkl isbatını tələb edirlər. O, kökdən və baxılan tranzaksiyadan kökə qədər olan budaqlardan ibarətdir, çünki istifadəçiyə digər tranzaksiyalar haqqında informasiya lazım deyil. Həmin heşləri toplayaraq onu köklə müqayisə etməklə müştəri əmin ola bilər ki, tranzaksiyalar qaydasındadır.

Belə yanaşma istənilən qədər böyük həcmdə verilənlərlə işləməyə imkan verir, çünki şəbəkəyə düşən yükü əhəmiyyətli dərəcədə azaldır, çünki yalnız lazım olan heşlər ötürülür. Məsələn, maksimal ölçülü beş tranzaksiya olan blok 500 Kbaytdan çoxdur. Bütün Merkl isbatı isə bu halda 140 baytdan böyük deyil.

Binar Merkl ağacları elementlər ardıcıllığını verifikasiya etmək üçün yaxşıdır, buna görə tranzaksiyaların strukturunu saxlamaq məsələsinin öhdəsindən gəlir. Lakin müştərilərə sistemin vəziyyəti haqqında məlumat almaq imkanlarını məhdudlaşdırır. Məsələn, verilmiş ünvan üzrə neçə bitkoinin olmasını öyrənmək mümkün deyil.

Məhdudiyyətləri aradan qaldırmaq üçün tədqiqatçılar yeni alqoritmlər yaradırlar. Məsələn, Ethereum blokçeyn-platformasında prefix Merkl ağacı istifadə edilir (Trie adlanır). Bu verilənlər strukturu açarların assosiativ massivini saxlayır.

Ethereum blokunun başlığında üç prefiks Merkl ağacı olur: tranzaksiyalar, onların yerinə yetirilməsi və vəziyyət haqqında. Belə yanaşma müştərilərə sistemdən bəzi suallara cavab almağa imkan verir: «Göstərilən blokda tranzaksiya varmı?», «Hesabda neçə sikkə var?» və «Bu tranzaksiya yerinə yetirildikdən sonra sistemin vəziyyəti necə olacaq?».

Binar Merkl ağacından fərqli olaraq, ağacın konkret qovşağını identifikasiya edən açar "dinamik"dir. Onun qiyməti ağacda yerləşdiyi yerlə müəyyən edilir və qrafın tillərinə mənimsədilmiş simvolları ağacın kökündən verilmiş qovşağa qədər birləşdirməklə formalaşdırılır.

Merkl ağaclarına daha bir alternativ Hewlett Packard Labs tərəfindən təklif edilmiş HashFusion yanaşmasıdır. Burada heşlərin qiymətləri mərhələlərlə hesablanır. Heşin komponentləri verilənlər əlyetər olan kimi dərhal hesablanırlar, sonra lazım olduqda bir-biri ilə birləşdirilirlər.

HashFusion-da heşin hissələri binar birləşdirmə funksiyasının köməyi ilə qurulur. O assosiativ və qeyri-kommutativdir, buna görə onu heşlər formalaşdırıldığı anda birləşdirmək üçün istifadə etmək olar. Bu onların saxlanması üçün tələb edilən yaddaşın həcmini azaltmağa imkan verir.

Metaverilənlərin emalı və Merkl ağacının qurulması proseslərinin optimallaşdırılması məqsədilə təklif edilmiş digər alqoritmlər də vardır. Onların arasından iSHAKE alqoritmini fərqləndirmək olar, burada heş ağacın qurulması prosesi tərs əməliyyatın tətbiqi ilə əvəzlənir. O, struktura yeni qiymətləri əlavə etməyə, silməyə və bərpa etməyə imkan verir. Həmçinin XMSS genişləndirilmiş Merkl imza sxemini (eXtended Merkle Signature Scheme) və SPHINCS alqoritmini də qeyd etmək olar.

Özünü yoxlamaq üçün suallar

1. Bitkoin bloku hansı dörd komponentdən ibarətdir?
2. Blok başlığına hansı altı sahə daxildir?
3. PreviousHash sahəsinin ölçüsü neçə baytdır?
4. PreviousHash sahəsinin ölçüsü hansı alqoritmlə müəyyən edilir?
5. Bitkoin qovşaqlarının hansı növləri var?
6. Bitkoin şəbəkəsində SVP-qovşaqların funksiyası nədir?
7. SPV-kliyentləri niyə “yüngül müştərilər” adlandırırlar?
8. Merkle Root neçə bayt yer tutur?
9. Ethereum platformasında hansı Merkl ağacı istifadə edilir?
10. Ethereum blokunun başlığında hansı prefiks Merkl ağacları olur?
11. Blokçeynlərdə Merkl ağacları hansı verifikasiyanı etməyə imkan verir?
12. Tranzaksiyalarda scriptSig sahəsi hansı hissələrdən ibarətdir?
13. Tranzaksiyalarda bir, yoxsa bir neçə Input sahəsi ola bilər?
14. Tranzaksiyalarda bir, yoxsa bir neçə Output sahəsi ola bilər?
15. Tranzaksiyalarda nə zaman bir neçə Output sahəsi ola bilər?
16. Emal gözləyən tranzaksiyaların saxlandığı yaddaş sahəsi necə adlanır?
17. Tranzaksiyalarda Output sahəsində Value hissəsi nəyin miqdarını göstərir?
18. HashFusion yanaşmasında heşlər necə hesablanır və hansı üsullar birləşdirilir?
19. iSHAKE alqoritmi struktur üzərində hansı əməliyyatlara imkan verir?
20. Tranzaksiyada Input sahəsi digər tranzaksiyalarda hansı sahələrə müraciət edir?

Mühazirə 3. Bitkoin mayninqi

3.1. Bitkoin mayninqinin mahiyyəti

Bitkoin hasilatı (istehsalı) mayninq vasitəsilə həyata keçirilir. Mayninq – Bitkoin şəbəkəsində zəruri və vacib prosesdir, onun nəticəsində aşağıdakı iki əsas məsələ həll edilir:

1. Yeni tranzaksiyalar blokunun blokçeynə yazılması.
2. Yeni bitkoinlərin emissiyası.

Beləliklə, mayninq zamanı yeni bitkoinlər mədəndən "çıxarılır", blokçeynə yazılacaq yeni bloku tapan mayner mükafat olaraq nəzərdə tutulmuş sayda bitkoin alır.

Bir blokun mayninqinə təxminən 10 dəqiqə gedir. Hər 10 dəqiqədən bir 6,25 yeni bitkoin buraxılır, onu bu bloku tapan, yəni son 10 dəqiqədə olan tranzaksiyaların blokunu yaradan alır. Bu emissiya sürəti Bitkoin protokolunda nəzərdə tutulub və hər 4 ildən sonra 2 dəfə azalır.

2016-cı ilin iyununa kimi hər 10 dəqiqədən sonra 25 bitkoin buraxılırdı, sonra bu sürət yarıya azaldıldı və hər 10 dəqiqədə 12,5 bitkoin buraxıldı. Bu 2020-ci ilə kimi belə davam etdi. Sonra sürət yenidən yarıya bölündü və 2024-cü ilə kimi 6,25 bitkoin buraxılacaq və s. Hazırda dövriyyədə neçə milyon bitkoin var? İlkin nəzərdə tutulduğuna görə, 2140-cı ilə kimi 21 milyon bitkoin buraxılacaq.

Bitkoin mayninqi kifayət qədər bahalı işdir, çünki bu işə nə qədər çox mədənçi cəlb edilibsə, bir o qədər çox bitkoin çıxarılır. Bitkoin şəbəkəsində çətinliyin artırılması mexanizmi var, onun sayəsində mayninq prosesi günbəgün çətin və məsrəfli olur.

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

Ümumiyyətlə, sutkada 1800 bitkoin generasiya edilir. Qazanc (mükafat) mədənçilərin elektrik, amortizasiya, avadanlığa xidmət və s. xərclərini ödəməlidir. Həm də, nəzərə almaq lazımdır ki, fermanın soyutma sistemi də elektrik enerjisi

tələb edir. Faktiki olaraq, sərf olunan elektrikin yalnız yarısı ASIC qurğuların qidalanmasına sərf olunur.

Fermalar maynerlərə hər ay milyonlarla dollar qazandıra bilər. Lakin bitkoinin qiymətinin tez-tez dəyişməsini nəzərə alsaq, mayninq prosesinə sərf olunan xərcləri və mayninqdən əldə edilən gəliri balansda saxlamaq heç də asan deyil.

Mayninq yeni blokların yaradılmasının yeganə texnologiyası deyil. Alternativlər forjing (bəzən mintinq də adlanır) və ICO-dur (Initial Coin Offering – ilkin token təklifi). Token (ing. token – jeton, talon) – kriptovalyuta layihəsinə investisiyalar cəlb etmək məqsədilə buraxılan rəqəmsal aktivdir. Kriptovalyutanın bir növüdür, lakin öz xassələrinə görə səhmlərə və ya istiqrazlara yaxındır. Tokenlər ICO gedişində buraxılır və sonra kriptovalyuta birjalarında satılır.

Forjinq (ing. forging) – yeni sikkələr və tranzaksiya haqları formasında mükafat almaq imkanı ilə PoS (Proof of Stake – hissəyə sahibliyin isbatı) sxemi əsasında müxtəlif kriptovalyuta blokçeynlərində yeni blokların yaradılmasıdır. Müxtəlif kriptovalyutalar forjinqdə iştirak etmək üçün əlavə şərtlər qoya bilər. Məsələn, Nxt prosesə qoşulmaq icazəsini ən azı 1440 təsdiq bloku olan məbləğlərə verir.

Adətən, yalnız bir mayninq texnologiyası istifadə edilir, lakin bəzi kriptovalyutalarda onların kombinasiyası da tətbiq edilir.

3.2. PoW konsensus mexanizmi

Mayninq sxemində T hədəf (ing. target) qiyməti istifadə edilir, onun cari qiyməti periodik olaraq yenidən hesablanır. Maynerlərin məqsədi elə $Nonce$ qiyməti tapmaqdır ki,

$$H(B.N) < T \qquad (1)$$

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

$$H(S) \coloneqq SHA256\big(SHA256(S)\big).$$

Bitkoində H heş funksiyası kimi ikiqat SHA256 seçilib, bu funksiya 0 ilə $2^{256}-1$ arasında müntəzəm paylanmış təsadüfi qiymətlər verir. (1) şərtinin ödənməsinə nail olmaq üçün mayner $Nonce$ qiymətini təsadüfi və ya sistematik şəkildə (məsələn, 0-dan başlayıb ardıcıl artırmaqla) seçir, həmin qiyməti blok başlığına yazır və onun heşini hesablayır. Əgər heş qiymət T-dən kiçik deyilsə, onda N-in qiymətini dəyişir, blok başlığına yazır və heşi yenidən hesablayır. Bu proses hədəf qiymətdən kiçik heş tapılana kimi təkrarlanır. Müvafiq N tapıldıqda blok

Bitkoin şəbəkəsinə göndərilir və blokçeynə əlavə edilir. Blokun tapılmasına görə onu tapan mayner mükafat olaraq hazırda 6,25 bitkoin əldə edir ("mədəndən çıxarır"). Buna görə N-in uyğun qiymətinin tapılması prosesinə *Bitkoin mayninqi* deyilir. Blokun yaradılması, blokçeynə yazılması və qovşaqlara göndərilməsi protokolu isə "görülmüş işin isbatı" (Proof of Work, PoW) protokolu adlanır.

Kriptovalyuta şəbəkəsinin bütün qovşaqları eyni hüquqludur, buna görə eyni anda iki blok tapıldıqda hansı blokun düzgün hesab edilməsi və şəbəkəyə əlavə edilməsi zamanı qeyri-müəyyənlik yaranır. Bundan qaçmaq üçün müxtəlif qərar qəbuletmə mexanizmləri təklif olunub. Belə mexanizm kimi Bitkoin, Ethereum və digər şəbəkələrdə PoW alqoritmi istifadə edilir. PoW alqoritmi formalaşmış bloku blokçeynə hansı qovşağın yazacağını müəyyən edir və bununla mayninq şəbəkəsində konsensusu təmin edir.

PoW konsensus mexanizmi Bitkoin şəbəkəsinin işləməsi və təhlükəsizliyi üçün çox vacibdir. Məsələn, o, blokçeyni dələduzlardan qoruyur. Əgər bir bitkoini iki dəfə xərcləmək istəyən tapılarsa, onda o, blokçeyndə müvafiq tranzaksiyanı yerləşdirmək üçün əvvəlcə, maynerlərin gördüyü həmin işi yerinə yetirməlidir. Bunun üçün böyük hesablama resurslarına malik olmalıdır. Çünki hər 10 dəqiqədən bir dəyişən heşi tapmaq məsələsini həll etmədən blokçeynə yazmağın başqa yolu yoxdur.

Lakin PoW mexanizminin problemi onun yan təsirindədir – PoW enerji sərfi baxımından effektiv deyil. Aydındır ki, söhbət saniyədə trilyonlarla heşdən gedirsə, bu hesablamalara çox böyük elektrik enerjisi lazımdır – hazırda Bitkoin şəbəkəsində sərf olunan elektrik enerjisi Danimarkada sərf olunan həcmdədir.

3.3. Bitkoində mayninqin çətinliyinin tənzimlənməsi

Çətinlik. Blokların tapılması, yəni bitkoinlərin çıxarılması sürətini Bitkoin şəbəkəsində (1)-dəki T hədəf qiymətini seçməklə idarə etmək olar. Lakin T şəbəkədə mövcud olan maynerlərin cari sayından və sürətindən asılıdır, bunu D çətinlik termini ilə ifadə edirlər. Çətinlik ilə T hədəf qiyməti arasındakı münasibət

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

düsturu ilə təyin edilir, burada T_{max} maksimal mümkün hədəf qiymətidir, $T_{max} = (2^{16} - 1)2^{208} \approx 2^{224}$.

Bitkoində H heş funksiyası elə seçilib ki, 0 ilə $2^{256} - 1$ arasında müntəzəm paylanmış qiymətlər versin. Beləliklə, verilmiş ixtiyari *Nonce* qiyməti üçün (1) şərtinin ödənməsi ehtimalı

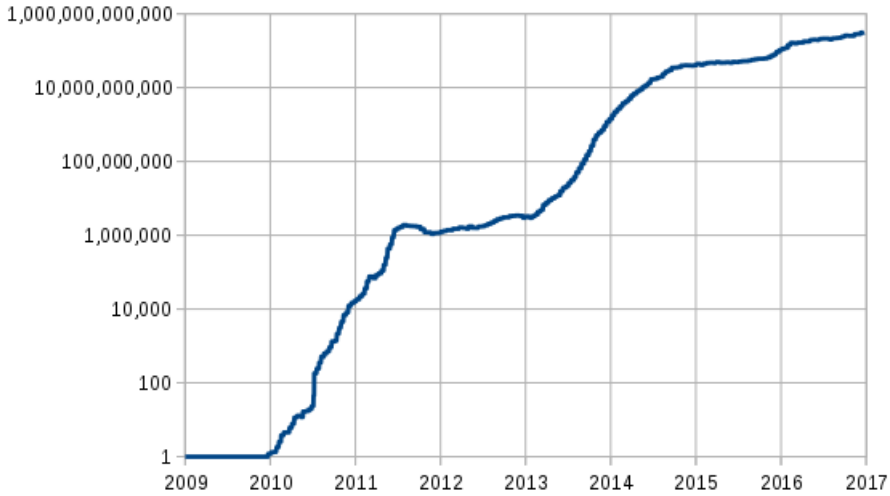
$$p = \frac{T}{2^{256}} = \frac{T_{max}}{D \cdot 2^{256}} \approx \frac{1}{D \cdot 2^{32}}$$

olacaq. Yoxlanılan hər bir *Nonce* qiyməti asılı olmayan sınaq kimi çıxış edir, buna görə blokun uğurla tapılmasına kimi sınaqların sayı həndəsi paylanmaya tabe olur. Beləliklə, bloku tapmaq üçün hesablanacaq heşlərin gözlənilən sayı $D2^{32}$ olacaq. Əgər heşlərin hesablanması sürəti R olarsa, onda bloku tapmaq üçün gözlənilən müddət

$$\mathbb{E}[t] = \frac{1}{p} \approx \frac{D \cdot 2^{32}}{R}$$

olar. Məsələn, əgər mayner Bitkoin heşini saniyədə 1 milyon heş sürəti ilə hesablaya bilirsə və çətinlik 4 250 217 92-dirsə, onda $\mathbb{E}[t] \approx 1.8 \times 10^{13}\ san$ olacaq.

D çətinliyinin qiyməti hər 2016 blokdan sonra (təxminən 2 həftə) yenidən hesablanır ki, bloklar arasındakı 10 dəqiqəlik interval təmin olunsun. Çətinlik dedikdə, bir həqiqi blokun axtarışı üçün hesablanmış heşlərin orta sayı nəzərdə tutulur. Yeni çətinliyi hesablamaq üçün son 2016 bloku hesabladıqda sərf edilən zaman müddəti bütün Bitkoin şəbəkəsinin ortalama heş sürətini qiymətləndirmək üçün istifadə edilir. Yeni çətinlik elə seçilir ki, həmin orta heş sürəti saxlandıqda növbəti 2016 blok 2 həftə müddətində yaradılsın. Əgər nəticədə alınmış yeni çətinlik əvvəlki çətinlikdən 4 dəfədən də çox çətindirsə (asandırsa), onda nəticə 4 dəfə çətinliklə məhdudlaşdırılır. Yolverilən çətinlik/hədəf qiymətlərə olan məhdudiyyətlər də tətbiq edilir.



Şəkil 1. Bitkoin şəbəkəsində çətinliyin illər üzrə qiymətləri

Şəkil 1-də Bitkoin şəbəkəsində çətinliyin illər üzrə qiymətləri göstərilib. Çətinliyin artması tendensiyasının səbəbi Bitkoin şəbəkəsində heşlərin hesablanması üçün nəzərdə tutulmuş hesablama resurslarının artmasıdır.

3.4. Mayninq hovuzları

Mayninqin çətinliyi daim artır. Bloka görə nəzərdə tutulmuş mükafatı almaq üçün "dəmirə" və elektrik enerjisinə böyük xərc çəkmək lazımdır, bu təkbaşına mədənçi üçün olduqca çətindir. Buna görə müxtəlif mədənçiləri birləşdirən "hovuzlar" yaradılır.

Təxminən 2010-cu ildə GPU-mayninq üçün ilk proqram təminatı işləndi, bu hesablamaları dəfələrlə sürətləndirməyə imkan verdi. Sonra bir neçə videokartlı kompüterlər (onları zarafatla "qazma vışkası" adlandırırlar), onların ardınca isə yüzlərlə videokartdan ibarət bütöv "fermalar", həmçinin kollektiv mayninq üçün saytlar ("hovuzlar") meydana çıxdı. Kriptovalyutalar tarixində ilk hovuz Bitcoin.cz hesab edilir, o, Slush's Pool kimi də tanınır. (Bu hovuz indiyə kimi işləyir?)

Hazırda hovuzların bir neçə növü var:

- **Klassik hovuz** – bir kriptovalyutanın mayninqini həyata keçirir. Belə hovuzu saniyədə yüzlərlə teraheş yaradan bir mayner kimi təsəvvür etmək olar. Hovuzun əsas serveri məsələləri maynerlər arasında paylayır.
- **Mərkəzləşməmiş hovuz** (P2Pool) – hovuzun bəzi idarəçiləri bədniyyətli ola bilərlər (məsələn, pulu mənimsəyib, serveri bağlayıb və izi itirmə halları olub), onlarla mübarizə üçün açıq kodlu P2Pool təklif edilib. Burada hər bir qovşaq yalnız sistemin elementlərindən biridir və maksimal mükafat almaq üçün iştirakçılar qovşaqlardan birində qalmalıdırlar. Bir qovşaqdan digərinə "atlayışlar" sərfəli deyil.
- **Birgə mayninq hovuzu** (ing. merged mining) – bir neçə kriptovalyuta eyni anda çıxarılır. Məsələn, Bitkoin blokunun formalaşması zamanı hesablanmış heşləri Bitkoinin paralel forkları üçün istifadə etmək olar. Bitkoinlə paralel mayninq edilə bilən forklardan Namecoin, Devcoin, IxCoin və I0Coin göstərilə bilər. Bitkoin üçün olan bəzi hovuzlar forklardan birinin, adətən Namekoin-in birgə mayninqinə icazə verir. O, maynerlərə 1-2% əlavə gəlir gətirə bilər.
- **Multi-hovuz** – baxılan anda mayninqi ən sərfəli olan kriptovalyutanın mayninqinə avtomatik qoşulur.

Son dövrlər "bulud mayninqi" (ing. Cloud Mining) də populyarlıq qazanır – heşləri "buludda" hesablamaq üçün Data-mərkəzlərin hesablama resursları icarəyə götürülür.

Kriptovalyuta infrastrukturunda mayninq hovuzları fiat valyutaları üçün prosessinq mərkəzlərinin rolunu oynayır ("fiat" – fərman, sərəncam kimi tərcümə olunur). Mayninq dayandığı halda kriptovalyuta da mövcudluğunu dayandırar. Bu səbəbdən mayninqə görə mükafat mayninqin mənfəətli olmasını təmin edəcək səviyyədə olmalıdır.

Hovuzlarda mayninq mükafatının bölünməsinin aşağıdakı metodları var:

- **PROP** (PROportional) – mükafat blokun tapılması zamanı maynerin göndərdiyi hissələrə mütənasib hesablanır.
- **POT** (Pay on Target) – ödəniş maynerin hovuza qaytardığı işin çətinliyinə uyğun hesablanır.
- **PPS** (Pay Per Share) – tapılmış hər bir hissəyə görə ödəniş edilir.
- **PPLNS** (Pay Per Last N Shares) – axırıncı *N* hissəyə görə ödəniş edilir.
- **DGM** (Double Geometric Method) – ödənişləri normallaşdırmaq üçün operator qısa raundlar zamanı vəsaitin bir hissəsini alır, uzun raundlar zamanı isə onu geri qaytarır.
- **MPPS** (Maximum Pay Per Share) – blokların tapılmasından gələn gəlirdən maynerlərə mümkün qədər çox, lakin heç vaxt müflis olmayacaq şəkildə ödəniş edilir.
- **BPM** (Bitcoin Pooled Mining) –blok raundunun başlanğıcında olan hissələrə cari hissələrə nisbətən daha az çəki verilir. Məqsəd raund ərzində hovuzlara qoşularaq mayninq sistemini aldatmağın qarşısını almaqdır.

2.5. Bitkoinin elektrik enerjisi sərfi (Əlavə oxu üçün)

Bitkoin fermalarının əsas xərcləri enerji sərfiyyatının ödənilməsinə yönəlir. Bitkoin fermalarının mayninq prosesindən əldə etdikləri gəlirin 60 %-ə yaxını enerji xərclərinə gedir. Aşağıdakı qrafikdə bir bitkoin tranzaksiyası və yüz min Visa tranzakiyasına sərf olunan enerji muqayisəli göstərilmişdir.

Hazırda 1 bitkoin tranzaksiyasına təxminən 200 kVt/saat elektrik enerjisi sərf edilir. Bu enerji bəzi evlərə 4 həftə bəs edərdi, məsələn Niderlandda ortabab ev həftədə 45 kVt/saat sərf edir. Bitkoin digər elektron ödəniş sistemləri ilə müqayisədə olduqca çox enerji işlədir. Müqayisə üçün Visa sistemində bir əməliyyata cəmisi 0,01 kVt/saat enerji sərf edilir. (Qeyd edək ki, Ethereum blokçeynində bir əməliyyata təxminən 37 kVT/saat sərf edilir.)

Morits Ştrube bütün Bitkoin şəbəkəsində sərf edilən elektrik enerjisini hesablamağa cəhd etmişdi. Avropada elektrik enerjisinin qiyməti yüksək olduğundan mayninq fermaları, məsələn, İslandiya, Venesuela kimi elektrik enerjisi

ucuz olan ölkələrdə yerləşir. Onun hesablamalarına görə bütün dünyadakı mayninq qurğuları ayda 1,17 teravatt-saat elektrik enerjisi işlədilir. Müqayisə üçün Sloveniyada isə ayda 1,08 teravatt-saat işlədilir.

Digiconomist saytının banisi Aleks de Vris qeyd edir ki, bir bitkoin tranzanzaksiyasının işlətdiyi enerji bir ailənin bir həftəyə işlətdiyi elektrik enerjisinə bərabərdir. Onun qiymətləndirilməsinə görə, bir sutkada dünyada təxminən 300 min bitkoin-tranzaksiya baş verir, hər bir tranzaksiyanın emalına isə 215 kilovatt-saat sərf olunur. Orta amerikan ailəsi isə ayda 901 kVt-saat işlədir, buradan alınır ki, bir bitkoin tranzaksiya bir ailənin bir həftəyə sərf etdiyi qədər elektrik enerjisi sərf edir. Bundan başqa, bitkoin istehsalının ətraf mühitə vurduğu ziyanı da nəzərə almaq lazımdır. Aleks de Vris misal kimi Monqolustandakı kömürlə işləyən elektrik stansiyasından ucuz enerji hesabına işləyən mayninq-fermasını göstərir. Analitikin hesablamalarına görə, hər bir belə şaxta çıxarılan hər bitkoin üçün atmosferə 8-13 min və ya saatda 24-40 min kiloqram karbon qazı buraxır.

Özünü yoxlamaq üçün suallar

1. Hazırda Bitkoində emissiya sürəti 10 dəqiqədə neçə bitkoindir?
2. Bitkoin-də emissiya sürəti neçə ildə 2 dəfə azalır?
3. Bitkoin şəbəkəsində cəmi neçə bitkoin buraxılacaq?
4. PoW konsensus mexanizminin əsas nöqsanı nədir?
5. Klassik hovuz necə işləyir?
6. Birgə mayninq hovuzu necə işləyir?
7. Mayninq Bitkoin şəbəkəsində hansı iki əsas məsələni həll edir?
8. Mərkəzləşməmiş hovuz (P2Pool) necə işləyir?
9. Hazırda mayninq fermaları daha çox hansı hesablama qurğuları ilə işləyir?
10. Hovuzlarda mayninq zamanı mükafatın bölünməsinin hansı metodları var?
11. Çətinlik dedikdə nə nəzərdə tutulur?
12. PoW alqoritmi necə işləyir?
13. PoW alqoritmi nəyi müəyyən edir?
14. Çətinlik ilə T hədəf qiyməti arasındakı münasibət hansı düsturla verilir?
15. Mayninq zamanı hansı dəyişənin qiyməti tapılır?
16. Blokçeyndə yeni blokların yaradılmasının mayninqdən fərqli hansı texnologiyaları var?
17. Token buraxılmasının məqsədi nədir?
18. ICO qısaltması necə açıqlanır?
19. Forjinq nədir?
20. Bitkoin şəbəkəsində çətinliyi necə artırırlar (tənzimləyirlər)?

Mühazirə 4. Ethereum və PoS konsensus mexanizmi

4.1. Ethereum (ETH) kriptovalyutası

Ethereum (Efirium) bazar kapitallaşmasına görə Bitkoindən sonra ikinci yeri tutur. Ethereum protokolunun işlətdiyi kriptovalyuta ETH (efir) adlanır.

Ethereum əsas protokolu 2013-cü ildə rus əsilli kanadalı proqramçı Vitalik Buterin tərəfindən işlənmişdi, şəbəkə isə 30 iyul 2015-ci ildə işə salınmışdı. Dagger-Hashimoto şifrləmə alqoritmindən istifadə edilir. Tokenlərin maksimal sayı təxminən 90 milyondur.

Ethereum-un əsas ideyası blokçeynin funksional imkanlarının genişləndirilməsi idi. Bu ideya "ağıllı müqavilə"lər vasitəsilə həyata keçirilmişdi.

Ağıllı müqavilə blokçeyndə saxlanan (istənilən) proqram kodudur. O, istənilən rəqəmsal aktivin transferini təmsil edə bilər. Onlar müəyyən şərtlər ödəndikdə icra olunur, buna görə "ağıllı" adlanırlar. Onları "müqavilə" də adlandırmaq olar, çünki onlar tərəflər arasında razılaşmaların yerinə yetirilməsini təmin edirlər.

Müqavilənin ünvanı var. Bu ünvanla qarşılıqlı əlaqə saxlamaq üçün istifadəçilər ona 2 ETH göndərməlidirlər. Bu müqavilənin kodunu aktivləşdirəcək. Şəbəkədəki bütün kompüterlər onu işə salacaqlar, ödəmənin edildiyini görəcəklər və onun çıxışını yazacaqlar.

Ethereum-a avtomat (vəziyyət maşını) kimi baxmaq olar. Bu o deməkdir ki, istənilən an fayl sisteminin obrazını götürmək və hesablardakı ağıllı müqavilələr haqqında məlumata baxmaq olar. Müəyyən hərəkətlər sistemin vəziyyətinin dəyişməsinə səbəb olur və bütün qovşaqlar dəyişikliyi əks etdirmək üçün öz obrazlarını yeniləyirlər.

Ethereum proqram kodunu paylanmış sistemdə işə salmağa imkan verir. Bu kənar şəxslərin proqramda dəyişiklik etməsinə imkan vermir. Bundan əlavə, blokçeyn bütün istifadəçilərə əlyetərdir, bunun sayəsində istifadəçi proqram kodunu işə salmazdan öncə onu yoxlaya bilər.

Ethereum-da yerinə yetirilən ağıllı müqavilələri tranzaksiyalar işə salır. İstifadəçi müqaviləyə tranzaksiya göndərdikdə, şəbəkədəki hər bir qovşaq müqavilə kodunu işə salır və çıxışı yazır. Bunun üçün ağıllı müqavilələri kompüterin başa düşə biləcəyi əmrlərə çevirən Ethereum Virtual Machine (EVM) istifadə olunur.

Vəziyyəti yeniləmək üçün Proof of Work alqoritmindən istifadə etməklə Bitcoin alqoritminə çox oxşar olan protokol həyata keçirilir.

Mayninq blokçeynin təhlükəsizliyi və yenilənməsi baxımından infrastrukturun ayrılmaz elementidir. Mayninq xeyli xərc tələb edir və sistem

maynerləri mükafatlandırmalıdır. Ağıllı müqaviləni icra etmək üçün müəyyən miqdarda "qaz" sərf olunmalıdır.

Qaz – Ethereum platformasında ödəniş kimi istifadə olunan termindir, bir tranzaksiyanın və ya müqavilənin icra qiymətini bildirir. Müxtəlif ağıllı müqavilələr tələb olunan tapşırığı yerinə yetirmək üçün fərqli həcmdə qaz tələb edir. Qaz ilə avtomobil üçün yanacaq arasında paralel qurmaq olar. Ümumi xərc qazın qiyməti ilə istifadə olunan qazın həcminin hasili kimi hesablanır. Qaz qiymətləri *gwei* (shannon) ilə göstərilir. Bir gwei 0,000000001 ETH dəyərindədir.

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

Çox zaman Bitkoini *birinci nəsil blokçeyn* adlandırırlar. O çox da mürəkkəb sistem kimi düşünülməmişdi və bu, təhlükəsizlik məsələlərində onun üstünlüyüdür. Bitkoin-in çevik olmaması – etibarlılığı daha çox təmin etmək üçün düşünülmüş bir qərardır. Bitkoində ağıllı müqavilə dili son dərəcə məhduddur və tranzaksiyalarla işləməyən tətbiqlər üçün çox da uyğun deyil.

Bitkoin – blokçeyn texnologiyasının konkret bir tətbiqidir, elektron ödəniş sisteminin reallaşdırılmasıdır. Lakin blokçeyn texnologiyasının imkanları daha genişdir və Bitkoin-də bu imkanların kiçik bir hissəsi reallaşdırılıb.

Ethereum *ikinci nəsil blokçeyn*lərin ilkidir və hazırda da bu seqmentin lideridir. İkinci nəsil blokçeynlər çox şeyə qadirdir. Maliyyə tranzaksiyalarını asanlaşdırmaqla yanaşı, bu platformalar daha çox proqramlaşdırıla bilir. Ethereum mərkəzi olmayan tətbiqlər (DApps) yaratmaq üçün böyük imkanlar verir.

"Kriptovalyuta yandırılması". Bitkoindən fərqli olaraq, Ethereum işə salındıqda sikkələrin emissiyası qrafikini müəyyən etməmişdi. Bitkoin öz dəyərini saxlamaq üçün bitkoinlərin sayını məhdudlaşdırmışdı və buraxılan bitkoinlərin sayını tədricən azaldır.

Ethereum-da isə "pul yandırma" istifadə edilir. Hər tranzaksiyada ETH yanması baş verir. İstifadəçilər tranzaksiyalar üçün ödəniş etdikdə, şəbəkə tərəfindən tələb əsasında müəyyən edilmiş baza qaz komissiyası məhv edilir.

Token yandırma təklifi azaltmaq və inflyasiya ilə mübarizə aparmaq üçün müəyyən miqdarda kriptovalyutanın məhv edilməsi prosesidir. Bir qayda olaraq, bu əməliyyatdan sonra aktivin dəyəri yüksəlir və ya sabitləşir. Yandırma bütün rəqəmsal valyuta əməliyyatları kimi hesablama prosedurudur və blokçeyndə qeyd olunur.

Yandırma – pulların dövriyyədən həmişəlik çıxarılması prosesidir. Bu, token dondurulmasına bənzəyir, lakin dondurma zamanı tokenlər müəyyən müddətə, yandırmada isə həmişəlik dövriyyədən çıxarılır.

4.2. The DAO və Ethereum Classic

Ethereum-un meydana çıxması həm də mərkəzi olmayan avtonom təşkilatların (Decentralized Autonomous Organization, DAO) yaradılmasını mümkün etdi. DAO – Ethereum blokçeynində yazılmış ağıllı müqavilələrin köməyi ilə idarə edilən, vahid lideri olmayan, tam avtonom, mərkəzi olmayan təşkilatdır. Burada proqram kodu ənənəvi təşkilatın strukturunu və qaydalarını əvəz edir, mərkəzləşmiş insan nəzarətinin zəruriliyini aradan qaldırır. DAO tokenləri alanların hamısına məxsusdur, lakin burada token aksiyaların hissə və ya paketi deyi, səs hüququ üçün ödənişdir.

The DAO belə bir sistemi yaratmaq üçün ilk və ən iddialı layihələrdən biri idi. O, Ethereum üzərində işləyən mürəkkəb ağıllı müqavilələrdən ibarət olmalı və avtonom vençur kapitalı fondu kimi çıxış etməli idi. The DAO tokenləri ICO-nun bir hissəsi kimi paylanmışdı və token sahiblərinə səsvermə hüququ ilə birlikdə sahiblik payı verirdi.

Lakin işə salındıqdan qısa müddət sonra bədniyyətlilər layihənin açıq mənbə kodundakı boşluqdan istifadə etdilər və DAO vəsaitlərinin demək olar ki, üçdə birini oğurladılar. O zaman The DAO ümumi ETH emissiyasının 14%-nə sahib idi və belə bir hadisə Ethereum şəbəkəsi üçün çox dağıdıcı idi.

Müəyyən müzakirələrdən sonra Ethereum iki hissəyə bölündü (hardfork). Yeni blokçeyndə bədniyyətli tranzaksiyalar ləğv edildi və vəsaitlər sahiblərinə qaytarıldı. Hazırda bu hissə Ethereum blokçeyni kimi tanınır. Tranzaksiyaların geridönməzliyini qoruyan hissə isə indi Ethereum Classic adlanır.

4.3. PoS konsensus sxemi

PoW (Proof of Work) tranzaksiyaların blokçeyndə təsdiqlənməsinin yeganə üsulu deyil. Bir neçə digər metod da var, onlardan ən ümidvericisi “Proof-of-Stake” (PoS) – “hissə ilə isbat” adlanır. Onun əsas üstünlüyü, hesablamalardan, ümumiyyətlə imtina etməyə imkan verməsidir. Buna görə əvvəlcə hesablamalara, sonra isə soyutmaya kilovattlarla enerji xərcləmək lazım gəlmir.

