AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

YÜKSƏK TƏHSİL İNSTİTUTU

Günel Seyidəhmədli Fərman qızı

Zəhra Rəhimli Elşən qızı

Coşqun Salahov Səlahəddin oğlu

“Zk-STARK SIFIR BİLİKLƏ İSBAT SXEMİNİN TƏDQİQİ”

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631 – “Kompüter mühəndisliyi”

İxtisaslaşma : “Kompüter təhlükəsizliyi”

Elmi rəhbər: Məhəmməd Aydın oğlu Hüseynli

BAKI-2024

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ
YÜKSƏK TƏHSİL İNSTİTUTU

MAGİSTRANTIN ANDI

zk-STARK sıfır biliklə isbat sxeminin tədqiqi mövzusunda təqdim etdiyimiz magistrlik dissertasiyasını elmi əxlaq normalarına və istinad qaydalarına tam riayət etməklə və istifadə etdiyimiz bütün mənbələri ədəbiyyat siyahısında əks etdirməklə yazdığıma and içirik və magistrlik dissertasiyasının AzTU Kitabxana İnformasiya Mərkəzində saxlanılması, həmin mərkəz tərəfindən AzTU Rəqəmsal Repozitoriyasına daxil edilərək repozitoriyanın veb saytında yerləşdirilməsinə icazə veririk.

Günel Seyidəhmədli	
(Adı, Soyadı)	(imza)
Zəhra Rəhimli	
(Adı, Soyadı)	(imza)
Coşqun Salahov	
(Adı, Soyadı)	(imza)

Tarix

MÜNDƏRİCAT

İXTİSARLARIN SİYAHISI

- AES: Advanced Encryption Standard — Təkmil Şifrələmə Standartı
- CRS: Common Reference Strings — Ümumi İstinad Sətirləri
- DECO: Distributed Evolutionary Computing — Paylanmış Təkamül Hesablamaları
- ECC: Elliptic Curve Cryptography — Elliptik Əyri Kriptoqrafiya
- FFT: Fast Fourier Transform — Sürətli Furye Çevrilməsi
- HTTPS: Secure Hyper Text Transfer Protocol — Təhlükəsiz Hiper Mətn Transfer Protokolu
- İOP: Interactive Oracle Proof — İnteraktiv Oracle İsbatı
- TLS: Transport Layer Security — Nəqliyyat Layerinin Təhlükəsizliyi
- ZKP: Zero-Knowledge Proof — Sıfır Bilik İsbatı
- zk-SNARK: Zero-Knowledge Succinct Non-interactive Argument of Knowledge — Sıfır Bilik Qısa Qeyri-interaktiv Bilik Arqument
- zk-STARK: Zero-Knowledge Scalable Transparent Arguments of Knowledge — Sıfır Bilik Ölçəklənən Biliyin şəffaf arqumentləri
-

GİRİŞ

Mövzunun aktuallığı: Rəqəmsal məlumatların həyatın müxtəlif aspektlərində əsas rol oynadığı bir dünyada onların məxfiliyinin və bütövlüyünün təmin edilməsi son dərəcə vacib olmuşdur. Bu kontekstdə zk-STARK (Zero-Knowledge Scalable Transparent Arguments of Knowledge) üzrə sıfır bilik isbat sxemi üzrə tədqiqatlar informasiya təhlükəsizliyinin həm elmi, həm də praktiki aspektlərində artan diqqəti cəlb etmişdir.

Sıfır bilik isbatının əsas məntiqi həssas məlumatları aşkar etmədən ifadələri isbat etmək və ya əməliyyatlar aparmaq bacarığıdır. Bu məntiq şəbəkədə məlumatı qorumaq üçün nəzərdə tutulmuş bir çox kriptoqrafik protokol və alqoritmlərin əsasını təşkil edir.

İnformasiya təhlükəsizliyində həmin sxemin rolunu qiymətləndirməmək olmaz. O, məlumatların sızması və ya icazəsiz giriş riskini minimuma endirərək, məlumatların yüksək səviyyədə qorunmasını təmin edir. Bu, maliyyə və səhiyyə sənayesi, hökumət və kommersiya təşkilatları kimi məxfiliyin kritik olduğu sahələrdə xüsusilə vacibdir.

Bu isbat sxemi blokçeyn, kibertəhlükəsizlik və məxfi hesablama daxil olmaqla müxtəlif sahələrdə tətbiqləri olan təhlükəsiz və səmərəli kriptoqrafik protokolların yaradılması üçün əsasdır.

zk-STARK riyazi təsnifatı bu dövrənin müxtəlif aspektlərini və xassələrini başa düşmək üçün mühüm vasitədir. Bu, tədqiqatçılara və tərtibatçılara xüsusi problemlər və tətbiqlər üçün ən uyğun yanaşma və metodları seçməyə imkan verir.

