Bitcoin texnologiyasının elmi-nəzəri və praktiki problemləri

Nilufər Hətəmova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

hatamovanilufar@gmail.com

***Xülasə*—Bitcoin əməliyyatların üçüncü şəxs və ya qurum olmadan,birin-birə həyata keçirildiyi elektron pul sistemidir. Bitcoinlər şəbəkəsi mərkəzi qurumdan asılı deyil və açıq mənbəli-kriptoqrafik protokola əsaslanır. Bitcoin şəbəkəsi şəbəkəyə qoşulu olan kompüter arasında paylanmışdır.Bitcoin kriptovalyutası aralıq maliyyə qurumu olmadan kompüter və ya smartfon vasitəsilə ödəmələri həyata keçirməyə imkan yaradır. Bu məqalədə Bitcoin şəbəkəsində mövcud olan elmi-nəzəri və praktiki problemlər, Bitcoin şəbəkəsinə qarşı yönəlmiş hücumlar, Bitcoin e-pulqabılarında təhlükəsizlik və anonimlik məsələləri analiz edilmişdir.**

Açar sözlər— Bitcoin, kriptovalyuta, P2P Bitcoin şəbəkəsi, blok, SHA256

I. GİRİŞ

Bitcoin müasir texnologiyaların sürətli inkişafı nəticəsində yaranan valyuta sistemidir. Bu valyuta sistemi kriptoqrafiyaya əsaslanaraq tranzaksiyaların, onlayn ödəmələrin təhlükəsizliyinin təmin edilməsinə şərait yaradır.Kriptovalyuta ideyası 1998-ci ildə Wei Dai tərəfindən irəli sürülmüşdür. Digər pul vahidlərindən fərqli olaraq kriptovalyuta heç bir qurum və dövlət tərəfindən tənzimlənmir,onun qiyməti tələb-təklif əsasında müəyyən olunur [1].

Bitcoin hər kəsə anında ödəmə imkanı verən mərkəzi olmayan ilk rəqəmsal valyutadır. 2008–ci ildə Satoshi Nakamoto ləqəbli bir şəxs və ya qrup tərəfindən bitcoin şəbəkəsinin iş prinsipini və protokolun təsvirini əks etdirən“Bitcoin: A Peer-to-Peer Electronic Cash System” adlı məqalə yayıldı [2]. Bitcoin ilk dəfə 2009-cu ildə istehsal olundu. Bitcoinin simvolu ฿, qısaltma adı isə BTC–dir. Bitcoinin ən kiçik vahidi satoşidir. 1 Satoshi $=10^{-8}$ ฿= 0. 00000001 ฿. 2^{160} sayda bitcoin ünvanı mövcuddur. 2140–ci ilə qədər 21 milyon bitcoin yaradıla bilər[3].

Bitcoinin yaradılması və mübadiləsi açıq açarlı kriptoqrafik protokola əsaslanır. Aşağı əməliyyat xərcləri, qlobal mövcudluq, artan istifadə sahəsi, təhlükəsiziyin və anonimliyin təmin edilməsi Bitcoin-i daha da populyar edir. Bitcoin rəqəmsal pul ekosisteminin əsasını təşkil edən konsepsiya və texnologiyaların toplusudur. Bitcoin istifadəçiləri birbaşa internet vasitəsilə bitcoin protokolundan istifadə edərək əlaqə saxlaya bilərlər.

Bitcoin şəbəkəsi blockchain texnologiyasından istifadə edir.Bu texnologiya kriptoqrafiya və mərkəzi olmayan şəbəkələrin təhlükəsizliyi sahəsində ən mühüm kəşfdir. Çünki blok zənciri texnologiyası tranzaksiyaların modifikasiyaya davamlı olmasına imkan yaradır, dəyişməz olaraq qalmasına kömək edir. Blok zəncirləri Bitcoin şəbəkəsində olan hər kəsə açıq olur.