Yanaşmanın mahiyyəti belədir. PoS metodu ilə işləyən maynerlər hesablama maşınlarının gücü ilə deyil, öz pulqabılarının “gücü” ilə yarışırlar. Bu təxminən belə baş verir: Maynerlər əvvəlki kimi sadə iştirakçılardan tranzaksiyaları toplayır və onların düzgünlüyünü yoxlayırlar. Blokçeynə yazmaq hüququ isə hər 10 dəqiqədən

bir püşklə müəyyən edilir – uduş ehtimalı maynerin hesabında olan məbləğlə düz mütənasibdir. Beləliklə, pulqabınızda nə qədər çox pul varsa, növbəti bloku blokçeynə yazmaq hüququnu sizin almanızın ehtimalı bir o qədər böyükdür.

Zahirən radikal fərqlərə baxmayaraq, PoS sxeminin PoW ilə göründüyündən də çox ortaq cəhətləri var. Birincisi, Bitkoin-mayninq üçün ferma qurmağa xeyli xərc çəkmək lazımdır. PoS-da isə təxminən həmin məbləği xüsusi hesaba yatırırsınız. İkincisi, PoS-da avadanlığın köhnəlməsi riski yoxdur. Daimi rəqabət zamanı mayninq avadanlığı sürətlə köhnəlir, onların istismarı sərfəli olmur, deməli, onların qurulmasına sərf olunan kapital itir. PoS-da sizin pullar müqayisədə az gəlir gətirsə də, pul olaraq qalır.

PoS sxemi nəzəri baxımından əsaslı işlənsə də, Bitkoin ölçüsündə olan heç bir blokçeyn sistemində praktiki reallaşdırılmayıb. PoS sxeminin təmiz şəkildə və ya hibrid reallaşdırdığı kriptovalyutalar olsa da (Dark, BitShares, Blocknet və digələri), onların heç biri yükünə və kapitallaşmasına görə Bitkoinlə müqayisə edilə bilməz. Məhz buna görə Bitkoini PoS sxeminə keçirmək barədə diskussiyalar hələlik nəzəri olaraq qalır. Əgər keçid baş tutarsa və PoS-da hər hansı məlum olmayan zəif yer aşkarlanarsa, onda nə baş verər?

PoS istənilən kiçik məbləğlə mayninqdə iştirak etməyə imkan verir. Böyük oyunçular arasında hipotetik sözləşmə halında PoS asanlıqla fork həyata keçirməyə və "günahkar" pulqabıları səs hüququndan həmişəlik məhrum etməyə də imkan verir. Lakin PoS istifadə edən kriptovalyutada "tiranı devirmək" mümkün deyil: varlılar daha çox varlanacaqlar, kiçik oyunçular isə əhəmiyyətsiz rolları ilə həmişəlik barışmalı olacaqlar. Kriptovalyutalarda vacib qərarlar səsvermə ilə qəbul olunur, yəqin ki, PoS sistemi dominatlıq edən eyni oyunçuların seçdikləri istiqamətlərdə hərəkət edəcək.

4.4. PoS konsensus sxeminə keçid

Ethereum layihəsi PoW blokçeyni ilə işə salınsa da, təsisçilər uzunmüddətli perspektivdə PoS modelinə keçidi planlaşdırmışdılar. Keçid başa çatdıqdan sonra Ethereum şəbəkəsində mayninqə ehtiyac qalmayacaq.

Ethereum 2022-ci ilin sentyabrında PoS sxeminə keçidə başlamışdır. Bəzi tədqiqatçılar bunu Ethereumun öz valideyninin (Bitkoinin) kölgəsindən çıxmaq, özünün müstəqil, proqressiv imicini təsdiqləmək üçün etdiyini söyləyirlər.

Casper – Ethereum şəbəkəsinin PoS alqoritminə keçməsini nəzərdə tutan yenilənməsidir (Ethereum 2.0 kimi də tanınır).

Ethereum ekosistemində yenilənmənin iki versiyası hazırlanmışdı: Casper CBC və Casper FFG. Ethereum 2.0-a keçid Casper FFG ilə başlayıb, lakin bu,

Casper CBC-nin istifadəyə yararsız qalacağı anlamına gəlmir. Əslində, gələcəkdə Casper FFG-ni əvəz etmək və ya əlavə etmək üçün istifadə edilə bilər.

Ethereum 1.0-dan 2.0-a keçid "Serenity" adlanır. O, üç fərqli mərhələdən ibarətdir. İlkin mərhələdə (mərhələ 0) *Beacon Chain* adlı yeni blokçeyn işə salınır. Casper FFG yeniləməsi ilə müəyyən edilmiş qaydalar yeni PoS əsaslı zəncirdə konsensus mexanizmini idarə edəcək.

Serenity-nin ilk mərhələsində validator olmaq üçün istifadəçilər steykə 32 ETH qoymalıdırlar – bunu keçmiş Ethereum 1.0 blokçeyninə əsaslanan xüsusi ağıllı müqaviləyə depozit kimi də təsvir etmək olar.

Özünü yoxlamaq üçün suallar

1. Ethereum 1.0 hansı blokçeyndən istifadə edir?
2. Ethereum 1.0 hansı konsensus protokolundan istifadə edir?
3. Qaz termini Ethereum-da nəyi bildirir?
4. ETH-in ən kiçik vahidi nədir?
5. “Kriptovalyuta yandırılması” nəyə xidmət edir?
6. Ethereum Classic forku Ethereum blokçeyninin hansı hissəsinə əsaslanır?
7. Ethereum-un forkuna hansı hadisə səbəb olmuşdu?
8. Ethereum-da PoS sxeminə keçmək üçün hansı yeniləmə versiyaları hazırlanmışdı?
9. DAO nədir?
10. The DAO nədir?
11. Ağıllı müqavilə nədir?
12. Ethereum Virtual Machine (EVM) nə iş görür?
13. PoS sxemi necə işləyir?
14. PoS sxeminin əsas üstünlüyü nədir?
15. Ethereum nə vaxt PoS sxeminə keçidə başlamışdır?
16. PoS sxemində maynerin uduş ehtimalı nə ilə mütənasibdir?
17. Ethereum 1.0-dan 2.0-a keçid neçə mərhələdən ibarətdir?
18. Ethereum 1.0-dan 2.0-a keçidin birinci mərhələsində hansı blokçeyn qurulacaq?
19. Ağıllı müqaviləni icra etmək üçün nə sərf olunmalıdır?
20. Ethereum 2.0-a keçid başa çatdıqdan sonra Ethereum-da nəyə ehtiyac qalmayacaq?

Mühazirə 5. Blokçeynlərdə kriptoqrafiya məsələləri

5.1. SHA-256 heş funksiyası

SHA-256 heş funksiyası NSA (National Security Agency) tərəfindən hazırlanmış SHA-2 kriptoqrafik heş funksiyaları ailəsinə daxildir. Kriptoqrafik heş funksiyası rəqəmsal məlumatlar üzərində aparılan riyazi əməliyyatlardır. Hesablanan "heş"i (alqoritmin çıxışı) məlumatın əvvəlcədən hesablanmış heş qiyməti ilə müqayisə edən şəxs məlumatların tamlığını müəyyən edə bilər. SHA-256 funksiyası istənilən uzunluqda veriləni 32 baytlıq (256 bitlik) heş qiymətə çevirir. Funksiyanın nəticəsi 16-lıq sistemdə yazılır. Əgər verilənlərdə xırda dəyişiklik edilsə, SHA-256 heş funksiyasının qiyməti tamamilə dəyişər. SHA-256 heş funksiyasının nəticəsi 256 ədəd 0 və 1-dən ibarət olur. $2^{256} \approx 1.15 \times 10^{77}$ fərqli heş qiyməti mövcuddur. Hər bir SHA-256 heşi 1 və $2^{256} - 1$ arasında olan təsadüfi ədəddir.

Heş funskiyalar biristiqamətlidir. Biristiqamətli heşi hər hansı bir məlumat üçün asanlıqla hesablamaq olar, lakin bu məlumatı heşdən geri bərpa etmək mümkün deyil. SHA-256 Bitkoin şəbəkəsinin müxtəlif hissələrində istifadə olunur:

- Mayninq prosesində iş alqoritminin təsdiqlənməsində;
- Təhlükəsizlik və məxfiliyi artırmaq üçün Bitkoin ünvanlarının yaradılmasında.

5.2. Bitkoin ECDSA imza alqoritmi

Bitkoində imza üçün elliptik əyrilər üzərində ECDSA (Elliptic Curve Digital Signature Algorithm) alqoritmi istifadə edilir. Elliptik əyriləri istənilən meydan üzərində təyin etmək olar. Sadə p moduluna görə qalıqlar meydanı üzərində elliptik əyrini aşağıdakı tənliklə vermək olar:

$y^2 = (x^3 + ax + b)\ mod\ p,$ burada $4a^3 + 27b^2 \neq 0$

Sonlu meydan üzərində elliptik əyri nöqtələr çoxluğundan ibarətdir. Misal üçün $y^2 = x^3 + 7\ \ (mod\ 11)$ tənliyinə baxaq, burada bütün hesablamalar 11-ə bölündükdə alınan qalıqlar üzərində aparılır.

Bu tənliyi ödəyən nöqtələr çoxluğu aşağıdakı kimi olacaq (şəkil 1):

$E = \{(2;2), (2;9), (3;1), (3;10), (4;4), (4;7), (5;0), (6;5), (6;6), (7;3), (7;8)\}$

$(2^3 + 7) \bmod 11 = 4$ və $y^2 = 4$-ün kökləri 2 və 9-dur: $2^2 mod\ 11 = 4;\ 9^2 mod\ 11 = 4.$

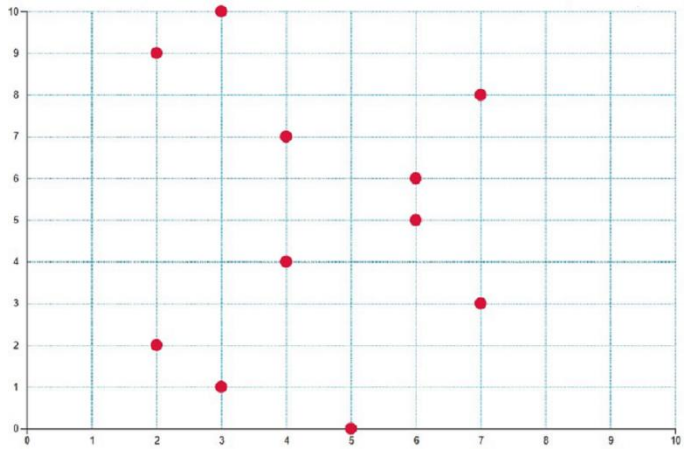
$(3^3 + 7) \bmod 11 = 1$ və $y^2 = 1$-in kökləri 1 və 10-dur: $1^2 mod 11 = 1;\ 10^2 mod 11 = 1.$

$(4^3 + 7) \bmod 11 = 5$ və $y^2 = 5$-in kökləri 4 və 7-dir: $4^2 mod\ 11 = 5;\ 7^2 mod\ 11 = 5.$

$(5^3 + 7) \bmod 11 = 0$ və $y^2 = 0$-ın kökü 0-dır.

$(6^3 + 7) \bmod 11 = 3$ və $y^2 = 3$-ün kökləri 5 və 6-dır: $5^2 mod\ 11 = 3;\ 6^2 mod\ 11 = 3.$

$(7^3 + 7) \bmod 11 = 9$ və $y^2 = 9$-un kökləri 3 və 8-dır: $3^2 mod\ 11 = 9;\ 8^2 mod\ 11 = 9.$



Şəkil 1.

Standartda təklif olunan elliptik əyrilər arasından secp256k1 seçilmişdir (http://www.secg.org/sec2-v2.pdf).

Secp256k1 elliptik əyrisinin tənliyi

$$y^2 = x^3 + 7 \ (mod\ p)$$

şəklindədir, burada $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ (hesablama p moduluna görə aparılır).

G baza nöqtəsi elliptik əyriyə aid olan seçilmiş nöqtədir, sıxılmış formada aşağıdakı şəkildədir:

G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

G baza nöqtəsinin tərtibi *n* aşağıdakı kimidir (kofaktor *h* = 1):

n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

Gizli açar 0 ilə $n - 1$ arasında istənilən ədəd ola bilər, $n \approx 1{,}158 \cdot 10^{57} < 2^{256}$

Gizli və açıq açarın generasiyası alqoritmi aşağıdakı kimidir:

1. Təsadüfi ədəd seçilir.
2. SHA256 alqoritmi tətbiq edilir. Heşin nəticəsi gizli açar olur (x).
3. Açıq açar *G* nöqtəsinin gizli açara skalyar hasili kimi hesablanır ($y = xG$).

Şnorr imzalarına keçid

23 mart 2017-ci ildə Bitcoin Core öz rəsmi veb-saytında hazırkı ECDSA rəqəmsal imza alqoritmindən Şnorr imza alqoritminə keçid planını açıqlamışdı, bu plan **Taproot** softfork-u ilə həyata keçirildi. Taproot 14 noyabr 2021-ci ildə Bitcoin-in protokoluna əlavə edilib və SegWit (2017) yenilənməsindən sonra ən

böyük texniki inkişaf hesab olunur. O, Bitcoin şəbəkəsində təhlükəsizlik, gizlilik və effektivliyi artıran ən mühüm yenilənmələrdən biridir.

Taproot, üç texniki təkmilləşdirməyə əsaslanır:

1. Schnorr imza alqoritmi
2. MAST (Merkelized Abstract Syntax Tree)
3. Tapscript – yeni skript dili.

MAST – Taproot (BIP 341) ilə Bitcoin şəbəkəsinə əlavə edilib. Əməliyyatı yerinə yetirmək üçün bir neçə skript variantı yaradılır. Hər skript Merkle ağacının bir yarpağı kimi saxlanılır. İstifadəçi yalnız istifadə etdiyi skripti və onun Merkle sübutunu təqdim edir. Blokçeyndə yalnız lazım olan skript hissəsi görünür.

Schnorr imza sxemi elliptic əyrilər kriptoqrafiyasına əsaslanır və üç əsas mərhələdən ibarətdir (BIP340 və ya BIP-Schnorr-da təsvir olunur):

1. Açar cütünün yaradılması
2. İmzanın yaradılması
3. İmzanın yoxlanması

1. Açar cütünün yaradılması

İstifadəçi öz gizli açarını seçir və onunla açıq açarını yaradır.

- Gizli açar: x – təsadüfi seçilən gizli ədəddir (məsələn, 256-bit ədəd).
- Açıq açar: $P = xG$ – gizli açarın G nöqtəsinə vurulması ilə alınır.

burada G – elliptik əyri üzərində təyin olunmuş ***generator*** nöqtədir**.**

2. İmzanın yaradılması

İstifadəçi m məlumatını imzalamaq istəyir.

1. Təsadüfi ədəd (nonce) yaradılır:

İmzanı yaratmaq üçün təsadüfi k ədədi seçilir. k – təhlükəsizlik üçün hər dəfə fərqli seçilməlidir.

2. İmza nöqtəsi hesablanır:

$R = kG$, burada R nöqtəsi elliptik əyri üzərində hesablanır.

$r = X(R)$, burada R-in X koordinatı $(mod\ q)$ götürülür.

3. Heş hesablanır:

Bitcoin kimi sistemlərdə SHA-256 heş funksiyası istifadə olunur:

$e = H(r \parallel P \parallel m)$

burada $r - X(R)$, P – imzalayan şəxsin açıq açarı, m – imzalanan məlumatdır.

24. İmza yaradılır:

$s = k + eX \bmod q$

İmza $\sigma = (r, s)$ cütlüyüdür.

3. İmzanın yoxlanması

İmzanı qəbul edən şəxs **(**r, s, P, m) verilənlərini yoxlayır.

3.1. Yenidən imza nöqtəsi hesablanır:

$$\boldsymbol{e = H(r \parallel P \parallel m)}$$

$$R' = sG - eP$$

Burada G – generator nöqtədir, P – imzalayan şəxsin açıq açarıdır, sG – elliptik əyri üzərində yeni nöqtədir. eP çıxılaraq *orijinal imza nöqtəsi* bərpa edilir.

3.2. Heş yoxlanır:

$$e' = H(X(R') \parallel P \parallel m)$$

Əgər $e' = e$ olarsa, ***imza doğrudur*** və məlumatın həqiqi olduğu təsdiqlənir.

Schnorr imzalarının üstünlüyü aşağıdakılardır:

- Multi-imza (Multi-Signature, MultiSig) əməliyyatlarını sadələşdirir.
- Bir neçə imzanı bir imzaya birləşdirir (imzaların aqreqasiyası).
- Gizlilik artır – hansı əməliyyatın multi-imza olduğu bilinmir.
- Daha az blok sahəsi istifadə olunur – əməliyyat haqları azalır.

5.3. Kriptovalyutalarda multi-imza sxemləri

Məlumdur ki, Bitkoin şəbəkəsində tranzaksiyalar geriyə dönməzdir, yəni onları ləğv etmək və ya geri qaytarmaq mümkün deyil. Əgər alıcının və ya satıcının niyyətinə şübhəniz varsa, onda hansısa müdafiə mexanizmi yaratmaq olarmı ki, sizi aldanmaqdan qoruya bilsin? Çıxış yolu – multi-imzalardır. Multi-imza əlavə imzanın hesabına pulqabıların təhlükəsizliyini gücləndirməyə xidmət edir. Əlavə imzanı üçüncü tərəf qoymalıdır, əks halda pulqabına daxil olmaq mümkün olmur.

Multi-imza sxemi ilk dəfə 2012-ci ildə təqdim olunub, lakin texniki xüsusiyyətləri səbəbindən yalnız 2014-cü ildə geniş tətbiq olunmağa başlanıb.

Multi-imza (ing. *multisignature*) – elektron imzanın reallaşdırılması sxemlərindən biridir, onun həqiqiliyi üçün *n* üzvdən ibarət qrupdan *m* üzvün imzası tələb edilir ($m < n$, "m-of-n").

2-of-3 multi-imza variantı çox geniş yayılıb. (*Çox zaman "imza" əvəzinə "açar" sözü işlədilir.*)

2-of-3 multi-imzası belə işləyir:

- 3 nəfərin hər birinin gizli açarı var.
- Əməliyyatı təsdiqləmək üçün ən azı 2 nəfərin imzası lazımdır.
- Əgər yalnız 1 nəfər imzalayarsa, əməliyyat baş tutmayacaq.

Multi-imzanın iş prinsipi alqı-satqı əməliyyatına nəzarətedici üçüncü şəxsin – hakimin daxil edilməsindən ibarətdir. Əməliyyatın birbaşa tərəfləri alqı-satqı haqqında razılaşdıqdan sonra onların və hakimin açıq açarları əsasında yeni ünvan generasiya edilir və onları heç kim dəyişdirə bilməz.

Bitkoində P2SH multi-imza mexanizmi var. Ethereum bu məqsədlə bir imza ilə əlavə ünvanlardan istifadə edir, onlara ağıllı müqavilələr nəzarət edir. Bu prosesi mürəkkəbləşdirsə də, proqramçılar üçün böyük çeviklik təmin edir.

Bitkoin multi-imzalarının əsas üstünlüklərinə aşağıdakıları aid etmək olar:

- Alqı-satqının təhlükəsizliyi yüksəlir.
- Müqavilənin şərtləri pozulduqda vəsaiti qaytarmaq imkanı var.
- Müxtəlif qruplarda (şirkətlər, maliyyə təşkilatları və s.) istifadə edilə bilər.

Multi-imzaların əsas nöqsanı ondan ibarətdir ki, tranzaksiya və əməliyyatlara üçüncü şəxs qoşulur. Onun yalnız nəzarətçi olmasına baxmayaraq, bir çoxları bu ideyanı bəyənmir, çünki bu, kriptovalyutaların təbliğ etdikləri demərkəzləşməni qismən pozur.

Kriptovalyuta pulqabılarının bir çoxunda multi-imza funksiyası mövcuddur. Multi-imza pulqabılar qurmaq üçün Electrum, Specter Wallet, Bitcoin Core, BlueWallet, Unchained Capital & Casa platformalarını istifadə etmək olar. Müxtəlif istehsalçılar onu fərqli şəkildə reallaşdırırlar. Bəziləri gizli açarları bilavasitə istifadəçidə saxlamağı təklif edir. Bəzi həllər gizli açarın surətini özündə saxlayır, onun pul göndərmək hüququ yoxdur, məqsəd açar itirildikdə onu bərpa edə bilməkdir.

5.4. Sıfır biliklə isbat protokolları

Təhlükəsizliklə yanaşı, blokçeynlərdə gizliliyin təmin edilməsi məsələsi də çox vacibdir və ilk blokçeyn – Bitcoin də bu məsələni həll etməyə çalışırdı. Lakin Bitcoin tranzaksiyaları tam anonimliyi təmin edə bilmir və tam anonimliyi təmin etdiyini iddia edən bir sıra altkoinlər yaradılmışdır.

Blokçeynlərdə anonimliyin təmin edilməsində *sıfır biliklə isbat protokolları*ndan istifadə edilir.

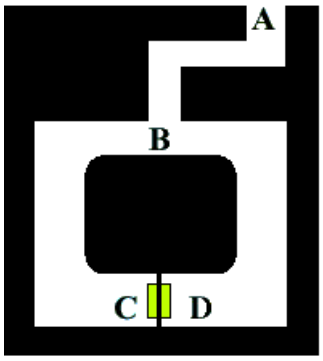
Sıfır biliklə isbat protokolları 1980-ci illərdən tədqiq olunur. Sıfır bilik isbatında iki tərəf iştirak edir: isbat edən (P) və yoxlayan (V). Sıfır biliklə isbatın məqsədi odur ki, yoxlayan isbat edənin müəyyən gizli parametri bildiyinə əmin olsun və isbat edən bu zaman heç bir məlumat açıqlamasın.

Sıfır biliklə isbat protokolunu izah etmək üçün "Ələddinin mağarası" kimi məşhur modelə baxaq.

Fərz edək ki, P deyir ki, o, Ələddinin mağarasında **C-D** qapısını açan (şəkil 1) sehirli sözü bilir və bunu ona inanmayan V-yə isbat etmək istəyir. Bu zaman P istəmir ki, V bu sözü öyrənərək mağaranın sirrini ələ keçirməsin.

Bunun üçün P və V aşağıdakı protokola uyğun addımları yerinə yetirirlər:

1. V **A** nöqtəsində qalır.
2. P mağaraya girir və **B** nöqtəsində sola və ya sağa dönür (V onu görmədiyindən, onun məhz hansı tərəfə döndüyünü bilmir.
3. V **B** nöqtəsinə keçir.
4. V xahiş variantını təsadüfi seçərək mağaraya qışqırıb P-dən **A** tərəfdən və ya **B** tərəfdən qayıtmağı xahiş edir.
5. V onun xahişini yerinə yetirir (əgər qapıdan digər tərəfə keçibsə sehirli sözdən istifadə edərək).



1-5 addımları *n* dəfə yerinə yetirilə bilər, əgər bu zaman V öz xahiş variantını həqiqətən təsadüfi seçirsə, (yəni P onu qabaqcadan tapa bilməz), o, əmin ola bilər ki, P doğrudan da sehirli sözü bilir (təsadüfi üst-üstə düşmə ehtimalı 2^{-n}-dir).

Sıfır bilik isbatları interaktiv və qeyri-interaktiv olurlar. İlk sıfır bilik isbatı protokolları interaktiv idi, yəni verifikasiya prosesində sübut edən və yoxlayan tərəflər bir neçə məlumat mübadiləsi edirlər. Qeyri-interaktiv isbat sübut edənlə hər hansı qarşılıqlı əlaqə olmadan, verilənlər bloku əsasında həyata keçirilir.

Hazırda blokçeynlərdə sıfır biliklə isbatın iki sxemi daha geniş tətbiq edilir: zk-SNARK və zk-STARK.

1) zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge – sıfır biliklə biliyin qısa qeyri-interaktiv arqumenti) protokolu Zcash-da, blokçeynə əsaslanmış JP Morgan Chase ödəniş sistemində və serverlərdə müştərilərin autentifikasiyasında istifadə edilir, Ethereuma da inteqrasiya edilib. "Qısa" termini onu bildirir ki, sübutların ölçüsü kiçikdir (bir neçə yüz bayt) və onları tez yoxlamaq olar. zk-SNARK qeyri-interaktiv protokoldur, sübut edən və yoxlayan yalnız bir sübut mübadilə edir. Bu protokolda tərəflər arasında başlanğıc etibarlı kökləmə, yəni açıq parametrlər tələb edilir. Adətən, bu mərkəzləşmə problemi yaradır, çünki parametrlər çox zaman çox böyük olmayan kiçik qruplar üçün formalaşdırılır. "Argument" termini zk-SNARK-ın hesablamalarla əsaslandırılmış olmasını nəzərdə tutur, yəni bədniyyətli yoxlayanın sistemi aldatmaq ehtimalı çox kiçikdir. Bu xassə "möhkəmlik" kimi tanınır və yoxlayanın məhdud hesablama gücünə malik olmasını fərz edir. Nəzəri olaraq, yetərli hesablama gücünə (məsələn, kvant kompüterlərə) malik olan yoxlayan saxta sübutlar yarada bilər. Qeyd edək ki, Zk-SNARK-da elliptik əyrilər kriptoqrafiyası tətbiq edilir və bu kriptoqrafik alqoritmlər kvant kompüterlərə qarşı zəif hesab olunurlar.

2) zk-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge – sıfır biliklə biliyin miqyaslanan şəffaf arqumenti) 2018-ci ildə təklif

edilib. zk-STARK şəffaf protokoldur, yəni məxfi məlumatların üçüncü tərəfə açıqlanmasını tələb etmir. Zk-SNARK ilə müqayisədə sübut verilənlərinin ölçüsü böyük olsa da, informasiya mübadiləsi prosesi çox sürətlidir. zk-STARK post-kvant kriptoqrafiyasından istifadə edir, bunun sayəsində kvant kompüterləri əsasında hücumlara daha dayanıqlı hesab olunurlar.

5.5. Anonimliyi təmin edən kriptovalyutalar

Tətbiq sahəsindən asılı olaraq, anonimliyin təmin edilməsini müxtəlif cür həll etmək olar. Anonimliyin təmin olunmasına görə kriptovalyutaları iki sinfə bölürlər:

1. *Tam anonim olmayan kriptovalyutalar* – tranzaksiyaları izləmək mümkündür (məsələn, Bitcoin, Litecoin, Ethereum);
2. *Tam anonim kriptovalyutalar* – tranzaksiyaları izləmək mümkün deyil (məsələn, Dash, Zcash, Monero).

Zcash – Bitkoin-dən daha təhlükəsiz olması iddia edilən kriptovalyutadır. Bu kriptovalyuta sıfır bilik verməklə isbat alqoritmindən istifadə edir. Zcash-da olan bu alqoritm konfidensiallığı təmin etmək üçün Ethereum-un Bizans adlı forklarına da əlavə edilib. Bu metod bəzi tərəflərə tranzaksiyaları görmək imkanı verir, bütün digərləri üçün isə bağlayır.

Zcash – öz sələflərindən anonimliyinə görə fərqlənən kriptovalyutadır. Onun layihəsi hələ 2014-cü ildə başlanmışdı (rəhbəri Ziko Uilkokos), lakin yalnız 2016-cı ildə layihə ictimaiyyətə təqdim edildi.

Tam anonimliyə nail olmaq üçün zk-SNARK protokolu istifadə edilir, onun köməyi ilə istifadəçilər həm anonim, həm də açıq tranzaksiyalar etmək imkanı əldə edirlər. Bunun üçün, pulqabı yaradılanda iki açar: açıq və gizli açar verilir.

Zcash şəbəkəsində diqqətçəkən mexanizmlərdən biri "sıfırlayıcıların" istifadə edilməsidir, onlar tranzaksiya həyata keçirildikdən dərhal sonra onun haqqında bütün məlumatları pozurlar.

Sikkələrin maksimal sayı Bitkoindəki kimi 21 milyon götürülüb. Bir blokun generasiyası müddəti 2,5 dəqiqədir, bu, Bitkoin şəbəkəsindən 4 dəfə sürətlidir. Yaradılmış hər bir blok üçün mükafat 12,5 Zcash sikkəsidir, onlardan 2,5 sikkə Zcash yaradıcılarına verilir.

Zcash kriptovalyutasında **Equihash** heş alqoritmi istifadə edilir (həmçinin Bitcoin Gold və s.). Kifayət qədər mürəkkəb heş funksiyadır və hesablanması üçün böyük operativ yaddaş tələb edir. GPU-mayninq üçün optimallaşdırılıb. Prinsipcə, Bitcoin Gold və Zcash-də PoW-un xüsusi növü tətbiq edilib (aksent hesablamaların sürətinə deyil, operativ yaddaşın həcminə edilir).

Monero (XMR) – tam anonimliyə iddia edən kriptovalyutalardan biridir, gizliliyi təmin etmək üçün halqa imzalarını tətbiq edir. Monero-nun əsasında

CryptoNote protokolu dayanır, əlavə olaraq, CryptoNight heş alqoritmi də istifadə edilir. CryptoNote fərdi məlumatların gizlədilməsi üçün qrup imzalarından və birdəfəlik açarların köməyi ilə əlaqələndirilə bilməyən tranzaksiyalardan istifadə edir. Qrup imza sxemlərində imzanın yoxlanması üçün bir neçə müxtəlif açıq açardan istifadə etmək olar. Qrupun hər bir üzvünün məxsusi gizli açarı və açıq açarı var. Qrupun istənilən üzvü öz gizli açarı ilə imzalaya bilər, imzanı yoxlayan şəxs isə kimin imzalandığını dəqiq müəyyən edə bilmir.

CryptoNote protokolunda göndərən tərəf təsadüfi verilənlərdən istifadə edir. Bunun nəticəsində hətta bütün tranzaksiyalarda göndərən və alan dəyişməsə belə, müxtəlif birdəfəlik açarlar istifadə edilir. Bundan başqa, hətta göndərən və alan eyni bir şəxs olduqda belə, bütün birdəfəlik açarlar tamamilə unikal olurlar.

Özünü yoxlamaq üçün suallar

1. Bitkoində imza üçün hansı alqoritm istifadə edilir?
2. Monero anonimliyi təmin etmək üçün hansı imza sxemindən istifadə edir?
3. Zcash tam anonimliyə nail olmaq üçün hansı protokoldan istifadə edir?
4. SHA-256 Bitkoin şəbəkəsinin hansı hissələrində istifadə olunur?
5. Multi-imza nədir?
6. Multi-imzaların hansı növü daha çox istifadə edilir?
7. ECDSA sxemində gizli və açıq açar generasiyasının alqoritmi necədir?
8. Bitkoin multi-imzalarının əsas üstünlüklərinə nələrdir?
9. Multi-imzanın əsas nöqsanı nədir?
10. P2SH multi-imza mexanizmi nədir?
11. Equihash heş alqoritminin əsas xüsusiyyəti nədir?
12. Equihash heş alqoritmi hansı kriptovalyutada istifadə edilir?
13. Sıfır biliklə isbat protokolunun mahiyyəti nədir?
14. Hansı kriptovalyutalar anonimliyi tam təmin etdiyini iddia edir?
15. ECDSA alqoritmində hansı əyrilər istifadə edilir?
16. zk-SNARK protokolu interaktiv, yoxsa qeyri-interaktivdir?
17. zk-SNARK protokolunda “Succint” (qısa) termini nəyi bildirir?
18. zk-SNARK protokolunda “Argument” termini nəyi nəzərdə tutur?
19. CryptoNote fərdi məlumatları gizlətmək üçün hansı imzalardan istifadə edir?
20. zk-STARK protokolunda “Transparent” termini nəyi bildirir?
21. zk-STARK protokolunda “Scalable” (miqyaslanan) xassəsi nəyin hesabına əldə olunur?

Mühazirə 6. Kriptovalyuta pulqabıları

6.1. Kriptovalyuta pulqabılarının mahiyyəti

Kriptovalyuta pulqabılarında, adi pulqabılar kimi gözləmək olardı ki, kriptovalyutalar saxlanacaq. Lakin onlarda hər hansı kriptovalyuta saxlanmır, kriptovalyutalar blokçeyndə saxlanır. Kriptovalyuta pulqabısı istifadəçilərə blokçeyn şəbəkələri ilə qarşılıqlı əlaqə saxlamağa imkan verən alətdir. Onlar Bitkoin və digər kriptovalyutaları blokçeyn tranzaksiyaları vasitəsilə almaq və göndərmək üçün məlumat generasiya edirlər.

Texniki baxımdan, pulqabı – gizli açarlar üçün konteynerdir. Kriptovalyuta pulqabılarının əksəriyyəti bir və ya bir neçə gizli və açıq açar cütü generasiya edə bilir. Açıq açar pulqabı ünvanını generasiya etmək üçün istifadə edilir, onlar ödənişləri almaq üçün lazımdır. Gizli açarlar rəqəmsal imzaların generasiyası və tranzaksiyaların verifikasiyası üçün istifadə edilir. Gizli açarlar hansı pulqabıdan istifadə etdiyinizdən asılı olmayaraq, sizə kriptovalyutalara giriş verir.

Bitkoin-də açarların generasiyasının ən sadə üsulu determinik generasiya üsuludur. Bu üsulda hər bir yeni gizli açar əvvəlki gizli açardan kriptoqrafik heş funksiyanın köməyi ilə alınır, onlar ardıcıllıq əmələ gətirirlər. Qeyri-determinik üsulda isə açarlar təsadüfi generasiya edilir.

Determinik pulqabılar. Gizli açarlar kriptoqrafik heş funksiya istifadə etməklə ortaq sid (ing. seed) əsasında yaradılır. Sid – təsadüfi ədəddir, digər verilənlər, məsələn, indeks nömrələri əsasında gizli açarlar yaratmağa imkan verir.

Determinik pulqabı üçün *sid-sözlərdən* (ing. seed-phrase) istifadə edirlər. Onlar ilk dəfə BIP39-da daxil edilib. BIP39 söz siyahısında 2048 söz var. Sid-sözlər pulqabıların ehtiyat nüsxəsini yaratmaq üçün asan yoldur. Əgər pulqabınıza girişi itirsəniz, vəsaitinizi bərpa etmək üçün sid-sözləri istənilən BIP32-uyarlı pulqabına yükləmək olar.

Bir çox istifadəçi öz gizli açarlarını itirir, bunun nəticəsində onlar öz rəqəmsal pullarına giriş əldə edə bilmirlər. Gizli açarları bərba etmək üçün sid-sözləri xüsusi diqqətlə saxlamaq və qorumaq lazımdır.

Sid-sözlər. Sid-sözlər (onlara *mnemonik kodlar* da deyirlər) – ingilis sözlərinin ardıcıllığıdır, onlar təsadüfi ədədi təsvir edirlər (kodlaşdırırlar).

Sid-sözlərin yaradılması alqoritmi (BIP39) belədir:

1. Uzunluğu 128 bitdən 256 bitə kimi olan təsadüfi ardıcıllıq (entropiya) generasiya edilir.
2. Onun SHA256 heşindən ilk bir neçə bit götürülərək təsadüfi ardıcıllığın nəzarət cəmi yaradılır.

3. Nəzarət cəmi təsadüfi ardıcıllığın sonuna əlavə edilir.
4. Ardıcıllıq uzunluğu 11 bit olan hissələrə bölünür və əvvəlcədən müəyyən edilmiş 2048 sözdən ibarət lüğətdə indeks kimi istifadə edilir.
5. 12-24 söz alınır və onlar sid-sözlər kimi istifadə edilir.

Məsələn, "*forget wing follow flip swallow achieve correct view dinner witness hybrid proud*".

BIP39 söz siyahısında sözlərin sayı 2048-dir, buna görə 12 sözdən ibarət sətirdə 128 təhlükəsizlik biti olur. Bu o deməkdir ki, bədniyyətli 12 sözdən ibarət toxumu təxmin etmək üçün 2^{128} əməliyyat yerinə yetirməlidir. Bu olduqca böyük ədəddir.

İyerarxik determinik pulqabılar (BIP32/ BIP44). İyerarxik determinik pulqabılarda açar ağacşəkilli struktur formasında saxlanır, buna görə valideyn açardan törəmə açarlar ardıcıllığı almaq olar. Öz növbəsində, onların hər birindən də törəmə açarların ardıcıllığı alınır və s. Prosesi dərinliyə məhdudiyyət qoymadan davam etdirmək olar.