Tədqiqatın məqsəd və vəzifələri: Bu tədqiqatın məqsədi zk-STARK sıfır bilik isbatı sxemini və onun informasiya təhlükəsizliyindəki rolunu, xüsusən kriptovalyutalar və blokçeyn texnologiyası kontekstində dərindən təhlil etmək və anlamaqdır. Bu məqsədə nail olmaq üçün bu mövzunun müxtəlif aspektlərini müəyyən etdik, o cümlədən:

- zk-STARK-ın əsas prinsiplərini;
- zk-STARK-ın riyazi təsnifatını və praktikada tətbiqini;

- Həmçinin başqa bir ümumi sıfır bilik isbat sxemi - zk- ilə müqayisəli təhlili;

- İnformasiya təhlükəsizliyində sıfır bilik isbatının rolunun müəyyən edilməsi;

- Azərbaycan Respublikasının bank və sığorta sektorunda risklərin idarə edilməsi;

- zk-STARK-ın məlumatların məxfiliyini və bütövlüyünü, eləcə də maliyyə sektoru və hökumət də daxil olmaqla müxtəlif sahələrdə tətbiqinin üstünlükləri və məhdudiyyətlərini təmin edilməsi istiqamətlərinin öyrənilməsi,

- Fərqlərin və çatışmazlıqlarını müəyyən etmək üçün zk-STARK və zk-SNARK-ın müqayisəli tədqiqi aparılması.

Tədqiqatın obyekti və predmeti: Tədqiqat işinin obyekti zk-STARK sıfır bilik isbat sxemidir, predmetini isə Onun əsas məntiqi və fəaliyyət mərhələləri, informasiya təhlükəsizliyinin təmin edilməsində rolu, kriptovalyutada əhəmiyyəti, həmçinin blokçeyn texnologiyası ssenarilərində tətbiqi araşdırılması təşkil edir.

Tədqiqat metodları: Tədqiqat metodlarına zk-STARK üzrə mövcud məlumatların və ədəbiyyatın təhlili, digər isbat sxemləri ilə müqayisəli təhlillərin aparılması və zk-STARK-ın iş prinsiplərini və effektivliyini öyrənmək üçün riyazi modelləşdirmə daxil ola bilər.

Tədqiqatın informasiya bazası: Dissertasiya işinin yazılmasında müxtəlif resurslardan istifadə edilir. Tədqiqat geniş informasiya bazasına, o cümlədən akademik məqalələrə, elmi nəşrlərə, kriptoqrafiya və informasiya təhlükəsizliyinə dair kitablara əsaslanacaq. Konfrans materialları, onlayn resurslar və zk-STARK və əlaqəli mövzular üzrə rəsmi sənədlərdən də istifadə olunacaq.

Tədqiqatın mədudiyyətləri: Tədqiqatın əsas məhdudiyyətlərindən biri mövzunun nisbi yeniliyi və mürəkkəbliyidir. zk-STARK-ın bəzi aspektləri ədəbiyyatda zəif əhatə oluna bilər və onun praktikada, xüsusən də blokçeyn texnologiyası kontekstində tətbiqi ilə bağlı məlumat çatışmazlığı var.

Tədqiqatın elmi yeniliyi: zk-STARK sxeminin tədqiqi elmi yeniliyi təmsil edir, çünki o, müasir informasiya təhlükəsizliyi metodlarına müraciət edir və kriptoqrafik protokollar haqqında anlayışı inkişaf etdirir.

Nəticələrin praktiki əhəmiyyəti və tətbiq sahələri: zk-STARK tədqiqatı informasiya təhlükəsizliyi və kriptoqrafiya sahəsində yüksək praktiki əhəmiyyətə malikdir. Onun nəticələri maliyyə texnologiyaları, blokçeyn, kibertəhlükəsizlik və məlumatların qorunması kimi müxtəlif sahələrdə tətbiq oluna bilər.

İşin aprobasiyası. Tədqiqat işinin nəticələri Ümumilli lider Heydər Əliyevin anadan olmasının 101-ci ildönümünə həsr olunmuş tələbə və gənc tədqiqatçıların "Mütərəqqi texnologiyalar və innovasiyalar" mövzusunda IX Respublika elmi-texniki konfransında qrup üzvləri Günel Seyidəhmədli, Zəhra Rəhimli, Coşqun Salahov tərəfindən "ZK-STARK TRANZAKSİYALARIN ŞİFRƏLƏNMƏSİ ÜÇÜN TƏDQİQ METODLARI" adlı məqaləsində müzakirə edilmişdir.

İddiaçıların töhvələri. Zəhra Rəhimli tərəfindən 1-ci fəsildə "Sıfır bilik protokolları: "Məlumatların məxfiliyinin və təhlükəsizliyinin qorunması" araşdırılaraq analiz edilmişdir.

2-ci fəsildə Günel Seyidəhmədli tərərfindən "Tranzaksiyalar zamanı istifadə edilən riyazi metodlar və şifrələmələr" araşdırılıb analiz edilmişdir.

3-cü fəsildə Coşqun Salahov tərəfindən "zk-STARK ilə digər sıfır bilik isbat protokollarının müqaisəli analizini" təhlil etmişdir. "zk-STARK protokolunun kriptovalyutadakı rolu" araşdırılıb analiz edilmişdir.