Bitcoin satıla, alına və başqa pul vahidləri ilə dəyişdirilə bilər. Bitcoin kompüter və ya smartfonlardan üçüncü bir maliyyə orqanı olmadan birbaşa köçürülə bilir. Bitcoin kriptoqrafik alqortimlərə əsaslanan elektron pul sistemidir. Bu elektron pul sistemi ənənəvi bank sistemi ilə oxşar funksiya və məqsədlərə sahib olsa da bir sıra cəhətlərə görə fərqlənir:

- Geri dönülməzlik – hər bir bitcoin əməliyyatı blockchain-ə daxil olduqdan sonra bu əməliyyatı geri qaytarmaq mümkün deyil.
- Təsdiqlənmə – ənənəvi bank əməliyyatları sistemindən fərqli olaraq, hər hansı bir BTC ölçülü bitcoin əməliyyatı tam təsdiqlənə bilər. Təsdiqlənmə yalnız rəqəmsal imza ilə həyata keçirilə bilər.
- Anonimlik – ənənəvi əməliyyat sistemi birdən çox əməliyyat üçün istifadəçinin həqiqi adını daşıyır. Bitcoin əməliyyatlarında isə istifadəçi istədiyi adla müxtəlif bitcoin ünvanlarına sahib ola bilər. İstifadəçinin gizliliyini qorumaq üçün, bitcoin əməliyyatları bir-biri ilə əlaqəli deyil.
- Əməliyyat haqqı: bitcoin əməliyyatı zamanı əməliyyat haqqı ənənəvi bank sistemləri ilə müqayisədə çox cuzi olur.
- Maliyyə azadlığı: Bitcoin tamamilə mərkəzləşdirilmiş olan ənənəvi bank sistemindən fərqli olaraq bitcoin şəbəkəsinin mərkəzləşdirilməməsi səbəbindən istifadəçilərə maliyyə vəziyyətinə görə azadlıq verir[4].

II. BITCOIN-İN YARADILMASI SXEMİ

Bitcoin şəbəkəsi P2P (“Peer-To-Peer”) şəbəkədir. Bu şəbəkəyə kompüter qovşaqları, mayner və istifadəçilər daxildirlər.

İstifadəçilər: Elektron ödəmə sisteminə qoşulan istifadəçilər nəzərdə tutulur. Bu istifadəçilər bitcoin şəbəkəsinin bir hissəsi olan digər istifadəçilərə bitcoin göndərə bilərlər və ya onlardan bitcoin qəbul edə bilərlər. Bu zaman tranzaksiyalar bitcoin kitabçasında qeyd olunur. İstifadəçi öz bitcoinləri ilə işləmək üçün açıq və gizli açara sahib olmalıdır.

Qovşaqlar: Bitcoin şəbəkəsini təşkil edən kompüterlərdir. Bu kompüterlərdə bitcoin kitabçasının son yenilənmiş forması, bloka daxil edilməyən problemli tranzaksiyaların və təsdiqlənməmiş tranzaksiyaların siyahısı saxlanır. Digər tərəfdən isə bu qovşaqlar digər kompüter qovşaqları, istifadəçi və maynerlərlə birləşərək əsas Bitcoin şəbəkəsini yaradır. Bu şəbəkədə qovşaqların əsas vəzifəsi tranzaksiya və bloklar

DOI: 10.25045/NCInfoSec.2017.26

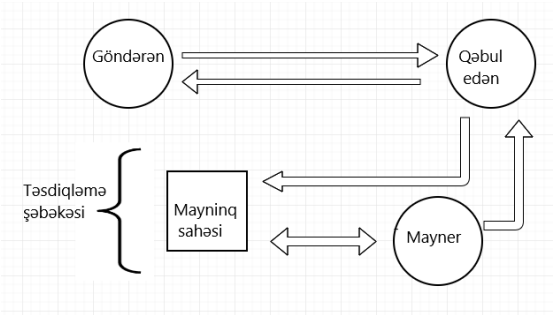
haqqında bütün məlumatların şəbəkədəki hər kəsə yəni,istifadəçi, mayner və qovşaqlara göndərilməsidir. Qovşaqlar istənilən istifadəçi tərəfindən quraşdırıla bilər. Hal-hazırda Bitcoin şəbəkəsində 11000–12000 arası qovşaq var. Bu qovşaqların 28%-nə yaxını ABŞ-dan qoşulan qovşaqlardır. Şəbəkəyə qoşulu olan bütün qovşaqlar hər blok və əməliyyatları yükləyir və Bitcoin əsas qaydalarına əsasən yoxlayır. [15]

