Blokçeyn texnologiyasının təhlükəsizlik məsələləri

Oqtay Ələkbərov
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
oqtayalakbarov@iit.ab.az

Xülasə — Tezisdə çoxfunksiyalı və çoxmərhələli blokçeyn texnologiyalarında müxtəlif növ tranzaksiya əməliyyatlarının yerinə yetirilməsi məsələləri araşdırılmışdır. Burada blokçeyn texnologiyasının təhlükəsizlik məsələlərinə baxılmış və perspektivlərindən bəhs edilmişdir.

Açar sözlər— Blokçeyn, mayner, bitkoin, kriptovalyuta, tranzaksiya

I. GİRİŞ

Blokçeyn texnologiyası (BT) son dövrlərin ən populyar texnoloji yeniliklərindən sayılır. Bu texnologiyanın sənaye, səhiyyə, maliyyə, elektron hökumət sahələrinə tətbiqi, onun perspektivlərini daha da artırmışdır. Qeyd edildiyi kimi, BT-nın bir çox sahələrə tətbiqi onun təhlükəsizlik məsələlərinin daha da dərindən araşdırılmasına tələb yaratmışdır. Blokçeyn texnologiyası haqqında məlumatlara XXI əsrin əvvələrində müəyyən elmi və texnoloji araşdırmaların tərkibində rast gəlmək olardı. Ümumilikdə isə 2008-ci ildə virtual ticarət məkanı üçün xüsusi kriptovalyuta olan bitkoinlərin İnternet istifadəçiləri arasında ödəniş vasitəsi kimi istifadəsi blokçeyn texnologiyasının geniş yayılmasına şərait yaratdı. Bitkoin kriptovalyutasının bazara daxil olması ilə BT yeni bir mərhələyə qədəm qoydu. Hal-hazırda aparılan bir sıra elmi araşdırmalar göstərir ki, bu texnologiya gələcəkdə ağıllı şəhərlərin, əşyaların internetinin və ümumiyyətlə maliyyə bazarının əsas özəyini təşkil edəcək. Hal-hazırda dünyanın bir sıra çox şirkət və təşkilatları BT-dən geniş istifadə etməyə başlamışlar. Bir çox audit şirkətlərinin əsas problemi bazada məlumatın doğruluğunun yoxlanımasıdır. İnsan faktorunu nəzərə alsaq istənilən məlumatı mərkəzi serverlərdə dəyişmək olur. BT əsasında istifadə olunan Factom Apollo proqram təminatı bu problemi aradan qaldırmışdır. BT-nın ən geniş yayılmış proqram təminatı BlockNotary-dır. Bu proqram təminatı virtual notarius rolunu oynayır. İstənilən şəxs özü haqqında məlumatların doğruluğunu bu proqram təminatı vasitəsilə təsdiqləyə bilər. Məsələn, hər hansı şəxsin bank sistemində əməliyyat aparması üçün onun şəxsiyyətinin təsdiqi vacibdir. BlockNotary proqram təminatı olduğunuz yeri tərk etmədən öz məlumatlarınızı təsdiqləməyə imkan yaradır. BT çoxfunksiyalı və sadə struktura malik olması, qeyd etdiyimiz sahələrdə məlumatların emalını, proseslərin avtomatlaşdırılmasını və eyni zamanda təhlükəsizlik məsələlərini dəfələrlə artıracaqdır. BT-yə güvənin artmasının başlıca səbəbi, onun bir neçə vacib elementə sahib olmasıdır. Hal-hazırda blokçeyn texnologiyasının 6 elementi vacib sayılır [1,2]:

- Mərkəzləşdirilməmiş server
- Açıq mənbə
- Məxfilik
- Avtonom rejim
- Sabit sistem
- Tranzaksiya şəffaflığı.

Qeyd elediyimiz elementlər blokçeyni digər bənzər sistemlərdən fərqləndirərək daha da üstün edir. BT-nın ümumi arxitekturası çox sadə formaya sahibdir. BT-də gedən proses vaxtı hər növbəti bloka məlumat ötürülməsi zamanı yeni blokdan özündən əvvəlki bloka isə informasiyanın doğruluğu haqqında məlumat ötürülür. Əgər bu prosses zamanı geri ötürülən təsdiq siqnallarının hər hansı birində məlumat uyğunsuzluğu olarsa, proses sistem tərəfindən avtomatik olaraq dayandırılır.