Dissertasiyanın strukturu və həcmi. Dissertasiya işi giriş, 3 fəsil, nəticə, ədəbiyyat siyahısı, istinad edilən mənbələrdən ibarətdir. İşin ümumi həcmi 74 səhifədən, 8 şəkildən və 1 cədvəldən ibarətdir. İşdə 28 adda ədəbiyyata istinad olunmuşdur.

Dissertasiya işinin "Sıfır bilik protokolları: Məlumatların məxfiliyinin və təhlükəsizliyinin qorunması" adlanan 1-ci fəsilində sıfır bilik isbatının əsas məntiqi, əsas mərhələləri, informasiya təhlükəsizliyində rolu və sıfır bilik isbatında zk-STARK ın əhəmiyyətinə baxılmışdır. "zk-STARK ın riyazi əsasları, tətbiqi tranzaksiya şifrələmə texnikaları və əsas blokçeyn konsepsiyaları" adlı 2 –ci fəsildə zk-STARK ın riyazi əsaslarına, şifrələnmə üçün tətbiq metodlarına və blokçeyn və zk-STARK ın əsas konseptləri tədqiq edilmişdir. "Sıfır bilik isbatının senari mexanizminin təhlili" adlı 3-cü fəsildə zk-STARK zk-SNARK la müqaisə edilərək

təhlili aparılıb. Kriptovalyuta ilə ödəniş zamanı əməliyyatları gizli saxlanılaraq təhlükəsiz əməliyyatlar həyata keçrilməsi ssenari üzərində tədqiq edilmişdir.

I FƏSİL "SIFIR BİLİK PROTOKOLLARI: MƏLUMATLARIN MƏXFİLİYİNİN VƏ TƏHLÜKƏSİZLİYİNİN QORUNMASI"

1.1. Sıfır bilik isbatının əsas məntiqi

Sıfır bilik isbat ilk dəfə 1985-ci ildə "İnteraktiv isbat sistemlərində bilik mürəkkəbliyi" adlı məqalədə təsvir edilmişdir. Bu gün hələ də geniş istifadə olunan sıfır bilik protokolunun tərifini ehtiva edir.

Zaman keçdikcə sıfır bilik isbatları daha da təkmilləşdi və indi bir neçə praktik tətbiqi var. İnformasiya təhlükəsizliyi və kriptoqrafiya dünyasında sirlərin açılmasına ehtiyac olmadan tərəflər arasında məlumat ötürülməsi zamanı məlumatların məxfiliyinin təmin edilməsində sıfır bilik isbatları əsas rol oynayır. Ən yenilikçi və perspektivli sıfır bilik isbat sxemlərindən biri zk-STARK-dır.

Əsas məntiqi riyazi prinsiplərə əsaslanır ki, bu da faktı konkret məlumat və ya faktla bağlı məlumatı açıqlamadan qəti şəkildə isbat etməyə imkan verir. Bu məntiq yüksək səviyyəli təhlükəsizlik və məxfilik təmin edərək, zk-STARK-ı fintech, blokçeyn və kibertəhlükəsizlik kimi müxtəlif sahələrdə istifadə üçün cəlbedici alətə çevirir (Bai, Hu, He, Fan, & An, 2022).

Sıfır bilik isbatları fərdlər üçün informasiya təhlükəsizliyini təkmilləşdirməyi vəd edən tətbiqi kriptoqrafiyada bir yenilikdir. Gəlin, məsələn, vətəndaşlığınızla bağlı digər tərəfə, məsələn, xidmət provayderinə iddianı necə isbat edə biləcəyinizi nəzərdən keçirək. Bunun üçün pasport və ya sürücülük vəsiqəsi kimi "isbat" təqdim etməlisiniz.

Lakin bu yanaşma problemlərlə üzləşir, ən başlıcası məxfi məlumatların sızmasıdır. Üçüncü tərəf xidmətləri ilə paylaşılan şəxsiyyəti müəyyənləşdirən məlumatlar (PII) haker hücumlarına məruz qalan mərkəzləşdirilmiş verilənlər

bazalarında saxlanılır. Şəxsiyyət oğurluğu təhlükəsi ilə məxfi məlumat mübadiləsi zamanı daha effektiv təhlükəsizlik tədbirlərinə ehtiyac var.

Bu sxem bir ifadənin etibarlılığını isbat etmək üçün məlumatların açıqlanması ehtiyacını aradan qaldıraraq bu problemi həll edir. Sıfır bilikli isbat protokolu onun doğruluğunun qısa isbatını yaratmaq üçün giriş kimi ifadədən ("şahid" adlanır) istifadə edir. Bu isbat, onu yaratmaq üçün istifadə olunan məlumatları açıqlamadan ifadənin doğru olduğuna etibarlı şəkildə zəmanət verir.

Vətəndaşlıq nümunəsinə qayıdaraq, bu iddianı isbat etmək üçün lazım olan yeganə sübut sıfır bilik sübutudur (Bai, Hu, He, Fan, & An, 2022). Doğrulayıcı yalnız əsas iddianın doğruluğunu təmin etmək üçün isbatın müəyyən xüsusiyyətlərinin doğru olub olmadığını yoxlamalıdır.

Bilik isbatı məzmununu və ya məlumat mənbəyini açıqlamadan ifadənin düzgünlüyünü isbat etmək imkanı verir. Bu üsul daxil olan və doğru və ya yalanı qaytaran alqoritmlərə əsaslanır.