Mayner: Maynerlərin məqsədi istifadəçilərin yaratdığı tranzaksiyaları bloklara yığmaqdır. Bitcoin qaydalarına əsasən ilk bloku yaradan mayner mükafat olaraq müəyyən miqdarda bitcoin qazanır. Bu şəxslər xüsusi güclü kompüterlər və proqram təminatından istifadə edirlər. Hər yeni bloku yaradan maynerin mükafatı hal-hazırda 12. 5 BTC-dir. 2009-cu ildə bu mükafat 50 BTC, 2012-ci ildə isə 25 BTC idi. [16]

P2P Bitcoin şəbəkəsi: P2P şəbəkəsi internet üzərində olan, Bitcoin protokoluna əsaslanan şəbəkədir. Bitcoin tranzaksiyaları heç bir qurumdan asılı olmadan P2P şəbəkəsi üzərində aparılır. Bu şəbəkədə bitcoini göndərən və qəbul edən şəxs bir-birləri ilə birbaşa üçüncü şəxs, qurum olmadan əlaqə saxlayır. P2P şəbəkəsində əlaqələr şifrələnmir, TCP kanalı üzərində işləyir. P2P şəbəkəsində həm də IPv4 və IPv6 dəstəklənir. Şəbəkə İnternetdən keçdiyi üçün tıxac və ya gecikmə problemlərinə məruz qalır [5].

III. BITCOIN TRANZAKSİYALARI

Bitcoin şəbəkəsində bitcoini göndərən istifadəçi bir başa qəbul edən istifadəçi ilə əlaqədə olur, onun bitcoin ünvanını daxil edərək bitcoinləri ona göndərir. Bu tranzaksiya mayninq sahəsinə daxil olur, mayner tərəfindən təsdiqləndikdən sonra bloka daxil edilir. Sonda SHA256 heş funksiyasından istifadə edilərək blok zəncirinə daxil edilir. Bitcoin sisteminin sxemi *şəkil 1*-dəki kimi təsvir edilə bilər:



Şəkil 1:Bitcoin sisteminin sxemi

SHA256 heş funksiyası. SHA-256 NSA tərəfindən hazırlanmış SHA-2 kriptoqrafik heş funksiyalarının üzvüdür. Kriptoqrafik heş funksiyaları rəqəmsal məlumatlar üzərində aparılan riyazi əməliyyatlardır. Hesablanan "heş" dəyər bilinən heş qiyməti ilə müqayisə edilərək məlumatların bütövlüyünü müəyyən etmək üçün istifadə oluna bilər. SHA256 funksiyası istənilən uzunluqda veriləni 32 baytlıq (256 bitlik) heş qiymətə çevirir. Funksiyanın nəticəsi 16-lıq sistemdə yazılır. Əgər veriləndə xırda dəyişiklik edilsə SHA256 heş funksiyasının qiyməti tamamilə dəyişər. Heş funskiyalar birtərəflidir. Hər hansı məlumatın heş dəyərini hesablamaq asandır,lakin heş dəyərdən məlumatı əldə etmək mümkün deyil. SHA-256 Bitcoin şəbəkəsinin müxtəlif hissələrində istifadə olunur:

- Mayninq prosesində blokların yaradılması üçün SHA-256 heş funsiyasından istifadə edir.
- Təhlükəsizlik və konfidensiallığı artırmaq üçün bitcoin ünvanlarının yaradılmasında SHA-256 heş funsiyasından istifadə olunur [7].

Rəqəmsal imza. İmzalama**.** Rəqəmsal imza açıq və gizli açarın birlikdə işlədiyi riyazi tərəfdən təhlükəsizliyi isbat olunmuş şifrələmə üsuludur. Rəqəmsal imzadan istifadə etmək istəyən şəxsin özünə aid gizli və açıq açarı olmalıdır. Rəqəmsal imza üsullarında şifrləmə üçün gizli açardan, deşifrləmə üçün isə açıq açardan istifadə olunur. Gizli açarla həyata keçirilən şifrələmə prosesi imzalama adlanır. Əvvəlcə məlumatın heş qiyməti hesablanır daha sonra isə imzalanır. Məlumatın heş qiymətinin alınması onun daha sürətli imzalanmasına və daha az yaddaş tutmasına səbəb olur.