Blokçeyn texnologiyasının 3 tipi var [3]:

- **Ümumi blokçeyn texnologiyası** – bütün istifadəçilərə bloklarda həyata keçirilən proseslər və eyni zamanda tranzaksiya haqqında məlumatları açıq formada əldə etməyə imkan verir.
- **Konsorsium blokçeyn texnologiyası** – burada adətən iki şirkət arasında baş verən tranzaksiya əməliyyatları vaxtı məxfiliyi təmin etmək üçün şəbəkənin bəzi aralıq bloklarından istifadə etməklə məlumatların məxfiliyi qorunur.
- **Özəl blokçeyn texnologiyası** – bu texnologiyada bloklarda gedən bütün əməliyyatların məxfiliyi qorunur. Prosesdə iştirak edən istifadəçilər əməliyyat haqqında məlumata sahib olmurlar. Yalnız ötürücü və qəbuledici tərəflər bütün trankzaksiyanın gedişatını izləyə bilirlər.

Qeyd etdiyimiz kimi BT sadə mərkəzləşdirilməmiş sistemə sahib olduğundan onun təhlükəsizlik məsələləri daim aktual olur.

II. BLOKÇEYN TEXNOLOGİYASININ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Blokçeyn texnologiyasının daha müstəqil fəaliyyət göstərməsi ona olan marağı artırır. Təbii ki, bu faktor BT-də təhlükəsizlik məsələlərini gündəmə gətirir. Blokçeyndə təhlükəsizlik 2 mərhələdə aparılır. 1-ci mərhələdə tranzaksiya zamanı təhlükəsizlik, 2-ci mərhələ isə tranzaksiya bitəndən

DOI: 10.25045/NCInfoSec.2018.11

sonra əldə olunan bitkoinlərin təhlükəsizliyi nəzərdə tutulur. BT-nin təhlükəsizliyinə bir neçə faktor təsir edə bilər. Bunlara aşağıdakıları göstərə bilərik [4]:

- **Tranzaksiyada çox hissəyə sahib olmaq**. Burada əsasən bloklarda gedən proseslərdə iştirak edən maynerlərin (tranzaksiyada iştirak edən virtual istifadəçi) şəxsi mənafeyi naminə bloka təsir etməsi nəzərdə tutulur. Belə ki, bloklarda gedən əməliyyatlar zamanı hər bir mayner göstərdiyi xidmətə görə müəyyən miqdarda bitkoinlə qiymətləndirilir. Aparılan araşdırmalar göstərir ki, hər hansı mayner proses zamanı 51%-dən artıq paya sahib olarsa, artıq tranzaksiyaya təhlükə yarada bilər. Belə olan halda mayner tranzaksiyaya bir neçə formada təsir edə bilər:
  - ✓ Tranzaksiya haqqında məlumatları dəyişmək;
  - ✓ DoubleSpending etməklə tranzaksiyanın xərcini artırmaq;
  - ✓ Tranzaksiyanın gedişatını saxlamaq;
  - ✓ Tranzaksiyaya daha çox fayda verən maynerin fəaliyyətinə təsir etmək;
- **Blokların saxta klonları.** Bu zaman kənardan kiberhücumlar etməklə tranzaksiyada saxta bloklar yaradılır. Təbii ki, blokçeynin mərkəzləşdirilməmiş sistemə sahib olması saxta blokların yaradılmasını asanlaşdırır. Belə ki, ümumi tranzaksiya əməliyyatı vahid mərkəzdən paylanılmır. Sistemdə səpələnmiş formada olur.
- **Bloklarda aparılan əməliyyatların həcmi.** Bildiyimiz kimi tranzaksiya əməliyyatlarının həcmi fərqli ola bilər. Əməliyyatın həcminin böyük olması həmin prosesdə daha çox mayner iştirakı deməkdir. Belə olan halda isə əməliyyatı yerinə yetirmək üçün daha çox resurs istifadə olunur. Təbii ki, daha çox resursun istifadəsi sonda əməliyyat üçün mükafatın həcmini daha da artırır və hakerlər üçün həmin tranzaksiyada gedən bloklara hücum etmək üçün stimul verir.
- **Bloklarda aparılan əməliyyatların vaxtı.** Yuxarıda qeyd etdiyimiz kimi tranzaksiyanın həcminin böyük olması maynerlərin çoxluğuna təsir edir. Eyni zamanda bloklarda gedən əməliyyatlara sərf olunan vaxt da kiberhücumlara şərait yaradır. Belə ki, prosesin uzun müddət davam etməsi kiberhücumlar edən hakerlərə daha çox sərf edir. Tranzaksiyaya sərf olunan vaxtın çox olması onun mükafat qiymətini artırır.
- **Tranzaksiyanın ümumi dəyəri.** Yuxarıda sadaladığımız bütün faktorlar tranzaksiyanın maliyyə dəyərini artırmaqla yanaşı eyni zamanda ona edilən kiberhücumların sayınıda artırır. Ona görə də zaman keçdikcə əməliyyatlara verilən mükafatın həcmi azaldılmaqla daha çox mayner arasında paylanılır. Belə olan halda sistemə edilən hücumların sayı və keyfiyyəti də azalır.