Sıfır bilik isbatı protokolu müəyyən meyarlara cavab verməlidir:

1. **Tamlıq:** Əgər daxiletmə düzgündürsə, protokol həmişə doğrunu qaytarmalıdır. Bu, şərtlər yerinə yetirildiyi təqdirdə sübutin qəbul edilməsini təmin edir.

2. **Etibarlılıq:** Protokol daxil edilmiş məlumatlar səhv olduqda "doğru"nu qaytarmaqla aldatmağa imkan verməməlidir. Bu, fırıldaqçılıqdan qorunma təmin edir.

3. **Sıfır Bilik:** Təsdiqləyici bəyanatın məzmunu haqqında onun həqiqət və ya yalan olmasından başqa heç bir məlumat almamalıdır. Bu, məlumatların məxfiliyinə zəmanət verir.

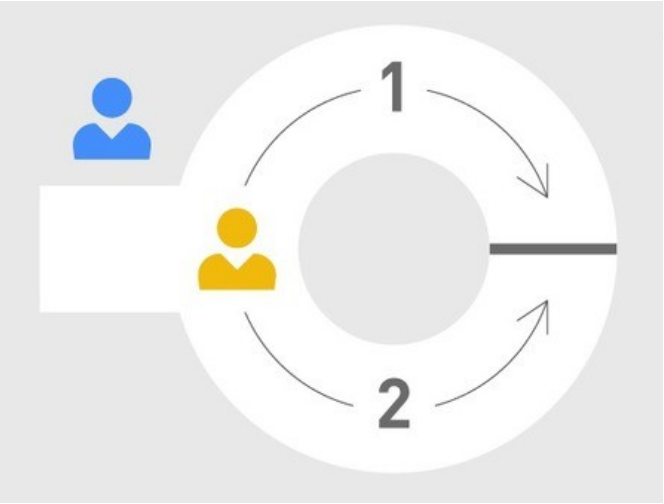
Qeyri-interaktiv sıfır bilik isbatları, hər iki tərəfin dəfələrlə qarşılıqlı əlaqədə olması lazım olan interaktiv isbatların məhdudiyyətlərinə cavabdır. Yeni üsul isbat edən və yoxlayan arasında ümumi açar təklif edir və məlumatın məzmununu açıqlamadan onun biliklərini isbat etməyə imkan verir. Bu, əlaqəni bir dövrəyə endirərək prosesi daha səmərəli edir. Qeyri-interaktiv isbatlar nəticələrin müstəqil yoxlama üçün əlçatan olmasını təmin edir, müasir sıfır bilik isbat sistemlərinin inkişafını asanlaşdırır.

ZKP (Zero-Knowledge Proof) üstünlüyü, həssas məlumatların Ethereum kimi ictimai blokçeynlər kimi şəffaf şəbəkələrdə istifadə oluna bilməsidir. Blokçeyn-in şəffaflığına baxmayaraq, ZKP istifadəçilərə və şirkətlərə ağıllı müqavilələrlə işləyərkən şəxsi məlumatları aşkar etmədən istifadə etməyə imkan verir.

Blokçeyn şəbəkələrində məxfiliyin qorunması ağıllı müqavilələrdən istifadə etmək istəyən, lakin ticarət sirlərini qorumalı olan təchizat zənciri şirkətləri, müəssisələr və banklar üçün vacibdir. Bu təşkilatlardan həmçinin GDPR və HIPAA kimi məlumatların qorunması qanunlarına riayət etmək tələb olunur.

1990-cı ildə kriptoqraf Jean-Jacques Quisquater (həmkarları ilə birlikdə) "Uşaqlara sıfır bilik protokollarını necə izah etmək olar" adlı məqalə dərc etdi. Bu məqalədə Əlibabanın mağarası məsəli ilə ZKP anlayışı təqdim edilmişdir (Lin & Liao, 2017).

Gəlin bir girişi və iki yan yolu ayıran sehrli qapısı olan dairəvi bir mağara təsəvvür edək. Bu sehrli qapıdan keçmək üçün düzgün gizli sözləri pıçıldamalısınız. Beləliklə, təsəvvür edin ki, Alis (o sarıdır) Boba (o mavidir) gizli sözləri bildiyini isbat etmək istəyir, lakin onları açmaq istəmir. Bunun üçün Bob mağaraya girərkən çöldə gözləməyə razılaşır və iki mümkün yoldan birini seçir. Bu nümunədə o, ilk yolu tutmağa qərar verir.(Şəkil1.1)