Məlumat göndərən şəxs məlumatın imzalanmış heş qiymətini vəməlumatı qarşı tərəfə göndərir. Qarşı tərəf imzalanmış heşqiyməti açıq açar ilə deşifrəliyir və məlumatı SHA256 ilə heşləyir. Alınan nəticələr eynidirsə, o zaman imza təsdiqlənir.

Bitcoin ünvanı. Bitcoin ünvanı bank sistemlərindəki hesab nömrəsinə bənzədilir. Bu ünvan əsasən 26-35 ədəd hərf-rəqəm simvoldan ibarət olur və 1, yaxud 3 rəqəmləri ilə başlayır. Bitcoin ünvanları istənilən bitcoin istifadəçisi tərəfindən tamamilə ödənişsiz yaradıla bilər. Bitcoin ünvanı açıq açardan, açıq açar isə gizli açardan tək istiqamətli funksiya vasitəsi ilə yaradılır. Bitcoin ünvanından açıq açarı almaq mümkün olmadığı kimi gizli açarı da almaq mümkün deyil.

BitCoin e-pulqabısı.Bitcoin şəbəkəsində e-pulqabı deyildikdə istifadəçi fayl sistemində bir fayl nəzərdə tutulur. E-pulqabında açıq və gizli açar cütü və yerinə yetirilmiş tranzaksiyalar qeyd olunur. Açarlar bitcoinlərin qəbul olunması və göndərilməsi üçün istifadə olunur. Açıq açarı bitcoinləri qəbul edən şəxs imzalamanı təsdiqləmək üçün, gizli açarı isə bitcoinləri göndərən şəxs imzalamaq üçün istifadə edir. İstifadəçinin e-pulqabı faylları bitcoinlərin təhlükəsizliyini təmin etmək üçün şifrələnmişdir.

Üç növ bitcoin e-pulqabıları mövcuddur:

- Onlayn e-pulqabılar: İstifadəçinin sahib olduğu bütün bitcoinlər onlayn olaraq saxlanılır.
- Oflayn e-pulqabılar: İstifadəçinin sahib olduğu bütün bitcoinlər aparat təminatı olan oflayn e-pulqabılarda saxlanılır. E-pulqabılar fiziki qurğularda yerləşir.
- Onlayn-oflayn e-pulqabılar. Bu e-pulqabılar onlayn e-pulqabına oxşayır.Bitcoin istifadəçisinə aid olan bütün BTC-lər onlayn olaraq saxlanılır. Onlayn e-pulqabından fərqi odur ki, bu e-pulqabılarında əməliyyatlar üçün istifadə olunan imza saxlanmır. Əksinə imza şəbəkəyə qoşulmayan başqa bir cihazda saxlanılır. [6]

Bitcoin tranzaksiyaları**.** Bitcoin tranzaksiyaları bir bitcoin e-pul qabından digərinə bitcoinlərin göndərilməsidir. Bitcoin əməliyyatları şifrələnmir, bloklarda toplanır. Bu əməliyyatlar təsdiqləndiyi halda onlar geri qaytarıla bilmir. Fərz edək ki, birinci şəxs ikinci şəxsə bitcoin göndərir. Belə halda, Bitcoin göndərilmə əməliyyatı 3 yerə bölünür:

- Giriş: Birinci şəxsə bitcoinleri göndərən bitcoin ünvanı.