6.2. Kriptovalyuta pulqabılarının növləri

Kriptovalyuta pulqabıların üç əsas növü var: proqram, aparat və kağız pulqabıları. Onları həmçinin işləmə üsuluna görə *soyuq pulqabı* və *isti pulqabı* kimi də təsnif edirlər. İsti pulqabılar İnternetə qoşula və beləliklə, hücumlara daha çox məruz qala bilərlər. Soyuq pulqabılarda açarlar hər hansı İnternet bağlantısı olmadan generasiya edilir, buna görə kiberhücumlara daha dayanıqlıdırlar.

Proqram pulqabılarının veb, desktop və mobil pulqabılar kimi növləri var.

Veb pulqabı – mahiyyətcə, brauzer interfeysidir, istifadəsi daha rahatdır, lakin eyni zamanda daha təhlükəlidirlər, çünki gizli açarları üçüncü tərəf idarə edir. Veb pulqabılara misal: MetaMask, MathWallet, Binance Chain Wallet.

Desktop pulqabı – kompüterə yüklənən proqram təminatıdır. Veb pulqabılarına nisbətən daha təhlükəsizdirlər, çünki gizli açarları istifadəçi özü idarə edir. Desktop pulqabılara misal: Electrum, Exodus.

Mobil pulqabılar – desktop pulqabılarına oxşardır, lakin smartfonlar üçün dizayn edilib. QR kodların istifadəsi onları çox rahat alternativə çevirir. Mobil kriptopulqabılara misal: TrustWallet, MetaMask.

Aparat pulqabıları – İnternetə heç bir qoşulma olmadan açarları generasiya edən və saxlayan fiziki cihazlardır. Adətən, açarlar təsadüfi ədədlər generasiya edən alqoritmlər əsasında yaradılır və cihazın özündə saxlanır. Məhdud əlçatanlığı nöqsan olsa da, aparat pulqabıları çox təhlükəsiz hesab edilir.

Kağız pulqabı – üzərində blokçeyn ünvanı və ona uyğun gizli açar olan kağızdır. Adətən, açarlar rəqəm və hərflərin uzun sətri kimi QR kod ilə birlikdə çap olunur. Onları skan edərək tranzaksiyaları yerinə yetirmək olar. Kağız pulqabıların istifadəsi köhnəlmiş və təhlükəli hesab edilir.

6.3. Bitkoin-də pulqabı ünvanları

Bitkoin-ünvanı 1 və ya 3 ilə başlayan və 27-34 latın hərf-rəqəm simvolundan ibarət identifikatordur (hesab nömrəsidir). Bitkoin ünvanını QR-kod şəklində də göstərmək olar. Bu ünvanlar anonimdirlər və sahibi haqqında heç bir məlumat daşımırlar. Bitkoin ünvanını pulsuz, məsələn, Bitcoin proqram təminatından istifadə etməklə əldə etmək olar.

Bitcoin-ünvana nümunə: **1BAL8xV4wgDvt94DeKTWx4Uxqkg6sjjKLc**

Bitkoin-ünvanda **0** (sıfır), **O** (böyük o), **I** (böyük i), **l** (kiçik L) kimi simvollar olmur, bu şərt ünvanı əllə yazanda həmin simvolları qarışdırmamaq üçün edilib.

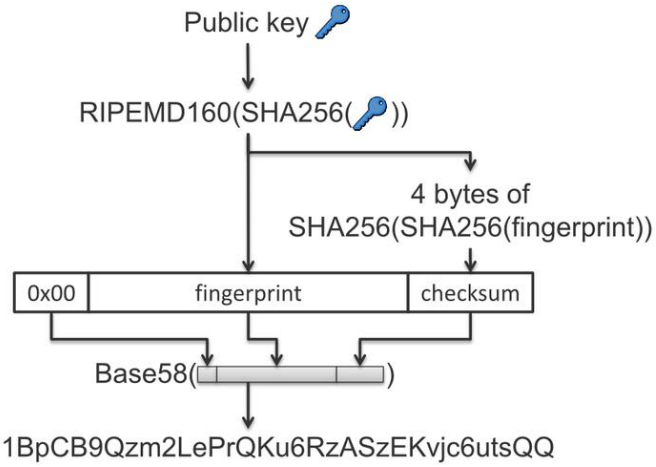
Hazırda Bitkoin-ünvan formatlarının iki növü geniş istifadə edilir:

- P2PKH (Pay-to-Pubkey Hash) ünvanı “1” simvolu ilə başlayır.
- P2SH (Pay-to-Script Hash) ünvanı “3” simvolu ilə başlayır. Məsələn, 35bSzXvRKLpHsHMrzb82f617cV4Srnt7hS.

Hər bir istifadəçinin qeyri-məhdud sayda ünvanı ola bilər, bunu tranzaksiyaların anonimliyini artırmaq üçün tövsiyə edirlər. Pulqabı ünvanı, mahiyyətcə, blokçeyndə xüsusi “yerləşmə yeri”dir ki, ora pul göndərmək olar.

İstifadəçinin bütün Bitkoin-ünvanları onun pulqabındakı açıq açarından xüsusi alqoritmlə generasiya edilir, buna görə yaradılmış ünvanlardan istənilən birinə göndərilmiş bitkoinlər balansda əks olunurlar. Bundan başqa, Bitkoin-ünvanda yoxlama kodu da olur, buna görə bitkoinləri düzgün olmayan ünvana göndərmək mümkün deyil. Lakin əgər ünvan düzgün formalaşdırılıbsa, lakin onun sahibi yoxdursa (və ya sahibi wallet.dat pulqabı faylını itiribsə), bu ünvana göndərilmiş bitkoinlər həmişəlik itiriləcək.

Bitkoin pulqabı-ünvanının generasiyası sxemi şəkildə göstərilib.



1. Açıq açar götürülür.
2. Açıq açarın SHA-256 ilə heş-kodu hesablanır.
3. Alınmış heş-koddan RIPEMD-160 ilə yeni heş hesablanır.
4. RIPEMD-160 heşinin qarşısına şəbəkənin identifikator-baytı əlavə edilir (0x00 əsas şəbəkə üçün).
5. Genişlənmiş RIPEMD-160 heşinə SHA-256 tətbiq edilir.
6. Əvvəlki SHA-256 heşə təkrar SHA-256 tətbiq edilir.
7. Alınmış heşin ilk 4 baytı götürülür.
8. Bu 4 bayt Addım 4-dəki genişlənmiş RIPEMD-160 heşinə əlavə edilir. Bu 25-baytlıq binar Bitkoin-ünvandır.
9. Addım 8-in nəticəsi Base58 sətrinə çevrilir. Bu Bitkoin-ünvanın ən çox istifadə edilən formatıdır.

Özünü yoxlamaq üçün suallar

1. Kriptovalyuta pulqabılarının hansı növləri var?
2. Bitkoin-ünvanın generasiyası zamanı hansı heş funksiyalar istifadə edilir?
3. Bitkoin pulqabı-ünvan formatlarının hansı növləri var?
4. Bitkoin pulqabı-ünvanı hansı açardan generasiya edilir?
5. Bitkoin pulqabı-ünvanı neçə baytdır?
6. Veb pulqabının təhlükəli olması nə ilə əlaqəlidir?
7. Mobil kriptovalyuta pulqabılarına hansı misallar göstərmək olar?
8. Bitkoin pulqabı-ünvanının generasiyası sxemini izah edin.
9. Sid-sözlərin yaradılması alqoritmini (BIP39) izah edin.
10. Bitkoin-ünvanda hansı simvollar olmur?
11. Hansı Bitkoin ünvanı “3” simvolu ilə başlayır?
12. İsti pulqabılar necə işləyir?

13. Bir istifadəçinin neçə pulqabı ünvanı ola bilər?
14. İyerarxik determinik pulqabılarda açar hansı strukturda saxlanır?
15. Bitkoin-də açarların generasiyasının hansı üsulları var?
16. Pulqabıların ehtiyat nüsxəsini yaratmaq üçün hansı məlumatlardan istifadə edilir?
17. BIP39 söz siyahısında neçə söz var?
18. Kriptovalyuta pulqabısı hansı funksiyanı yerinə yetirir?
19. Bitkoin-də açarların generasiyasının ən sadə üsulu hansıdır?
20. Sid-sözlər ilk dəfə hansı sənəddə daxil edilib?

Mühazirə 7. Altkoinlər və stabilkoinlər

7.1. Altkoinlərin təsnifatı

Bitkoin "rəqəmsal qızıl" kimi tanınır və ən məşhur kriptovalyutadır. Bununla belə, onun bir çox alternativləri də vardır. Bitkoindən başqa bütün digər kriptovalyutaları ***altkoin*** ("**alt**ernativ+**koin**") adlandırırlar. Altkoinləri Bitkoinin alternativləri adlandırırlar, çünki altkoinlərin əksəriyyəti ya Bitkoini əvəz etməyi, ya da onun parametrlərindən ən azı birini yaxşılaşdırmağı hədəfləyirlər.

Hazırda 10 minlərlə altkoin var, hər gün yeni altkoinlər meydana çıxır. Altkoinlərin çoxu Bitkoinin sadəcə klonlarıdır ("fork"udurlar), onun 1-2 xarakteristikasını, məsələn, blokun uzunluğunu, tranzaksiyaların sürətini, tokenlərin paylanması metodunu və ya mayninq alqoritmini dəyişməyə cəhd edirlər. Hətta CountepParty və MasterCoin kimi bəzi altkoinlər öz işləri üçün Bitkoin blokçeynindən istifadə edirlər.

Tarixən ilk altkoin 2011-ci ildə təqdim olunmuş Namecoin (NMC) olmuşdur. Valyuta olsa da, onun yaradılmasının əsas məqsədi domen adlarının qeydiyyatı (DNS) sahəsində demərkəzləşmə etməkdir, bu, dövlət tərəfindən İnternetin senzurası prosesini daha çətin edir. Hazırda Namecoin bazar kapitallaşması üzrə altkoinlər arasında 200-cü yerləri tutur.

Bəzi altkoinlərin yaradılması zamanı Bitkoin ilkin kodunda əhəmiyyətli dəyişikliklər edilir. Məsələn, Darkcoin tamamilə anonim tranzaksiyalar təmin etməyə çalışır, Bitshares isə özünü kriptovalyutalar üçün Nyu-York fond birjasının (Uoll Stritin) oxşarı kimi təqdim edir. 2011-ci ildə meydana çıxan Ripple-də özünəməxsus konsensus protokolu istifadə edilir və mayninq prosesi yoxdur. Ripple kriptovalyuta dünyasında ilk "fork olmayan" valyuta hesab edilir.

Qeyd edildiyi kimi, hazırda altkoinlərin sayı bir neçə minə çatır. Həm kriptovalyutalarla ötəri maraqlanan adi istifadəçilər, həm də kriptovalyutalara yatırım qərarı vermək istəyən investorlar üçün altkoinlərin təsnifatı çox faydalı olardı. Altkoinləri aşağıdakı siniflərə bölmək mümkündür:

- Tam anonim olmayan altkoinlər – tranzaksiyaları izləmək mümkündür. Misallar: Litecoin, Ethereum, Cardano, NEO.
- Tam anonim altkoinlər – tranzaksiyaları izləmək mümkün deyil. Misallar: Dash, Zcash, Monero.
- Sürətli və ucuz tranzaksiyalar üçün yaradılmış altkoinlər. Misallar: Ripple, NEM, Stellar, Nano (RaiBlocks).
- Stabil-koinlər – real valyutalara bağlı kriptovalyutalar. Misallar: Tether, TrueUSD, Basecoin.

7.2. Kriptovalyutalarda hardfork və softfork

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

Fork (ing. «çəngəl») – proqram təminatında məhsulun hər biri müstəqil inkişaf etdirilən bir neçə paralel budağa ayrılmasıdır və ya çoxdan mövcud olanın əsasında yeni məhsulun buraxılmasıdır.

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

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

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

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

Hardforkun səbəbləri də softforkun səbəbləri ilə oxşardır, yaradıcıları kriptovalyutanın iş qaydalarına müvafiq dəyişikliklər etmək istəyirlər. Fərq ondadır ki, hardfork zamanı onlar mövcud sistemi yeniləmək yox, "blokçeyni və maynerləri olan öz Bitcoin"lərini yaratmaq istəyirlər.

Bitkoin üçün ən məşhur hardfork **Bitcoin Cash** hesab olunur. Yeni valyuta blokun ölçüsünün 1 MB-dan 8 MB-a artırılması ilə fərqlənir. Bu tranzaksiyaları daha sürətlə yerinə yetirməyə imkan verir, lakin köhnə sistemlə uyarlıq itir.

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

7.3. Litecoin (LTC) kriptovalyutası

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

Litecoin-in əsas xüsusiyyətləri:

- Yeni blokların generasiyası sürəti artırılıb. Əgər Bitkoin şəbəkəsində bir blok təxminən hər 10 dəqiqədə yaradılırsa, Litecoin-də hər 2.5 dəqiqədə yaradılır;
- Tranzaksiyaların təsdiqlənməsi sürəti artırılıb. Əgər Bitkoin şəbəkəsində tranzaksiya 1 saatdan 2 sutkaya kimi çəkirsə, Litecoin şəbəkəsində tranzaksiya praktiki olaraq ani yerinə yetirilir;
- GPU istifadə etməklə mayninq etmək olar;
- Litecoin ümumi emissiyası 84 milyon LTC-dir;
- Atomar tranzaksiyaların edilməsi (müxtəlif blokçeynlərdən olan kriptovalyutaların mübadiləsi) mümkündür;

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

2017-ci ilin mayında Blockstream işçiləri Lightning Network istifadə etməklə əsas Litecoin şəbəkəsində tarixdə ilk dəfə həcmi 0.00000001 LTC olan mikro-tranzaksiyasını həyata keçirmişdilər. Bu tranzaksiya **1 saniyədə** yerinə yetirilmişdi.

2017-ci ilin sentyabrında Charlie Lee Decred/Litecoin və Litecoin/Vertcoin şəbəkələri arasında bir neçə mikro-tranzaksiya etmişdi. Bir qədər sonra 10 LTC kriptovalyuta 0.1137 BTC-yə mübadilə edilmişdi. Bütün bunlar göstərir ki, Lightning Network yaxın zamanlarda üçüncü şəxslər olmadan müxtəlif blokçeynlərdən olan kriptovalyutaların mübadiləsi üçün yol açacaq.

7.4. Dash (DASH) kriptovalyutası

Dash − Bitkoinin forklarından biridir, 2014-cü ildə bazara çıxıb. Digər altkoinlər kimi, Dash da bitkoini təkmilləşdirmək ideyası ilə yaradılıb (Evan Daffild

tərəfindən). Təşəkkül prosesində üç ad dəyişib: əvvəlcə Xcoin, sonra DarkCoin adlanırdı, 2015-ci ildən indiki adını alıb.

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

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

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

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

Bu mexanizm təkrar istifadə problemini həll edir, həm də bu zaman Bitkoində olduğu kimi təsdiqi uzun müddət gözləmək lazım gəlmir. Bunun sayəsində Dash-ın bank sisteminə inteqrasiyası üçün Wirex onlayn-bankinq xidməti ilə müqavilə imzalanıb.

DAO – layihədə demərkəzləşmə təkcə iştirakçıların bərabərhüquqlu olmasl ilə deyil, şəbəkənin inkişafına təsir etmək imkanı ilə də təmin edilir. Masternodlar öz təkliflərini verə və səsvermədə iştirak edə bilərlər. Layihənin səsverməyə çıxarılmasının qiyməti 5 sikkədir. Məsələn, bu yolla blokun ölçüsünün 1-dən 2 MBayta artırılması qərarı bir sutkada qəbul olunmuşdu. Digər kriptovalyutalarda isə belə məsələlər illərlə müzakirə edilir.

Dash mayninqi. Yeni sikkələrin mədəndən çıxarılması şəbəkə sturukturunun birinci səviyyəsində baş verir. Bitkoin kimi, Dash mayninqinin də çətinliyi artır və bloka görə mükafat azalır. Fərq ondadır ki, Dash kriptovalyutasının çıxarılmasının enerji xərcləri daha azdır. Buna yeni X11 alqoritmi imkan verir, on bir heş-funksiyanın zəncirindən ibarətdir. Dash kriptovalyutasının protokolunda PoS istifadə edilir.

X11 alqoritmi mayninq üçün xüsusi avadanlığın istifadə edilməsinin qarşısını almağa yönəlmişdi. Təəssüf ki, Dash üçün də ASIC yaradılıb və onu Çin saytlarından almaq olar (hazırda ən effektivi *iBeLink*-dir).

Dash mayninqi ilə solo məşğul olmaq, hovuza qoşulmaq da olar. İnternetdə Dash hovuzların siyahısı var. Adətən, hovuzun saytında kalkulyator da olur, o gözlənilən gəliri hesablamağa imkan verir. Gəlir bir çox faktordan asılıdır ki, mayninq kalkulyatorları onları nəzərə almır: Dash kursu, dolların kursu, yeni avadanlığın meydana çıxması. Buna görə hesablamalar təxminidir.

Mayninq gəlirinin bölünməsinin aşağıdakı xüsusiyyətləri var:

- 45% mədənçilərə,
- 45% masternodlara və
- 10% şəbəkənin inkişafına ayrılır.

Masternod olmaq asan deyil. Tam blokçeynlə yanaşı, 1000 token girov da qoymaq lazımdır. Mükafatlar xüsusi pulqabılara köçürülür. Blok üçün mükafat hər 4 ildən bir 2 dəfə azalır.

7.5. Cardano

Cardano (ADA) – PoS konsensus protokolu əsasında qurulmuş blokçeyn protokoludur, böyük enerji xərcləri olmadan tranzaksiyaları təsdiqləyir. Haskell proqramlaşdırma dilində yazılıb. Blokçeyn tokeni ADA-dır və 19-cu əsr riyaziyyatçısı Ada LoveLace şərəfinə adlandırılıb.

2017-ci ilin sentyabrında Ethereum həmtəsisçilərindən Charles Haskinson tərəfindən yaradılıb, 3-cü nəsil blokçeyn hesab edilir (1-ci nəsil Bitcoin, 2-ci nəsil – Ethereum).

Cardano-nun məqsədi yüksək miqyaslanan və enerji sərfi effektiv olan ağıllı müqavilə platforması qurmaq idi.

ADA kriptovalyutasını Coinbase firmasında almaq-satmaq olar. ADA-nın dəyəri saxlamaq (öz kriptoportfelinizin bir hissəsi kimi), ödənişləri göndərmək, almaq, hissə yerləşdirmək və Cardano şəbəkəsində tranzaksiya haqqını ödəmək üçün istifadə etmək olar.

ADA-nı Coinbase birjasında, Coinbase Wallet-də, həmçinin bir sıra digər kriptobirjalarda və pulqabılarda saxlamaq olar.

Cardano blokçeyni iki ayrı laya bölünüb: CSL (Cardano Settlement Layer) və CCL (Cardano Computing Layer). CSL-də hesabların və balansların reyestri olur, burada tranzaksiyalar Ouroboros konsensus mexanizmi ilə təsdiqlənir.

CCL səviyyəsində blokçeyndə icra edilən əməliyyatlar üçün hesablamalar yerinə yetirilir – ağıllı müqavilələrdə əməliyyatlar vasitəsilə. Blokçeyni iki hissəyə bölməkdə ideya – Cardano şəbəkəsində saniyədə milyon tranzaksiya emal etməyə imkan yaratmaqdır.

7.6. Polkadot

Polkadot – istənilən növ verilənlərin və aktivlərin kross-blokçeyn transferlərini mümkün edən protokoldur. Bir neçə blokçeyni birləşdirməklə Polkadot yüksək dərəcədə təhlükəsizlik və miqyaslanma əldə etməyi hədəfləyir. DOT bu blokçeynin idarəetmə tokenidir və onu şəbəkənin təhlükəsizliyini təmin etmək və ya yeni zəncirləri birləşdirmək (“bağlamaq”) üçün istifadə etmək olar.

Polkadot, bir çox post-Bitcoin kriptovalyutası kimi, həm Coinbase kimi birjalar vasitəsilə alına və ya satıla bilən bir tokendir, həm də mərkəziyətsiz protokoldur.

Polkadot protokolu müxtəlif blokçeynlərin bir-biri ilə təhlükəsiz “danışmasına” imkan verməkk üçün nəzərdə tutulub ki, dəyər və ya məlumat heç bir vasitəçi olmadan blokçeynlər arasında axsın (məsələn, Ethereum və Bitcoin arasında). O, bir çox paralel blokçeyndən (və ya “parachain”-dən) istifadə etməklə sürətli və miqyaslanan olmaq üçün nəzərdə tutulmuşdur, paraçeynlər emal yükünün çox hissəsini əsas blokçeynin (“relay chain” adlanırlar) üzərindən götürürlər .

Polkadot şəbəkəsinə həmçinin birləşdirici təbəqə və ya “körpü” də daxildir. Körpülər əksər blokçeynlər arasında dəyər və məlumatların ötürülməsinə imkan verir, onları hətta blokçeyn olmayan verilənlər bazalarına qoşulmaq üçün də istifadə etmək olar.

Polkadot şəbəkəsinin təhlükəsizliyini təmin etmək, tranzaksiyaları yoxlamaq və yeni DOT yaratmaq və yaymaq üçün PoS konsensus mexanizmindən istifadə edir. DOT sahiblərinin steykinq sistemi ilə qarşılıqlı əlaqədə olmasının bir neçə yolu var:
Validator – işin əsas hissəsini görür, şəbəkəni təşkil edən qovşaqlardan birini minimal boşdayanma ilə işlətməli və öz DOT-larının əhəmiyyətli hissəsini steykinq etməlidir. Bunun müqabilində validator tranzaksiyaları yoxlamaq, “relay chain”-nə tranzaksiyaların yeni “bloklarını” əlavə etmək və yeni yaradılmış DOT-ları, tranzaksiya komissiyasının bir hissəsini və “çaypulu” qazanmaq hüququ əldə edir. (Digər tərəfdən, validator həm də zərərli hərəkətlər etmək, səhv etmək və ya hətta texniki çətinliklərlə üzləşmək səbəbindən steykinq etdiyi DOT-ların bir hissəsini və ya hamısını itirə də bilər).
Nominator – adi investorlara steykinq prosesində dolayısı ilə iştirak etməyə imkan verir. Nominator oz DOT-larının bir hissəsini etibar etdiyi validatora həvalə edir. Bunun müqabilində həmin validatorun qazandığı DOT-ların bir hissəsini əldə edir. Validatorun seçimində diqqətli olmaq lazımdır – validator qaydaları pozarsa, nominator da payınının bir hissəsini itirə bilər.
Kollator – etibarlı paraçeyn tranzaksiyalarını izləyir və onları “relay chain” validatorlarına təqdim edir.
Fisherman – şəbəkə daxilində pis davranışları tapır və bu barədə məlumat verir.

Yuxarıdakı rollardan hər hansı biri vasitəsilə DOT mükafatları əldə etmək olar. DOT sahibləri həm də şəbəkənin idarə edilməsində söz sahibidirlər və proqram təminatının təklif olunan təkmilləşdirilməsi ilə bağlı səs verə bilərlər.

7.7. Stabilkoinlər – Stabil kriptovalyutalar

Kriptovalyutaların volabilliyi çox yüksəkdir, bu onları spekylyantlar üçün cəlbedici və geniş istifadə üçün yararsız edir. İdeal kriptovalyuta öz alıcılıq qabiliyyəti baxımından stabilliyini saxlamalı, yaxud kiçik inflyasiyaya məruz qalmalıdır. Belə ideal kriptovalyuta stabilkoin (ing. stablecoin) adlanır. Ən sadə formada stabilkoin fiat valyutasında stabil dəyəri olan adi kriptovalyutadır. Fiat pulları – dəyər nişanlarıdır, həqiqi pulların əvəzedicilərıdir.

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

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

Hazırda bazarda stabilkoinlərin üç növü təmsil olur:

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

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

İkinci metod – kriptovalyutalarla təminat da əvvəlki metoda oxşayır, lakin bu halda stabilkoin ənənəvi aktivlərlə deyil, kriptoaktivlərlə təmin edilir. Kriptovalyutaların volatilliyi nəzərə alınaraq, bu stabilkoinlər çox zaman ehtiyat ilə təmin olunurlar. Yəni 100 $ məbləğində stabilkoin buraxmaq üçün təminat vermək lazımdır – məsələn, ETH ilə 200 $ məbləğında təminat yaratmaq lazımdır. Beləliklə, əgər hətta baza aktivinin qiyməti 20 % düşsə də, stabilkoin öz dəyərini saxlayacaq. Lakin təminatçı aktivi dəyərsizləşdirən görünməmiş hadisə – «qara qu quşu» hadisəsi baş versə, stabilkoin də dəyərini itirəcək və təminatçı daha böyük

zərərə düşəcək, çünki stabilkoinlər izafi ehtiyatla təmin olunublar. Məhz buna görə bəzi ekspertlər belə yanaşmanın əleyhinə çıxış edirlər.

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

Stabilkoin kursunu bir səviyyədə saxlamaq üçün emitentlər onun təklif olunan həcmini ağıllı müqavilələrin köməyi ilə nəzarət edirlər. Bu zaman kriptovalyuta sahibləri gələcək senyorajda pay aksiyaları əldə edirlər. Bu konsepsiya "*seigniorage shares*" adını almışdır. Onu 2014-cü ildə Robert Sems təklif edib və Basecoin və Havven kimi layihələr ona əsaslanır.

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

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

MakerDAO – mərkəziyətsiz avtonom təşkilatdır, onun valyutası ABŞ dollarına bağlıdır, lakin ETH ilə tam təmin olunur. Bir DAI bir dollara uyğundur. Qiymətin stabilliyi avtonom ağıllı müqavilə sisteminin köməyi ilə dəstəklənir.

Basecoin – ABŞ dollarına bağlıdır, qiyməti 1 dollara uyğundur, lakin təmin olunmamış stabilkoindir. Token buraxılışının artırılması və ya azaldılması qərarı konsensus əsasında qəbul edilir.

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

Digər stabilkoin layihələri də var:

- Arccy
- Stably
- BitShares
- Sweetbridge
- Havven
- Globcoin
- Augmint
- Fragments
- Carbon
- Kowala
- X8X

Özünü yoxlamaq üçün suallar

1. Kriptovalyutalarada hardforkun mahiyyəti nədir?

2. Kriptovalyutalarada softforkun mahiyyəti nədir?
3. Tam anonim altkoinlərə misallar söyləyin.
4. Blokçeynə əsaslanmayan kriptovalyuta hansıdır?
5. Kross-blokçeyn transferləri üçün hansı kriptovalyuta nəzərdə tutulub?
6. Polkadot hansı konsensus mexanizmindən istifadə edir?
7. Nominator Polkadot-da necə iştirak edir?
8. Bitcoin Cash hardforku Bitcoin-dən nə ilə fərqlənir?
9. Bitcoin softforkuna misal söyləyin.
10. Təmin olunmamış stabilkoinlərin stabilliyi nəyin hesabına təmin olunur?
11. Cardano-nun yaradılmasında məqsəd nə idi?
12. Cardano blokçeynini iki hissəyə bölməkdə əsas ideya (hədəf) nədir?
13. Dash ikiranqlı arxitekturasında hər səviyyənin funksiyası nədir?
14. Masternodlar hansı servisləri yerinə yetirir?
15. Dash-da mayninq mükafatı necə bölünür?
16. Dash-da hansı konsensus mexanizmi istifadə edilir?
17. Dash-da hansı kriptoqrafik heş funksiyası istifadə edilir?
18. Dash-da PrivateSend necə işləyir?
19. SegWit və Lightning Network mexanizmlərinə ilk keçən kriptovalyuta hansıdır?
20. Kriptovalyutalarda atomar tranzaksiyalar nədir?

Mühazirə 8. Rəqəmsal tokenlər. DeFi anlayışı

8.1. ICO (Initial Coin Offering) anlayışı

ICO (Initial Coin Offering) – kriptovalyuta layihələri üçün investisiyaların cəlb edilməsi formasıdır. ICO təşəbbüskarı investorlara tokenlər satır. Tokenlərin real dəyəri layihə birjaya çıxana qədər qeyri-müəyyən olur. Tokeni alan tərəf, yəni investorlar bu startap tokenini gələcəkdə ICO-da nəzərdə tutulmuş servisləri, xidmətləri və malları əldə etmək üçün istifadə edə bilərlər. Yaxud layihə birjaya çıxdıqdan və dəyəri artdıqdan sonra, dividendlər əldə edə və ya tokeni sata bilərlər.

İlk ICO 2013-cü ildə həyata keçirilmiş Mastercoin olmuşdur (hazırda Omni). Təşəbbüskarlar 5 milyon dollar toplamağa nail olmuşdular. Sayca ikinci ICO ən uğurlulardan biri oldu (2013-cü il, NXT layihəsi). NXT onunla fərqlənir ki, onun bütün emissiyası (1 milyard sikkə) əvvəlcədən 73 investor arasında bölünmüşdü. 2017-ci ilin payızında isə kapitallaşma 70 milyon dollar təşkil edirdi. Ethereum üçün başladılan ICO layihəsində 18 milyon dollar investisiya toplanmışdı.

ICO Stats saytında uğurlu ICO-ların siyahısına baxmaq olar. Qeyd edək ki, 2017-ci ildə ICO-ların 90 %-dən çoxu Ethereum platformasında aparılmışdı (ICO Crazy).

Kriptovalyuta ilə token arasındakı fərq aşağıdakından ibarətdir. Kriptovalyuta – açıq blokçeynin daxili hesablaşma vahididir. Onun emissiyası xüsusi proqram əsasında mayninq vasitəsilə kompüter texnologiyalarının köməyi ilə həyata keçirilir. Maynerin özü heç bir fəal hərəkət etmir, hər şeyi kompüter edir. Token – rəqəmsal aktivdir, qiymətli kağızın və ya öhdəliyin virtual analoqudur, onlar investora hansısa faydanın əldə edilməsini vəd edir. Tokenlərin emissiyasını ICO təşkil edən şirkət layihənin dəyəri haqqında öz mülahizələrindən çıxış edərək həyata keçirir. Tokenə görə ödəniş kriptovalyuta ilə edilir, kriptovalyutanı investor fiat pula alır. Nadir hallarda tokenə görə ödəniş fiat pulla edilir. Lakin bu halda pul münasibətləri qanunvericiliklə tənzimlənən dövriyyə sahəsinə keçir, bunu ICO operatorları və iştirakçıları məmnuniyyətlə qarşılamır.

Beləliklə, ICO-lar tələb yaratmaqla kriptovalyutaların pul dövriyyəsinə daxil edilməsi funksiyasını yerinə yetirir.

ICO təşkilatçılarınının məsələlərindən asılı olaraq tokenlərin aşağıdakı növləri fərqləndirilir:

- tokenlər – ICO kriptovalyutasının jetonları və sikkələridir. Bu kateqoriyaya appkoinlər və ya tətbiqi proqram koinləri aiddir, onlar daxili kriptovalyuta kimi istifadə olunurlar;
- səhm tokenləri – investorlara dividendlərin ödənilməsi nəzərdə tutulur. Misallar: Tierion, Civic, Binance Coin;

- kredit (yığım) tokenləri – investorlar faiz gəliri əldə edirlər.

Bundan başqa, tokenlər onları alan investorun əldə etdiyi hüquqların məzmununa görə də fərqlənirlər. Bu müəyyən aktivlərin (mal və xidmətlərin) əldə edilməsi hüququ və ya şirkətin idarə edilməsində iştirak hüququ ola bilər. Həm də bu hüquqların reallaşması yalnız layihə uğurla həyata keçdiyi halda mümkündür. Uğursuzluq zamanı investisiyaların qaytarılması praktiki olaraq mümkün deyil, çünki maliyyə münasibətlərinin bu sahəsi nə milli, nə də beynəlxalq səviyyədə hələlik tənzimlənmir.

ICO-maniya. Qeyd edək ki, 2017-ci ildə dünyada 902 ICO təşkil edilmişdi, onlardan 418-i uğursuz olmuşdu, yəni kifayət sayda token yerləşdirə bilməmişdilər, 113-ü isə yarım-müflis vəziyyətdə idilər. Buna baxmayaraq, 5,6 milyard dollar toplaya bilmişdilər.

Tokenlərin buraxılmasını emitentlə müqavilə üzrə xüsusi blokçeyn platformalar buraxır, onlardan ən populyarları Ethereum, Waves, NEM, Nxt, EOS, KickICO-dur. Onlar tətbiq edilən alqoritmlərin xüsusiyyətləri, tokenlərin buraxılması sürəti, təhlükəsizlik səviyyəsi, digər kriptovalyuta meydançalarına çıxmaq imkanı və qiymətlə fərqlənirlər. Demək olar ki, bütün ICO-lar eyni cür təşkil olunurlar. Təşkilatçılar öz elektron pulqabının ünvanını göstərirlər, investorlar ora pul göndərirlər, vəsait yığımı başa çatdıqdan sonra investorların pulqabına müəyyən məbləğdə token göndərilir. Nəticədə emitent-şirkət müəyyən həcmdə kriptovalyuta əldə edir, onu fiat pullara çevirə və ya kriptovalyuta birjalarında istifadə edə bilər.

8.2. SAFT modeli

SAFT, hərfən, Simple Agreement for Future Tokens – gələcək tokenlər üçün sadə müqavilə deməkdir. SAFT rəqəmsal tokenlər vasitəsilə vəsaitlərin cəlb edilməsinin alternativ modelidir, amerikan hüquqşünasları və maliyyə texnologiyaları mütəxəssisləri tərəfindən işlənmişdir. O, ABŞ-ın maliyyə və vergi qanunvericiliyinə tam uyğundur.

Öz mahiyyətinə görə SAFT – layihənin developerləri ilə investorlar arasında investisiya müqaviləsidir. SAFT mexanizmi aşağıdakı kimi işləyir. Tokenə əsaslanmış mərkəzləşmiş şəbəkənin developerləri akkreditasiya olunmuş investorlarla yazılı müqavilə bağlayırlar. SAFT-a uyğun olaraq, investorlar layihə həyata keçirildikdən sonra tokenləri almaq hüququna görə investorlara pul vəsaiti ödəyirlər. Beləliklə, ICO keçirilməsi mərhələsində öncədən satış tokenləri buraxılmır. Developer toplanmış vəsaiti şəbəkənin yaradılmasına istifadə edir və platformanın funksionalı hazır olduqca tokenlər buraxır və onları investorlara göndərir. İnvestorlar tokenləri öz bildikləri kimi istifadə edirlər, o cümlədən onları açıq bazarda sata bilərlər.

SAFT modelində token əvəzinə tokenin qiymətli kağızları çıxış edir, onlar qiymətli kağızlar haqqında qanunvericilik normaları üzrə vençur maliyyələşdirmə tələbləri ilə qeydiyyatdan keçirilirlər. Bu sxemin üstünlüyü tokenlərin buraxılmasının legitimliyidir, həmçinin kriptovalyutaların fiat pullara konvertasiyası problemi də qalmır, bu problem maliyyələşmənin həcmi böyük və layihənin reallaşması müddəti uzun olduqda xeyli çətindir.

8.3. ERC-20 standartı

ERC-20 eyni zamanda bir neçə funksiya yerinə yetirə bilər.

ERC-20 texnologiyası ağıllı müqavilələrin bağlanması üçün bir neçə parametri nəzərdə tutur. Bunlardan 6-sı məcburidir, 3-ü isə məcburi deyildir, lakin uyğunluq üçün tövsiyə olunur.