III. BLOKÇEYNƏ EDİLƏN HÜCUMLARIN QARŞISININ ALINMASI

Bitkoinə marağın artması ona edilən hücumların da sayını artırmağa başladı. İlk kütləvi hücum 2011-ci ilə təsadüf edir. 2011-ci ildə Tokyo şəhərində yerləşən MT.Gox şirkətinə kiberhücumlar olunmuşdur. Nəticədə şirkətin virtual kriptohesabından 9 milyon dollar civarında bitkoin oğurlanmışdır. Daha bir kiberhücum 2013-cü ildə ABŞ-da yerləşən İnstaWallet şirkətinə olunmuşdur. Şirkətin yaydığı məlumata əsasən İnstaWallet-ə 5 milyon dollar ziyan vurulmuşdur. Bundan sonra da dəfələrlə belə hücumlar qeydə alınmışdır. Amma blokçeyn tarixinin ən böyük kiberhücumu 2014-cü ilə təsadüf edir. Yenidən MT.Gox şirkətinə edilmiş hücum nəticəsində şirkətə 470 milyon dollara yaxın ziyan dəymişdir. Bütün bu halların baş verməsi blokçeynin təhlükəsizlik məsələlərinə başqa prizmadan yanaşmağa məcbur etmişdir [5].

Tranzaksiya bitdikdən sonra əldə olunan bitkoinlərin təhlükəsizlik məsələləri aşkarlanır. Bitkoinlərin təhlükəsizliyini təmin etmək üçün aşağıdakı metodlardan istifadə olunur.

1. ***İdentifikasiya***— Blokçeyndə təhlükəsizliyin əsasını istifadə olunan açarın şifrələnməsi təşkil edir. Belə ki, kibercinayətkar ilk növbədə istifadəçinin kompüterində və ya smartfonunda yerləşən elektron açara hücum edir. Həmin elektron açar vasitəsi ilə istifadəçi öz elektron cüzdanına (e-wallet) daxil ola bilər və ya ona göndərilən tranzaksiya prosesini izləyə bilər. Açarın bu texnologiyada vacib rol alması onun təhlükəsizlik məsələlərini daha da artırmışdır. Belə ki, kənardan hücumların qarşısını almaq üçün ikimərhələli təhlükəsizlik identifikasiyası təklif olunmuşdur: 1-ci mərhələdə istifadəçi tərəfindən parol daxil olunur, 2-ci mərhələdə isə ECDSA təhlükəsizlik protokolundan istifadə etməklə sistemə giriş şifrələnir [6].
2. **Təhlükəsizlik cüzdanı** — Qeyd etdiyimiz kimi, istifadəçi əldə olunan bitkoini xüsusi elektron cüzdanlarda saxlayır. Kibercinayətkarlar üçün ən asan metod məhz bu elektron cüzdanlara hücum etməkdir. Bu hücumların qarşısını almaq üçün multisig xidməti təklif olunur. Bu xidmət istifadəçinin imzasını onlayn rejimdə qəbul edir. Hətta kənar şəxs cüzdana giriş parollarını bilsə belə həmin hesabdan heç bir transfer və ya ödəniş edə bilməyəcək. Çünki yekunda istifadəçinin elekton imzası tələb olunacaq. Bu elektron imzanı xüsusi USB fləşlərə proqram vasitəsi ilə yazılmaqla və həmin USB-ni personal kompüterə daxil etməklə elekton imzanı aktivləşdirmək, hətta oflayn rejimdə də istifadə etmək olar [7].
3. **Proqram təminatı təhlükəsizliyi** — Zaman-zaman BT-nin proqram təminatında da problemlərə rast gəlinir. Belə ki, proqramda baş verən xətalar müəyyən problemlərə yol açır. Ən böyük proqram təminatı xətası 2010-cu ildə baş vermişdir. CVE-2010-5139 protokolunda baş verən xəta böyük fəsadlara yol açmışdır. Proqramda baş verən yanlışlıq səbəbindən

0,5 bitkoin əməliyyatın sonunda sistem tərəfindən 184 trillion bitkoin qeydə alınmışdır. Daha bir proqram xətasına 2011-ci ildə rast gəlinmişdir. Bu zaman bloklarda səviyyələrarası keçid zamanı BerKeleyDB-dən LevelDB-yə 0,1 saniyə gecikmə baş vermişdir. Nəticədə bütün blokların sinxronizasiyası zamanı uyğunsuzluq yaranmışdır.