- Miqdar: göndərilən bitcoin miqdarı
- Çıxış:İkinci şəxsin bitcoin ünvanı

Bitcoin tranzaksiyasındakı giriş bir əvvəlki tranzaksiyadakı çıxışa istinad edir. Əksər hallarda bir tranzaksiyda birdən çox giriş və çıxış ola bilər. Bitcoin tranzaksiyalarının birləşmiş və paylanmış növləri vardır. Birləşmiş tranzaksiyalarda bir neçə giriş və bir çıxış olur. Paylanmış tranzaksiyalarda isə bir giriş və bir neçə çıxış olur. Tranzaksiyalarda giriş və çıxış miqdarı həmişə eyni olmur. Bitcoin tranzaksiyalarında daxil edilmiş bitcoinin miqdarı çıxışdakı bitcoin miqdarından az miqdarda yuxarı olur. Bu fərqi əməliyyatda iştirak edən mayner tərəfindən toplanan, kiçik bir ödəniş, kimi nəzərdə tutulan "əməliyyat haqqı" deməkdir.[8]

BitCoin Mayninq**.**Hər yeni blokun yaranma prosesi mayninq adlanır. Mayner əldə etdiyi qiymət hədəfdən kiçik olana qədər blok başlığının 256-bitlik heşini hesablayır. Hədəf bütün bitcoin istifadəçilərinin paylaşdığı 256 bitlik ədəddir. Hədəf kiçildikcə bloku yaratmağın çətinliyi artır. Bitcoin mayninq prosesində iştirak edən maynerlər üçün xüsusi aparat təminatları vardır. Bunlara CPU(Central processing unit)/GPU(Graphics processing unit), FPGA(Field Programmable Gate Array) , ASİC (Application Specific Integrated Circuits) qurğuları daxildir.[9]

CPU əvvəllər daha çox istifadə olunurdu. Maynerler fərdi şekildə mayninq ilə məşğul olmasına imkan yaradırdı. CPU-lar hal-hazırdada istifadə olunasa da bugünün standartlarına görə zəifdirlər. GPU isə mürəkkəb hesablamaları daha qısa müddətdə həyata keçirə bildiklərindən SHA256 heş funksiyasının hesablamalarında daha sürətlidirlər. GPU –lar CPU-lara nəzərən 50-100 dəfə sürətli olurlar GPU-lar əsasən bir qrup insanın mayninqlə məşğul olunmasında istifadə olunur. Buna misal olaraq ATI və Nvidia göstərmək olar.

FPGAperfromansı CPU və GPU dan üstündür. 1 FPGA çipi Megaheş/san sürətə malikdir.

ASIC xüsusi ilə bitcoin miningi üçün hazırlanmış cihazlardırlar. Çox böyük surətə malikdirlər. Əsasən 5-500 Gigaheş/san sürətlə heş funksiyaları həll edirlər. Elə ASİC lər var ki, 2 Teraheş/san sürətə malikdirlər.

IV. BITCOIN-IN TƏHLÜKƏSİZLİYİ

Bitcoin heç bir fiziki mövcudluğu olmayan tamamilə rəqəmsal valyutadır. Valyuta təhlükəsizliyi ilə bağlı məsələlər əvvəllər olduğu kimi hələ də müzakirə mərkəzindədir. Rəqəmsal valyutada tranzaksiya və mayninq proseslərində təhlükəsizliyi artırmaq üçün səylər göstərilsə də, virtual valyutanın qarşısında hələ də bəzi təhlükələr mövcuddur. Bitcoin-ə yönəlmiş əsas hücumlara aşağıdakılar aiddir:

- “Double-spending”hücumu;
- “Timejacking” hücumu;
- “Dust Transactions”hücumu;
- Kodyönümlü hücumlar.

“Double-spending” –İkiqat xərcləmə hücumları. Bitcoin tranzaksiyası şəbəkədə saniyələr içərisində yayılır lakin təsdiqlənməsi zaman tələb edir. Sahib olduğu bitcoinləri rəqəmsal olaraq imzalayaraq xərcləyən istifadəçinin başlatdığı tranzaksiya etibarlı tranzaksiya sayılır. Bitcoin ünvanına etibarlı bir ödəniş bir neçə saniyə ərzində şəbəkədəki bütün istifadəçilərinə görünə bilər, lakin bunun təsdiq olunacağına dair bir zəmanət yoxdur. Əməliyyatın təsdiq olunmasının gecikməsi səbəbindən ikiqat xərcləmə imkanı mövcuddur. Eyni bitcoinlərin bir dəfədən çox xərcləmə prosesi ikiqat xərcləmə adlanır. Əməliyyat başlamış və hələ təsdiq edilməmişsə eyni bitcoinlər alıcı və ya satıcı tərəfindən yenidən istifadə edilə bilər.