Məcburi parametrlərə aşağıdakı funksiyalar daxildir:

- **totalSupply** – rəqəmsal pulların toplam emissiyası üçün lazımdır, maksimum qiymətə çatdıqda yenilərini yaratmaq imkanının olmamasını təmin edir.
- **balance0f** – ICO təşkilatçılarının konkret ünvanına təyin edilmiş tokenlərin ilkin sayını müəyyən etmək üçün tələb olunur.
- **transfer** – ICO dövründə sərmayə qoyan istifadəçi-investorlara tokenlərin verilməsinə zəmanət vermək üçün lazımdır.
- **transferFrom** – müxtəlif istifadəçilər arasında ödəniş əməliyyatları üçün tələb olunur (son iki funksiya tokenləri standarta uyğun köçürmək yollarıdır, onlar valyutanın əməliyyatlar və istifadəçilər arasında paylanması üçün lazımdır)
- **approve** – elektron tokenlərin ağıllı müqavilə üzrə paylanmasının, ümumilikdə, emissiyaya əsaslanmaqla həyata keçirilməsinin mümkünlüyünü yoxlamaq üçün lazımdır.
- **allowance** – rəqəmsal sikkələrin başqa ünvana göndərilməsi üçün konkret ünvanda kifayət qədər balansın olub-olmadığını yoxlamaq üçün tələb olunur (approve və allowance – elektron sikkələrin köçürülməsi üsullarının yoxlanılması prosesinə cavabdeh funksiyalardır).

Məcburi olmayan üç parametr – onluq nöqtədən sonra maksimum kəsr işarələrinin aşkarlanması (məsələn, Bitkoin-də nöqtədən sonra 8 onluq rəqəm var), tokenin adı və onun simvoludur. Bu məlumatlar toplusu provayderlərə və birjalara bütün ERC-20 ağıllı müqavilələri ilə qarşılıqlı əlaqə qurmağa imkan verən vahid kod bazası yaratmağa kömək edir.

8.4. DeFi anlayışı

DeFi (Decentralized Finance) – blokçeyn üzərində yaradılmış xidmətlər və tətbiqlər şəklində mərkəzsiz maliyyə alətləridir. DeFi – bank sektoruna müasir

alternativdir, maliyyə sisteminin ənənəvi texnologiyalarını açıq kodlu protokollarla əvəzləyir.

Çox sayda insana mərkəziyətsiz kredit və yeni investisiya platformalarına giriş verir, həmçinin kriptovalyuta aktivlərindən passiv gəlir əldə etməyə imkan yaradır.

DeFi tətbiqlərinin pioneri 2017-ci ilin sonunda istifadəyə verilmiş MakerDAO platforması idi. Həmin vaxtdan bəri, DeFi protokollarında yerləşdirilən vəsaitlərin (TVL, Total Value Locked) ümumi həcmi durmadan artır. Mövcud DeFi-lərin əksəriyyəti Ethereum blokçeynində qurulub, lakin digər blokçeynlərdə də DeFi fəallığı artır.

Bəzi populyar DeFi-tokenləri: Uniswap (UNI), SushiSwap (SUSHI), PancakeSwap (CAKE), Wrapped Bitcoin (WBTC), Dai (DAI), Compound (COMP), Avalanche (AVAX), Chainlink (LINK).

DeFi komponentləri. DeFi blokçeyn sahəsində hazırlanmış müxtəlif texnologiyalardan istifadə edir:

- Blokçeynlər – çox zaman Ethereum şəbəkəsi istifadə edilir, həmçinin Solana, BSC, Polygon və digər şəbəkələr də tətbiq edilir.
- Rəqəmsal aktivlər (DeFi tokenləri) – blokçeyn şəbəkəsində alqı-satqı və ya köçürülə bilən dəyər təmin edən. Bitcoin və digər kriptovalyutalar blokçeyn əsaslı ilk rəqəmsal aktivlər idi.
- Pulqabılar – blokçeyndə saxlanılan aktivləri idarə etmək üçün proqram interfeysləri (mobil – Trust Wallet, veb – MetaMask) .
- Ağıllı müqavilələr – əvvəlcədən müəyyən edilmiş şərtlərə və qaydalara uyğun olaraq müvafiq hadisələri və hərəkətləri icra edən, idarə edən və sənədləşdirən blokçeyn əsaslı proqram kodudur.
- DApps (Mərkəziyətsiz tətbiqlər) – birjalarda DeFi-tokenlərin alqı-satqısı üçün istifadə edilir; ağıllı müqavilələr əsasında yaradılır, çox zaman ənənəvi veb texnologiyaları və DAO istifadə edilməklə istifadəçi interfeysi ilə inteqrasiya olunur. DAO – qaydaları ağıllı müqavilələrlə müəyyən edilən və idarə olunan mərkəzsiz avtonom təşkilatlardır.
- Stabilkoinlər – dəyəri fiat valyutasına və ya sabit qiymətə malik digər aktivlərə bağlanmış rəqəmsal aktivlərdir. DeFi-tokenləri əldə etmək üçün istifadə edilir.

2021-ci ilin əvvəlində DeFi layihələrinə 30 milyard dollardan çox sərmayə qoyulmuşdu. 2023-cü ilin yanvarında bu rəqəm 50 milyard dollara çatmışdı. Bəzi DeFi layihələri aşağıda verilib:

Uniswap (UNI tokeni) – kriptovalyuta bazarında likvidliyi təmin edən mərkəziyətsiz birjadır. Platforma və token Ethreum-da işləyir. UNI tokeni universal

ERC-20 tokenindən istifadə edir, bu o deməkdir ki, onu bir çox digər tokenə dəyişmək olar.

Avalanche (AVAX) – kapitallaşmasına görə ən böyük DeFi layihələrdən biridir.

Chainlink (LINK) – orakların blokçeyn-şəbəkəsidir. SWIFT ilə əməkdaşlıq edir, bunun sayəsində bankların verilənlər bazalarına girişi var. (ing. Oracle – blokçeyn ekosistemi ilə xarici verilənlər mənbəyi arasında körpü rolunu oynayan obyektlərdir; ağıllı müqavilələrin xarici sistemlərlə qarşılıqlı əlaqədə olmasına imkan verir. Ən yaxşı orakl layihələrindən biri API3-dür).

DeFi-nin üstünlükləri – mərkəzin olmaması, insan faktorunun olmaması, şəffaflıq (vicdanlı audit mümkündür), inkluzivlik (bankların və tənzimləyicilərin icazəsi tələb edilmir); trans-sərhəd – vasitəçilər və süründürməçilik yoxdur.

DeFi-nin nöqsanları – sistemin sürəti (məhsuldarlığı) aşağıdır; istifadəçinin səhvetmə riski yüksəkdir; xaotiklik – ekosistemdə stabillik yoxdur.

DeFi tətbiqləri: kredit, kriptolendinq, likvidlik hovuzları, gəlirli fermerçilik.

Gəlirli fermerçilik. Mürəkkəb, lakin populyar alətdir. Standart sxemi belədir:

1) İnvestor token alır və onu likvidlik hovuzuna yerləşdirir, hovuzda iştirakın təsdiqi olaraq investora xüsusi LP-tokenləri verilir;
2) LP-tokenləri xüsusi ağıllı müqaviləyə steyk edilir.
3) Bundan sonra, investor layihə tokenləri ilə müntəzəm ödənişlər alır. Obrazlı deyilsə, o əslində LP-ni "əkir" və ondan yeni pulsuz tokenlər "böyüyür" – "fermerçilik" termini buradan yaranıb.

Özünü yoxlamaq üçün suallar

1. ICO (Initial Coin Offering) nədir?
2. Kriptovalyuta ilə token arasındakı fərqlər nədən ibarətdir?
3. Tokenlərin hansı növləri var?
4. Səhm tokenləri nəyi nəzərdə tuturlar?
5. ERC-20 standartında məcburi parametrlərə hansı funksiyalar daxildir?
6. ERC-20 standartı nəyə xidmət edir?
7. ERC-20 standartında məcburi olmayan parametrlər hansılardır?
8. SAFT mexanizmi necə işləyir?
9. DeFi nədir?
10. DeFi-nin komponentləri hansılardır?
11. DeFi-də stabilkoin nə üçün istifadə edilir?
12. Populyar DeFi-tokenlərinə aid misallar söyləyin.
13. DeFi-nin nöqsanları hansılardır?
14. DeFi-nin üstünlükləri hansılardır?
15. DeFi tətbiqləri hansılardır?

16. Uniswap kriptovalyuta bazarında nəyi təmin edən birjadır?
17. Chainlink hansı obyektlərin blokçeynidir?
18. Chainlink-in hansı əməkdaşlığın hesabına bank məlumatlarına girişi var?
19. Orakl nədir?
20. Gəlirli fermerçilik sxemi necə işləyir?

Mühazirə 9. Ağıllı müqavilələr. DApps tətbiqləri

9.1. Ağıllı müqavilələr

Etherum-un yaradılmasının əsas hərəkətverici ideyası tranzaksiyanın – kriptovalyuta protokolunun əsas vahidinin ağıllı müqavilə ilə əvəz edilməsi idi. Ethereum ağıllı müqavilələri praktikada geniş istifadə edən ilk platformadır.

Ağıllı müqavilə vasitəçi olmadan, avtomatik yerinə yetirilən müqavilələrdir. Müqavilə şərtlərinin və ödənişin yerinə yetirilməsinə xüsusi proqram nəzarət edir. Ağıllı müqavilə daxilində təkcə pul vahidinin bir hesabdan digərinə keçirilməsini deyil, istifadəçilər arasında qarşılıqlı əlaqənin daha geniş məntiqini və şərtlərini təsvir etmək olar.

Ağıllı müqavilə elektron alqoritm və ya şərtdir, onun yerinə yetirilməsi zamanı tərəflər pul, aksiya, daşınmaz əmlak və ya digər aktivləri mübadilə edə bilərlər. Ağıllı müqavilələrin istifadəsi ideyasını 1994-cü ildə Nik Sabo təklif etmişdi. Lakin o vaxt bu ideyanı tam miqyasda reallaşdırmağa imkan verən alət – bütün iştirakçıları bərabərhüquqlu olan mərkəziyətsiz şəbəkə yox idi. Blokçeyn texnologiyasının hesabına ağıllı müqavilələr paylanmış reyestrdə saxlanır və tərəflərdən heç birinin onu dəyişmək imkanı yoxdur. Kriptovalyuta isə maliyyə aləti kimi istifadə edilir.

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

Ethereumda ünvanlar. Ethereum-da hesabların (ünvanların) iki növü var:

EOA (External Owned Account) – istifadəçilərə məxsus ünvanlar; gizli açarla idarə olunur. Gizli açar ağıllı müqavilələrlə qarşılıqlı əlaqədə lazımi autentifikasiya proseslərini idarə edir, həmçinin hesabdakı vəsaitin xərclənməsi üçün tələb olunan rəqəmsal imzaların yaradılmasında istifadə olunur.

CA (Contract Account) – müqavilə ünvanları; gizli və açıq açarları yoxdur, öz kodu ilə özünü idarə edir. Ağıllı müqavilənin ünvanı onun yaradılması üzrə tranzaksiya yerinə yetirilərkən yaradılır.

Ağıılı müqavilə yazıldıqdan sonra onu **xüsusi tranzaksiya**nın köməyi ilə Ethereum şəbəkəsində yerləşdirirlər. Tranzaksiyada göndərən və **alan** olmalıdır. Buna görə bu xüsusi tranzaksiya **xüsusi ünvana** göndərilməlidir. Yeni yaradılmış ağıllı müqavilənin təyinat ünvanı sıfır-ünvan olur:

0x0000000000000000000000000000000000000000.

Əgər təyinat sahəsində sıfır-ünvan göstərilibsə, EVM başa düşür ki, bu tranzaksiya yeni ağıllı müqavilənin yaradılması üçündür. Ethereum şəbəkəsində mədənçilər belə tranzaksiyanı yeni ağıllı müqavilənin yaradılması üzrə təlimat kimi yerinə yetirirlər.

Ağıllı müqavilələrin yenilənməsi. Ethereum şəbəkəsində yerləşdirildikdən sonra ağıllı müqaviləyə yeni funksiyalar əlavə etmək mümkün deyil. Bununla belə, əgər ağıllı müqavilənin koduna SELFDESTRUCT ("özünü məhv etmə") funksiyasını daxil edilibsə, o, gələcəkdə ağıllı müqaviləni "silmək" və yenisi ilə əvəz etmək olar. Əgər SELFDESTRUCT funksiyası əvvəlcədən koda daxil edilməyibsə, ağıllı müqaviləni silmək mümkün deyil.

Qeyd edək ki, yenilənən ağıllı müqavilələr proqramçılara müqavilənin dəyişməzliyi ilə bağlı daha çox çeviklik verir. Müxtəlif mürəkkəblikdə yenilənən ağıllı müqavilələr yaratmağın bir çox yolu var. Sadələşdirilmiş bir misala baxaq. Təsəvvür edin ki, ağıllı müqavilə bir neçə kiçik müqaviləyə bölünüb. Bəziləri dəyişməzdir, digərlərində isə silmə funksiyası aktivdir. Bu o deməkdir ki, kodun bir hissəsini (bəzi ağıllı müqavilələr) çıxarmaq və dəyişmək olar, digər funksiyalar isə toxunulmazdır.

9.2. Solidity dili barədə ilkin məlumat

Ağıllı müqavilələr – müxtəlif obyektyönlü dillərdə reallaşdırıla bilən xüsusi siniflərdir. Ağıllı müqavilələr yazarkən, adətən, Solidity istifadə olunur, lakin Vyper və Yul kimi variantlar da var. Biz Solidity ilə davam edəcəyik. Solidity ilə yazılmış ağıllı müqavilə kompilyasiya edildikdə baytkod yaranır. Baytkod aşağı səviyyəli maşın kodlarıdır, EVM (Ethereum Virtual Machine) mühitində işləyir. Virtual maşının vəziyyətinin dəyişməsini Türinq-tam olan senari dilində yazmaq olar. (Türinq-tamlıq istənilən hesablana bilən funksiyanı reallaşdırmağın mümkünlüyünü bildirir.)

Solidity EVM-də işləyən statik tipli, obyektyönlü ağıllı müqavilə proqramlaşdırma dilidir. Ethereum-da və digər blokçeyn arxitekturalarında geniş istifadə olunur.

Solidity C++, Python və JavaScript kimi proqramlaşdırma dillərinə əsaslanan yüksək səviyyəli dildir. Bu dillərdən hər hansı birini bilirsinizsə, Solidity sizə tanış görünəcək.

Solidity varisliyi dəstəkləyir, ona görə də bir müqavilədəki funksiyalar, dəyişənlər və digər xüsusiyyətlər digərində istifadə oluna bilər. Solidity strukturlar və siyahılar kimi istifadəçi tərəfindən müəyyən edilmiş mürəkkəb tipləri də dəstəkləyir.

Bu dildə yazılmış kodlar Solidity Compiler (*solc*) ilə kompilyasiya edilir və EVM-də işləyəcək baytkod çıxışı yaradır. Hazırlanmış ağıllı müqavilə digər

müqavilələrdən və ya Web3 proqramlarından çağırılırsa, ABI (Application Binary Interface) çıxışı da yaradılır.

Solidity ilə yazılmış çox sayda ağıllı müqavilə nümunələri üçün Remix IDE (https://remix.ethereum.org/) səhifəsini ziyarət etmək olar. Remix brauzer əsaslı IDE mühitidir, hesab açmağa və sistemə daxil olmağa ehtiyac yoxdur. Ağıllı müqavilə yazmağa, kompilyasiya, test etməyə birbaşa başlaya bilərsiniz.

```
//SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract Testet {
  function hello() public pure returns(string memory) {
    return "Hello Blockchain";
  }
}
```

Qeyd etmək zəruridir ki, Ethereum proqramlaşdırma dilinin istifadəsi istənilən hesablama funksiyasını reallaşdırmağa imkan verir – bunu istifadəçilər müsbət qiymətləndirirlər. Lakin uçot yazısı sındırıldıqda istifadəçinin bütün verilənlərinə təhlükə yaranır ki, bunu sistemin mənfi cəhəti hesab etmək olar.

9.3. DApps tətbiqləri

Ağıllı müqavilələr müxtəlif mərkəziyətsiz onlayn tətbiqlərin (DApps) yaradılması üçün platformadır.

DApps tətbiqləri – açıq kodlu tətbiqlərdir, şəbəkə və onun istifadəçiləri arasında bağlanmış müqavilədən ibarətdirlər və paylanmış reyestr (ing. ledger) texnologiyasına, məsələn, Bitkoin və ya Ethereum blokçeyninə əsaslanırlar. Bu tətbiqlərin xüsusiyyəti ondan ibarətdir ki, heç bir təşkilat bu müqavilələrə nəzarət etmir və onlara münasibətdə tələb etməyə qanuni hüquqları yoxdur, bütün qərarlar isə (məsələn, protokolun təkmilləşdirilməsi haqqında) istifadəçilərin kompüter kodunun əsasında konsensusa nail olması nəticəsində qəbul edilir.

Tətbiq o zaman həqiqətən mərkəziyətsiz hesab edilir ki, onun həm protokolu, həm də verilənləri açıq girişli mərkəziyətsiz blokçeyndə saxlanır (mərkəzi imtina nöqtəsinin varlığından qaçmaq üçün), onların düzgünlüyü isə mərkəziyətsiz verifikasiya mexanizmindən (məsələn, PoW) istifadə etmək yolu ilə təsdiqlənir.

Lazımi qaydada mərkəziyətsiz tətbiqlər bütün tranzaksiyalar üzrə etibarlı uçot yazılarının saxlanmasını hətta əsas veb-saytlar və interfeyslər oflayn rejimdə olduqda da təmin edir. Bundan başqa, sonradan heç kim paylanmış reyestrdə yazıları silə və ya dəyişdirə bilməz.

DApps tətbiqlərini aşağıdakı siniflərə bölmək olar:

Tip 1: Öz blokçeyni olan mərkəziyətsiz tətbiqlər
Misallar: Bitcoin, Altcoin, Litecoin.

Tip 2: Tip 1 DApps blokçeynindən istifadə edən mərkəziyətsiz tətbiqlər
Misal: Omni protokolu (Bitkoin blokçeyni üzərində qurulmuş proqram təminatı layı).
Tip 2 DApps tətbiqləri protokollardır və özlərinin tokenlərindən istifadə edirlər.

Tip 3: Tip 2 DApps blokçeynindən istifadə edən mərkəziyətsiz tətbiqlər
Misal: SAFE şəbəkəsi, Safecoin tokenlərini buraxmaq üçün Omni protokolundan istifadə edir.

Özünü yoxlamaq üçün suallar

1. Ağıllı müqavilələrin istifadəsi ideyasını kim irəli sürüb?
2. Ağıllı müqavilə nədir?
3. EVM (Ethereum Virtual Machine) hansı funksiyanı yerinə yetirir?
4. Ethereum-da hesabların (ünvanların) hansı növləri var?
5. EOA (External Owned Account) ünvanları hansı açarla idarə olunur?
6. CA (Contract Account) ünvanları hansı açarlarla idarə olunur?
7. DApps tətbiqlərini hansı siniflərə bölmək olar?
8. Ağıllı müqaviləni silmək üçün ona əvvəlcədən hansı funksiyanı daxil etmək lazımdır?
9. Ağıllı müqavilənin ünvanı nə zaman yaradılır?
10. Yeni yaradılmış ağıllı müqavilənin təyinat ünvanı necə olmalıdır?
11. Əgər təyinat sahəsində sıfır-ünvan göstərilibsə, EVM onu necə yerinə yetirir?
12. Ağıllı müqavilələri hansı proqramlaşdırma dillərində yazmaq olar?
13. Solidity dilində yazılmış proqram hansı kompilyator ilə kompilyasiya edilir?
14. Solidity ağıllı müqaviləsini EVM üçün kompilyasiya etdikdə hansı kod yaranır?
15. Solidity varisliyi dəstəkləyir – bu nə deməkdir?
16. Solidity istifadəçi tərəfindən müəyyən edilmiş hansı mürəkkəb tipləri də dəstəkləyir?
17. ABI (Application Binary Interface) çıxışı hansı məqsədlə yaradılır?
18. DApps tətbiqləri hansı tətbiqlərə deyilir?
19. DApps tətbiqlərini hansı siniflərə bölmək olar?
20. Tip 1 DApps tətbiqlərinən əsas xüsusiyyəti nədir?

Mühazirə 10. Blokçeyn konsensus protokolları

10.1. Bizans generallarının məsələsi

Bizans generallarının məsələsi 1982-ci ildən tədqiq olunur, onu müxtəlif şəkildə ifadə edirlər (mərkəzli, mərkəzsiz, sinxron, asinxron, generalların konkret sayı və s.). Biz bu məsələyə aşağıdakı şəkildə baxacıq.

Bizans ordusu bir şəhəri mühasirəyə alıb və ordu n legiondan ibarətdir, hər legiona bir general rəhbərlik edir. Düşmən ordusunu məğlub etmək üçün heç bir generalın ordusu təkbaşına yetərli deyil.

Döyüşün mümkün nəticələri belə ola bilər:

- Əgər generalların hamısı hücum etsə – Bizans düşməni məhv edəcək (əlverişli nəticə).
- Əgər generalların hamısı geri çəkilsə – Bizans ordusunu saxlayacaq (əlverişli nəticə).
- Əgər bəzi generallar hücuma keçsə, bəziləri geri çəkilsə – düşmən Bizansın bütün ordusunu məhv edəcək (əlverişsiz nəticə).

Beləliklə, aşağıdakı məqsədləri nəzərdən keçirə bilərik:

- Hər bir general qərar qəbul etməlidir: hücum etmək və ya geri çəkilmək (Hə və ya Yox);
- Qərar qəbul etdikdən sonra onu dəyişmək mümkün deyil;
- Bütün generallar razılığa (*konsensusa*) gəlib eyni qərar verməli və onu sinxron şəkildə həyata keçirməlidirlər.

Bu senari sadə görünür, lakin bəzi problemlər var:

1) Generalların bir-biri ilə əlaqə saxlaması və hücum vaxtını razılaşdırması üçün onlar bir-birinə düşmən düşərgəsindən keçməklə çapar (kuryer) göndərməli, öz qərarlarını (və hücuma başlama vaxtını) çatdırmalıdırlar. Bu zaman çaparın düşmən tərəfindən tutulması və xəbərin çatdırılmaması ehtimalı var. Bu ona gətirib çıxara bilər ki, bəzi generalların ordusu hücuma keçəcək, bəziləri isə geri çəkiləcək.

2) Eyni zamanda, Bizans tənəzzül dövrünü yaşayır və generalların bəziləri satqındır. Onlar öz qərarları barədə yanlış məlumat verə bilərlər, hücuma keçməyərək öz legionlarını geri çəkə bilərlər.

Əgər bu dilemmanı blokçeyn kontekstinə tətbiq etsək, hər bir general şəbəkənin qovşağıdır və bu qovşaqlar sistemin cari vəziyyəti (blokçeynə yazılacaq blok) barədə konsensusa (razılığa) gəlməlidirlər. Başqa sözlə, paylanmış şəbəkədə qovşaqların əksəriyyəti tam imtinanın qarşısını almaq üçün razılaşmalı və eyni hərəkəti yerinə yetirməlidirlər.

İsbat edilib ki, m səhv işləyən qovşaq ("satqın general") olan bir sistemdə yalnız $2m + 1$ düzgün işləyən qovşaq ("sadiq general") olduqda, yəni "sadiq"lərin sayı ümumi sayın 2/3-sindən ciddi böyük olduqda konsensusa gəlmək olar.

Buna görə də, bu tip paylanmış sistemlərdə konsensusa nail olmağın yeganə yolu ən azı ⅔ və ya daha çox etibarlı şəbəkə qovşaqlarının olmasıdır. Bu o deməkdir ki, şəbəkənin böyük hissəsi bədniyyətli hərəkət etmək qərarına gəlsə, sistem imtinalara və müxtəlif hücumlara (məsələn, 51% hücumu) həssas olacaq.

Lamport, Pease və Shostak Bizans generalları məsələsinin həlli üçün bir alqoritm təklif ediblər (1982). Alqoritm iki mərhələdən ibarətdir:

- Mərhələ 1: Məlumat toplama mərhələsidir, $m + 1$ raund var. Bu mərhələdə qovşaqlar davamlı olaraq məlumat alır və göndərirlər.
- Mərhələ 2: Qərar qəbuletmə mərhələsidir. Mərhələ 1-də toplanmış məlumat əsasında sistem qərar verir.

Bəzi blokçeynlərdə BFT (**Byzantine Fault Tolerance – Bizans imtinalara dayanıqlığı**) konsensus alqoritmlərinin müxtəlif versiyaları istifadə edilir. BFT – kifayət qədər mürəkkəb konsepsiyadır, paylanmış sistemlərin "Bizans generalları məsələsi"nə dayanıqlığının xarakteristikasıdır – bədniyyətli və sıradan çıxmış elementlər olduqda sistemin etibarlı qalması imkanını göstərir. BFT-əsaslı konsensus protokollarının əksəriyyətində yeni bloku təqdim edəcək validator dairəvi yanaşma ilə seçilir. Kvorumun digər iştirakçı-qovşaqları blokun və ondakı tranzaksiyaların həqiqiliyinə səs verirlər. Əksər hallarda səslərin 2/3-ni qazandıqdan sonra blokçeynə daxil edilir.

BFT-nin üstünlüklərindən – miqyaslanma və ucuz tranzaksiyaları, nöqsanlarından isə müəyyən qədər mərkəzləşməni göstərmək olar. BFT alqoritmlərinin müxtəlif variantları Hyperledger, Ripple, Stellar və Tendermint blokçeynlərində konsensus alqoritmlərinin əsasında dayanır.

10.2. BFT konsensus protokolları

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

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

FBA (Federated Byzantine Agreement) protokolu Stellar və Ripple-də istifadə edilən BFT variantlarından biridir. Ümumi ideya ondan ibarətdir ki, öz məxsusi zəncirinə cavabdeh olan hər bir general (validator) özünün etibar etdiyi validatorların

siyahısını müəyyən edir (**ing. quorum slice**). Ripple-də validatorlar əvvəlcədən seçilir. Stellar-da istənilən qovşaq validator ola bilər, hansı validatora etibar etməyi sitifadəçi özü seçir.

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

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

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

10.3. DPoS (Delegated Proof-of-Stake) protokolu

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

DPoS protokolunda hər bir istifadəçi validator qovşağı olmağa öz namizədliyini irəli sürə bilər, Sonra bütün istifadəçilər arasında namizədlərə səsvermə keçirilir, hər bir səsin çəkisi səs verənin aktivlərinin miqdarı ilə müəyyən edilir. Səsvermə nəticəsində N namizəd seçilir (N-i icma müəyyən edir, adətən, 20-50 namizəd) və onlar yeni blok

formalaşdırmaq hüququ qazanırlar. Əgər səsvermədə iştirak edən aktivlərin böyük hissəsinə düzgün istifadəçilər nəzarət edirsə, protokolun qaydaları düzgün qərar qəbul edilməsini təmin edir.

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

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

PoW və PoS-dan fərqli olaraq, DPoS-da mədənçilər blok yaratmaq üçün rəqabət yox, əməkdaşlıq edə bilərlər. Blokların yaradılmasını qismən mərkəzləşdirməklə DPoS digər alqoritmlərin əksəriyyətindən dəfələrlə sürətlə işləyir. DPoS protokolundan istifadə edən EOS blokun blokçeynə yazılmasına 2 saniyədən az vaxt sərf edilən ilk blokçeyn olmuşdu. Bu, Bitcoin-dəki 10 dəqiqədən dəfələrlə sürətlidir.

Özünü yoxlamaq üçün suallar

1. Bizans generallarının məsələsi nədən ibarətdir?
2. Bizans çətinləşdirən problemlər hansı
3. m səhv işləyən qovşaq ("satqın general") olan sistemdə hansı şərtdə konsensusa nail olmaq mümkündür?
4. Bizans generalları məsələsinin həlli alqoritmi (Lamport, Pease və Shostak) hansı mərhələlərdən ibarətdir?
5. Lamport, Pease və Shostak alqoritminin birinci mərhələsi neçə raunddan ibarətdir?
6. Lamport, Pease və Shostak alqoritminin birinci mərhələsində nə iş görülür?
7. Lamport, Pease və Shostak alqoritminin ikinci mərhələsində nə iş görülür?
8. BFT protokolunun üstünlükləri nədir?
9. BFT protokolunun nöqsanları nədir?
10. PBFT (Practical BFT) alqoritmi hansı blokçeyndə istifadə edilir?
11. Hyperledger Fabric-də əvvəlcədən seçilmiş neçə PBFT validatoru olur?
12. PBFT konsensus qovşaqlarının ən çoxu neçə hissəsinin bədniyyətli olmasına dayanıqlıdır?

13. Hyperledger-də tranzaksiyanın təsdiqlənməsi üçün qovşaqların ən azı neçə faizi onu bəyənməlidir?
14. FBA (Federated Byzantine Agreement) protokolunun əsas ideyası nədən ibarətdir?
15. Delegated BFT (DBFT) protokolunda qovşaqların hansı növləri olmalıdır?
16. DBFT protokolunda uçot qovşağı olmaq üçün hansı tələblər gözlənilməlidir?
17. DPoS protokolunda validator namizədləri necə seçilir?
18. DPoS protokolunda validatorların növbəsi necə yaradılır?
19. DPoS-da səs verənlər yeni səsverməni hansı zamanda keçirə bilərlər?
20. DPoS nəyin hesabına digər alqoritmlərlə müqayisədə sürətlə işləyir?

Mühazirə 11. Blokçeynlərin təkmilləşdirilməsi üzrə texnolji həllər

11.1. Blokçeyn texnologiyalarının təkmilləşdirilməsi istiqamətləri

Blokçeynin ən aktual problemlərindən miqyaslanma, təhlükəsizlik və gizliliyin təmin edilməsi məsələlərini qeyd etmək olar.

Geniş yayılmış blokçeyn texnologiyası kimi Bitcoinin əsas problemi tranzaksiyaların emal sürətinin olduqca aşağı olmasıdır (saniyədə 6-7 tranzaksiya); müqayisə üçün qeyd edək ki, bu göstərici VISA sistemində 2000-dir. Ümumiyyətlə, blokçeyn-şəbəkənin miqyaslanması məsələsi əlaqəli üç parametrin – təhlükəsizlik, demərkəzləşmə və miqyaslanmanın optimallaşdırılması arasında balans yaratmağı tələb edir. V.Buterinin "**blokçeynin miqyaslanması trilemması**"na görə, blokçeyn bu parametrlərdən yalnız ikisi üzrə yaxşı nəticə göstərə bilər. Tranzaksiyaların emal sürətini yüksəltmək üçün blokçeyn ya təhlükəsizliyi, ya da demərkəzləşməni qurban verməlidir. Praktikada yüksək sürət nümayiş etdirən blokçeynlərdə, adətən, demərkəzləşmə güzəştə gedilir və hazırda mərkəzləşmə meylləri üstün gəlir.

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

Miqyaslanmanın təmin edilməsi üçün bəzi yanaşmaları xatırlatmaq olar:

- qlobal reyestrin qovşaqların bir qrupu tərəfindən idarə edilən daha kiçik altreyestrlərə bölünməsi,
- saxlanmanı optimallaşdırmaq üçün köhnə tranzaksiyaların silinməsi
- blokçeynlər iyerarxiyasından istifadə edilməsi (məsələn, Lighting Network texnologiyası)
- blokçeynin seqmentlərə bölünməsi (ing. sharding)
- blokun ölçüsünün artırılması (məsələn, SegWit) və s.

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

Məlum olduğu kimi, kriptoqrafiyada ən çətin məsələ açarların idarə olunması problemidir və bu kriptovalyutalarda da öz qüvvəsində qalır. Bitcoin-in mövcudluğu illərində xeyli hallar olmuşdu ki, istifadəçilər bütün bitkoinlərini itirmişdilər: sərt diski atmışdılar, parolu unutmuşdular və ya pulqabını qorumaq üçün zəruri tədbirlər görməmişdilər. Buna görə açarların itirilməsinin və ya oğurlanmasının qarşısını almağa

imkan verən daha etibarlı həllər tələb edilir. Bitcoin-də istifadə edilən multi-imza metodu və ya sirrin bölgüsü metodları belə həllər ola bilər. Lakin bu həllərin təhdid modelinə uyğunluq dərəcəsi qiymətləndirilməlidir.

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

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

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

11.2. Saydçeyn texnologiyası

Saydçeyn (ing. sidechain – yan zəncir) – əsas zəncirdən ayrı mövcud olan blokçeyndir.

Saydçeyn hazırda fəal inkişaf mərhələsində olan texnologiyadır, bir blokçeynin tokenlərinin və digər rəqəmsal aktivlərinin digər blokçeyndə təhlükəsiz şəkildə istifadə edilməsinə və sonra (zəruri olduqda) ilkin blokçeynə qayıtmasına imkan verir. Saydçeyn konsepsiyası ilk dəfə 2014-cü ildə *Blockstream* şirkətinin mütəxəssisləri tərəfindən yazılmış "ağ məqalə"də təklif edilmişdi.

Saydçeyn konsepsiyasında bir-biri ilə sıx əlaqəli blokçeynlərin geniş qlobal şəbəkəsi nəzərdə tutulur, onların hər birinin öz protokolu, qaydaları və funksiyalar çoxluğu var. Lakin onların hər biri Bitkoinə bağlanacaq və onun mayninq şəbəkəsi ilə qorunacaq. Saydçeynlərdən Bitkoin proqram kodlarında ediləcək dəyişiklikləri modelləşdirmək üçün də istifadə etmək olar.

Saydçeynin iş prinsipi. Saydçeyn valideyn-blokçeynə ikitərəfli əlaqə ilə bağlanmış ayrıca bir blokçeyndir. Valideyn blokçeyn əsas zəncir, əlavə zəncirlər isə saydçeyn adlanır.

Valideyn-blokçeynin istifadəçisi əvvəlcə tokenləri çıxış ünvanına göndərməlidir, burada tokenlər federasiya iştirakçıları tərəfindən «kilidlənir», bu onların başqa yerdə istifadəsinin qarşısını almaq üçündür. Tranzaksiya qurtaranda onun iştirakçıları

təsdiqləmə alırlar, lakin əlavə təhlükəsizlik üçün bu müəyyən gözləmə müddətindən sonra baş verir. Bundan sonra tokenlərin ekvivalent miqdarı saydçeynə keçirilir və istifadəçinin onları xərcləmək imkanı yaranır. Tokenlər saydçeyndən əsas blokçeynə göndərilərkən əks proses gedir.

Saydçeyn federasiyası. Federasiya – əsas blokçeynlə onun saydçeynlərindən biri arasında aralıq nöqtə rolunda çıxış edən operatorlar qrupudur. Federasiya istifadəçinin tokenlərinin nə vaxt kilidləndiyini və onların nə vaxt xərclənə biləcəyini müəyyən edir.

Saydçeyni yaradanlar (təsisçilər) federasiyanın üzvlərini seçə bilərlər. Belə modelin nöqsanı əsas blokçeynlə saydçeyn arasında əlavə layın iştirak etməsidir ki, nəticədə mərkəzləşmə riskləri yaranır.

2017-ci ilin yanvarında güclü federasiyalar üçün yeni "ağ məqalə" çıxmışdı, burada yenilənmiş konsensus mexanizmləri və etimad modelləri, həmçinin göndərilmiş vəsaitin uğursuzluq halında əsas şəbəkəyə qaytarılmasını təmin edən mexanizmlər var.

Faktiki olaraq, güclü federasiyalar yaxşı layihələndirilmiş multi-imza ünvanlarıdır, onlarda bitkoinlər kilidlənir. Onları yalnız yetərli sayda açar sahibi ödəmənin həqiqiliyini təsdiqlədikdən sonra açmaq olar.

Saydçeyn platformaları. Liquid hazırda ən məşhur platformadır. O, Blockstream tərəfindən yaradılıb, Bitkoin birjalarına, prosessinq mərkəzlərinə və treyderlərə xidmət üçün nəzərdə tutulub. O müxtəlif hesablar arasındakı tranzaksiyaların yerinə yetirilməsi üçün tələb edilən zamanı qısaldır.

RSK (Rootstock) da geniş məşhurluq qazanıb. Türinq-tam olan virtual maşınlı Bitkoin saydçeynidir, Ethereum DApp interfeysi ilə uyardır. Platformanın Bamboo adlı əsas şəbəkəsi 2018-ci ildə işə salınıb. RSK şəbəkəsində blokların generasiyası Bitkoin ilə birgə mayninq rejimində aparılır.