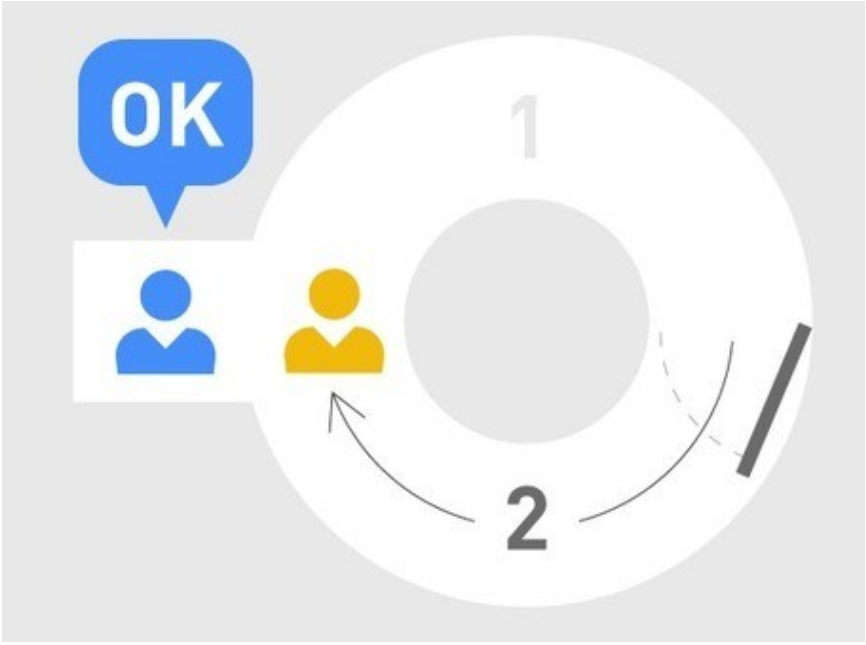


Şəkil 1.1: İki mümkün yoldan birini seçilməsi

Bir müddət sonra Bob girişin yanından keçir və Alisin hansı tərəfdən çıxmasını istədiyini bildirərək yüksək səslə qışqırır (bu halda 2-ci yol).(Şəkil 1.2)

Şəkil 1.2: Alis şifrəli qapıdan kecir.

Əgər Alisdə həqiqətən də sirr varsa, o, mütləq Bobun seçdiyi yola düşəcək. (Şəkil 1.3)



Şəkil 1.3: Alis başlanğıc nöqtəyə qayıdır.

Alisin seçiminin təsadüfi olmaması üçün bütün proses bir neçə dəfə təkrarlana bilər. Əlibaba və Mağara məsəli zk-STARK protokollarının bir hissəsi olan sıfır bilikli isbatlar anlayışını göstərir. ZKP, bu barədə məlumatı açıqlamadan müəyyən biliklərə sahib olduğunu isbat edə bilər.

Şəxsi blokçeynlərlə paralel olaraq, ZKP qurumlara məlumatlarına nəzarəti davam etdirərkən ictimai blokçeynlərlə təhlükəsiz qarşılıqlı əlaqədə olmağa imkan verir. Bu, innovasiyaları stimullaşdırmaq və qlobal iqtisadiyyatın inkişafına töhfə verməklə ictimai blokçeynlərdən istifadə üçün yeni imkanlar açır.

Zcash kimi ZKP həlləri blokçeyn sistemlərində pul məbləği, göndərən və alıcı ünvanları haqqında təfərrüatları gizlətməklə əməliyyat məxfiliyini təmin etmək üçün istifadə olunur. Mərkəzləşdirilməmiş oracle şəbəkələri məlumatların özünü aşkar etmədən zəncirdən kənar məlumatlar haqqında faktları yoxlamaq üçün ZKP-dən də istifadə edə bilər.

Hazırda inkişaf mərhələsində olan DECO (Distributed Evolutionary Computing) oracle protokolu zəncirdən kənar mənbələrdən ötürülən zaman məlumatların məxfiliyini təmin etmək üçün ZKP-dən istifadə edir. HTTPS (Secure Hyper Text Transfer Protocol)/TLS(Transport Layer Security) funksionallığını genişləndirməklə DECO sizə məlumatların məzmununu açıqlamadan təhlükəsiz şəkildə ötürməyə imkan verir. Bu protokol TLS-in müasir versiyaları ilə birlikdə işləyir və server tərəfində dəyişikliklər tələb etmir.

DECO kimi ZKP texnologiyası ağıllı müqavilələrin imkanlarını genişləndirir, məsələn, təminatlı kreditlərin verilməsində, burada borcalanlar həssas məlumatları açıqlamadan kredit qabiliyyətini isbat edə bilərlər. O, həmçinin istifadəçilərə öz etimadnamələrinə nəzarət etməyə imkan verən mərkəzləşdirilməmiş şəxsiyyət protokollarının yaradılmasını dəstəkləyir.

DECO kimi ZKP həlləri, həmçinin məlumat təminatçılarına məlumatların özü əvəzinə, yalnız məlumatlar haqqında faktları isbat edən sertifikatlar təqdim etməklə, öz məlumat dəstlərini şəxsi şəkildə pul qazanmağa imkan verir. Bu, məlumat provayderləri üçün yeni bazarlar yaradır, mənfəəti artırır və məlumat sızmasının qarşısını alır.

Blokçeyn-in şəffaflığını ZKP-nin məxfiliyi ilə birləşdirmək müəssisələrə məxfiliyini qoruyarkən məlumatlarını ağıllı müqavilələrdə istifadə etməyə imkan verir.