“Timejacking” hücumu**.** Hər bir qovşaq kompüterdə şəbəkə zamanı sayğacı olur**.** Bu qovşaq cütlüklərinin median zamanına əsaslanır. Əgər median zamanı 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.

Yeni blokları təsdiqləmək üçün şəbəkə vaxtından istifadə olunur. Blokun yaradılma vaxtı blok başlığında göstərilir. Əgər bir blokun yaranma vaxtı şəbəkə vaxtından 2 saat öndə olarsa, o zaman qovşaqlar onu rədd edir. Hücumçu zamanı həqiqi zamandan 190 dəq fərqlənən yeni blok yaradır. Mayner məntiqinə görə isə blokun yaranma zamanı şəbəkə sayğacından 120 dəq-dən çox keçməyibsə mayner bu bloku qəbul edəcəkdi. Nəticə olaraq timejacking hücumda hücumçu şəbəkə zaman sayğacını dəyişdirir və aldadılmış qovşaq bloku alternativ bir blok zəncirinə qəbul edə bilər. Bu ikiqat xərclənmə hücumuna və hesablama resurslarının israfına səbəb ola bilər[11].

“Dust Transactions”hücumu. Bu hücumda maliyyə dəyəri çox kiçik olan lakin blokzəncirinə daxil olan tranzaksiyalar həyata keçirilir. Bitcoinin ən kiçik vahidi satoşidir. Bir satoşi 0. 00000001 bitcoinə bərabərdir. Əvvəllər tranzaksiyalarda bir satoşi göndərmək mümkün idi. Hücumçu bundan istifadə edərək tranzaksiyalar kiçik maliyyə dəyərli tranzaksiyalar həyata keçirərək maynerləri, hesablama qurğularını boş yerə məşğul edir. Bitcoin kliyentinin yeni versiyasında tranzaksiyanın ən kiçik dəyəri 5.43 satoşi ola bilər. Bu da təqribən 0. 0003 dollara bərabərdir . 5.43 satoşi də kiçik miqdar hesab olunsa da “Dust Transactions” hücumunu müəyyən qədər çətinləşdirir. [12]

“Kodyönümlü**”** hücumlar**.** Bitcoin şəbəkəsi üçün mənbə kodu “Satoshi kliyent” olaraq bilinir. Bu kod açıq mənbəlidir və Github platformasında saxlanılır. Kodda bəzi tamamlanmamış hissələr vardır ki, bu hissələr bitcoinin gələcək xüsusiyyətləri üçün nəzərdə tutulmuşdur. Bu kod üzərində daimi olaraq proqramçılar işləyir. Kod açıq mənbəli olduğuna görə pis niyətli proqramçı, yəni hücumçu kodda dəyişiklər edə bilər, tamamlanmamış hissələri öz niyətinə uyğun tamamlaya bilər. [12] *Cədvəl 1*-də qeyd edilən hücumların hədəfləri təsvir edilmişdir.

CƏDVƏL 1:HÜCUMLAR VƏ HƏDƏFLƏRİ

Hücum	**Hədəf**
Double-spending	Tranzaksiya prosesi
Timejacking	Tranzaksiya prosesi, mayninq prosesi
Dust-Transactions	Tranzaksiya prosesi, mayninq prosesi
Kodyönümlü	Bitcoinin proqram kodu

Bitcoin e-pulqabısının təhlükəsizliyi**.** Bitcoin e-pulqabısı daxilində açıq və gizli açarı və bitcoin ünvanını saxlayan fayldır. Bu faylı ələ keçirən istənilən şəxs bitcoin balansını idarə edə bilər. Bu fayl fiziki təhlükəsizliyi aşmaqla hücumçular tərəfindən ələ keçirilə bilər. Lakin bir çox hallarda

şəbəkə üzərindən pis niyətli proqram təminatlarından istifadə etməklə bu faylı ələ keçirirlər.