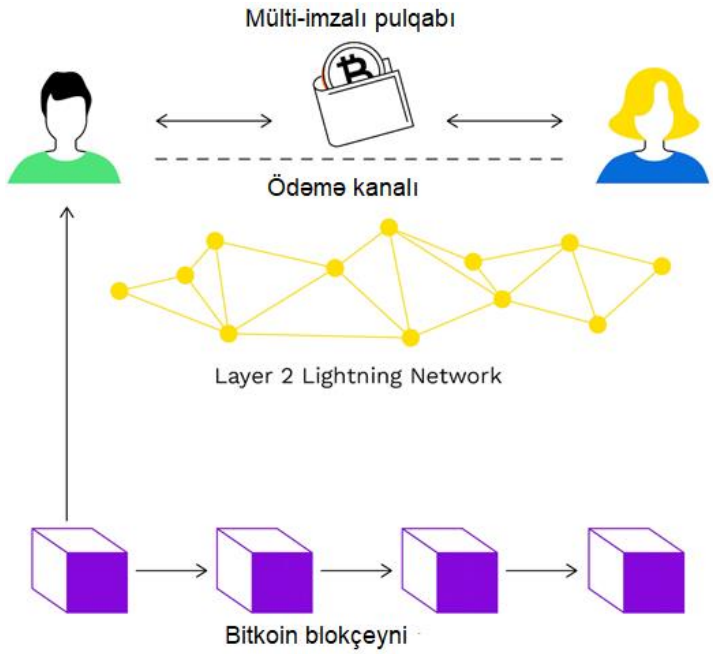
Ardor saydçeyn texnologiyasını biznes üçün həllər kimi təqdim edir – Nxt komandasının ikinci nəsil mərkəziyətsiz servislər üçün blokçeyn platformasıdır. Onun əsas fərqi konsensus alqoritmi kimi PoS istifadə etməsidir, əsas blokçeynlə sıx inteqrasiya edilən saydçeynlər isə "övlad zəncirlər" adlanırlar (ing. childchains).

Kriptovalyuta sənayesində saydçeyn texnologiyasını tədqiq edən daha bir nümayəndə Ethereum üçün əsas rəqib hesab edilən **Lisk** layihəsidir. Lisk blokçeynə əsaslanan mərkəziyətsiz tətbiqlərin yaradılması üçün platformadır və LSK tokenini istifadə edir. DApp tətbiqlərinin yaradılmasında Javascript proqramlaşdırma dili istifadə edilir. Lisk-də DPoS konsensus alqoritmi istifadə edilir.

11.3. Ligthning Network texnologiyası

Lightning Network (LN) – yeni blokçeyn texnologiyalarından biridir, mikro-tranzaksiyaları praktiki olaraq sıfır komissiya ilə etməyə imkan verir. Blokçeynə

tranzaksiyanın bütün detalları deyil, yalnız yekun balans yazılır. Lightning Network-u əsas blokçeyn şəbəkəsi üzərində 2-ci səviyyə şəbəkəsi kimi qəbul etmək olar.



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

LN ödəmə kanallarının iş prinsipi iki insanın eyni məbləğdə pul qoyduğu seyfə oxşayır, onların hər biri seyfi öz qıfılı ilə bağlayır. Təsəvvür edin ki, A və B hərəsi seyfə 10 BTC pul qoyub. Əgər A B-yə 2 BTC göndərmək istəyirsə, bunu necə edir? Bunun üçün o özünün ümumi seyfdəki 2 BTC pulunun sahiblik haqqını B-yə verir. Əgər bundan sonra seyf açılsa, A seyfdən 8 BTC, B 12 BTC götürəcək. Əgər onlar öz aralarında tranzaksiyaları davam etdirmək istəyirlərsə, seyfi açmırlar. Məsələn, sonrakı gün B A-ya 1 BTC göndərməlidirsə, eyni hərəkəti edəcək – öz bitkoinlərindən birinin sahiblik haqqını A-ya verəcək. Əgər bu iki tranzaksiyadan sonra seyf açılsa, A 9, B 11 BTC alacaq.

Ödəmə kanalları pulların birləşdirilməsi və əvvəlcədən razılaşdırılmış şərtlərlə bu pullara sahiblik haqqının ötürülməsidir. Əgər A və B kanalı bağlamaq istəsələr, bunu istənilən an edə bilərlər. Kanalın bağlanması seyfi açmaq və öz pullarını götürmək deməkdir. Seyfin açılması blokçeyndə baş verdiyinə görə, açılma anında kimin nə qədər

pula sahib olması həmişəlik qeydə alınır. Lakin LN-in həqiqi potensialı onlar şəbəkə yaradaraq birgə işlədikdə açılır. Ödəmə kanalları sayəsində böyük sayda tranzaksiyaları blokçeyndən kənarda yerinə yetirmək olar.

Şəbəkədə marşrutlama (routing). Təsəvvür edək ki, üç nəfər var: A, B və C. A və B arasında ödəmə kanalı açılıb, B ilə C arasında da kanal var. Lakin A və C arasında ödəmə kanalı yoxdur.

Əgər A C-yə 2 BTC vermək istəyirsə, o bunu B və C arasındakı ödəmə kanalı ilə edə bilər. A B-dən 2 BTC-nin sahiblik haqqını B-C kanalı ilə C-yə verməyi xahiş edir. Sonra isə B-yə 2 BTC-ni A-B kanalı ilə qaytarır.

İki iştirakçı arasında ödəmə kanalı hər iki tərəf blokçeyndə 2-dən-2 multi-imzalı tranzaksiya yaratdıqda və tərəflərdən heç olmasa biri reyestrə 2-dən-2 multi-imzalı vəsait göndərdikdə yaranır. Hər bir istifadəçinin bir gizli açarı var, tranzaksiya isə yalnız hər iki iştirakçı imzaladıqda yerinə yetirilir.

Ödəmə kanallarının xüsusiyyətləri. Adi tranzaksiyalarla müqayisədə ödəmə kanallarının bəzi xarakterik xüsusiyyətləri var.

Ödəmə kanalını açmaq və müvafiq olaraq, gec və ya tez bağlamaq lazımdır. Bu ayrıca on-chain tranzaksiyalarla yerinə yetirilir. Onlar üçün tranzaksiya haqqı ödəmək lazımdır və təsdiqlənmələrini gözləmək zəruridir. Açan tranzaksiya üçün tam təsdiqlənməni gözləmək daha yaxşıdır.

Konkret kanalın daxilində ödəmələr yalnız əvvəlcədən müəyyən edilmiş məbləğ çərçivəsində mümkündür. Onu iştirakçıların özləri müəyyən edirlər və lazımi məbləği xüsusi Bitkoin skriptinin köməyi ilə dondururlar.

Ödəmə kanalı reallaşdırılma metodikasından asılı olaraq bir-istiqamətli (ing. mono-directional) və ya iki-istiqamətli (ing. bi-directional) ola bilər.

Kanalın yaşama müddətini və ödəmələrin maksimal sayını məhdudlaşdırmaq olar, metodikadan asılı olaraq, onlar qeyri-məhdud da ola bilərlər. Uyğun olaraq, kanalı müəyyən vaxt keçdikdən və ya vaxtından əvvəl bağlamaq olar. Kanalı həm hər iki iştirakçının qarşılıqlı razılığı ilə, həm də onlardan birinin istəyi ilə (bəzi xüsuslar var) bağlamaq olar.

Lightning Network texnologiyasının hazırki vəziyyəti. Lightning BOLT (Basis of Lightning Technology) adlı vahid spesifikasiya altında fəaliyyət göstərir. Lightning-in bu spesifikasiyanı həyata keçirən dörd əsas tətbiqi var: Lightning Network Daemon, CoreLightning, Eclair və Lightning Dev Kit.

Lightning-in beta versiyası Bitcoin Mainnet-də 15 mart 2018-ci ildə işə salınmışdı, lakin ciddi təhlükəsizlik məhdudiyyətləri də vardı. Təhlükəsizlik üçün göndərilən kriptovalyuta vahidlərinin sayına məhdudiyyət qoyulmuşdu – kanal 1 400 $ və bir ödəniş 400 $ ilə məhdudlanmışdı.

1ml.com saytından alınmış statistikaya görə (oktyabr, 2022), Lightning Network-da 11563 qovşaq var, onlardan 6379-u aktiv kanal işlədir. Ümumilikdə, 36328 kanal var və onların tutumu 897.91 BTC-dir.

Lightning şəbəkəsi Bitkoinin saniyədə milyon tranzaksiya sürətinə kimi miqyaslanması və tranzaksiya haqlarının sentin hissələrinə kimi azaldılması üçün potensial həll təklif edir. Lakin hələlik Lightning şəbəkəsinin Bitkoinin miqyaslanma problemini həll edə biləcəyini və texnologiyanın necə inkişaf edəcəyini söyləmək tezdir. Əgər uğurlu olacaqsa, onun Bitkoin ekosisteminə, xüsusilə Bitkoin maynerlərinə təsirini müşahidə etmək maraqlı olacaq (texnologiya Bitkoin mayninqin iqtisadi tərəfini dəyişə bilər). Bundan başqa, Lightning şəbəkəsinin uğuru Bitkoinin potensial tətbiq üsullarını da kökündən dəyişdirəcək. Sürətli və praktiki olaraq pulsuz tranzaksiyalar mikro-ödənişlər etməyə imkan verəcək, kütləvi populyarlaşma potensialını artıracaq və Bitkoini yeni səviyyəyə qaldıracaq.

Lightning Network sisteminin ilk texniki spesifikasiyasının həmmüəllifi Taddeus Driyya deyir: "Əgər siz fikirləşirsinizsə ki, Lightning şəbəkəsi Visa-nı əvəzləyəcək və dünyanı fəth edəcək, bu səhvdir." Onun sözlərinə görə, Lightning – Bitkoinin inkişafında vacib faktordur, lakin o hesab edir ki, digər tədbirlər, o cümlədən SegWit və aqreqasiya imzaları da tələb edilir.

11.4. SegWit-ə keçid problemləri

Segregated Witness (SegWit) konsepsiyası blokçeynlərdə miqyaslanma probleminin həlli üçün 2015-ci ildə hazırlanmışdı.

Məlum olduğu kimi, tranzaksiyalar iki əsas komponentdən ibarətdir: Input və Output. Input göndərənin açıq ünvanını, Output isə alıcının açıq ünvanını ehtiva edir. Bununla belə, göndərən digər istifadəçiyə köçürmək üçün lazımi miqdarda vəsaitə malik olduğunu sübut etməli və bunu rəqəmsal imza ilə təsdiqləməlidir.

SegWit-in əsas ideyası blokdakı məlumatları yenidən elə təşkil etməkdir ki, imzalar tranzaksiya məlumatlarından ayrı yerləşdirilsin. Başqa sözlə, SegWit-in yenilənməsi şahidləri (imzaları) tranzaksiyalardan ayırmaqdan ibarətdir. Bu, bir blokdakı tranzaksiyaların sayını artırmaqla şəbəkənin buraxma zolağını artırmağa imkan verir. Bundan əlavə, SegWit "tranzaksiyaların plastikliyi" səhvini də həll edir.

SegWit yenilənməsi 2017-ci ilin avqustunda Bitcoin şəbəkəsində softfork kimi kimi həyata keçirildi. Hazırda SegWit-dən istifadə edən bir neçə kriptovalyuta var, o cümlədən Bitcoin və Litecoin.

SegWit olmadan, imza məlumatları bütün blokun 65%-ni tuta bilər. SegWit, tranzaksiyanın girişlərindən imzaları silməyə imkan verir. Bu mühəndislik həlli blokun effektiv ölçüsünü 1 MB-dan təxminən 4 MB-a qədər artırmağa imkan verir.

Lakin SegWit blokun özünün ölçüsünün artırılması demək deyil (bu, yalnız hardfork halında mümkündür). Həqiqi blok ölçüsü yenə də 1 MB-dır, lakin effektiv ölçü həddi 4 MB olacaq.

Blokun ölçüsü anlayışı əvəzinə SegWit "blok çəkisi" anlayışını daxil edir. Prinsipcə, blok çəkisi tranzaksiya məlumatları (1 MB) və artıq Input-un bir hissəsi olmayan imzalar (3 MB-a qədər) daxil olmaqla blokun bütün məzmununu ehtiva edən ölçüdür.

SegWit-in üstünlükləri aşağıdakılardır:

- blokda daha çox tranzaksiya yerləşdirmək olur;
- blokun mayninqinə ayrılmış sabit zaman ərzində daha çox tranzaksiya emal olunur və deməli, bir saniyədə emal olunan tranzaksiyaların sayı (TPS, transactions per second) artır;

TPS-in artması Bitcoin şəbəkəsində əməliyyat xərclərini də azaldır. Yenilənməyə qədər tranzaksiyalar üçün 30 dollar ödənirdisə, SegWit komissiya xərcini 1 dollardan aşağı salır.

Tranzaksiyaların plastikliyi. Bitkoinlə bağlı əsas problemlərdən biri tranzaksiyanın rəqəmsal imzasını saxtalaşdırmaq imkanı idi. İmzada ən kiçik dəyişiklik olsa, bu, iki tərəf arasında bütün tranzaksiyaya təsir göstərər. Blokçeyndə saxlanan məlumatlar praktiki olaraq dəyişməz olduğundan, bu cür əməliyyatlar blokçeyndə əbədi olaraq qala bilər.

SegWit sayəsində imzalar artıq tranzaksiyaların bir hissəsi deyil və bu da öz növbəsində bu cür məlumatların dəyişdirilməsi imkanını aradan qaldırır. Bu düzəliş ikinci səviyyə protokolları və ağıllı müqavilələr də daxil olmaqla, blokçeynlərdə əlavə yeniliklərə imkan verdi. Ən populyar 2-ci səviyyə protokollarından biri Lightning Network və ofçeyn mikroödəmə şəbəkəsidir.

SegWit2x. SegWit geriyə doğru uyğunluğu olan softfork-dur. Başqa sözlə, Bitcoin şəbəkəsində yenilənməmiş qovşaqlar tranzaksiyaları emal etməyə davam edə bilərlər. Bununla belə, SegWit-in şəbəkənin hardforkunu nəzərdə tutan SegWit2x (S2X) adlı başqa bir versiyası da təklif edilmişdi.

SegWit və SegWit2x arasındakı əsas fərq – hardfork versiyası tranzaksiyaların paketlənmə qaydasını dəyişdirməklə yanaşı, həm də blok ölçüsünü artırır (1 MB-dan 2 MB-a qədər).

Digər diqqətəlayiq fərq, SegWit yeniləməsinin Bitcoin icması tərəfindən dəstəklənməsi və həyata keçirilməsidir. Belə hadisə UASF (user-activated soft fork) adlı konsepsiyanın yaranmasına səbəb oldu.

Digər tərəfdən, SegWit2x Bitkoini idarə edən əsas qaydalardan birinə əhəmiyyətli dəyişiklik təklif edirdi. Lakin yeniləmənin qəbulu və tətbiqi ilə bağlı konsensus əldə edilmədiyinə görə, SegWit2x-in inkişafı dayandırıldı.

11.5. Ethereum-un miqyaslanması mexanizmləri

Miqyaslanma Ethereum blokçeynində də əsas problemlərdən biridir. Ethereum-un buraxma qabiliyyəti və sürət baxımından üzləşdiyi mövcud məhdudiyyətlər onun daha qlobal miqyasda istifadəsinə mane olur.

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

Ethereum Plasma. Ethereum-da miqyaslamanı artırmağın yollarından biri Plasma-dır, onu başqa blokçeynlər üçün də tətbiq etmək olar. Plasma-nın konsepsiyası 2017-ci ilin avqustunda işlənmişdi, həmmüəlliflərdən biri Bitkoin üçün Lightning Network konsepsiyasını hazırlayanlardan biri idi. Plasma və Lightning Network blokçeynin miqyaslanması üçün təkliflərdir, lakin hər birinin öz mexanizmi və xüsusiyyətləri var.

Ethereum Plasma-nın əsas ideyası off-chain freymvorku yaratmaqdır, yan zəncirlər əsas blokçeynlə mümkün qədər az qarşılıqlı əlaqədə olurlar. Belə freymvork blokçeyn ağacı ilə işləmək üçün nəzərdə tutulub. Ağac yerarxik şəkildə elə qurulub ki, əsas blokçeyn üzərində çox sayda kiçik zəncirlər yaratmaq olar. Bu kiçik zəncirlərə Plasma deyilir.

Plasma strukturu ağıllı müqavilələr və Merkl ağaclarından istifadə etməklə qurulur, bu da əsas Ethereum blokçeyninin mahiyyətcə daha kiçik nüsxələri olan qeyri-məhdud sayda kiçik zəncir yaratmağa imkan verir. Hər kiçik zəncirin üzərində çox sayda başqa zəncirlər də yaratmaq olar, ağac strukturu da məhz bunun nəticəsində yaranır.

Ethereum Plasma-nın MapReduce funksiyası çox sayda blokçeynlərdə verilənləri təşkil edir və hesablayır.

Özünü yoxlamaq üçün suallar

1. Blokçeyn şəbəkəsinin miqyaslanması hansı üç parametr arasında balanslaşdırmanı tələb edir?
2. Blokçeynin miqyaslanması trilemması nədir?
3. Saydçeynin iş prinsipi nədir?
4. Miqyaslanmanın təmin edilməsi üçün hansı yanaşmalar var?
5. SegWit-in əsas ideyası nədən ibarətdir?
6. Sharding nədir?

7. Praktikada yüksək sürəti olan blokçeynlərdə, adətən, nədə güzəştə gedilir?
8. Kriptoqrafiyada ən çətin məsələ hansı məsələdir?
9. Hansı texnologiya blokçeynlərin iyerarxiyasından istifadə edir?
10. Təklif edilmiş blokçeyn həllərini hansı kriteriyalara görə qiymətləndirmək zəruridir?
11. Hansı saydçeyn platformaları var?
12. Saydçeyn federasiyası nədir?
13. Güclü saydçeyn federasiyasında hansı mexanizmlər var?
14. Ethereum Plasma-nın əsas ideyası nədir?
15. Lightning Network-da ödəmə kanallarını hansı müddətdən sonra bağlamaq olar?
16. Blokun ölçüsü anlayışı əvəzinə SegWit-də hansı anlayış daxil edilir?
17. SegWit və SegWit2x arasındakı əsas fərq nədir?
18. SegWit konsepsiyası blokçeynlərdə hansı problemi həll etmək üçün nəzərdə tutulub?
19. SegWit olmadan, imza məlumatları bütün blokun neçə faizini tuta bilər?
20. SegWit hardforkdur, yoxsa softfork?

Mühazirə 12. Blokçeyn platformaları. Blokçeynin tətbiq sahələri

12.1. Ekskluziv blokçeynlər üçün freymvorklar

Ekskluziv blokçeynlər üçün freymvorkların işlənməsinə bir neçə il əvvəl başlanıb. Onların əksəriyyəti açıq kodludur. Populyar freymvorklardan aşağıdakıları göstərmək olar:

- **IBM Fabric.** IBM şirkəti öz blokçeyn freymvorkunun yaradılmasına 2015-ci ildə başlamışdır. Freymvork Go dilində yazılıb və ağıllı müqavilələri reallaşdırmaq üçün doker-konteynerləri istifadə edir. IBM şirkəti 2016-cı ildə The Linux Foundation idarəsi altında Hyperledger layihəsinin təsisçilərindən biri olmuşdur – blokçeynlər və paylanmış reyestrlər üçün sənaye standartlarının işlənməsinə yönəlmişdir.
- **Intel Sawtooth Lake.** Intel blokçeynə Əşyaların İnterneti baxımından yanaşır (Internet of Things). Sawtooth Lake-in xüsusiyyətlərindən PoET (Proof of Elapsed Time) konsensus alqoritmini göstərmək olar, bu alqoritm son nəsil Intel prossessorlarında olan SGX etibarlı hesablamalar moduluna əsaslanır. Python-da reallaşdırılıb.
- **R3 Corda.** Corda — dünyanın ən böyük banklarını birləşdirən R3 konsorsiumunun işinin nəticəsidir (R3 konsorsiumu 2015-ci ildə yaradılmışdı). Baxılan digər freymvorklardan fərqli olaraq Corda blokçeyn deyil, paylanmış reyestrlər qurur: Corda-da blok anlayışı və verilənlərin böyük miqyaslı replikasiyası anlayışı yoxdur. Corda sistemi Kotlin-də yazılıb və JVM-ə uyğun istənilən dildə yazılmış ağıllı müqavilələri dəstəkləyir.
- **Enterprise Ethereum**. Ethereum açıq blokçeyn olsa da, onun yaradıcıları proqram kodunun ekskluziv blokçeynlərin yaradılması üçün də istifadə edilməsinə böyük diqqət ayırırlar. 2017-ci ilin əvvəlində onlar Enterprise Ethereum alyansının yaradıldığını elan etmişlər, onun məqsədi biznesə yönəlmiş funksiyaların işlənməsidir (məsələn konsensus alqoritminin ayrıca modula salınması).

Sadalanmış həllərdən başqa bir çox digər freymvorklar da vardır: Chain, Monax, Symbiont, Axoniи və s. Bitkoin blokçeynini korporativ mühitə yaxınlaşdıran bəzi təşəbbüslər də vardır, məsələn, BloqEnterprise.

12.2. Hyperledger layihəsi

Hyperledger layihəsi blokçeyn ekosistemini dəyişməyi, onu daha güclü və məhsuldar etməyi hədəfləyir. Hyperledger – açıq ilkin koddur və kriptovalyutaya heç bir aidiyyəti yoxdur.

Layihə komitəsinin texniki tərkibinə 12 üzv-şirkət daxildir. Layihənin əsas üzvləri – Microsoft, IBM, Fujitsu, SAP, Huawei, Nokia, Intel, Samsung və digər texnologiya nəhənglərdir.

Bundan başqa, üzv-şirkətlər siyahısına maliyyə institutları (Deutsche Börse, American Express, J.P. Morgan və s.), həmçinin blokçeyn-startapları (Netki, Lykke, Factom, Consensys və s.) daxildir.

Hyperledger platformasının məqsədi – yüksək məsuldarlıqlı və etibarlı blokçeynlərin və paylanmış reyestrlərin yaradılması yolu ilə sahələrarası əməkdaşlığı inkişaf etdirməkdir. Nəticədə platforma əsas texnologiya, maliyyə və təchizat zəncirlərinin qlobal biznes-tranzaksiyalarını dəstəkləməlidir.

Hyperledger "çətiri" altındakı layihələr. Hyperledger blokçeyni bir sıra biznes tətbiqləri inkişaf etdirməyə kömək edir – paylanmış bazalar, ağıllı müqavilələr, qrafiki interfeyslər, kliyent kitabxanaları, xidməti proqramlar. Açıq proqram kodu geniş yayılmış tətbiqi proqramları təkrar istifadə etməyə imkan verir. Artıq mövcud olan platformalara innovasiyalar, yeni servislər və imkanlar inteqrasiya etmək olar.

Qlobal layihənin «çətir» strategiyası ilk növbədə, qlobal biznesin genişlənməsinə və bütün iştirakçılar arasındakı proseslərin təkmilləşdirilməsinə yönəlib. Bura Əşyaların İnternetindən, loqistikadan, sənayedən və s. layihələr də aiddir.

Hazırda Hyperledger blokçeynində beş əsas freymvork inkişaf etdirilir:

1 **Hyperledger Burrow** – modul blokçeyn-kliyentdir, 2014-cü ildə işlənib. Ağıllı müqavilə interpretatoruna malikdir, Ethereum vrtual maşınının (EVM) spesifikasiyası üçün qismən işlənmişdir.
2 **Hyperledger Fabric** – qoşulan platformadır, geniş miqyaslanan tətbiqlərin işlənməsi üçün baza rolunu oynayır. Çevik icazələr səviyyəsinə malikdir. Layihənin konsepsiyası IBM-ə məxsusdur.
3 **Hyperledger Iroha** – paylanmış reyestr əsasında işləyir. Onun əsas məsələsi – infrastruktur layihələrinə asanlıqla qoşulmaqdır.
4 **Hyperledger Sawtooth** – yeni Proof of Elapsed Time (PoET) konsensus alqoritmi ilə modul platformadır. Onunla paylanmış reyestrlərin işi reallaşdırılır. PoET-in xüsusiyyəti – resurslardan minimal istifadə və sosiumda tətbiq edilməsidir.
5 **Hyperledger Indy** – mərkəziyətsiz identifikasiya üçün istifadə edilir. Layihə müstəqil rəqəmsal identifikatorların yaradılması və tətbiqi üçün dəfələrlə istifadə edilən servislər təqdim edir.

Hyperledger alətləri. Blokçeynin açıq kodlu alətləri layihələrin işini asanlaşdırmağa, prosesi daha rahat və sadə etməyə imkan verirlər. Aşağıdakı Hyperledger alətlərini göstərmək olar:

- Hyperledger Cello – “blokçeyn xidmət kimi” reallaşdırılması üçün alətdir. Blokçeyn-şəbəkədə şəbəkənin işini idarə etmək, yaratmaq və başa çatdırmaq üçün istifadə edilir;
- Hyperledger Composer – biznes-şəbəkələr üçün modeldir, ağıllı müqavilələrin yaradılmasını sürətləndirir;
- Hyperledger Explorer – şərti olaraq “brauzer” adlandırmaq olar. Blokçeynlərdə tranzaksiyalara və əlaqədar verilənlərə baxmağa və istifadə etməyə icazə verir.
- Hyperledger Quilt – rəqəmsal fərdi verilənlər üçün tətbiqi komponentlərdir. ILP (Interledger Protocol) ödəniş protokolu əsasında işləyir.

12.3. Blokçeyn bulud xidməti kimi

Blokçeyn texnologiyaları sürətlə inkişaf edir, yeni məhsullar, yeni tətbiq sahələri, yeni istifadə senariləri meydana çıxır, yeni alyanslar və konsorsiumlar yaradılır. Yeni istiqamətlərdən biri də Blokçeyn bulud xidməti kimi (Blockchain as a Service, BaaS) təşkil olunmasıdır.

Bulud növləri ilə blokçeynin aşağıdakı variantlarda bir çox inteqrasiya senariləri mövcuddur:

- IaaS (Infrastructure as a Service) – mayninq;
- PaaS (Platform as a Service) – ekosistem, proqram təminatının işlənməsi;
- SaaS (Software as a Service) – müxtəlif blokçeyn xidmətləri.

Azure BaaS – blokçeyn ilə buludların birgə tarixinin başlanğıcıdır. Layihə 2015-ci ilin noyabrında Microsoft Azure, Ethereum və ConsenSys şirkəti ilə birlikdə işə salınmışdı, əvvəlcə Azure Ethereum BaaS adlanırdı. Proqram təminatı yaradıcılarına və prosessinq şirkətlərinə yönəlib.

Azure BaaS ekosisteminə aşağıdakılar daxildir:

- BlockApps STRATO
- Ether.Camp IDE
- Go Ethereum client
- C++ Ethereum client
- Augur (proqnozlaşdırma)
- Stock.it (IoT)
- Ethereum on Windows Server

BlockApps STRATO – Azure BaaS Marketplace-də sertifikat almış ilk məhsuldur (2016-cı ilin fevralı). Ethereum tətbiqlərin sürətli prototipləşdirilməsi üçün yaratma və testetmə platformasıdır. Linux virtual maşını Azure üçün ConsenSys tərəfindən təqdim olunur. Haskell-də yazılıb, mikroservis arxitekturasına malikdir və

REST API-ni dəstəkləyir. Ethereum Solidity ağıllı müqavilə dilini dəstəkləyən Block SDK daxildir. Qiyməti saatda 0,214 avrodan başlanır (ayda 159 avro).

Azure BaaS tətbiq etmək üçün Azure Marketplace, Azure Resource Manager şablonları və Azure DevTestLab artefaktlarını istifadə etmək olar.

BaaS-ın ilk uğuru R3 CEV testləridir. 2016-cı ilin yanvarında R3 CEV (Crypto, Exchanges, Ventures) bank konsorsiumu Ethereum platforması əsasında yaradılan banklararası maliyyə xidmətlərini uğurla test etmişdi. Əlaqəlilik, tranzaksiyalar reyestrinin aparılması, autentifikasiya və validasiya yoxlanmışdı. Testlər Azure Ethereum BaaS bulud servislərində aparılmışdı.

R3 CEV testlərinin iştirakçıları: Barclays, BMO Financial Group, Credit Suisse, Commonwealth Bank of Australia, HSBC, Natixis, Royal Bank of Scotland, TD Bank, UBS, UniCreditand Wells Fargo idi.

BAAS-ın bulud provayderləri üçün aşağıdakı üstünlükləri var:

- BaaS bulud provayderinin xidmətlər portfelinin genişlənməsinə şərait yaradır və onun bulud resurslarının istehlakının artmasına səbəb olur.
- Konkret blokçeyn-platformasına və ya konkret blokçeyn servisinə bağlı deyil. Provayderin təqdim etdiyi müxtəlif platforma və servislər nə qədər çoxdursa, bu provayder üçün bir o qədər yaxşıdır.
- Blokçeyn-cəmiyyəti daim genişlənir, o cümlədən bulud texnologiyaları ilə iş təcrübəsi olanlar artır, bu təcrübədən onlar blokçeynlə əlaqəli məsələlərin həlli üçün də istifadə edəcəklər.
- Blokçeynin tətbiq sahələri daim genişlənir, deməli, yeni biznes sahələri BaaS üçün buluda gələcəklər.
- Blokçeyn platforma (dizayn, alqoritmlər, protokollar, proqram kodu) açıqdır. Heç bir birbaşa lisenziya ödəmələri yoxdur. Bulud provayderi yalnız istehlak edilən resurslara görə haqq alır.

12.4. Blokçeyn texnologiyasının tətbiq sahələri

"Blockchain. Blueprint for a New Economy" kitabında Melanie Swan blokçeyn texnologiyasının üç tətbiq sahəsini fərqləndirir:

- Blockchain 1.0 – kriptovalyutalar (maliyyə tranzaksiyaları ilə əlaqəli olan müxtəlif sahələrdə tətbiq edilir, məsələn, pul köçürmələri və elektron ödəniş sistemlərində);
- Blockchain 2.0 – müqavilələr (alətlərin müxtəlif növləri ilə – səhmlər, istiqrazlar, fyuçerslər, aktivlər, kontraktlar və s. ilə işləyən iqtisadiyyat, maliyyə və bazarlar sahəsində tətbiqlər);
- Blockchain 3.0 – maliyyə tranzaksiyaları və bazarlarından fərqli sahələrdə tətbiq edilir (dövlət idarəçiliyi, səhiyyə, elm, təhsil və s. sferalarına yayılır).

Blokçeynin dövlət sektorunda potensial istifadəsinin vacib üstünlükləri təhlükəsizlik (tranzaksiyaların təsdiqlənməsi üçün kriptoqrafiya), dəyişilməzlik

(blokçeynin cari vəziyyəti əvvəlki tranzaksiyalardan asılıdır) və şəffaflıqdır (açıq və paylanmış saxlanma sayəsində).

- Kriptovalyutalar – ilk tətbiq sahələrindən biridir
- Maliyyə: banklararası hesablaşmalar, hüquqi və fiziki şəxslər arasındakı hesablaşmalar, ödənişlər, qiymətli kağızlar, kredit tarixçələri
- Notarius, kadastrlar, mülkiyyət hüququ reyestrləri, zəmanət institutu, depozit
- Vergilər və müavinətlər, pozuntu və cərimələr
- Vətəndaşların identifikasiyası (pasportlaşdırma), vətəndaş vəziyyəti aktlarının qeydiyyatı, dövlət xidmətləri
- Səhiyyə: tibbi sığorta, tibbi kartlar, xəstəlik tarixçələri
- Təhsil: imtahan nəticələri, diplomlar, rezümelər
- İncəsənət obyektlərinin və müəllif hüququ obyektlərinin transferi
- Təchizat, malların mənşəyinin izlənməsi, saxta mallarla mübarizə
- Ədalətli seçki sistemləri
- Loyallıq proqramları
- Lotereyalar, proqnozlaşdırma bazarı
- Sənəd dövriyyəsi sistemləri, istənilən paylanmış verilənlər saxlancları
- İstifadəçilərin autentifikasiyası, mesencerlər, DNS
- IoT

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

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

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

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

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

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

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

Özünü yoxlamaq üçün suallar

1. Ekskluziv blokçeynlər üçün hansı populyar freymvorklar var?
2. IBM Fabric ağıllı müqavilələri reallaşdırmaq üçün nədən istifadə edir?
3. Enterprise Ethereum hansı blokçeynlər üçün nəzərdə tutulub?
4. R3 Corda freymvorku blokçeynlərlə, yoxsa paylanmış reyestrlərlə işləyir?
5. Hyperledger layihəsinin məqsədi nədir?
6. Hyperledger layihə komitəsinin texniki tərkibinə hansı üzv-şirkətlər daxildir?
7. Hazırda Hyperledger blokçeynində hansı freymvorklar inkişaf etdirilir?

8. Hansı Hyperledger alətlərini göstərə bilərsiniz?
9. Blockchain 1.0 hansı sahələrdə tətbiqi nəzərdə tutur?
10. Blockchain 2.0 hansı sahələrdə tətbiqi nəzərdə tutur?
11. Blockchain 3.0 hansı sahələrdə tətbiqi nəzərdə tutur?
12. Hyperledger Indy hansı servislər təqdim edir?
13. Blokçeynin dövlət sektorunda potensial istifadəsinin vacib üstünlükləri nədir?
14. Hyperledger Explorer nəyə imkan verir?
15. Hyperledger platforması hansı zəncirlərdə qlobal tranzaksiyaları dəstəkləməlidir?
16. Sawtooth Lake hansı konsensus alqoritmini istifadə edir?
17. Hyperledger Quilt hansı ödəniş protokolu əsasında işləyir?
18. Intel Sawtooth Lake blokçeynə necə yanaşır?
19. Enterprise Ethereum alyansının məqsədi nədir?
20. Hyperledger Composer hansı işi sürətləndirir?

Mühazirə 13. Yeni kriptovalyuta növü: NFT

13.1. NFT-nin iş prinsipi

NFT (Non-Fungible Token – qarşılıqlı dəyişdirilə bilməyən token) son illər kriptovalyuta sənayesinin əsas trendlərindən biridir. Tənqidlərə baxmayaraq, NFT-lər populyarlıq qazanmağa və GameFi kimi əlaqəli sahələrdə tətbiqlər tapmağa davam edir.

Qeyd edək ki, FT (Fungible Token) – ERC-20 kimi standartlar əsasında yaradılmış dəyişdirilə bilən tokenlərdir (məsələn, kriptovalyutalar).

NFT tokenləri hər hansı unikal elementin rəqəmsal obrazını yaradan sertifikatdır (uçot vahididir). Onlar: rəsmlər, fotolar, videolar, musiqilər, giflər – bir sözlə, ən azı hər hansı unikallığa iddia edən istənilən kontent ola bilər. Onlar kolleksiyaçılar, oyunçular və sənət həvəskarları arasında yüksək qiymətləndirilir və hərraclar vasitəsilə alınıb satılır.

NFT standart kriptovalyuta tokenindən onunla fərqlənir ki, o, heç bir şəkildə bölünə, dəyişdirilə və ya saxtalaşdırıla bilməz. Beləliklə, hər bir NFT virtual obyekt üçün sertifikatdır, ona eksklüziv hüquqlar verir və orijinallığını təmin edir.

Tokenlər blokçeyndə saxlanır. NFT unikal əşyaları real dünyadan blokçeynə ötürmək üçün bir yoldur. Bu tokenlərin hər biri unikaldır, bölünməzdir və yeganə nüsxədə mövcuddur. Bundan əlavə, bu barədə bütün lazımi məlumatlar blokçeyndə etibarlı şəkildə saxlanır.

Unikallıq müxtəlif ola bilər. Məsələn, ilk SMS 150 min dollara satılıb, Twitter-in qurucusu Cek Dorsinin ilk tvitini az qala 3 milyona alıblar. Bundan sonra digər məşhurlar da NFT-yə yönəlməyə başlayıblar.

NFT-lərə yalnız unikallıq baxımından qiymətli bir şey kimi qəbul etmək lazım deyil, onlar həm də əla investisiya alətidir.

NFT-lərlə işləyən bir çox platforma var. Bəziləri dar ixtisaslaşmış bazar-yerləridir (Huobi NFT, NFT Stars) və satılan obyektlərin kateqoriyalarına görə fərqlənirlər: yalnız video oyunlar, rəqəmsal incəsənət əşyaları və s.