1.2. Sıfır bilik isbat sxeminin əsas mərhələləri

zk-STARK kimi sıfır bilik isbat sxemini araşdırarkən, sxemin əsas addımlarını başa düşmək vacibdir. Onlar isbat zamanı hərəkətlərin qaydasını və tərəflər arasında qarşılıqlı əlaqə prosesini müəyyən edirlər. Belə bir sxemin əsas mərhələlərini təhlil edək. (Şəkil 1.4)

Şəkil 1.4: ZKP sxeminin əsas mərhələləri

➢ **İnsiallaşdırma:** Bu mərhələ isbatın özü başlamazdan əvvəl hazırlıq işlərini əhatə edir. Bu mərhələdə isbat edən və yoxlayıcı protokolun parametrləri barədə razılığa gələ, lazımi ilkin məlumatları mübadilə edə və isbatı həyata keçirməyə hazır olduqlarına əmin ola bilər.

Sıfır bilik isbatı sxemində başlanğıc mərhələsi bütün prosesin uğurlu icrasını təyin edən əsas addımlardan biridir. Bu mərhələdə, ilkin parametrlərin təyin edilməsi və bütün lazımi məlumatların və dəyişənlərin işə salınması daxil olmaqla, isbatın özü üçün hazırlıqlar aparılır. Başlanğıc mərhələsində ilk addım isbat ediləcək ifadəni və onunla əlaqəli parametrləri və dəyişənləri müəyyən etməkdir. Bu, isbatda istifadə olunacaq məlumatların, habelə isbatın özünün məqsəd və tələblərinin müəyyən edilməsini əhatə edə bilər. Sonra isbat sxeminin ilkin şərtlərinin və parametrlərinin quraşdırılması gəlir. Buraya kriptoqrafik alqoritmlərin seçimi, təsadüfi ədədlərin yaradılması və isbatın təhlükəsizliyini və səmərəliliyini təmin etmək üçün zəruri olan digər parametrlər daxildir.

Bundan sonra, isbat prosesində istifadə olunacaq bütün lazımi məlumat strukturları və dəyişənlər işə salınır (Sun, Yu, Zhang, Sun, Xie, & Peng, 2021). Buraya Mark ağaclarının, heş cədvəllərinin, siyahılarının və isbat zamanı məlumatı saxlamaq və emal etmək üçün istifadə ediləcək digər məlumat strukturlarının

yaradılması daxil ola bilər. İşə salma mərhələsinə onların düzgün işləməsini və müəyyən edilmiş tələblərə cavab verməsini təmin etmək üçün isbat dövrəsinin bütün komponentlərinin ilkin yoxlamaları və sınaqları daxil ola bilər. Bu, faktiki isbat başlamazdan əvvəl hər hansı səhvləri və ya uyğunsuzluqları müəyyən etməyə və düzəltməyə imkan verir.

Qeyd etmək vacibdir ki, bütün parametrlərin və məlumatların düzgün işə salınması bütün sıfır biliklərin isbatı prosesinin uğurlu icrası üçün ilkin şərtdir. Qeyri-kafi və ya yanlış inisializasiya isbatın səhvlərinə və ya uğursuzluğuna səbəb ola bilər ki, bu da onun etibarlılığına və nəticəsinə mənfi təsir göstərə bilər.

Beləliklə, başlatma mərhələsi bütün lazımi parametrlərin və məlumatların düzgün şəkildə hazırlanmasını və prosesin uğurla başa çatması üçün qurulmasını təmin etməklə sıfır bilik isbatı prosesində mühüm rol oynayır.

- **İsbat generasiyası:** Bu mərhələ prosesin əsas hissəsini təmsil edir. Prover heç bir məxfi məlumatı üzə çıxarmadan bəyan edilmiş iddianın doğruluğunu isbat edən isbat yaratmaq üçün giriş məlumatlarından və xüsusi alqoritmdən istifadə edir. zk-STARK vəziyyətində bu, isbat yaratmaq üçün istifadə olunan çoxsaylı ölçü və tənliklərin yaradılması və sınaqdan keçirilməsini əhatə edə bilər.

İsbat yaratma mərhələsində ilk addım isbat edilməli olan isbat və ya məlumatları hazırlamaqdır. Bu, mətn məlumatları, rəqəmli dəyərlər, hesablama nəticələri və s. daxil olmaqla müxtəlif növ məlumat ola bilər. Bu məlumatın emal oluna və isbat kimi istifadə oluna bilən formatda təqdim edilməsi vacibdir.

Sonra sıfır bilik isbatı yaratmaq üçün uyğun kriptoqrafik protokol və ya alqoritmin seçilməsi gəlir. Bu məqsədlə istifadə edilə bilən bir neçə müxtəlif üsullar, o cümlədən homomorf şifrələrə əsaslanan alqoritmlər, Edvards əyriləri və s. (Abdolmaleki, Baghery, Lipmaa, & Zajac, 2019).

Protokol və ya alqoritm seçildikdən sonra isbatın yaradılması prosesi başlayır. Bu, xam məlumatların kriptoqrafik hesablamalarda istifadə edilə bilən formata çevrilməsini, həmçinin isbat yaratmaq üçün müvafiq riyazi əməliyyatların tətbiqini nəzərdə tutur.