Onlayn e-pulqabıları hücumlara qarşı daha zəifdirlər. Hücumçu bitcoin e-pulqabısını asanlıqa deşifrələyə bilər və bitcoinləri ələ keçirər. Mövcud kopyalama imkanları istifadəçiyə tranzaksiya fayllarının alınmasına və analiz edilməsinə imkan yaradır. Hücumçu istifadəçi kimliyini ələ keçirməklə bu faylları da ələ keçirə bilər. Onlayn e-pulqabılardan fərqli olaraq oflayn e-pulqabılar daha təhlükəsiz hesab olunur. Lakin oflayn bir bitcoin e-pulqabısı oğurlandıqda və ya itirildikdə bitcoinlər bərpa edilə bilməz. Bu ehtimal minimal və ya sıfırdır. Onlayn-oflayn bitcoin e-pulqabılarında isə imza oflayn olaraq hansısa qurğuda saxlanılır. Əgər oflayn imzanın saxlanıldığı cihaz və ya qurğu itsə və ya oğurlansa, bitcoinlərin təhlükəsizliyi sona çatır. İstifadəçi özünün bitcoin e-pulqabısının təhlükəsizliyini təmin etmək üçün bu qaydalara riayət etməlidir.

- E-pulqabını və ya smartfonu şifrələmək. Bu bitcoinləri oğrulardan qorunmağa kömək edir. Bu zaman seçilən parol güclü olmalı və unudulmamalıdır.
- E-pulqabının nüsxəsini almaq. Bitcoin e-pulqabısının nüsxəsini almaq şifrəli saxlanılan halda mobil telefondan və ya kompüterdən e-pulqabı oğurlanarsa e-pulqabını bərpa etməyə imkan yaradır.
- Oflayn e-pulqabından istifadə. Təhlükəsizliyi ən yüksək səviyyədə təmin edir. E-pulqabını şəbəkə ilə bağlı olmayan təhlükəsiz yerdə saxlamaq vacibdir. Nüsxələmə və şifrləmə əməliyyatı oflayn e-pulqabının təhlükəsizliyini artırır [13].

V. BITCOIN TEXNOLOGİYASINDA ANONİMLİK

Bitcoin tranzaksiyalarında anonimlik qorunsa da, anonimliyin təmin olunması əsas məsələlərdən deyil. Bitcoin şəbəkəsində baş verən hər bir bitcoin əməliyyatı, hansı bitcoin ünvanından hansı bitcoin ünvanına göndərilməsi bitcoin kitabçasında qeyd olunur və şəbəkədə olan hər kəs bütün bitcoin əməliyyatlarını görə bilir. Lakin bitcoin ünvanı bitcoinin mənsub olduğu şəxs haqqında heç bir məlumat vermir. Buna baxmayaraq, əgər hər hansı bitcoin ünvanı istifadəçinin həqiqi məlumatları ilə əlaqələdirsə, o zaman bu bitcoin ünvanının kimə mənsub olduğunu tapmaq mümkündür. Əgər hücumçu bitcoin ünvanının həqiqi sahibi haqqında məlumat əldə edə bilirsə, o zaman bitcoin şəbəkəsində istifadəçi anonimliyinin tam təmin olunmadığını qeyd etmək mümkündür [14]

Bitcoin şəbəkəsində bütün əməliyyatlar ictimaiyyətə açıq olur. Əməliyyatı yerinə yetirən şəxsin anonimliyi onun əsl şəxsiyyəti ilə əlaqəsi olmayan yalançı addan istifadə etməsinə əsaslanır. Belə nəticəyə gəlmək olar ki, bitcoin şəbəkəsində istifadə olunan mövcud metod anonimliyi tam təmin etmir.

NƏTİCƏ

Min illər boyunca istifadə edilən pullarla müqayisədə Bitcoin olduqca yenidir. Onun gətirdiyi texnologiyalar isə olduqca perspektivli və inkişafa açıqdır. Bitcoindən sonra çoxlu rəqəmsal valyuta istifadə olunsa da, ən geniş yayılan rəqəmsal valyuta Bitcoindir. Bitcoin ilə edilən xərcləmələrə banklar, səlahiyyətli qurumlar və hökumətlər əməliyyat xərcləri və məhdudiyyətlər qoya bilmir. Bitcoin fərdlər üçün maliyyə azadlığı təmin edir. Bitcoinin ənənəvi ödəniş vasitəsi, pul və ya rəqəmsal pul istifadə edilməsi gün keçdikcə artmaqdadır.