Tanınmış platformalara OpenSea, Rarible, Nifty Gateway və SuperRare daxildir. Platformalar ETH ilə komissiya haqqı alırlar (NFT-lər Ethereum infrastrukturunun əsasında yaradılıb). Komissiya haqqı dəyişkəndir, lakin adətən, bir neçə on dollar olur.

Hazırda NFT-lərin yaradılması üçün ən populyar blokçeyn Ethereum-dur: mövcud NFT-lərin 90%-i onun vasitəsilə satılır. NFT-lər Ethereum-a alternativ olan digər blokçeynlərdə də yaradıla bilər. Bunlara Binance Smart Chain, Cardano, Solana, Tezos daxildir.

Ethereum şəbəkəsində NFT-lər üçün populyar standartlar ERC-721 və ERC-1155-dir. ERC-721 bir NFT üçün istifadə edilir. ERC-1155 isə tokenlər paketi (batch) üçün nəzərdə tutulub və genişlənmiş funksionala malikdir.

Tarixi məlumat. NFT-lər nisbətən yeni fenomendir. Konsepsiya kimi NFT 2010-cu illərin ortalarından məlum idi, lakin ilk NFT layihələri yalnız 2017-ci ildə həyata keçirilib. NFT-lərin populyarlaşması CryptoKitties-in xidmətidir, bu, virtual pişiklər yetişdirilən bir oyundur. Oyun son dərəcə populyar olmuş və rəqəmsal pişiklər 100 min dollardan artıq qiymətə satılmışdı. 2021-ci ildə NFT-lərin ümumi satış həcmi 24,9 milyard dollar olmuşdu.

13.2. NFT-tokenin yaradılması, alınması və satılması

NFT yaratmaq üçün sizə kripto-pulqabı və rəqəmsal məzmunlu fayl lazımdır. NFT yaratmaq istəyən istifadəçilər platformaya faylı yükləyirlər, ona ad və təsvir fikirləşirlər. NFT rəqəmsal məzmunu: video, mahnı və ya rəsmi blokçeyndə yazıya çevirməklə yaradılır. NFT yaradıldıqdan sonra o, hərraca çıxarıla bilər. Eyni zamanda, NFT yaradıcısı orijinalın nüsxələrinin sayını məhdudlaşdıra və hər satışdan qonorar ala bilər.

OpenSea (https://opensea.io/) timsalında NFT-tokenin yaradılmasını aşağıdakı addımlarla etmək olar (hər hansı kriptopulqabı tələb edilir).

1. Saytı açırıq.
2. **Create – My collections** seçirik.
3. Kolleksiyanı yaradırıq, ona ad veririk, təsvirini və loqotipini əlavə edirik.
4. Kolleksiyaya tokenlər əlavə edirik. Bunun üçün **Add items**, sonra isə **Add new item** seçmək lazımdır.
5. Tokeni uğurla yüklədikdən sonra onu hərraca (auksiona) çıxarırıq.

NFT-nin yaradılması üçün platfotma saytı ya token göründükdən dərhal sonra, ya da satış zamanı istifadəçidən komissiya alacaq.

NFT almaq istəyənlər bunu müəllifə bildirir və pul köçürdükdən sonra onlara unikal blokçeyn məlumatları olan rəqəmsal sertifikat verilir. O, aktivi cihazda – telefonda və ya kompüterdə saxlaya bilər. Sahib obyektin həqiqiliyini təsdiqləmək üçün surət çıxarılarkən digər istifadəçilərə açıq açarlar vermək hüququna malikdir.

NFT özü əbədi saxlancda (Inter-Planetary File System) saxlanır. Alıcıdan əlavə, bütün istifadəçilər onu izləyə və yükləyə bilərlər, lakin yalnız alıcıda sertifikat olur.

NFTgo analitik portalının statistikasına görə, NFT bazarının kapitallaşması təxminən 22 milyard dollar təşkil edir. Ən böyük payı NFT avatarlar tutur, ikinci yerdə rəqəmsal kolleksiya əşyalarıdır, daha sonra oyunlar üçün NFT-lərdir.

13.3. NFT və Metaverse üçün tokenlər

Blokçeyn şirkətləri artıq bir müddətdir ki, virtual reallıq yaratmaqla məşğuldurlar. Decentraland, Sandbox və Somnium Space xüsusi sosial platformalar yaradırlar, burada

insanlar qarşılıqlı əlaqədə ola bilər, rəqəmsal daşınmaz əmlak və digər malları satın ala və istifadə edə bilərlər və biznes edə bilərlər. Metaverse (metakainat) hazırda kriptovalyuta cəmiyyətində aktual mövzudur və bir çox layihələr buna diqqət yetirirlər. Bəzi tokenlər ümumi sıradan fərqlənirlər, onlar "oyna-qazan" (Play-to-Earn) modelindən istifadə edirlər, bu model oyunçuların metakainat oyunlarında aktivliyinə görə kriptovalyuta ilə mükafatlandırılmasını nəzərdə tutur. Aşağıda bu tokenlərdən bəziləri barədə qısa məlumat verilir.

Decentraland (MANA) – açıq kodlu metakainatdır, qeyri-kommersiya Decentraland Fondunun nəzarəti altında 2020-ci ilin fevralında işə salınıb. İstifadəçilər MANA kriptovalyutası ilə ödəniş edərək Decentraland-da NFT şəklində virtual torpaq sahələri və əşyalar ala bilərlər. Layihənin saytına görə, bu, "istifadəçilərin özlərinə məxsus olan ilk virtual dünyadır".

Decentraland oyunçuları avatar-personaj vasitəsilə virtual dünya ilə qarşılıqlı əlaqədə olurlar. Personaj Decentraland dünyasında sərbəst hərəkət edə, digər istifadəçilərlə ünsiyyət saxlaya və digər hərəkətlər edə bilər, məsələn, rəsmlər ala, kazinoda oynaya, mühazirələrdə iştirak edə bilər.

Avatarları tam fərdiləşdirmək olar. Seçmək üçün yüzlərlə pulsuz geyim var. Avatarı fərdiləşdirmək üçün MANA ilə unikal geyim əşyaları almaq olar.

Hər bir avatarın Decentraland pasportu var, pasport istifadəçinin Ethereum pulqabına qoşulur. Pasportda oyunçunun bütün MANA və əşyaları qeyd edilir.

Gələcəkdə Decentraland Universitetinin açılması planlaşdırılır, istifadəçilər müəyyən sahələr üzrə tamhüquqlu təhsil ala biləcəklər, onlara sertifikatlar veriləcək və iş imkanları olacaq.

Decentraland metakainatının təməl daşı LAND NFT tokenləri (ERC-721) formatında virtual torpaq almaq imkanıdır. Bu torpaqda müxtəlif obyektlər və binalar tikmək olar. Sonra torpağı pula çevirmək və ya satmaq olar. LAND sahələri ilə yanaşı, Estate tokenləri də var.

Yeni və ya artıq istifadə edilmiş torpaq sahələri almaq olar. Hərraclar da mövcuddur. Torpaq aldıqdan sonra orada müxtəlif obyektlər və hətta bütöv ekosistemlər tikmək olar. Məsələn, ağacları olan bir sahə əkə, üzərində villa və ya kvartal tikə, yadplanet və ya fantastik mühiti simulyasiya edə bilərsiniz. Tikinti üçün proqramlaşdırma tələb edilmir: Decentraland istənilən sahəyə tətbiq oluna bilən çoxlu hazır səhnələr və obyektlər təklif edir.

Hər bir sahənin və ya rayonun qiyməti onun Genesis Plaza, yollar, kəsişmələr və s. kimi digər mühüm obyektlərə yaxınlığı ilə bağlıdır. Ən bahalı sahələr Prime adlanır.

LAND tokenlərinin sayı məhduddur: 90 min. Hər bir torpaq sahəsinin ölçüləri 33x33 fut və ya 10.05x10.05 metrdir. Binaların hündürlüyünə heç bir məhdudiyyət

yoxdur, buna görə də nəzəri olaraq Decentraland sahələrində tikilinin hündürlüyü sonsuz ola bilər.

MANA tokeninin özü 2017-ci ilin sentyabrında hər biri 2,5 sentlə ticarətə başlamışdı. Ən yüksək səviyyəsi olan 5,4792 dollara 24 noyabr 2021-ci ildə çatıb, hazırda 0,5465 dollara düşüb.

Axie Infinity (AXS) – Axie adlanan fantastik personajların sahiblərinin icmasıdır. Layihənin veb saytı dəqiqləşdirir ki, Axie – *«oyunçuların qismən sahib olduğu və idarə etdiyi yeni oyun növüdür»*. İstifadəçilər onları alıb sata, döyüşdürə, çoxalda bilərlər. Əsas Axie siniflərinə vəhşi heyvanlar, həşəratlar, bitkilər, sürünənlər, quşlar, suda üzənlər daxildir. Axie-lər oyun yaradıcılarının Lunacia adlandırdıqları dünyada yaşayırlar. İstifadəçilər oynamaqla AXS tokenləri qazanırlar və onları oyunun gələcəyini müəyyən etmək üçün istifadə edirlər.
Oyunun məqsədi Axie-lərdən mümkün qədər daha güclü və unikal ordu toplamaqdır. Bunun üçün digər oyunçularla birləşmək də olar. Formalaşdırılan ordunu digər oyunçulara qarşı döyüşə göndərmək olar. Onlar həmçinin macəra axtarışında Lunacia ətrafında səyahət edirlər.
AXS 2020-ci ilin noyabrında tokeni 0,15 dollar olmaqla bazara çıxmışdı və 6 noyabr 2021-ci ildə 160,36 dollar maksimumuna qalxmışdı, hazırda 7.74 dollardır.

Enjin (ENJ) NFT-yə hədəflənmiş kriptovalyutadır, NFT-nin istifadəsini asanlaşdırır: «*Biznesi inkişaf etdirmək, qazanmaq və ticarət etmək, oyunlar və proqramlarla inteqrasiya etmək üçün istifadə edə biləcəyiniz NFT-lər*» yaratmağa kömək edir.
ENJ 2017-ci ilin noyabrında token 1,7 sent olmaqla bazara çıxıb. 24 noyabrda kriptovalyuta $4,6858 pik qiymətə çatıb, bu sətirlər yazılanda $0.3844 qiymətinə düşmüşdü.

The Sandbox (SAND) – onlayn oyun platformasıdır, "qum yeşiyi" (sandbox) janrında virtual dünyadır. 2012-də işə salınıb, NFT və metakainata yönəlmiş kriptovalyutalardan biridir. Onun saytında qeyd edilir: *«Sandbox – virtual metakainatdır, burada oyunçular oynaya, yarada və öz virtual qarşılıqlı əlaqələrini pula çevirə bilərlər. Biz rəssamlara, yaradıcılara və oyunçulara öz kreativliklərini üzə çıxarmaq üçün vasitələr təqdim etməklə həmişə istədikləri platformanı yaratmağa imkan veririk»*.

Layihənin metakainatı "kubik" qrafiklərdən istifadə edən Minecraft-ı xatırladır. İstifadəçilər virtual dünyanı sərbəst inkişaf etdirə, daşınmaz əmlak və obyektlər yarada, yerdəyişmə edə və mini-oyunlarda iştirak edə bilərlər. Sandbox metakainatı NFT şəklində təqdim olunan obyektlərdən qurulub. Obyektlərə binalar, əşyalar və daşınar elementlər daxildir.

Metakainat 166464 sahədə yerləşir (408x408). Hər bir sahənin ölçüsü 96x96 metrdir. Metakainat voksellərdən (həcmli piksellərdən) ibarətdir. Virtual aləmdə bir kubmetr üç koordinat üzrə 32 vokselə bölünür.

Oyunçunun bir neçə ərazisi olan daşınmaz əmlakı ola bilər. Müxtəlif ölçülü daşınmaz əmlak var:

- Kiçik: 9 sahə daxildir (3x3 ölçüdə);
- Orta: 36 sahə daxildir (ölçüsü 6x6);
- Böyük: 144 sahə daxildir (ölçüsü 12x12);
- Çox böyük: 576 sahə daxildir (ölçüsü 24x24).

Layihə Ethereum blokçeynində qurulub. Oyunçular metakainatın hissələrinə sahibdirlər, hissələr LAND tokenləridir (NFT). İstifadəçilər NFT şəklində təsvir olunan virtual dünya obyektlərini də yarada bilərlər.

Rəqəmsal daşınmaz əmlak və obyektlər Sandbox Marketplace-də satılır. Nativ SAND tokenləri metakainat ilə qarşılıqlı əlaqədə olmaq, platformada ödənişlər etmək və digər məqsədlər üçün istifadə olunur.

SAND avqust 2020-də bazara çıxıb, token 5,1 sent idi, 24 noyabr 2021-ci ildə 8,4022 dollara çatmışdı. Hazırda SAND-ın qiyməti $0.5751 ABŞ dollar ətrafındadır.

Özünü yoxlamaq üçün suallar

1. NFT nədir?
2. FT nədir?
3. NFT standart kriptovalyuta tokenlərindən nə ilə fərqlənir?
4. NFT-lərin yaradılması üçün ən populyar blokçeyn hansıdır?
5. Hansı NFT platformaları populyardır?
6. NFT-lər Ethereum-a alternativ hansı blokçeynlərdə yaratmaq olar?
7. NFT və metakainata yönəlmiş kriptovalyutaya misallar söyləyin.
8. Əsas Axie siniflərinə nələr daxildir?
9. Decentraland platformasında istifadəçilər hansı kriptovalyuta ilə ödəniş edirlər?
10. Decentraland platformasında ödəniş edərək NFT şəklində nə almaq olar?
11. Axie Infinity-də oyunun məqsədi nədir?
12. NFT-lər hansı fayl sistemində saxlayırlar?
13. NFT-tokenin yaradılması hansı addımlarla həyata keçirilir?
14. NFT-lərin populyarlaşmasına hansı virtual oyun təkan verib?
15. The Sandbox-da hansı NFT istifadə edilir?
16. The Sandbox-da rəqəmsal daşınmaz əmlak harada satılır?
17. The Sandbox hansı ildə işə salınıb?
18. The Sandbox metakainatı hansı oyunu xatırladır?
19. The Sandbox hansı blokçeyndə qurulub?
20. The Sandbox-da daşınmaz əmlakın ölçüləri necə ola bilər?
21. The Sandbox metakainatına NFT şəklində hansı obyektlər daxildir?

Mühazirə 14. Web3.0 və Metaverse

Bu mühazirədə Web3.0 və Metaverse anlayışları araşdırılır. Web3.0 internetin yeni nəsil versiyası olaraq daha müstəqil və təhlükəsiz bir mühit yaratmağa çalışır. Digər tərəfdən, Metaverse isə rəqəmsal və fiziki aləmin inteqrasiya olunduğu virtual dünyadır. Bu iki konsepsiya gələcəyin texnoloji inkişafında mühüm rol oynayacaq.

14.1. Web3.0 nədir?

Web3.0 internetin təkamül prosesində Web1.0 və Web2.0-dan sonra gələn yeni mərhələdir. Onun əsas xüsusiyyətləri aşağıdakılardır:

- **Demərkəzləşmə:** Web3.0 blokçeyn texnologiyasına əsaslanır və mərkəzləşdirilmiş qurumlardan asılılığı azaldır.
- **Tokenləşdirmə:** Rəqəmsal və ya fiziki aktivlərin blokçeyn texnologiyası vasitəsilə tokenlərə çevrilməsi prosesidir. Bu tokenlər mülkiyyət sübutları (ing. ownership proof) kimi çıxış edir və müxtəlif isahələrdə stifadə oluna bilər. Web3.0 ekosistemində iqtisadi və sosial əlaqələri dəyişdirən əsas texnologiyalardan biridir. Tokenləşdirmənin bəzi aspeklərinin qeyd edək:
    - Fiziki əmlak (məsələn, daşınmaz əmlak, incəsənət əsərləri) blokçeyn üzərində tokenləşdirilə bilər.
    - Rəqəmsal aktivlər (NFT-lər, musiqi, video, sənədlər) Web3.0 platformalarında unikal tokenlər şəklində saxlanılır.
    - "Security" tokenləri – Real dünya investisiyalarını (məsələn, səhmlər və istiqrazlar) təmsil edən tokenlər.
    - DAO-lar idarəetmə və səsvermə hüquqlarını tokenlər vasitəsilə həyata keçirir.
    - İstifadəçilər müəyyən bir platformada idarəetmədə iştirak etmək üçün tokenlər əldə edə bilərlər.
    - Virtual dünyalarda torpaq sahələri, geyimlər və digər aktivlər NFT-lər vasitəsilə mülkiyyət hüququ ilə təmin edilir.
- **Süni intellekt və maşın öyrənməsi:** Web3.0-da mühüm rol oynayır, çünki bu texnologiyalar interneti daha ağıllı, avtomatlaşdırılmış və interaktiv hala gətirir:
    - Web3.0 platformalarında məlumatları avtomatik analiz edir və qərar qəbuletmə proseslərini təkmilləşdirir.
    - Blokçeyn üzərində saxtakarlıq və zərərli fəaliyyətləri analiz edərək daha təhlükəsiz sistemlər qurmağa imkan verir.
    - Ağıllı müqavilələrin daha təhlükəsiz və optimal olmasını təmin edir.
- **Fayl paylaşımı:** IPFS (InterPlanetary File System) mərkəziyətsiz fayl saxlama və paylaşma sistemidir. Ənənəvi HTTP protokolundan fərqli olaraq, IPFS

məlumatları mərkəzi serverlərdə deyil, P2P şəbəkəsində saxlayır və paylayır. Bu sistemdə fayllar, onların saxlanıldığı yerə görə deyil, məzmunun unikal kriptoqrafik heşinə görə indekslənir, daha sürətli, etibarlı və səmərəli məlumat mübadiləsi təklif edir.

- **Ağıllı müqavilələr:** Ethereum kimi blokçeynlər üzərində işləyən ağıllı müqavilələr, vasitəçiləri aradan qaldıraraq birbaşa və avtomatik əməliyyatlar aparmağa imkan verir.

14.2. Metaverse nədir?

Metaverse istifadəçilərin real həyatda olduğu kimi sosiallaşa, işləyə və hətta ticarət apara biləcəyi virtual aləmdir. Bu mühitin əsas komponentləri aşağıdakılardır:

- **Virtual Reallıq (VR) və Artırılmış Reallıq (Aaugmented Reality, AR):** Bu texnologiyalar Metaverse-i daha interaktiv hala gətirir.
- **NFT və rəqəmsal mülkiyyət:** İstifadəçilər virtual əşyalar alıb sata bilirlər.
- **DAO-lar:** Metaverse-in idarə edilməsində blokçeyn əsaslı DAO-lar əhəmiyyətli rol oynayır.
- **Rəqəmsal iqtisadiyyat:** İnsanlar burada virtual torpaq alıb sata, rəqəmsal bizneslər qura bilərlər.
- **Avatarlar və rəqəmsal şəxsiyyət:** İstifadəçilər Metaverse-də unikal rəqəmsal şəxsiyyətlər yaratmaq imkanına malikdirlər.
- **İnteroperabellik:** Müxtəlif Metaverse platformaları arasında qarşılıqlı əlaqənin olması istifadəçilərə daha rahat və genişmiqyaslı təcrübə təqdim edir.

14.3. Web3.0 və Metaverse-in əlaqəsi

Web3.0 və Metaverse qarşılıqlı əlaqəli anlayışlardır. Web3.0 Metaverse-in texnoloji bazasını təşkil edir və onun inkişafına kömək edir. Blokçeyn, ağıllı müqavilələr və NFT-lər Metaverse-in iqtisadiyyatının əsasını formalaşdırır.

- **Metaverse-də Web3.0 tətbiqləri:** Web3.0 texnologiyası Metaverse-in təhlükəsizliyini və şəffaflığını artırır.
- **DAO-ların rolu:** Virtual dünyalarda icmaların idarə edilməsində DAO-lar əsas mexanizm rolunu oynayır.
- **Play-to-Earn (P2E) modeli:** Oyunlar blokçeyn üzərində işləyir və oyunçulara kriptovalyuta və ya NFT-lər şəklində mükafatlar verilir. Qazandıqları tokenləri oyun daxilində istifadə edə, bazarda sata və ya digər aktivlərə dəyişdirə bilərlər. Oyunda aktiv iştirak edənlər daha çox token və ya NFT qazana bilərlər. Bəzi oyunlar "staking" və ya DAO idarəetmə sistemləri təklif edərək,

oyunçulara əlavə qazanc imkanları yaradır. Məşhur Play-to-Earn oyunları: Axie Infinity (AXS, SLP), Decentraland (MANA), The Sandbox (SAND).

14.4. Tətbiq sahələri

Web3.0 və Metaverse texnologiyaları müxtəlif sahələrdə geniş istifadə olunur:

- **Təhsil:** Virtual siniflər və interaktiv dərs mühitləri yaradılır.
- **Biznes və iqtisadiyyat:** Şirkətlər Metaverse-də mağazalar açır və rəqəmsal aktivlər satır.
- **Oyun sənayesi:** Blokçeyn əsaslı oyunlar və NFT-lər oyunçulara yeni imkanlar yaradır.
- **Sosial media:** Web3.0 əsaslı sosial şəbəkələr istifadəçilərə daha çox nəzarət imkanı verir.

14.5. Metaverse-i tətbiq edən ölkələr

- **ABŞ:** Facebook (Meta), Microsoft və digər texnologiya şirkətləri Metaverse layihələrinə milyardlarla dollar sərmayə yatırır.
- **Cənubi Koreya:** Hökumət Seul şəhərinin Metaverse versiyasını qurur və dövlət xidmətlərini rəqəmsal aləmə inteqrasiya edir.
- **Çin:** Çin Metaverse texnologiyalarına sərmayə qoyur, lakin kriptovalyuta və Web3.0-un bəzi aspektlərini tənzimləyir.
- **Birləşmiş Ərəb Əmirlikləri:** Dubay Metaverse strategiyası çərçivəsində virtual iqtisadiyyat yaratmağı hədəfləyir.
- **Avropa İttifaqı:** Avropa ölkələri Metaverse üçün hüquqi çərçivə hazırlayır və Web3.0 texnologiyalarına sərmayə qoyur.

14.6. Metaverse-lə bağlı təhlükəsizlik riskləri

Web3.0 və Metaverse-lə bağlı aşağıdakı əsas təhlükələrə toxunmaq olar:

- **Kibertəhlükəsizlik riskləri:** Ağıllı müqavilələrdə boşluqlar, blokçeyn hücumları (51% hücumu, Sybil hücumu və s.), dələduzluq və phishing hücumları.
- **Məlumat gizliliyi:** İstifadəçilərin rəqəmsal identifikasiyası və şəxsi məlumatlarının qorunması.
- **NFT və kriptovalyuta fırıldaqları:** Piramida sxemləri, saxta NFT satışları və dəyəri manipulyasiya olunan tokenlər.
- **Metaverse-də hüquq pozuntuları:** Rəqəmsal mülkiyyət hüquqları, dələduzluq halları və qanunvericiliyin yetərsizliyi.
- **Psixoloji və sosial risklər:** Virtual aləmə həddindən artıq bağlılıq, kiberzorbalıq və identifikasiya oğurluğu.

14.7. Metaverse – mənfi cəhətləri

Metaverse-in potensial faydaları olsa da, bir çox mənfi cəhətləri də mövcuddur. Bu mənfi cəhətlər həm texnoloji, həm də sosial sahələrdə özünü göstərə bilər. Aşağıda Metaverse-in bəzi mənfi cəhətləri qeyd olunub:

1. **Gizlilik və təhlükəsizlik problemləri**: Metaverse-in inkişafı ilə istifadəçi məlumatları, fəaliyyətləri və şəxsi məlumatları daha çox izlənilə və toplanıla bilər. Bu da məxfilik məsələlərini gündəmə gətirir. Ayrıca, Metaverse-də qarşılaşa biləcəyimiz yeni kibertəhlükələr, heklənmə və şəxsiyyət oğurluğu kimi riskləri artırır.
2. **Sosial təcrid və izolyasiya**: Metaverse-ə daxil olan insanlar daha çox virtual dünya ilə əlaqəli olurlar və bu da real dünya ilə sosial əlaqələrin azalmamasına səbəb ola bilər. İnsanlar daha çox ekran qarşısında vaxt keçirərək, real dünyadakı münasibətləri zəiflədir və sosial izolyasiyaya səbəb ola bilər.
3. **Asılılıq və psixoloji təsirlər**: Metaverse-dəki immersiv təcrübələr istifadəçilər üçün çox cəlbedici ola bilər, bu da asılılıq yarada bilər. Uzun müddət Metaverse-də qalmaq, istifadəçilərin real dünyadakı həyatlarını və sosial əlaqələrini unutmalarına səbəb ola bilər. Bu, həm də psixoloji narahatlıqlara (depressiya, narahatlıq və ya sosial fobiya) yol açа bilər.
4. **Fiziki sağlamlıq riskləri**: Virtual reallıq (VR) və artırılmış reallıq (AR) texnologiyalarından istifadə uzun müddət ərzində fiziki sağlamlıq problemlərinə səbəb ola bilər. Məsələn, VR gözlükləri və digər cihazlarla uzun müddət istifadə etmək baş ağrıları, göz yorğunluğu, vertigo və fiziki diskomforta səbəb ola bilər.
5. **İqtisadi qeyri-bərabərlik**: Metaverse inkişaf etdikcə, bu mühitə daxil olma imkanları yalnız yüksək texnologiyalı və zəngin insanlara məxsus ola bilər. Yüksək keyfiyyətli avadanlıqlar və internetə çıxış ehtiyacı olanlar üçün bu, böyük bir maliyyə yükü ola bilər və bu, cəmiyyətin müxtəlif təbəqələri arasında iqtisadi bərabərsizliyi daha da artıra bilər.
6. **Tənzimləmə və hüquqi məsələlər**: Metaverse-in tənzimlənməsi çətin ola bilər. Hər bir dövlətin fərqli qanunları və qaydaları olduğundan, virtual məkanda hüquqi məsələlər (əqli mülkiyyət hüquqları, cinayət fəaliyyətləri, yalan məlumatlar və s.) həll etmək çətinləşə bilər. Bu həm də qlobal miqyasda münaqişələrə səbəb ola bilər.
7. **Texnoloji asılılıq və infrastruktur tələbləri**: Metaverse üçün güclü texnoloji infrastruktura ehtiyac var. Bu, hər kəsin yüksək keyfiyyətli internet bağlantısı və güclü kompüter avadanlığına sahib olması deməkdir. Kifayət qədər güclü

cihazlara və əlaqələrə sahib olmayan insanlar Metaverse-dən faydalana bilməyəcəklər, bu da rəqəmsal uçurum yaradacaq.

Metaverse-in inkişafı ilə bu mənfi cəhətlərin necə həll ediləcəyi və idarə olunacağı hələ tam aydın deyil. Bununla yanaşı, bu texnologiyanın gələcəkdə daha yaxşı idarə olunması üçün müvafiq qanunvericilik və etik standartların yaradılması vacibdir.

Özünü yoxlamaq üçün suallar

1. Web3.0 nədir?
2. Web3.0-ün əsas xüsusiyyətləri hansılardır?
3. Web3.0-da süni intellekt hansı imkanlar yaradır?
4. IPFS nədir?
5. Tokenləşdirmə nədir?
6. Fiziki əmlakı tokenlərə çevirmək olarmı?
7. “Security” tokeni nədir?
8. Metaverse nədir?
9. Metaverse-in əsas komponentləri hansılardır?
10. Metaverse-də interoperabellik nədir?
11. Play-to-Earn modelinin mahiyyəti nədir?
12. Məşhur Play-to-Earn oyunlarıı hansılardır?
13. Metaverse-in iqtisadiyyatının əsasını hansı texnologiyalar formalaşdırır?
14. Hansı ölkələrdə Metaverse tətbiq edilir?
15. Avropa İttifaqında Metaverse sahəsində hansı işlər görülür?
16. Birləşmiş Ərəb Əmirliklərində Metaverse sahəsində hansı işlər görülür?
17. Metavese-in təhlükəsizlik riskləri nələrdir?
18. Metaverse-də hansı kibertəhlükəsizlik riskləri var?
19. Metaverse-də hansı hüquq pozuntuları ola bilər?
20. Metaverse-in mənfi tərəfləri nələrdir?
21. Metaverse-də hansı fiziki sağlamlıq riskləri ola bilər?

Mühazirə 15. Blokçeynlərdə təhlükəsizlik problemləri

15.1. Kriptovalyutalarla bağlı bəzi insidentlər

Kriptovalyutalara təkcə investorlar və entuziastlar deyil, cinayətkarlar da böyük maraq göstərirlər.

Silk Road hadisəsi. 2011-ci ilin fevralında Silk Road adlı anonim elektron ticarət meydançası işə salınmışdı. Ona yalnız Tor-brauzer vasitəsilə qoşulmaq olurdu, ödəniş üçün isə sövdələşən tərəflər ən təhlükəsiz üsuldan – bitkoinlərdən istifadə edirdilər. Malların yarıdan çoxu narkotik maddələr idi, arzu edən istənilən şəxs silah, özgələrin bank kartı rekvizitlərini və fərdi məlumatlarını, qadağan olunmuş pornoqrafik materialları satın ala bilərdi. Hətta insan orqanlarının satışı və killer xidmətləri haqqında elanlara da rast gəlmək olardı. 2012-ci ildə Silk Road satışlarının həcmi 15 milyon dollara çatmışdı; platformanın mövcud olduğu müddətdə istifadəçilər ümumi məbləği 9,5 milyon bitkoin olan milyondan çox alqı-satqı etmişdilər.

Silk Road yaradıcısı Ross Uilyam Ulbrixti 2013-cü ilin oktyabrında həbs etmək mümkün olmuşdu. Bu zaman Ulbrixt dəfələrlə bildirmişdi ki, işləyən onlayn-mağazanı onun həqiqi yaradıcısından – MtGox-in qurucusu Mark Karpelesdən satın alıb. Bu hadisə ilə əlaqəli daha bir maraqlı fakt da var: Silk Road saytının fəaliyyətini təhqiq edən agent Ulbrixtin şəxsiyyətini onun həbsindən çox əvvəl müəyyən etmiş və təxminən bir il müddətində özünü istifadəçilərdən biri kimi qələmə verərək onu şantaj edərək bitkoinlərlə təxminən 800 min dollar almış və bu vəsaitin bir hissəsini CoinMKT kriptovalyuta birjasına qoymuşdu.

Kriptovalyuta sistemlərinə haker hücumları. Bitkoin məşhurlaşan kimi, ona haker hücumları da intensivləşdi. 13 iyun 2011-ci ildə Bitcoin Forumunun üzvlərindən biri pulqabısından 25 000 BTC-nin oğurlandığını bildirmişdi. Həmin vaxtdakı mübadilə məzənnəsinə görə, bu təxminən 375 000 ABŞ dolları idi.

Bundan bir həftə sonra 2011-ci ilin yayında MtGox birjasının verilənlər bazası sındırıldı. Hakerlər 60 min istifadəçinin loqin, e-poçt və parol heşlərini İnternetdə yerləşdirmişdilər. Elə həmin gün hakerlər administratorlardan birinin parolunu ələ keçirərək buradan yüz minlərlə bitkoin almağa sifariş vermişdilər. Nəticədə bitkoin kursu 17.51 dollardan 1 sentə düşmüşdü. MtGox bitjanı bir həftəliyə bağlamağa məcbur olmuşdu.

2012-ci il mayında bitkoin birjası Bitcoinica-nın onlayn pulqabısı hakerlər tərəfindən boşaldılmışdı, 18 547 virtual pul oğurlanmışdı (o vaxtkı məzənnə ilə təxminən 90 min dollar). Bu birinci hal deyildi – həmin ilin martında hostinq-provayderin serveri sındırıldıqda 43 min bitkoin oğurlanmışdı.

2013-də hakerlər iştifadəçilərin kompüterlərini Fareit virusu ilə yoluxdurmaqla bitkoin mayninqi üçün CG Miner adlı zərərli proqram yazmışdılar.

2018-ci ilin yanvarında CoinCheck (Yaponiya) bitkoin ticarət meydançasının hesabından hakerlər 500 milyon NEM (396 mln dollar) çıxarmışdılar. Həmin vaxt NEM kriptovalyutası kapitallaşma həcminə görə dünyada 10-cu yerdə idi.

2017-ci ilin dekabrında oxşar hadisə baş vermişdi: Nice Hash kriptobirjasına haker hücumu nəticəsində 4800 bitkoin (68 milyon dollar) oğurlanmışdı.

2018-ci ilin yayında kriptovalyuta birjası Bitkoex informasiya sızması haqqında məlumat vermişdi. İstifadəçilərin 620 min dollar vəsaiti təhlükəyə məruz qalmışdı. Əməkdaşlardan biri Kakao tətbiqinin qrup çatında Karma tokenlərinə investisiyalar haqqında məlumat yerləşdirmiş və 19 müştərinin elektron poçtunu, pulqabılarını və gizli açarlarını göstərmişdi. İyunun əvvəlində hakerlər Cənubi Koreyada Coinrail kriptobirjasını sındıraraq 40 milyon dollar oğurlamışdılar.

Gizli açarların itirilməsi. Bir çox istifadəçi öz gizli açarlarını itirir, bunun nəticəsində onlar öz rəqəmsal pullarına giriş əldə edə bilmirlər.

Chainalysis-in verdiyi məlumatlar əsasında Wall Street Journal yazır ki, istifadəçilərin öz gizli açarlarını unutması səbəbindən 20 milyardlıq bitkoinlər həmişəlik itirilib. ABŞ Federal Təhqiqatlar Bürosu itirilmiş 1 milyard dollarlıq virtual pullara girişi bərpa edə bilmişdi.

Wallet Recovery Services istifadəçilərə öz rəqəmsal pullarına girişi bərpa etməyə kömək edir, lakin bunu 30 % halda etmək mümkün olur. Cəhdin uğurlu olması giriş açarının bərpa ediləcəyi informasiyanın korrektliyindən asılıdır.

BitGo əvvəllər bildirmişdi ki, 6 mln bitkoin həmişəlik itirilib. Onlardan 2 milyonu oğurlanıb.

15.2. Bitkoin şəbəkəsinə qarşı hücumlar

Bitkoin heç bir fiziki mövcudluğu olmayan, tamamilə rəqəmsal valyutadır. Valyuta təhlükəsizliyi ilə bağlı məsələlər həmişə müzakirə mərkəzindədir. Virtual valyutada tranzaksiya və mayninq proseslərində təhlükəsizliyi artırmaq üçün səylər göstərilsə də, virtual valyutanın qarşısında hələ də bəzi təhlükələr mövcuddur. Eyni zamanda müştərilər üçün təklif olunan onlayn pulqabı xidmətlərinə qarşı da bir sıra təhlükələr var. Hətta mübadilə xidmətləri də hücumların hədəfi ola bilər.

Bitkoin dizayn edildikdə nəzərə alınmış əsas hücum “Double spending” idi (qeyd edək ki, ənənəvi pullarda bu hücum mümkün deyil).

“Double-spending” (İki dəfə xərcləmə) hücumu: Bitkoin tranzaksiyası şəbəkədə saniyələr içərisində yayılır, lakin təsdiqlənməsi zaman tələb edir. Sahib olduğu bitkoinləri rəqəmsal şəkildə imzalayaraq xərcləyən istifadəçinin başlatdığı tranzaksiya etibarlı tranzaksiya sayılır. Bitkoin ünvanına etibarlı bir ödəniş bir neçə saniyə ərzində şəbəkədəki bütün istifadəçilərə görünə bilər, lakin bunun təsdiq

olunacağına zəmanət yoxdur. Tranzaksiyanın təsdiq olunmasının gecikməsi səbəbindən ikidəfə xərcləmə imkanı mövcuddur. Eyni bitkoini bir dəfədən çox xərcləmə prosesi *iki dəfə xərcləmə* adlanır. Tranzaksiya başlayıb və hələ təsdiq edilməyibsə, eyni bitkoinlər alıcı və ya satıcı tərəfindən yenidən istifadə edilə bilər. Mümkün iki dəfə xərcləmə hücumlarına *"Race"* hücumu, *Finney* hücumu, *kobud güc* hücumu, *51%* hücumu daxildir.