İsbat yaratma prosesində əsas addımlardan biri isbat edənin təqdim edilmiş isbat və ya məlumat əsasında kriptoqrafik hesablamalar aparmasıdır. Bu, seçilmiş protokoldan asılı olaraq şifrələmə, hashing, mesajın imzalanması və s. kimi müxtəlif əməliyyatların yerinə yetirilməsini əhatə edir.

Hesablamalar tamamlandıqdan sonra yekun isbat yaradılır və yoxlayıcıya təqdim olunur. Bu isbat adətən açıq alqoritmlər və metodlardan istifadə etməklə yoxlanıla bilən riyazi düsturlar və ya kriptoqrafik imzalar şəklində olur.

Qeyd etmək vacibdir ki, isbat yaratmaq dəqiqlik və təfərrüata diqqət yetirməyi tələb edir, belə ki, hətta kiçik səhvlər və ya qeyri-dəqiqliklər də yanlış nəticəyə və ya isbatın qəbuledilməz olmasına gətirib çıxara bilər. Buna görə də isbatların yaradılması və yoxlanılması prosesində hər bir addımı diqqətlə izləmək lazımdır.

Bütövlükdə, isbat yaratma mərhələsi isbatların etibarlı və səmərəli şəkildə yaradılmasını və həssas məlumatları aşkar etmədən doğruluğunun təsdiqlənməsini təmin etməklə sıfır bilik sxemi prosesində mühüm rol oynayır.

- **İsbatın yoxlanılması:** İsbat edən isbat yaratdıqdan sonra yoxlayıcı onun düzgünlüyünü yoxlayır. O, bəyanatın həqiqətən də doğru olduğuna inandırmaq üçün protokolun ictimai parametrlərindən və isbatın özündən istifadə edir. Qeyd etmək vacibdir ki, rəyçi isbatların yaradılmasında istifadə olunan həssas məlumatlara və ya məlumatlara daxil ola bilməz.

İsbatın yoxlanılması mərhələsində ilk addım isbatın özünü isbat edəndən əldə etməkdir. Bu, istifadə olunan protokoldan asılı olaraq kriptoqrafik imzalar, riyazi düsturlar və ya digər xüsusi qeydlər şəklində təqdim oluna bilər.

Sonra isbatın düzgünlüyünü yoxlamaq üçün kriptoqrafik metodların və alqoritmlərin tətbiqi gəlir. Bu, ictimai alqoritmlər və açarlardan istifadə etməklə şifrənin açılması, hashing, mesaj imzalarının yoxlanılması və s. kimi müxtəlif əməliyyatların yerinə yetirilməsini nəzərdə tutur.

İsbatın yoxlanılması prosesində əsas məqamlardan biri yoxlama nəticələrini gözlənilən dəyərlər və ya tələblərlə müqayisə etməkdir. Məsələn, əgər sübut müəyyən bir iddianın doğruluğunu nümayiş etdirməkdirsə, o zaman test iddianın faktiki olaraq

isbatlarla dəstəkləndiyini təmin etməlidir (Abdolmaleki, Baghery, Lipmaa, & Zajac, 2019).

Yoxlamanın nəticələri gözləntilərə və tələblərə cavab verirsə, isbat təsdiqlənmiş hesab olunur və növbəti mərhələ və ya fəaliyyət davam etdirilə bilər. Bununla belə, hər hansı uyğunsuzluq və ya uyğunsuzluq varsa, əlavə yoxlamalar aparılmalı və ya yeni isbatlar tələb edilməlidir.

Qeyd etmək vacibdir ki, isbatın yoxlanılması mərhələsi təfərrüata və dəqiqliyə yüksək diqqət tələb edir, çünki nəticənin etibarlılığı yoxlamanın düzgünlüyündən asılıdır. Buna görə etibarlı alqoritmlər və metodlardan istifadə etməklə yoxlama aparmaq, həmçinin prosesin bütün mərhələlərini izləmək lazımdır.

- **Nəticələrin təsdiqi:** Isbatın uğurla yoxlanılmasından sonra yoxlayıcı onu düzgün hesab edir. Bu, sıfır bilik isbat prosesini tamamlayır və isbat edənin söylədiyi iddianın həqiqətən doğru olduğunu təsdiqləyir.

Sıfır bilikli isbat sxeminin nəticə yoxlama mərhələsi isbatın icrasından sonra əldə edilən nəticələrin düzgünlüyünün və etibarlılığının təmin edilməsində əsas rol oynayır. Bu mərhələ isbat prosesi zamanı əldə edilən nəticələrin təhlilini, onların gözlənilən dəyərlər və ya tələblərlə müqayisəsini və bu nəticələr əsasında gələcək fəaliyyətlərə qərar verməyi əhatə edir (Petkus, 2018).

Nəticələrin yoxlanılması mərhələsində ilk addım isbatın həyata keçirilməsindən nəticələri əldə etməkdir. Bu, bəyanatın etibarlılığının yoxlanılması, məlumatların bütövlüyünün yoxlanılması və ya müəyyən şərtlərin yerinə yetirildiyini təsdiqləmək kimi müxtəlif nəticələr ola bilər.