Kriptovalyuta sistemlərində bir sıra aktual problemləri də mövcuddur. Bitcoin istifadəçi gizli açarını itdiyi vəziyyətində mülkiyyət hüququnu da itirmiş olur. Bununla yanaşı, bitcoin istifadəçisinin anonimliyin tam şəkildə təmin olunmur.

Kriptovalyutanın mərkəzi olmadığı üçün hər hansı ödəmə geri alına bilməz. Əgər istifadəçi səhvən ödəmə həyata keçirmişdirsə, bu ödəməni geri qaytara bilməz.

Bitcoin-in təhlükəsizliyi çox güclü hesab olunsa da, hal-hazırda bir çox hücumlara qarşı həssaslığı davam edir. Hücum edənlər Bitcoin müştərilərindən e-pulqabılarını bədniyətli proqram təminatı ilə ələ keçirə bilirlər.

ƏDƏBİYYAT

[1] Vyas C. A., Munindra L. Security Concerns and Issues for Bitcoin.“National Conference cum Workshop on Bioinformatics and Computational Biology”, 2014, pp. 10–12.

[2] S. Nakamoto. (2008). “Bitcoin: A peer-to-peer electronic cash system” https://bitcoin.org/bitcoin.pdf

[3] Baumann A., Fabian B., Lischke M. Exploring the Bitcoin Network.“InternationalConferenceonWebInformationSystemsandTechnologies”, 2014, pp. 369–374

[4] Dikshit P. , Kunwar S. “Efficient weighted threshold ECDSA for securing bitcoin wallet” Asia Security and Privacy (ISEASP), 2017.

[5] Senmarti R. E. “Analysis of Reward Strategy and Transaction Selection in Bitcoin Block Generation”. PhD diss. , 2015

[6] Tiwari K. “Secure Digital Wallet Authentication Protocol”, Dalhousie University, diss. 2017.

[7] https://en. bitcoin. it/wiki/SHA-256

[8] Andreas M. A. Mastering Bitcoin, O’Reilly, 2014. pp 18

[9] Gervais A. , Ghassan O. “Is Bitcoin a decentralized currency?” IEEE security & privacy 12. 3, 2014, pp. 54–60.

[10] Vyas C. A. , Munindra L. Security Concerns and Issues for Bitcoin. / “National Conference cum Workshop on Bioinformatics and Computational Biology”, 2014, pp. 10–12.

[11] “Timejacking & Bitcoin.” May 2011. http://culubas.blogspot.co.uk/ 2011/05/timejacking-bitcoin_802.html.

[12] Bradbury D. “The problem with Bitcoin.”Computer Fraud & Security2013. 11, 2013,pp 5-8

[13] "Secure your wallet" - https://bitcoin. org/en/secureyour-wallet

[14] https://en.bitcoin.it/wiki/Anonymity

[15] https://bitnodes.earn.com/

[16] https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/

SCIENTIFIC-THEORETICAL AND PRACTICAL PROBLEMS OF BITCOIN TECHNOLOGY

Nilufar Hatamova
Institute of Information Technology of ANAS, Baku, Azerbaijan.
hatamovanilufar@gmail.com

Abstract – Bitcoin is an electronic monetary system, where transactions are carried out without a third party . The Bitcoins network is not dependent on the central organization .Bitcoin is based on an open cryptographic protocol. The Bitcoin network is distributed between a computer connected to the network. Bitcoin allows you to pay through a computer or smartphone without financial organizations. In this article, we analyzed the scientific-theoretical and practical issues in the Bitcoin network, attacks on the Bitcoin network, security and anonymity issues in the Bitcoin e-wallet .

Keywords – Bitcoin, Cryptocurrency, P2P Bitcoin Network, Blockchain, SHA256