"Race" (*yarış*) *hücumu* – Yeni başlamış tranzaksiyadakı bitkoinin təsdiqlənməyi bir müddət vaxt tələb etdiyinə görə hücumçu bu bitkoini təkrar istifadə edə bilər. Eyni bitkoin bir neçə tranzaksiyada istifadə olunubsa hansı tranzaksiyanın təsdiqlənəcəyini tapmaq çətindir. Heç bir zərər görmək istəməyən satıcı təsdiqlənməmiş ödənişi qəbul etməməli və ən azı 6 təsdiqlənməni gözləməlidir. Daha sadə dillə desək, müştərinin göndəriyi bitkoinləri təsdiqlənməmiş halda pulqabısına qəbul edən satıcı 6 təsdiqlənməni almadan müştəriyə xidmət edərsə, bu zaman zərərə uğrama ehtimalı var. Çünki bu proses ikidəfə xərcləmə ola bilər, sistem sonra bu tranzaksiyanı rədd edə bilər.

Kobud güc (*Brute-force*) *hücumu* – Bir qrup saxta mədənçi ikidəfə xərcləmə tranzaksiyalarının daxil olduğu blokları təsdiqləyir və təsdiq gözləyən alıcıya göndərir. Hücumun uğurlu olması ehtimalı alıcının neçə təsdiq gözləməsindən və saxta mədənçi qrupunun şəbəkənin neçə faizini təşkil etməsindən asılıdır. Məsələn, saxta mədənçi qrupu şəbəkənin 10 %-ni təşkil edirsə və alıcı 6 təsdiq gözləyirsə, o zaman hücumun uğurlu olma ehtimal 0.1 %-dir.

Bitkoin-ə qarşı yönəlmiş hücumların a aşağıdakılar aiddir:

1. Konsensus protokoluna hücumlar – bunlar əsasən Bitkoin-in konsensus qaydalarını manipulyasiya edərək şəbəkəyə təsir etməyə yönəlirlər.

1) 51% hücumu – Əgər bir qrup mədənçi şəbəkənin ümumi heş gücünün 51%-dən çoxunu ələ keçirsə, o zaman onlar öz bloklarını istədikləri kimi təsdiqləyə, digər tranzaksiyaları bloklaya və hətta *iki dəfə xərcləmə* həyata keçirə bilərlər. Bitcoin şəbəkəsinin geniş paylanmış olması və böyük mədənçilik hovuzlarının tarazlığı qoruması bu hücumun qarşısını qismən alır.

2) Timejacking hücumu – Bitkoin qovşaqları blokların zaman möhürü (ing. timestamp) qiymələrini əsas götürərək sinxronlaşdırırlar. Hücumçu saxta vaxt qiymətləri göndərərək qovşaqları köhnə blok zəncirlərinə qoşulmağa məcbur edə bilər. Çözüm olaraq, yeni Bitcoin versiyalarında timestamp yoxlamaları gücləndirilib.

"Timejacking" hücumu barədə əlavə qeyd. Yeni blokları təsdiqləmək üçün şəbəkə saatından istifadə olunur. Blokun yaradılma zamanı blok başlığında göstərilir. Hər bir Bitkoin qovşağında şəbəkə zaman sayğacı olur. Bu qovşaq cütlüklərinin median zamanına əsaslanır. Əgər median zaman sistem zamanından

70 dəqiqədən çox fərqlənirsə, şəbəkə zaman sayğacı sistem zamanına qayıdır. Hücumçu bir neçə müxtəlif qovşaqdan şəbəkəyə qoşularaq şəbəkə zaman sayğacında dəyişiklik edə bilər. Sayğac ya yavaşladılır, ya da sürətləndirilir.

Əgər bir blokun yaranma zamanı şəbəkə zamanından 2 saat öndə olarsa, qovşaqlar onu rədd edir. Hücumçu zamanı həqiqi zamandan 190 dəqiqə fərqlənən yeni blok yaradır. Mədənçi məntiqinə görə isə, blokun yaranma zamanı şəbəkə sayğacından 120 dəqiqədən çox keçməyibsə, mədənçi bu bloku qəbul edə bilər. Nəticə olaraq timejacking hücumda hücumçu şəbəkə zaman sayğacını dəyişdirir və aldadılmış qovşaq bloku alternativ bir blok zəncirinə qəbul edə bilər. Bu isə iki dəfə xərcləmə hücumuna və hesablama resurslarının israfına səbəb ola bilər.

2. Zəif blok və tranzaksiya hücumları – Bu tip hücumlar Bitcoin şəbəkəsində bloklar və tranzaksiyalar üzərində manipulyasiya etməyə çalışır.

1) Transaksiyaların plastikliyinə hücum (ing. malleability) – Hücumçu bir tranzaksiyanın heş qiymətini blokçeyndə təsdiqlənmədən əvvəl dəyişdirə bilər. Məsələn, 2014-cü ildə Mt. Gox kriptovalyuta birjası bu cür hücum nəticəsində 850,000 BTC itirdiyini bildirmişdi. Qeyd edək ki, SegWit yenilənməsi bu problemi əsasən həll edib.

2) Finney hücumu – Hücumçu əvvəlcədən bir tranzaksiyanı mədənçilik etdiyi bloka yerləşdirir**,** amma həmin tranzaksiyanı hələ şəbəkədə paylaşmır. Sonra mağazadan Bitcoin ilə məhsul alıb, tranzaksiya yayılandan sonra "köhnə" blok ilə ödəməni ləğv edir. Çözüm olaraq, Bitcoin ödənişlərinin bir neçə blok təsdiqi alması tövsiyə edilir.

3) Vector76 hücumu – Finney və yarış hücumlarının kombinasiyasıdır, 2011-ci ildə təsvir olunub, tranzaksiyaların təsdiqi mexanizmlərindəki zəifliklərdən və blokların Bitcoin şəbəkəsi üzrə yayılmasında vaxt gecikmələrindən istifadə edir. Vector76 hücumunda bədniyyətli əvvəlcə iki tranzaksiya yaradır: biri öz Bitcoin ünvanına vəsait göndərmək, digəri isə eyni vəsaiti satıcının Bitcoin ünvanına göndərmək üçün. Sonra o, satıcını təsdiqlənməmiş tranzaksiyanı qəbul etməyə inandırmağa çalışır, eyni zamanda şəbəkədə o biri tranzaksiyanı yayır. Bədniyyətli öz tranzaksiyasını satıcının təsdiqləməsindən daha tez başa çatdıra bilsə, vəsait satıcının deyil, bədniyyətlinin ünvanına göndəriləcək.

3. P2P şəbəkəsinə qarşı hücumlar – Bitcoin şəbəkəsinin paylanmış olması onu bəzi P2P hücumlarına qarşı həssas edir.

1) Tutulma hücumu (ing. Eclipse attack) – Hücumçu bir qovşağın bütün əlaqələrini idarə edərək ona səhv və ya saxta məlumatlar göndərə bilər. Bu, 51% hücumu və ikidəfə xərcləmə hücumlarına zəmin yarada bilər. Çözüm Bitcoin

qovşaqlarının təsadüfi peer seçməyə və fərqli bağlantılar qurmağa üstünlük verməsidir.

2) Sibil hücumu (ing. Sybil attack) – Hücumçu saxta node-lar yaradaraq şəbəkədə yanlış məlumat yaymağa çalışır. Çözüm PoW mexanizmi və reputasiya əsaslı sistemlər ilə bu hücumun təsirini azaltmaqdır.

4. Ağıllı müqavilə və skript hücumları – Bitcoin-in skript dili Ethereum-dakı ağıllı müqavilələrə nisbətən məhdud olsa da, bəzi təhlükəsizlik boşluqları mövcuddur.

1) "Dust transaction" hücumu – Hücumçular "**dust" transaksiyalar** (çox kiçik məbləğlər) vasitəsilə istifadəçilərin pulqabılarını spam edə bilərlər. Çözüm Bitcoin qovşaqlarının müəyyən "dust" tranzaksiyalarını filtirləməsidir.

Bitkoinin ən kiçik vahidi *satoşi*dir. Bir satoşi 0.00000001 bitkoinə bərabərdir. Əvvəllər tranzaksiyalarda bir satoşi göndərmək mümkün idi. Hücumçu bundan istifadə edərək kiçik maliyyə dəyərli tranzaksiyalar həyata keçirərək, mədənçilərin hesablama qurğularını boş yerə məşğul edir. Bitcoin Client-in sonrakı versiyasında tranzaksiyanın ən kiçik dəyəri 5.43 satoşi-dir. Bu da təqribən 0.0002 dollara bərabərdir (2017-ci ilin sentyabrında). 5.43 satoşi də kiçik miqdar olsa da, "Dust Transactions" hücumunu müəyyən qədər çətinləşdirir.

2) Ödəniş çalma hücumu – Hücumçular köhnə blokları geri qaytararaq yüksək komissiya ilə yeni bloklar əlavə etməyə çalışırlar. Çözüm komissiya sistemlərinin təkmilləşdirilməsidir.

Ağıllı müqavilələrin təhlükəsizliyi

Ağıllı müqavilələr mərkəzsiz maliyyə infrastrukturunun təməl daşlarından biridir, onlarda buraxılmış kod səhvləri və zəifliklər ciddi maliyyə itkilərinə səbəb ola bilər. Ağıllı müqavilələrə aşağıdakı hücumlar məlumdur:

1. **Təkrar giriş hücumu** (ing. Reentrancy) – hücumçu, müqavilənin funksiyasından çıxmazdan əvvəl yenidən eyni funksiyanı təkrar çağırır və balansdan artıq vəsait çıxarır. Misal olaraq, 2016-cı ildəki DAO hücumunu göstərmək olar. Təkrar giriş hücumları ağıllı müqavilələrdə ən dağıdıcı hücum hesab edilir.
2. **Yuxarı daşma/Aşağı daşma** (ing. Overflow/Underflow) – Bu hücumları başlatmaq nisbətən asandır və icazəsiz giriş qiymətlərini qəbul edən tranzaksiyalarda baş verir. Ağıllı müqavilədə yuxarı daşma əsasən maksimum qiymətdən böyük qiymət alındıqda baş verir. Müqavilələr əsasən 256-bitlik ədədlərlə işləyən Solidity-də yazılır, beləliklə, 1 vahid artım yuxarı daşmaya səbəb ola bilər. Ağıllı müqavilələrdə yuxarı daşma zəifliyini müəyyən etmək üçün ənənəvi test yanaşmaları yararlı deyillər.

Ağıllı müqavilənin “aşağı daşması” yuxarı daşmanın əksi olaraq baş verir. Aşağı daşma hücumlarını yerinə yetirmək daha sadədir, çünki yuxarı daşmaya səbəb olmaq üçün tələb olunan tokenə nail olmaq bədniyyətliyə çox vaxt çətin olur.

3. **Qabaqlama hücumu** (ing. Front-running) – hücumçu, başqasının göndərmək istədiyi əmri əvvəlcədən görüb daha yüksək qaz ilə öz əməlini blokçeynə birinci yerləşdirir. DEX-lərdə token alqı-satqısı, NFT minterlər kimi sahələrdə tətbiq edilə bilər.
4. **Zaman möhürü asılılığı** (ing. Timestamp dependency) – müqavilənin davranışı blok vaxtına əsaslandıqda mədənçi həmin vaxtı manipulyasiya edə bilər. Fayda əldə etmək üçün mədənçi zaman möhürünü bir neçə saniyəyə yenidən nizamlaya bilər. Bu, Ethereum şəbəkəsini sinxronlaşdırılmış qlobal saatdan ayırmağa imkan verir. Məsələn, ağıllı müqavilə lotereya nəticəsini müəyyən etmək üçün təsadüfi ədədlər yaratmaq üçün cari zaman möhüründən istifadə edir. Ağıllı müqavilə mədənçilərə blok təsdiqləndikdən sonra 30 saniyə ərzində zaman möhürü qoymağa icazə verdiyi üçün bu, mədənçiyə istismar üçün daha çox imkan verir. Beləliklə, təsadüfi ədədlər generatorunun nəticəsi fayda əldə etmək üçün dəyişdirilə bilər.
5. **Tranzaksiya sıralaması asılılığı** (ing. Transaction ordering dependency) – bədniyyətli mədənçilərin ağıllı müqavilələrə ciddi təsir göstərməsinə imkan verə bilən boşluqdur. Bu boşluq tranzaksiyanın icra sırasına əsaslanaraq, ağıllı müqavilədə çox yayılmış təhlükəsizlik səhvidir. Məsələn, tutaq ki, yeni yaradılan blok eyni ağıllı müqaviləni tətbiq edən 2 tranzaksiyadan ibarətdir. Bu cür süjetlər istifadəçilərə müqavilənin vəziyyətini və ya hansı tranzaksiyanın nə vaxt başladığını müəyyən etmək üçün kifayət qədər məlumat vermir. Buna görə də, hər iki tranzaksiyanın nəticəsi sıradan asılı olduqda, müqavilə tranzaksiya sıralaması asılılığı boşluğu ilə nəticələnir.
6. **Qısa ünvan hücumu** – Ethereum Virtual Maşının (EVM) zəifliyi səbəbindən baş verir. EVM, düşmənlərə istismar ilə nəticələnən xüsusi hazırlanmış ünvanlar göndərməyə imkan verən qeyri-dəqiq padding edilmiş arqumentlərə icazə verir. Qısa ünvan hücumu SQL inyeksiya səhvi kimi oxşar hücum strategiyasını izləyir. Aşağı daşma aşkar edildikdə, EVM 256 bitlik məlumat tipindən ibarət olmasını təmin etmək üçün ünvanın sonunda sıfır əlavə edir. Bədniyyətli efir ünvanından sonuncu sıfrı buraxmaqla bu zəiflikdən istifadə edə bilər. Bu zəiflik girişin doğrulanması səhvidir və əsasən göndərən tərəfdə baş verir.
7. **Defolt görünürlük** – Solidity funksiyasındakı görünürlük spesifikatoru funksiyanın çağırılma qaydasına nəzarət edir. Görünürlük spesifikatoru həm

də istifadəçilərə törəmə müqavilələr vasitəsilə xarici funksiyaları çağırmağa icazə verərkən nəzarəti öz üzərinə götürür. Görünürlük spesifikatorunun düzgün tətbiq edilməməsi ağıllı müqavilədə ciddi təsirlərə səbəb ola bilər. Defolt görünürlük həmişə funksiyalar üçün *publik* olaraq təyin edilir, funksiyalar üçün görünürlük açıq şəkildə qeyd etmədikdə xarici müqavilələrə müraciət etməyə imkan verir. Bu boşluq, görünürlük spesifikatorunu *private* kimi təyin etməyə məhəl qoyulmadıqda yaranır.

8. **Xidmətdən imtina hücumu (DoS)** – hücumçu sistemin işləməsini qeyri-mümkün edir, məsələn, tranzaksiyanın qaz limitini aşır.
9. **Orakl manipulyasiyası –** orakllardan məlumat alan müqavilələrdə, həmin oraklın verdiyi məlumatlar hücumçu tərəfindən manipulyasiya edilir. Məsələn, qiymət orakl hücumları ilə DeFi protokolları aldadılır.
10. **Girişə nəzarətin səhv konfiqurasiyası** – sahiblik və icazələr düzgün təyin edilmədikdə, icazəsiz istifadəçilər kritik funksiyaları çağırırlar.
11. **Məntiqi səhvlər** – ağıllı müqavilələrin yanlış və ya dəyişən məntiqə əsaslanması.

Təhlükəsiz ağıllı müqavilələr yazmaq üçün kod auditləri (müstəqil ekspertlər və ya qurumlar tərəfindən), formal verifikasiya (müqavilənin düzgün işləməsini formal isbat etmək), geniş əhatəli testlər (blok, inteqrasiya və fuzzing testləri), idarəetmədə vaxt gecikməsi qoyulması (zaman kilidləri), bug bounty proqramları gerçəkləşdirmək tövsiyə olunur.

Analiz alətlərindən MythX, Slither, Oyente, test və gəlişdirmə freymvorklarından – Hardhat, Foundry, Truffle, audit olunmuş müqavilə modulları kimi OpenZeppelin müqavilələrini nəzərə çatdırmaq olar.

Özünü yoxlamaq üçün suallar

1. Silk Road-a qoşulmaq üçün hansı brauzer istifadə edilirdi?
2. Silk Road-da ödənişlər hansı valyuta ilə edilirdi?
3. Silk Road ilə bağlı insidentin mahiyyəti nədən ibarətdir?
4. Silk Road saytının fəaliyyətini araşdıran agent hansı hərəkəti etmişdi?
5. 2011-ci ilin yayında MtGox birjasına edilən hücumun mahiyyəti nə idi?
6. 2011-ci ilin yayında MtGox birjasına edilən hücumun nəticəsi nə oldu?
7. Double spending hücumu nədir?
8. Double spending hücumunu hansı növləri var?
9. Timejacking hücumu nədir?
10. 51% hücumu nədir?
11. Finney hücumu nədir?
12. Konsensus mexanizmlərinə hücumların hansı növləri var?
13. P2P şəbəkəsinə qarşı hücumların hansı növləri var?

14. Zəif blok və tranzaksiya hücumlarının hansı növləri var?
15. “Dust transaction”hücumu nədir?
16. Vector 76 hücumu nədir?
17. Ağıllı müqavilələrə təkrar giriş hücumu nədir?
18. Ağıllı müqavilələrə qabaqlama hücumu nədir?
19. Ağıllı müqavilələrdə orakl mianipulyasiyası hücumu nədir?
20. Ağıllı müqavilələrdə yuxarı daşma hücumu nədir?
21. Ağıllı müqavilələrdə aşağı daşma hücumu nədir?
22. Ağıllı müqavilələrdə tranzaksiya sıralaması asılılığı hücumu nədir?
23. Ağıllı müqavilələrdə zaman möhürü asılılığı hücumu nədir?
24. Ağıllı müqavilələrdə defolt görünürlük hücumu nədir?
25. Ağıllı müqavilələrdə qısa ünvan hücumu nədir?

İxtisarlar

AML (*Anti Money Laundering*) – qeyri-qanuni fəaliyyət nəticəsində əldə edilmiş pulların yuyulması ilə mübarizə
API (*Application Programming Interface*) – müxtəlif proqramların bir-biri ilə əlaqə qurmasını təmin edən interfeys
ASIC (*Application Specific Integrated Circuits*) – xüsusi təyinatlı inteqral sxemlər
ATH (*All Time High*) – kriptovalyutanın maksimal kursu
BFT (*Byzantine Fault Tolerance*) – şəbəkədəki bəzi qovşaqların səhv işləməsinə baxmayaraq, şəbəkənin düzgün işləməsini təmin edən konsensus mexanizmi
BIP (*Bitcoin Improvement Proposal*) – Bitkoinin təkmilləşdirilməsi layihəsi
BPI (*Bitcoin Price Index*) – bitkoinin qiymət indeksi – Coindesk saytı tərəfindən işlənib, dünyanın böyük birjalarında bitkoinin orta qiyməti kimi hesablanır.
CPU (*Central Processing Unit*) – mərkəzi prosessor
DAO (*Decentralized Autonomous Organization*) – blokçeyn üzərində mərkəzsiz idarə olunan avtonom təşkilat
Dapp (*Decentralized Application*) – mərkəziyətsiz tətbiq – avtonom işləyən və öz verilənlərini blokçeyndə saxlayan açıq kodlu proqram
DeFi (*Decentralized Finance*) – mərkəziyətsiz maliyyə xidmətləri sistemi
DEX (*Decentralized Exchange*) – mərkəziyətsiz kriptobirja platforması
DGW (*Dark Gravity Wave*) – mayninqin çətinliyini tənzimləmə alqoritmi
DLT (*Distributed Ledger Technology*) – paylanmış uçot reyestri texnologiyası (Bitkoin blokçeyni) – P2P şəbəkəni, verilənlərin paylanmış saxlanmasını və kriptoqrafiyanı birləşdirir.
DPoS (*Delegated proof-of-stake*) – mərkəziyətsiz mühitdə konsensus alqoritmi; istifadəçilər nümayəndələr seçərək konsensus əldə edirlər.
ECDSA (*Elliptic Curve Digital Signature Algorithm*) – Bitcoin protokolunda tranzaksiyaları təsdiqləmək üçün istifadə edilən alqoritm
EEA (*Enterprise Ethereum Alliance*) – Ethereum əsasında texnologiyaların və standartların inkişafı və dəstəklənməsi məqsədilə maliyyə və texnologiya şirkətləri və fondlarının qeyri-kommersiya alyansı
ETH (*Ether***)** – Ethereum şəbəkəsinin kriptovalyutası
EVM (*Ethereum Virtual Machine*) – Ethereium virtual maşını
FOMO (*Fear of Missing Out*) – bazarda fürsəti qaçırmaq qorxusudur.
FPGA (*Field Programmable Gate Array*) – proqramlaşdırılan məntiqi inteqral sxem
FUD (*Fear, Uncertainty, Doubt*) – bazar haqqında mənfi məlumat yayaraq qiymətləri manipulyasiya etmə strategiyası

GPU (*Graphics Processing Unit*) − videoprosessor
HODL – Kriptovalyutaları uzun müddət saxlama strategiyası
XRP – Ripple-in banklararası köçürmələr üçün nəzərdə tutulmuş kriptovalyutası
XRPL – RippleNet üçün istifadə edilən, yüksək sürətli və aşağı komissiyalı blokçeyn şəbəkəsi
ICO (*Initial Coin Offering*) – yeni tokenlərin ilkin satışı; layihə üçün maliyyə toplanması məqsədi daşıyır.
IDEX (*Identity Exchange*) – Ethereum və Binance Smart Chain üzərində qurulmuş mərkəzsiz kriptobirja platforması
IPFS (*InterPlanetary File System*) – mərkəziyətsiz fayl paylaşım sistemi
JIT (*Just-In-Time*) – lazım olduqda resursların təmin edilməsi metodu
JVM (*Java Virtual Machine*) – Java proqramlarının işlədiyi virtual mühit
KYC (*Know Your Customer*) − "öz müştərini tanı" – dələduzluq və pulların yuyulması ilə mübarizə üçün pul vəsaitləri ilə işləyən istənilən şirkət maliyyə tranzaksiyanı həyata keçirməzdən öncə kontragenti identifikasiya etməlidir.
LN (*Lightning Network*) – Bitkoin və digər kriptovalyutaların (Lightcoin və s.) miqyaslanması üçün texnoloji həll
MAST (*Merkelized Abstract Syntax Trees*) – Merkl abstrakt sintaksis ağacları
MEV (*Miner Extractable Value*) – Mədənçinin tranzaksiya sıralamasını dəyişdirərək əlavə gəlir əldə etməsi
NIP (*Nostr Improvement Proposal*) – Nostr protokoluna təklif olunan dəyişiklikləri ifadə edən sənəd
NIST – (*National Institute of Standards and Technology*) – ABŞ Milli Standartlar və Texnologiya İnstitutu
NSA (*National Security Agency*) – ABŞ Milli Təhlükəsizlik Agentliyi
P2P (*Peer to Peer*) – birranqlı kompüter şəbəkəsi
P2SH (*Pay to Script Hash*) – multi-imza texnologiyası
PoI (*Proof-of-Importance*) – vacibliyin isbatı – PoW-a alternativ konsensus alqoritmi.
PoS (*Proof of Stake*) – token sahiblərinin paylarına əsasən şəbəkəni doğrulamasını təmin edən konsensus üsulu
PoW (*Proof-of-Work*) – yerinə yetirilmiş işin isbatı – Bitkoin mayninqi şəbəkəsində konsensus alqoritmi
PPLNS (*Pay Per Last N Shares*) – hovuzda mayninq üçün mükafat metodu. Axırıncı N hissəyə görə ödəniş.
PPS (*Pay per Share*) – hovuzda mayninq üçün mükafat metodu. Tapılmış hər bir hissəyə görə ödəniş.
PROP (*Proportional*) – hovuzda mayninq üçün mükafat metodu. Mükafat blokun tapılması zamanı maynerin göndərdiyi hissələrə mütənasib hesablanır.

RLP (*Recursive Length Prefix*) – Ethereum-da məlumatların seriyalanması üçün istifadə olunan kodlaşdırma üsulu
RPC (*Remote Procedure Call*) – Blokçeyn qovşaqları ilə proqram təminatı arasında əlaqəni təmin edən kommunikasiya protokolu
SegWit (*Segregated Witness* – «ayrılmış sübut») – Bitcoin bloklarında məlumatı ayrı saxlamaqla daha çox tranzaksiya yerləşdirməyə imkan verən texnologiya
SHA (*Secure Hash Algorithm*) – kriptoqrafik heş alqoritmi
SPV (*Simplified Payment Verification*) – ödənişlərin sadələşdirilmiş verifikasiyası – Bitkoin protokolunun xüsusiyyəti, bütün blokçeyni yükləmədən tranzaksiyanı təsdiqləməyə imkan verir.
TCR (*Token Curated Registry*) – İcmanın token səsverməsi ilə idarə etdiyi məlumat siyahısı və ya reyestr
TGE (*Token Generating Event*) – ICO-da tokenlərin buraxılması və satılması (*Token sale*) mərhələsidir.
TPS (*Transactions per second*) – şəbəkənin saniyədə icra edə bildiyi tranzaksiya sayı
TSS (*Threshold Signature Scheme*) – Açarların hissələrə bölünüb birləşdirilərək tranzaksiyaların imzalanması üsulu
TVL (*Total Value Locked*) – DeFi platformasında kilidlənmiş ümumi aktivlərin dəyəri
TWAP (*Time-weighted Average Price*) – Qiymət dəyişikliklərini hesablamaq üçün zaman çəkili ortalama qiymət
UASF (*User-Activated Soft Fork*) – İstifadəçilərin qovşaq proqramlarını yeniləməklə protokol dəyişikliyinə səs verdiyi model
UBI (*Universal Basic Income*) token – Blokçeyn vasitəsilə hər kəsə bərabər və şəffaf şəkildə paylanan gəlir tokeni.
UI (*User Interface*) – istifadəçinin blokçeyn tətbiqi ilə qarşılıqlı əlaqə qurduğu vizual interfeys
UTXO (*Unspent transaction output*) – xərclənməmiş tranzaksiya çıxışı – Bitkoində hesab və balans anlayışları yoxdur; yalnız UTXO anlayışı istifadə edilir.
VDF (*Verifiable Delay Function*) – yoxlama üçün verilmiş sayda ardıcıl addımların yerinə yetirilməsini tələb edən və çıxışı asanlıqla yoxlanıla bilən kriptoqrafik funksiya
VRF (*Verifiable Random Function*) – blokçeyn üzərində təsadüfi qiymətlərin təhlükəsiz və təsdiqlənə bilən şəkildə yaradılması
WASM (*WebAssembly*) – Blokçeyn platformalarında (Polkadot, Near və s.) ağıllı müqavilələrin icrası üçün optimallaşdırılmış format
WBTC (*Wrapped Bitcoin*) – Bitcoin-in Ethereum şəbəkəsində ERC-20 formatında tokenləşdirilmiş versiyasıdır və DeFi tətbiqlərində BTC istifadə etməyə imkan verir.
WETH (*Wrapped Ether*) – Ether-in ağıllı müqavilələrdə istifadə edilən ERC-20 uyğun versiyası
ZKP (*Zero Knowledge Proof*) – sirri açıqlamadan onu bildiyini isbatlamağa imkan verən kriptoqrafiya üsulu

Qlossari: Blokçeyn terminləri

Address – kriptovalyuta alqı-satqısı üçün istifadə olunan unikal identifikator
Airdrop – yeni tokenlərin istifadəçilərə pulsuz paylanması prosesi
Altcoin – Bitcoin xaricindəki bütün digər kriptovalyutalar
Arbitrage – eyni aktivin fərqli bazarlarda qiymət fərqindən yararlanma strategiyası
Atomic swap – iki fərqli kriptovalyutanın birbaşa və etibarlı mübadiləsini təmin edən texnologiya

Block – blokçeyndə verilənləri saxlayan və birləşdirən struktur vahidi
Block height – blokun blokçeyndə genesis (0-cı) blokuna nəzərən sıra nömrəsi
Block depth – blokun blokçeyndə ən son əlavə edilmiş bloka nəzərən sıra nömrəsi
Block reward – blok yaradıcılarına verilən mükafat
Blockchain – verilənlərin bloklar şəklində şəbəkə üzərində paylanaraq saxlanıldığı mərkəzsiz verilənlər bazası
Burning – tokenlərin istifadə edilə bilməyəcək şəkildə "yandırılması" prosesi

Coin – öz blokçeyn şəbəkəsinə malik olan rəqəmsal valyuta
Cold wallet – İnternetə bağlı olmayan, fiziki cihazlarda saxlanan kriptovalyuta pulqabı
Collateral – kredit və ya borcun təminatı üçün qoyulan aktiv
Consensus mechanism – paylanmış şəbəkədə verilənlərin doğruluğunu təsdiqləmə mexanizm
Contract address – ağıllı müqavilənin yerləşdiyi unikal blokçeyn ünvanı

Double Spending – Eyni rəqəmsal valyutanın bir neçə dəfə xərclənməsi riski

ERC-20 – Ethereum şəbəkəsində tokenlərin yaradılması üçün standart
ERC-721 – unikal tokenlərin yaradılması üçün standart
Escrow – tərəflər arasında etibarlı əməliyyatların təmin edilməsi üçün vasitəçi hesabı
Ethereum – ağıllı müqavilələr və DApp-lər üçün mərkəzsiz platforma
Ethereum classic – Ethereum-un orijinal versiyası

Faucet – yeni istifadəçilərə kiçik miqdarda kriptovalyuta paylayan platforma
Fiat currency – dövlət tərəfindən qəbul edilən rəsmi valyuta
Fungible token – Eyni dəyərə malik, dəyişdirilə bilən tokenlər
Fork – Blokçeyn şəbəkəsinin iki fərqli yola ayrılması

Gas – Ethereum şəbəkəsində tranzaksiyaların yerinə yetirilməsi üçün tələb olunan hesablama resursu
Genesis block – blokçeyn şəbəkəsinin ilk bloku
Governance token – şəbəkə qərarlarında səsvermə hüququ verən tokenlər
GPU mining – qrafik kartları ilə kriptovalyuta mədənçiliyi
Gas limit – bir tranzaksiyanın icrası üçün maksimum qaz həcmi məhdudiyyəti
Grin – gizliliyi təmin edən və MimbleWimble protokolunu istifadə edən kriptovalyuta

Halving – kriptovalyutanın mədənçilik mükafatının yarıya endirilməsi prosesidir.
Hard fork – şəbəkə qaydalarının köklü şəkildə dəyişdirilməsi və əvvəlki versiyalarla uyğunluğun itirilməsi vəziyyəti
Hash – məlumatın heşlənmiş nəticəsi
Hashrate – mədənçinin saniyədə hesablaya bildiyi heş sayı

Immutable – dəyişdirilə və ya silinə bilməyən
Inflation – kriptovalyutanın təklifinin artması nəticəsində qiymət azalması
Interoperability – müxtəlif blokçeyn şəbəkələrinin bir-biri ilə əlaqə qurma qabiliyyəti

Jailbreak – cihazda istehsalçı tərəfindən qoyulmuş məhdudiyyətlərin aradan qaldırılması

Key pair – kriptovalyuta pulqabında istifadə olunan açar cütü
Killer app – bazarda inqilabi dəyişikliklərə səbəb olan tətbiq
Karma – istifadəçinin şəbəkə üzərindəki etibarlılığını göstərən göstəricidir.
Kusama – Polkadot şəbəkəsinin "canlı" test şəbəkəsidir.

Launchpad – yeni kriptovalyuta layihələrinin başladılmasını və vəsait toplama proseslərini dəstəkləmək üçün istifadə edilən platforma və ya xidmətdir.
Launchpool – **y**eni kriptovalyuta layihələrində erkən mərhələdə iştirak etmək üçün yaradılan hovuzlardır.
Layer 1 – əsas blokçeyn infrastrukturudur (məsələn, Ethereum, Bitcoin).
Layer 2 – Layer 1 şəbəkəsinin üzərində qurulmuş və onu miqyaslandıran əlavə protokollardır (məsələn, Optimism, Arbitrum)
Ledger – tranzaksiyaların dəyişməz şəkildə qeydə alındığı rəqəmsal reyestrdir.
Lightning Network – Bitcoin üçün hazırlanmış, sürətli və ucuz ödənişlərə imkan verən Layer 2 həlli
Limit order – istifadəçinin müəyyən qiymətə alış və ya satış əmri verdiyi ticarət növü
Liquidity – bir aktivin sürətli və dəyər itirmədən pula çevrilə bilmə qabiliyyətidir.

Liquidity mining – likvidlik təmin edən istifadəçilərə mükafat olaraq token verilməsi prosesi
Liquidity pool – istifadəçilərin tokenlərini depozit qoyduğu və avtomatlaşdırılmış ticarəti təmin edən hovuzdur.
Liveness – blokçeyn şəbəkəsinin fəaliyyətini dayandırmadan yeni bloklar əlavə etmə qabiliyyəti
Lock-up period – tokenlərin müəyyən müddət ərzində satıla və ya transfer edilə bilmədiyi dövr

Mainnet – tranzaksiyaların real zamanda baş verdiyi əsas blokçeyn şəbəkəsi
Merkle tree – böyük verilənlərin effektiv və təhlükəsiz yoxlanması üçün istifadə edilən kriptoqrafik verilənlər strukturu
Metamask – Ethereum və digər EVM əsaslı şəbəkələr üçün məşhur veb brauzer pulqabı
Mining – yeni blokların yaradılması və şəbəkənin təhlükəsizliyini təmin edən hesablama prosesi
Minting – yeni token və ya NFT-nin yaradılması əməliyyatı
Multisig (Multi-signature) – əməliyyatın icrası üçün birdən çox şəxsin təsdiqini tələb edən təhlükəsizlik metodu
Market cap (Market capitalization) – kriptovalyutanın ümumi bazar dəyəri (qiymət × dövriyyədəki miqdar)
Meta-transaction – istifadəçinin qaz ödəmədən üçüncü tərəf vasitəsilə tranzaksiya göndərmə üsulu
Merkle root – Merkle ağacının əsas heş qiyməti; verilənlərin dəyişdirilmədiyini sübut edir.

Node – blokçeyn şəbəkəsində məlumat paylaşan və ya doğrulayan kompüter və ya cihaz
Nonce – blokçeyn tranzaksiyalarında və mədənçilikdə yalnız bir istifadə edilən təsadüfi ədəd
Network fee – tranzaksiyaların blokçeyn üzərində yerinə yetirilməsi üçün ödənilən xidmət haqqı
Nakamoto consensus – Bitcoin və digər PoW şəbəkələrində istifadə edilən konsensus mexanizmi
Native token – bir blokçeyn şəbəkəsinin əsas kriptovalyutası (məsələn, Ethereum-da ETH).
Node operator – şəbəkədə qovşaq işlədən və ya idarə edən şəxs və ya təşkilat
Nonce reuse – eyni nonce qiymətinin təkrar istifadəsi – təhlükəli kriptovalyuta əməliyyat səhvi
Network latency – blokçeyn şəbəkəsində məlumatın ötürülməsi üçün tələb olunan vaxt

Oracle – blokçeynə real dünya məlumatlarını ötürən üçüncü tərəf xidməti
Off-chain – blokçeyn xaricində baş verən, lakin blokçeynlə əlaqəli məlumat və tranzaksiyalar
On-chain – bütün tranzaksiya və məlumatların blokçeyn şəbəkəsində qeydə alınması
Open source – kodu açıq və hər kəs tərəfindən istifadə edilə bilən proqram təminatı
Order book – alqı-satqı əmrlərinin saxlandığı və idarə edildiyi verilənlər strukturu
Optimistic rollup – Ethereum kimi şəbəkələrdə Layer 2 miqyaslama üsulu; tranzaksiyalar əvvəlcə etibar edilərək sonra yoxlanılır
Overcollateralization – kredit təminatı üçün tələb olunan məbləğdən daha çox aktivin bloklanması
Offboarding – istifadəçinin sistemdən çıxarılması və ya aktivlərin fiat valyutaya çevrilməsi prosesi
Ommer (Uncle) block – ana blokdan kənarda yaradılan və əsas blok zəncirinə daxil edilməyən blok
Osmosis – Cosmos əsaslı DEX və likvidlik platforması

Private key – pulqabılara və aktivlərə giriş imkanı verən gizli açardır.
Public key – açıq şəkildə paylaşılaraq tranzaksiyalar üçün istifadə olunan açardır.
Pump and dump – token qiymətinin süni şəkildə artırılıb sonradan sürətlə satılması strategiyası

Quantum computing – mövcud şifrləmə metodlarını təhlükəyə ata biləcək kvant əsaslı hesablama texnologiyası
QR code payment – kripto ödənişləri üçün istifadə edilən sürətli və skan edilə bilən ödəniş metodu
Quorum – icazəli blokçeyn şəbəkəsi üçün hazırlanmış enterprise səviyyəli Ethereum forku
Quickswap – Polygon şəbəkəsində fəaliyyət göstərən sürətli və ucuz DEX platforması
Query layer – məlumatların indekslənməsi və blokçeyndən axtarış üçün istifadə edilən orta qat texnologiyası (məsələn, The Graph).