Bulud texnologiyalarının inkişafı BT-yə da təsirsiz ötüşməmişdir. Əvvəlki dövrlərdə bitkoin istifadəçiləri haqqında məlumat, onların təhlükəsiz formada saxlanılması problemli məsələ idi. Bulud texnologiyasından istifadə etməklə bu problemlər öz həllini tapdı. Belə ki, əvvəllər hər hansı istifadəçi öz parolunu və ya elektron cüzdana giriş açarlarını unudurdusa sistemə yenidən bərpa olunmaq uzun vaxt aparır, bəzən isə heç mümkün olmurdu. Bulud texnologiyalarının tətbiqi ilə istifadəçi parolları, elektron cüzdanın açarlarını, şəxsi məlumatlarını buludlarda rezerv etməklə bu çatışmazlıqlar aradan qaldırıldı. Bununla bulud platformalarında rezerv edilən elektron cüzdanların təhlükəsizlik mərhələsi bir pillə daha da artır. İstifadəçi hər dəfə bulud vasitəsilə sistemə daxil olanda bulud platforması tərəfindən xüsusi giriş açarı təqdim olunur. Əgər bu açarla istifadəçi imzası arasında hər hansı uyğunsuzluq olarsa, sistemə giriş məhdudlaşdırılır. Bu hal 3 dəfə təkrarlanarsa, onda sistem özünü qorumaq məqsədi ilə bütün məlumatları rezervləməklə silir [8].

NƏTİCƏ

İnformasiya texnologiyalarının sürətli inkişafı və virtual mühitdə onlardan daha da geniş istifadə olunması blokçeyn texnologiyasını aktual edir. BT-nın ağıllı şəhərlərə, əşyaların internetinə tətbiqi və bulud texnologiyalarında istifadəsi ilə bu texnologiyanın geniş yayılmağa başlaması onun təhlükəsizlik məsələlərini daim nəzarətdə saxlamağı tələb edir. Məqalədə qeyd edildiyi kimi BT-nın təhlükəsizlik məsələləri daim analiz edilməli və problemlərin vaxtında həlli yolları tapılmalıdır. Eyni zamanda bu texnologiyalarda tranzaksiya zamanı və tranzaksiya bitdikdən sonra əldə olunan bitkoinlərin təhlükəsizliyi təmin edilməlidir.

ƏDƏBİYYAT

[1] N. T. Courtois and L. Bahack, "On subversive miner strategies and block with holding attack in bitcoin digital currency," CoRR, vol. abs/1402.1718, 2014.

[2] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," arXiv preprint arXiv:1311.0243, 2013.

[3] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,” in IEEE Symposium on Security and Privacy, pp. 104–121, May 2015.

[4] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, ‘‘Eclipse attacks on bitcoin’s peer-to-peer network,’’ in 24th USENIX Security Symposium, pp. 129–144, Washington, D.C., 2015.

[5] Beikverdi, A.; JooSeok, S. Trend of centralization in Bitcoin’s distributed network. In Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015.

[6] Y. Yuan, F.Y Wang,. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016.

[7] T. Bamert, C. Decker, R. Wattenhofer; S. Welten, BlueWallet: The Secure BitcoinWallet. In Security and Trust Management; Mauw, S., Jensen, C., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 65–80.

[8] I. Eyal; G.S Emin, Majority is not enough: Bitcoin mining is vulnerable. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Gemany, 2014.

SECURITY ISSUES IN BLOCKCHAIN TECHNOLOGY

Oqtay Alakbarov
Institute of Information Technology of ANAS
Baku, Azerbaijan
oqtayalakbarov@iit.ab.az

Abstract – The paper studies various transaction operations within multifunctional and multidimensional blockchain technologies. Security issues and perspectives are also analyzed in this study.

Keywords – Blockchain, miner, bitcoin, cryptocurrency, transaction.