Raiden network – Ethereum üçün hazırlanmış off-chain ödəniş kanalı Layer 2 miqyaslama həlli.
Rebasing token – token miqdarı dinamik olaraq dəyişən və dəyərin sabit qalmasını hədəfləyən token növü.
Reentrancy attack – ağıllı müqavilələrdə icra zamanı funksiyanı təkrar çağırmaqla vəsait oğurluğuna səbəb olan hücum

Relay chain – Polkadot kimi multizəncir platformalarda fərqli zəncirləri birləşdirən əsas şəbəkə
Replay attack – əvvəlki bir tranzaksiyanının icazəsiz şəkildə başqa bir şəbəkədə təkrar icrası
RollApp – Layer 3 səviyyəsində, yüksək sürətli və modulyar blokçeyn tətbiqidir, rollup-a əsaslanır. Dymension şəbəkəsinin əsas komponentidir.
Rollup – tranzaksiyaların blokçeyn xaricində toplanıb blokçeyndə yığcam formada qeydə alınması üsulu
Rug pull – DeFi layihəsində yaradıcıların investisiya topladıqdan sonra layihəni tərk edib pullarla qaçması

Satoshi – 1 BTC-nin yüz milyonuncu (0.00000001) hissəsi; ən kiçik Bitcoin vahidi
Scalability – blokçeyn şəbəkəsinin tranzaksiya sayını və sürətini artırmaq qabiliyyəti
Security token – ənənəvi maliyyə aktivlərini təmsil edən və tənzimlənən kriptovalyuta
Sequencer – optimistik rollup-larda tranzaksiyaları sıralayan və bloklara çevirən operator və ya qovşaq növü
SHA-256 – Bitcoin şəbəkəsində istifadə olunan kriptoqrafik heş alqoritmi
Sharding – blokçeyn məlumat bazasının hissələrə bölünərək emal edilməsi üsulu
Sidechain – əsas blokçeynə paralel işləyən, onunla etibarlı şəkildə bağlı olan şəbəkə
Slashing – staking zamanı şəbəkə qaydalarını pozan validatorların cəzalandırılması prosesi
Slippage – ticarət zamanı gözlənilən qiymətlə faktiki qiymət arasındakı fərq
Slot (Ethereum) – Ethereum 2.0-da blokların yaradılması üçün zaman bölgüsüdür.
Smart contract audit – ağıllı müqavilənin təhlükəsizlik baxımından yoxlanması
Stablecoin – qiyməti sabit qalmaq üçün fiat və ya digər aktivlərə bağlanmış kriptovalyuta
State channel – Blokçeyn xaricində tranzaksiyaların aparıldığı və yalnız son nəticənin zəncirdə qeyd edildiyi Layer 2 həlli
Synthetic asset – real mövcud olan aktivləri blokçeyn üzərində təqlid edən tokenlər (məsələn, sUSD, sBTC)

Testnet – əsas şəbəkəyə çıxmazdan əvvəl yeni tətbiqlərin sınaqdan keçirildiyi blokçeyn şəbəkəsi
Token – əsas blokçeyn üzərində yaradılan, müxtəlif istifadə məqsədləri olan rəqəmsal aktiv
Tokenomics – tokenlərin yaradılması, paylanması, alqısı və satqısı ilə bağlı məsələləri əhatə edən iqtisadi modeldir.
Trustless – tranzaksiyaların üçüncü tərəfə etibar etmədən icra edilə bilmə xüsusiyyəti

Turing complete – ağıllı müqavilələrin istənilən məntiqi əməliyyatı icra edə biləcək funksionallığa sahib olması
Time-lock contract – token və ya tranzaksiyaların yalnız müəyyən vaxt keçdikdən sonra aktivləşməsinə imkan verən müqavilə
Tornado cash – tranzaksiyaların izini itirmək üçün istifadə olunan mərkəzsiz qarışdırma (ing. mixing) xidməti
Transaction fee – blokçeyn şəbəkəsində tranzaksiya həyata keçirmək üçün ödənilən haqq
Tendermint – PBFT əsaslı konsensus mexanizmi və Cosmos SDK-nin əsas hissəsi
Tangle – DAG (Directed Acyclic Graph) strukturuna əsaslanan, IOTA tərəfindən istifadə olunan blokçeynsiz sistem

Uniswap – Ethereum üzərində qurulmuş mərkəzsiz mübadilə platforması
Universal wallet – çoxsaylı blokçeyn şəbəkələrini dəstəkləyən pulqabı növü
Unspent gas refund – Ethereum tranzaksiyası zamanı istifadə olunmamış qazın istifadəçiyə qaytarılması prosesi
Upgradable smart contract – zamanla dəyişdirilə və ya inkişaf etdirilə bilən ağıllı müqavilə
Upgradeable proxy – ağıllı müqavilələrin sonradan dəyişdirilə bilən versiyasını dəstəkləyən proksi strukturu
Utility token – müəyyən bir ekosistem daxilində xidmət və ya funksionallıq təmin edən token növü
UTXO consolidation – Bitcoin tranzaksiyalarında çoxlu xırda qalığın bir tranzaksiyada birləşdirilməsi

Validator – PoS şəbəkələrində tranzaksiyaları yoxlayan və bloklar əlavə edən iştirakçı
Validator set – blokçeyn şəbəkəsində hazırda blok doğrulayan qovşaqların siyahısı
Vampire attack – yeni bir DeFi platformasının, rəqiblərin likvidliyini təşviqlərlə cəlb etməyə çalışması
Vault – DeFi platformalarında aktivlərin qorunduğu və idarə olunduğu ağıllı müqavilə
Verkle Tree – Ethereum-un gələcək versiyalarında istifadə ediləcək daha səmərəli məlumat strukturu
Vesting – tokenlərin müəyyən müddət ərzində tədricən istifadəçiyə keçməsi mexanizmi
Volatility – kriptovalyutaların qiymətində sürətli və gözlənilməz dəyişiklik dərəcəsi

Wallet – kriptovalyutaları saxlamaq, göndərmək və qəbul etmək üçün istifadə edilən proqram və ya cihaz

Watch-only wallet – aktivlərin vəziyyətinə baxmaq üçün istifadə olunan, lakin imza hüququ olmayan pulqabı növü
Watchtower – Lightning Network-də fırıldaqçılığın qarşısını alan və kanalların monitorinqini təmin edən xidmət
Web3 – İnternetin mərkəziyətsiz və istifadəçi yönümlü növbəti mərhələsini ifadə edən anlayış
Whale – bazarda böyük miqdarda kriptovalyutaya sahib şəxs və ya təşkilat
Whitepaper – kriptovalyuta və ya blokçeyn layihəsinin texniki və iqtisadi əsaslarını izah edən sənəd
Withdrawal credential – Ethereum 2.0 staking sistemində validatorların çıxış ünvanlarını idarə edən struktur
Wrapped token – bir blokçeyndə başqa bir blokçeynə aid aktivin tokenləşdirilmiş versiyası (məsələn, WBTC)
Wrapped token bridge – aktivləri bir blokçeyndən digərinə köçürmək üçün istifadə olunan ağıllımüqavilə sistemi

Yield farming – DeFi platformalarında aktivlərin istifadəyə verilməsi müqabilində gəlir əldə etmə üsulu
Yield optimizer – DeFi platformalarında gəliri maksimuma çatdırmaq üçün strategiyaları avtomatik idarə edən protokol (məsələn, Yearn Finance)
Yubikey – pulqabılara və hesab girişlərinə fiziki təhlükəsizlik təmin edən USB əsaslı cihaz
Zether – gizliliyin təmini üçün ZKP-əsaslı, Ethereum üzəri anonim ödəniş protokolu
Zilliqa – Sharding əsaslı, yüksək performanslı blokçeyn platforması
Zinc – Zk-SNARK əsaslı ağıllı müqavilə yazılması üçün proqramlaşdırma dili
Zk-Rollup – ZKP-əsaslı və Ethereum üzərində miqyaslanmanı təmin edən Layer 2 texnologiyası

Əlavə 1. Bitkoinin qısa tarixi

Bitkoinə qədər kriptovalyutalar olubmu? Bəlkə də, bir çoxları təəccübləcəklər, lakin Bitkoinə qədər bir neçə rəqəmsal pul təklif edilmişdir. Bitkoin blokçeyn əsasında ilk kriptovalyutadır, lakin ilk rəqəmsal pul deyil.

Digicash. Rəqəmsal pulları ilk dəfə 1983-cü ildə Kaliforniya Universitetində oxuyan 28 yaşlı Devid Çaum özünün ilk elmi əsərində təsvir etmişdi. Bu işdə Çaum rəqəmsal pulun kredit kartları ilə edilən ödənişlərdən əsas fərqini – anonimliyi göstərmişdi.

Pulları anonim etmək üçün Çaum "kor" rəqəmsal imzadan istifadə etmişdi. Kor imzaların əsas ideyası aşağıdakından ibarətdir.

1. A sənədi şifrləyir və onu B-yə göndərir.
2. B sənədin məzmununu görmədən, onu imzalayır və A-ya geri qaytarır.
3. A şifri götürür və sənəddə yalnız B-nin imzasını saxlayır.

Devid Çaum 1989-cu ildə öz firmasını təsis etdi, DigiCash virtual valyutasını yaratdı. DigiCash ilə İnternetdə təhlükəsiz və rahat ödənişlər etmək olardı.

Lakin rəqəmsal pulların işləməsi üçün elektron ticarət şəklində tələbat zəruri idi, elektron ticarət isə yalnız 1990-ci illərin ortalarından inkişaf etməyə başladı. Lakin DigiCash 1990-cı illərdə də çətinlik çəkirdi: Çaumun valyutası hələ mövcud olmayan problemi – anonimliyi həll etməyə çalışırdı. Həmin vaxt istifadəçilər İnternet rahat alış-veriş etmək istyirdilər və əlbəttə ki, onlara tanış olan kredit kartlarına üstünlük verirdilər.

Bundan başqa, Çaumun özü də biznes məsələlərində çox səriştəli deyildi – aylarla şirkətlərlə müqavilələri müzakirə edir, sonda is imzalamaqdan imtina edirdi. Bill Qeyts və həmin dövrdə məşhur olan Netscape brauzerinin operatoru DigiCash-ı öz məhsullarına inteqrasiya etməyi istəyirdilər, lakin onların təklif etdikləri şərtlər Çaumu təmin etmirdi. 1999-cu ildə Çaumun firması iflas etdi və onun rəqəmsal valyutası unuduldu.

E-gold. 1996-cı ildə həkim-onkoloq Douglas Jackson və hüquqşünas Berri Dauni (Barry Downey) İnternet-kommersiyanı inkişaf etdirmək üçün belə bir ideyanı reallaşdırdılar: onlar bank hücrəsinə qızıl sikkələr qoydular, sonra bu sikkələrin rəqəmsal hissələrini satmaq üçün veb-sayt yaratdılar. Bu hissələr e-gold adını almış yeni valyutada denominasiya edilirdi.

Sonrakı dörd il ərzində e-gold inkişaf ediərək populyarlıq qazandı – nəticədə ilk rəqəmsal ödəniş sistemini ən azı milyon insan istifadə etməyə başlamışdı. E-gold kredit kartları olmadan ilk ödəniş servisi idi və onu İnternet-mağazalara inteqrasiya etmək olardı. Öz inkişafının pik nöqtəsində e-goldun bazar kapitallaşması 2 milyard dollar təşkil edirdi. Lakin e-goldun populyarlığı hakerlər arasında da artırdı və yaxşı müdafiə olunmayan sistem hücumlara məruz qalırdı və bir çox müştəri öz vəsaitlərini itirirdi.

2001-ci ildə Cekson və Dauni lisenziyaları olmadığından məhkəm qarşısında dayanmalı oldular. Vergi orqanları onların qızıl ehtiyatlarını dondurdu və istifadəçilərin çoxu e-gold sistemini tərk etdilər. Sahibkarlar lisenziya ala bilmədilər və e-gold-un tarixi bununla sona çatdı.

B-Money. Wei Dai B-Money elektron sistemini 1998-ci ildə yaratmışdı, burada istifadəçilərə iki protokol təklif edilirdi. Onlardan biri sinxron əlaqə kanalının yaradılmasını nəzərdə tuturdu. Layihə Bitkoinə oxşamır və dəstək qazana bilməmişdi. Lakin onu anonim və təhlükəsiz ödəniş sistemi yaradılmasına ilk ciddi cəhd hesab etmək olar. Müstəqil şəbəkədə vəsaitlərin ötürülməsi üçün istifadəçilərin təxəllüsləri istifadə edilirdi. Tranzaksiyalar edilən zaman vasitəçilərə ehtiyac olmurdu. Wei Dai öz işinin analizini dərc etsə də, çox sayda investor cəlb edə bilməmişdi. Qeyd etməyə dəyər ki, Nakamoto «White Paper»-də B-Money sisteminin bəzi cəhətlərinə istinad edir, buna görə, Bitkoin yaradıcısının bu şəbəkə ilə yaxından tanış olması güman edilir.

Bit Gold. Bu sistem 20-ci əsrin son illərində meydana çıxmışdı. Onu Nik Sabo yaratmışdı, bunun üçün işin isbatı alqoritmi istifadə edilmişdi. Şəbəkə daxilindəki proseslər bir çox cəhətdən blokçeyni xatırladırdı, lakin ən vacib cəhət mərkəzləşmiş iş prinsipindən imtina idi. Bit Gold-da vahid idarəetmə mərkəzindən asılılıq aradan qaldırılmışdı. Sabonun məqsədi nəcib metalın rəqəmsal analoqu və vasitəçilər olmadan işləmək idi. B-money kimi, Bit Gold da uzun müddət davam etmədi, lakin bir çox kriptovalyuta üçün şablon oldu.

Hashcash. Ən populyar rəqəmsal valyutalardan biri 1990-cı illərin ortalarında meydana çıxmışdı. 1997-ci ildə Adam Bek spamdan müdafiəyə həsr olunmuş Hashcash layihəsini işə salmışdı. Məsələ belə ifadə olunurdu: «x-in elə qiymətini tapın ki, SHA(x) heşində N böyük bit sıfır olsun».

Onun yaradıcıları müxtəlif məqsədlər güdürdülər və spam və DDoS-hücumlardan müdafiə olunmuş şəbəkə qurmuşdular. Ödəniş sistemində çox sayda imkan nəzərdə tutulmuşdu, lakin onların çoxunu məhsulda reallaşdırmaq mümkün olmamışdı.

Hashcash-in işləməsi üçün *işin yerinə yetirilməsinin isbatı* prinsipi tətbiq edilmişdi, onun sayəsində yeni daxili sikkələr yaranırdı və paylanırdı. Ödəniş sisteminin populyarlaşması hesablama güclərinin çatışmamasına gətirib çıxardı. Nəticədə şəbəkə tədricən öz tərəfdarlarını itirdi və öz fəaliyyətini dayandırdı. Ən yaxşı günlərində Hashcash müştərilər tərəfindən çox tələb edilirdi, buna görə Bitkoin yaradıcıları onun prinsiplərindən bir çoxunu götürmüşdülər.

Bitkoin yuxarıda danışılan institutlardan sonra meydana çıxmışdı və demərkəzləşmə ilə və blokçeynin tətbiqi ilə fərqlənirdi. Yuxarıda sadalanan sələflər olmadan, ilk rəqəmsal aktiv və minlərlə digər müasir kriptovalyuta meydana çıxa bilməzdi.

Bitkoin. Dünya Bitkoin haqqında ilk dəfə 31 oktyabr 2008-ci ildə Mərkəzi Avropa vaxtı ilə 8.10-da eşitmişdi. Satoşi Nakamoto adlı birisi aşağıdakı cümlə ilə başlayan qısa məlumat göndərmişdi:

"Mən tamamilə birranqlı olan və etibarlı üçüncü tərəflərin iştirakını nəzərdə tutmayan elektron pul sistemi yaratmışam."

Məlumatda Bitkoinin texniki təsviri olan doqquz səhifəlik "Ağ məqalə"yə istinad verilirdi. Ağ məqalə çıxdıqdan üç ay sonra sonra Bitkoin kliyentinin ilk versiyası işə salınmışdı. 3 yanvar 2009-cu ildə ilk 50 bitkoin "generasiya" edildi, üç gün sonra isə Satoşi Nakamoto ilə kriptovalyuta fəalı Hel Finny arasında ilk tranzaksiya edildi. Həmin ilin oktyabrında ilk mübadilə baş verdi: 1 dolları 1309 bitkoinə dəyişdilər. Onlar qiyməti sərf olunan elektrik enerjisinin dəyəri əsasında müəyyən etmişdilər.

2010-cu ilin mayında ilk dəfə bitkoinlə mal alınmışdı – 10 min bitkoinə 2 pizza sifariş edilmişdi (çatdırılmaqla). Bitkoin tədricən populyarlaşmağa başladı və 2011-ci ildə ilk kriptovalyuta birjası yaradıldı.

"Ağ məqalə"də bir sualdan başqa bütün suallara cavab verilirdi: Satoşi Nakamoto kimdir? İndiyə kimi məlum deyil ki, belə bir adam həqiqətən də varmı, bu təxəllüslə kim(lər) gizlənir? Bitkoinin populyarlaşdıqca, onun yaradıcısını tapmağa bir çox cəhdlər edildi, lakin indiyə kimi heç bir nəticə yoxdur.

Bitkoinin müəllifi özünü Satoshi Nakamoto adlandırır.

Satoshi adı yapon dilindən «müdrik», Nakamoto soyadı – «mürəkkəb (qapalı) sistemin daxilində yerləşən» kimi tərcümə edilir.

Əlavə 2. Bitkonlə əlaqəli bəzi hadisələrin xronologiyası

- **2007-2008** – Böyük Depressiyadan (1930-cu illər) sonra ən pis **qlobal maliyyə böhranı** baş verib.
- **15 avqust 2008**– Neal Kin, Vladimir Oksman və Charles Bry şifrləmə patenti üçün ərizə təqdim edirlər.
- **18 avqust 2008** – **bitcoin.org** domeni qeydiyyatdan keçirilir.
- **31 oktyabr 2008** – Satoşi Nakamoto yeni pul sisteminin texnologiyasını təsvir edən "Bitcoin: A Peer-to-Peer Electronic Cash System" (**"Bitkoin: Pirinq elektron pul sistemi"**) məqaləsini saytda yerləşdirir.
- **9 noyabr 2008** – Bitcoin layihəsi **SourceForge.net** saytında qeydiyyatdan keçirilir.
- **3 yanvar 2009** – Satoşi Nakamoto ilk Bitkoin blokunu (**Genesis**) generasiya etmiş və onun bitkoin-ünvanına ilk 50 bitkoin daxil olmuşdu. Birinci bloka ***"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*** mətni daxil edilmişdi.
- **9 yanvar 2009** – Satoşi Nakomoto **Bitcoin Core v.0.1** proqramının birinci relizi ***Cypherpunks*** göndəriş siyahısında yerləşdirib.
- **10 yanvar 2009** – Bitkoin şəbəkəsinə **qovşaq №2** qoşulub. Bitkoinin ikinci istifadəçisi Hel Finni olmuşdur. Həmin gün **blok №78** generasiya etmişdi və onun bitkoin ünvanına 50 bitkoin daxil olmuşdu.
- **12 yanvar 2009** – bitkoinin göndərilməsi üzrə ilk tranzaksiya edilmişdi – Satoşi Nakamoto Hel Finninin bitkoin-ünvanına 10 bitkoin göndərmişdi. Bu **blok №170**-də qeydiyyata alınıb.
- **5 oktyabr 2009** – **New Liberty Standard** saytında bitkoinin ABŞ dollarına ilk mübadilə kursu nəşr olunub.
- **30 dekabr 2009** – mayninqin çətinliyi ilk dəfə artırılıb.
- **6 fevral 2010** – Bitkoin almaq üçün ilk servis olan Bitcoin market veb-saytı yaradılıb.
- **22 may 2010** – bitkoinlə ilk tranzaksiya həyata keçirilir; proqramçı Laszlo Hanyecz 10 min bitkoinə 2 pitza sifariş etmişdi.
- **11 iyul 2010** – kompüterçilər arasında populyar olan Slashdot portalında Bitkoin haqqında çıxan yazı Bitkoin istifadəçilərinin sayını kəskin artırır.
- **12 iyul 2010** – Bitkoinin dəyəri 10 dəfə artır (beş gün ərzində US$0.008/BTC-dən US$0.080/BTC-yə).
- **17 iyul 2010** – MtGox valyuta mübadiləsi birjası işə başlayır.
- **15 avqust 2010** – Bitkoin sistemində aşkarlanmış boşluqdan istifadə edən eksployt 184 milyard bitkoin generasiya edir.

- **18 sentyabr 2010** – Slush mayninq hovuzu özünün ilk blokunu generasiya edir.
- **28 yanvar 2011** – bütün bitkoinlərin 25%-i generasiya edilir (Blok 105000).
- **9 fevral 2011** – Bitkoin kursu ilk dəfə ABŞ dolları ilə bərabərləşir, MtGox-da kurs US$1.00/BTC olur.
- **25 mart 2011** – Bitkoin mayninqin çətinliyi ikinci dəfə azaldılır (təxminən 10 %).
- **27 mart 2011** – Bitkoini Britaniya funt-sterlinqinə dəyişən birja açılır.
- **31 mart 2011** – Bitkoini Braziliya realına dəyişən birja açılır.
- **5 mart 2011** – Bitkoini avroya və digər valyutalara dəyişən BitMarket.eu açılır.
- **16 aprel 2011** - TIME jurnalında Bitkoin barədə məqalə nəşr edilir ("Online Cash Bitcoin Could Challenge Governments, Banks")
- **12 iyun 2011** – Bitkoin qiymətinin böyük faizdə aşağı düşməsi. MtGox birjasında Bitcon mübadilə kursu 31.91 dollar pik nöqtəsinə çatdıqdan cəmi dörd gün sonra 10 dollara düşmüşdü. Bu insidentə "2011-ci ilin Böyük Qabarcığı" adı verilmişdir.
- **20 avqust 2011** – Nyu-Yorkda World Expo çərçivəsində ilk Bitkoin konfransı keçirilir.
- **25 noyabr 2011** – "Bitcoin & Future Technology European Conference" keçirilir.
- **27 fevral 2012** – Bitcoin Magazine jurnalı çıxır.
- **17 dekabr 2017-ci il** – Bitkoin kursu ən yüksək qiymətə çatır (19 783 $).
- **16 dekabr 2024-cü il –** Bitkoin kursu tarixdə ən yüksək qiymətə çatır (108 000$).

Əlavə 3. Bəzi kriptovalyutaların qısa adları (tikerləri)

BTC – *Bitcoin* (Bitkoin) – ilk kriptovalyuta

BCH – *Bitcoin Cash* – Bitkoinin birinci forku

BTG – Bitkoin Qold (*Bitcoin Gold*) – Bitkoinin ikinci forku

DASH – Daş (*Dash*) – əvvəllər **XCoin** (XCO) və **Darkcoin** adı ilə tanınırdı

ETC – Efir klassik (*Ether Classic*) – **ETH**-in forku

ETH – Efir (*Ether*) – Ethereum platformasında kriptovalyuta

LTC – Laytkoin (*Litecoin*) – Bitkoinin forku

MIOTA – Yota (*IOTA*) – Əşyaların İnternetində maşınlar arasında təhlükəsiz əlaqə və ödənişlərin təmin edilməsinə yönəlmiş kriptovalyuta

WAVES – Veyvs (Waves – «dalğalar») – kriptoqrafik tokenlərin buraxılması və kraudfandinq kampaniyalarının aparılması üçün eyniadlı blokçeyn platformasının daxili kriptovalyutası (tokeni)

XEM – Nem (*NEM*) – mayninqi **PoI** alqoritmi əsasında aparılan kriptovalyuta (prosesin hər bir iştirakçısının inkişaf və irəliləyişə töhfəsi)

XMR – Monero (*Monero – esperanto dilində «sikkə»*) – anonim pul tranzaksiyaları üçün nəzərdə tutulmuş kriptovalyuta

XRP – Ripl (*Ripple – hərfən «zəif ləpələr»*)–paylanmış ödəniş sisteminin daxili kriptovalyutası, etibarlı vasitəçi prinsipindən istifadə edir, mayninq nəzərdə tutulmayıb

ZEC (Zcash) – **Zerocoin Electric Coin Company** şirkəti tərəfindən buraxılmış, konfidensiallığı və seçmə şəffaflığı təmin edən kriptovalyuta

Əlavə 4. Kriptovalyutaların kəsr vahidləri

Bütün pulların əsas vahidləri ilə yanaşı, kəsr hissələri də var. Məsələn, ABŞ **dollar**ı üçün kəsr vahidi **sent**dir. Əsas kriptovalyutaların da kəsr hissələri var və onlara məxsusi ad da verilib.

Bitkoin

Bitkoin kriptovalyutasının əsas mübadilə vahidi də ***bitkoin*** adlanır, lakin kiçik hərflə yazılır. İşarə üçün **BTC qısaltması və Ƀ** simvolu istifadə edilir (aşağı hissəsində üfüqi xətt olan **B** hərfi).

Ƀ simvolu xüsusi olaraq **Yunikoda** (U+0243) və **HTML-ə** (Ƀ) daxil edilib. Bu simvol bitkoinin alternativ işarələrindən biri kimi istifadə edilir. `bitcoinsymbol.org` saytından daha ətraflı məlumat almaq olar. ₿ işarəsi də geniş istifadə edilir, Yunikod 10.0 versiyasına daxil edilib və U+20BF nömrəsi verilib.

Bitkoin simvolu üçün ฿ da geniş istifadə edilirdi – onun Yunikod nömrəsi U+0E3F və **HTML-kodu** ฿-dir.

Bitkoinin kəsr hissələri

Bitkoinin ən kiçik və çox istifadə edilən vahidi **satoshi** adlanır – 1/100 000 000 (0,000 000 01 BTC) – **Satoşi Nakamoto**nun şərəfinə adlandırılıb.

Hazırda bitkoinin digər hissələrinin adları barədə də çox müzakirə aparılır. Əsas namizədlər aşağıdakılardır:

- 1/100 (0,01 BTC) = **1 cBTC** = 1 sent-bitkoin və ya santi-bitkoin (**bitsent** kimi də tanınır)
- 1/1 000 (0,001 BTC) = **1 mBTC** = 1 milli-bitkoin (**mbit** və ya **millibit** kimi də tanınır)
- 1/1 000 000 (0,000 001 BTC) = **1 µBTC** = 1 mikro-bitkoin (yubit və ya **mikrobit** də adlanır)

Laytkoin (Litecoin)

Bitkoinin «kiçik qardaşının» – laytkoinin (**LTC**) də kəsr hissələri var:

- 1⁄1 000 (0,001 LTC) – mLTC (**millikoyn**)
- 1⁄1 000 000 (0,000001 LTC) – µLTC (**mikrokoyn**)

Efirium (Etherium)

Efirium kriptovalyutasının əsas mübadilə vahidi *Ether* (*efir*) adlanır. İşarə üçün **ETH** qısaltması və Ξ simvolu (yunan hərfi Ksi) istifadə edilir.

Efirin kəsr hissələrinin öz adları var:

- 1/1 000 (0,001 ETH) = **1 finney** (finni) – kriptoloq *Hal Finni-nin şərəfinə adlandırılıb*;

- 1/1 000 000 (0.000001 ETH)= **1 szabo** (sabo) – ağıllı müqavilələri təklif edən kriptoloq Nik Sabonun (Nick Szabo) şərəfinə adlandırılıb;
- 1/1 000 000 000 (0,000000001 ETH)= **1 Gwei** (qiqavey – milyard vey);
- 1/1 000 000 000 000 000 000 (0,000000000000000001 ETH)= **1 wei** – **B-money yaradıcısı, proqramçı və kriptopank VeyDay**ın (Wei Dai) şərəfinə adlandırılıb.

Əlavə 5. Kriptovalyutalar üzrə faydalı veb-resurslar

1. **Bitcoin.org** – ilk Bitcoin veb saytının istifadə etdiyi addır, əvvəlcə Satoşi Nakamoto və martti Malminin adına qeydiyyata alınmışdı. 2011-2013-cü illərdə əsasən Bitcoin Core adlanan proqram təminatının yeni versiyalarının yüklənməsi üçün istifadə edilirdi. 2013-cü ildə sayt yenidən dizayn edilmiş və ona bir çox səhifələr əlavə edilmişdir (bir neçə dil dəstəklənir). Ayrıca səhifədə Bitcoin Core proqram təminatının– Bitkoin proqram-kliyentin son versiyasını yükləmək mümkündür.
2. **BitcoinWiki.org** – Bitkoin haqqında Vikipediya. Bitkoin və kriptovalyutaların müxtəlif aspektləri üzrə ensiklopedik məqalələr toplusu.
3. **BitcoinTalk.org** – Bitkoin və kriptovalyutalar haqqında ən böyük beynəlxalq forum (2009-cu ildən mövcuddur).
4. **Blockchain.info** – Bitkoin-pulqabının populyar veb-versiyası. Bitcoin Cash və Etherium pulqabılarını da dəstəkləyir. Bu saytda Bitkoin şəbəkəsi haqqında olduqca çox sorğu və statistika məlumatları var.
5. **CoinDesk.com** – Bu saytda digər məlumatlarla yanaşı, bitkoinin dollara nisbətən kursunun tam tarixçəsi var.
6. **GoBitcoin.io** – informasiya-məlumat saytıdır, bir neçə faydalı alət də təklif edilir: 1) Bitkoin-ünvan üçün QR-kod generatoru; 2) "51 % hücumu"nun qiyməti; 3) Bitkoin kursunun volatilliyi (ABŞ dolları ilə); 4) Digər alətlər (vidjetlər, real zamanda tranzaksiyalar və s.).
7. **CoinMap.org** – Bitkoinlə işləyən şirkətlərin və təşkilatların dünya üzrə yerləşməsini göstərən interaktiv xəritə.
8. **Spendabit.co** – Bitkoinlə almaq mümkün olan malların axtarışı üçün sistem.
9. **Coin.Dance** – Bitkoin şəbəkəsi üzrə qlobal statistika saytı. Texnoloji və maliyyə statistikası ilə yanaşı, demoqrafik statistika da daxildir.
10. **cryptocurrencyjobs.co** – Blokçeyn və kriptovalyuta işləri üçün elanlar lövhəsi
11. **BitNodes.earn.com** – qovşaqların interaktiv xəritəsi və ölkələr üzrə verilənlər daxil olmaqla, Bitkoin qovşaqları üzrə tam statistika.
12. **BitcoinClock.com** – Bloka görə mükafatın (bitkoin emissiyasının) dəyişməsini izləyən saat.
13. **BitcoinBlockalf.com** – Bloka görə mükafatın (bitkoin emissiyasının) dəyişməsini izləyən digər bir saat. Orada digər statistika da var, o cümlədən, buraxılmış bitkoinlərin ümumi sayı, qalan bitkoinlərin sayı, Bitkoinin ümumi kapitallaşması, mqyninqin çətinliyi və s.
14. **Bitkoin statistikası üzrə bəzi veb-resurslar:**
    - BitcoinTicker.com
    - BitInfoCharts.com

- TradeBlock.com/bitcoin/

15. **BitAddress.org** – gizli açarı müştəri tərəfdə olan Bitkoin pulqabıların generatoru, JavaScript kodu açıqdır. İnternetə qoşulmadan işləyir. Yeni bitkoin-ünvanı və onun gizli açarını təsadüfi generasiya etməyə imkan verir. Nəticədə kağız daşıyıcıda bitkoin-pulqabı əldə etmək olar.
16. **Blok-eksplorerlər** – blok və tranzaksiya haqqında məlumatı birbaşa blokçeyndən almağa imkan verirlər. Bəzi blok-eksplorerlər:
    - https://www.blockexplorer.com/
    - https://www.blockchain.com/explorer
    - https://btcscan.org/
    - https://btc.com/
    - https://www.coinbase.com/en-sg/explore

Əlavə 6. Bəzi konsensus alqoritmləri

- dPoS (delegated PoS) – səlahiyyət şəbəkənin bütün iştirakçıları tərəfindən ümumi səsvermə ilə seçilən müəyyən sayda qovşağa verilir.
- PoA (Proof-of-Audit) – auditin, yəni yenilənmiş sənəddə dəyişiklərin olmasının yoxlanmasının isbatına əsaslanan müdafiə mexanizmidir;
- PoB (Proof-of-Burn) – az yayılmış konsensus protokoludur.
- PoC (Proof-of-Capacity) – tərpənməz diskdə və ya digər daşıyıcılarda boş yerin varlığının isbatına əsaslanan müdafiə mexanizmidir;
- PoET (Proof of Elapsed Time) – bu konsensus alqoritmi son nəsil Intel prossessorlarında olan SGX etibarlı hesablamalar moduluna əsaslanır.
- PoI (Proof-of-Importance, vacibliyin isbatı) – PoW və PoS alqoritmlərinin konsepsiyalarını birləşdirir,
- PoP (Proof-of-Process) – sənədin yeniləndiyinin isbatına əsaslanan müdafiə mexanizmidir;
- PoR (Proof-of-Resource) – hesablama resursları ilə təmin olunmanın isbatına əsaslanan müdafiə mexanizmidir;
- PoS (Proof-of-Storage) – saxlancın isbatı; az yayılmış konsensus protokoludur;
- RoE (Proof-of-Existence) – sənədin bu şəkildə müəyyən zamanda mövcud olduğunun isbatına əsaslanan müdafiə mexanizmidir;

Ədəbiyyat

1. Nakamoto S., Bitcoin: A peer-to-peer electronic cash system, 2008. https://www.bitcoincash.org/bitcoin.pdf
2. Antonopoulos A. M., Harding D. A., Mastering Bitcoin: Programming the open blockchain. O'Reilly Media, 2023, 400 p.
3. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S., Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press, 2016, 336 p.
4. Bashir I., Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3. 4th ed., Packt Publishing, 2023, 818 p.
5. Burniske C., Tatar J., Cryptoassets: The innovative investor's guide to Bitcoin and beyond. McGraw Hill, 2018, 368 p.
6. Hətəmova N., Bitkoin texnologiyasının elmi-nəzəri və praktiki problemləri / "İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı, 2017, s. 111-114.
7. İmamverdiyev Y., Blokçeyn texnologiyaları: Komponentləri, tətbiqləri və problemləri // İnformasiya Cəmiyyəti Problemləri, 2019, 10(2), s. 18-32.
8. İmamverdiyev Y., Sadıyeva F., Kriptovalyutalarda konfidensiallıq və anonimlik problemləri / "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" V respublika konfransı, 2019, s.61-65.
9. İmamverdiyev Y., Muradova G., Fərdi məlumatların mühafizəsi üçün blokçeyn texnologiyaları: imkanları və perspektivləri / "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" V respublika konfransı, 2019, s.184-187.
10. Hətəmova N., Bitkoin texnologiyası. Bakı: İnformasiya Texnologiyaları nəşriyyatı, 2019. 72 s.
11. İmamverdiyev Y., Sadıyeva F., Kriptovalyuta verilənlərinin intelektual analizi məsələləri // İnformasiya texnologiyaları problemləri, 2020, №1, s. 82–89.