Sonra, müvafiq üsul və vasitələrdən istifadə edərək əldə edilmiş nəticələri təhlil etməlisiniz. Buraya nəticələrin gözlənilən dəyərlərə və ya tələblərə cavab verməsinin yoxlanılması, onların düzgünlüyünün və etibarlılığının qiymətləndirilməsi daxil ola bilər.

Əldə edilmiş nəticələrlə gözlənilən dəyərlər arasında hər hansı uyğunsuzluq aşkar edilərsə, bu uyğunsuzluqların səbəblərini müəyyən etmək üçün əlavə təhlil aparılmalıdır. Buraya daxil edilmiş məlumatların düzgünlüyünün yoxlanılması,

istifadə olunan metodların və alqoritmlərin təhlili, isbatın icrası zamanı mümkün səhvlərin və ya qeyri-dəqiqliklərin qiymətləndirilməsi daxil ola bilər.

Nəticələri təhlil etdikdən və hər hansı uyğunsuzluqların səbəblərini müəyyən etdikdən sonra gələcək tədbirlər haqqında qərar qəbul edilməlidir. Bu, düzəldilmiş məlumat və ya metodlardan istifadə edərək isbatın yenidən işə salınmasını, əlavə testlərin və ya təhlillərin aparılmasını və müəyyən edilmiş səhvlər və ya qeyri-dəqiqliklər əsasında nəticələrin tənzimlənməsini əhatə edə bilər.

Nəzərə almaq lazımdır ki, nəticələrin yoxlanılması mərhələsi təfərrüata və dəqiqliyə yüksək diqqət tələb edir, çünki əldə edilən nəticələrin və qərarların etibarlılığı nəticələrin düzgün təhlilindən asılıdır. Buna görə etibarlı üsul və vasitələrdən istifadə edərək yoxlama aparmaq, həmçinin prosesin bütün addımlarını və mərhələlərini izləmək lazımdır.

Ümumiyyətlə, nəticənin yoxlanılması mərhələsi isbatın icrasından əldə edilən nəticələrin və nəticələrin düzgünlüyünü və etibarlılığını təmin edən sıfır bilik isbatı dizayn prosesinin mühüm hissəsidir.

Bu addımların hər biri sıfır bilik isbatı prosesini səmərəli və təhlükəsiz etmək üçün əsas rol oynayır. Onlar protokolun düzgün icrasını, məxfiliyin qorunmasını və nəticələrin etibarlılığını təmin edirlər. zk-STARK sıfır bilik isbatı sxemi daxilində bu addımları araşdırmaq bizə bu sistemin necə işlədiyini və məlumat təhlükəsizliyi və məxfiliklə bağlı müxtəlif sahələrdə potensial tətbiqlərini daha yaxşı anlamağa imkan verir (Lin & Liao, 2019).

1.3. İnformasiya təhlükəsizliyində sıfır bilik isbatının rolu

ZKP kriptoqrafiya, blokçeyn texnologiyası və təhlükəsiz kommunikasiya protokolları kimi müxtəlif domenlərdə tətbiqi ilə informasiya təhlükəsizliyi sahəsində mühüm irəliləyişi təmsil edir. ZKP sxemlərinin müxtəlif massivləri arasında sıfır bilik rəqəmsal qarşılıqlı əlaqədə məxfiliyin və təhlükəsizliyin artırılması üçün əhəmiyyətli potensial təklif edərək unikal xüsusiyyətləri və imkanları ilə seçilir.

Özündə sıfır bilik isbatı bir tərəfə (təsdiq edənə) ifadənin özünün həqiqətindən kənar heç bir əlavə məlumat aşkar etmədən digər tərəfə (təsdiq edənə) ifadənin

etibarlılığını nümayiş etdirməyə imkan verir. Əslində, o, isbat edənə heç bir əsas məlumatı və ya sirri açıqlamadan ifadənin doğruluğuna yoxlayanı inandırmağa imkan verir. Bu konsepsiya autentifikasiya prosesləri, şəxsiyyətin yoxlanılması və əməliyyatın təsdiqi kimi məxfiliyin və məxfiliyin əsas olduğu ssenarilərdə böyük dəyərə malikdir.

Xüsusən də zk-STARK protokolu genişlənmə və şəffaflıq xüsusiyyətləri ilə fərqlənir. Əvvəlki bəzi ZKP sxemlərindən fərqli olaraq, zk-STARK isbat edən və yoxlayıcı arasında çoxlu əlaqə dövriyyəsinin tələb olunduğu interaktiv isbatların hesablama baxımından intensiv prosesinə etibar etmir. Əvəzində zk-STARK qeyri-interaktivliyə nail olmaqla onu daha səmərəli və sürət və hesablama resurslarının məhdud olduğu real dünya tətbiqləri üçün uyğun edir.

zk-STARK şəffaflıq təklif edir, yəni yaradılan isbatlar hesablama gücündən və təcrübəsindən asılı olmayaraq istənilən tərəf tərəfindən qısa və asan yoxlanılır. Bu şəffaflıq xüsusiyyəti bir çox maraqlı tərəflərin mərkəzləşdirilmiş orqana etibar etmədən əməliyyatların və ya məlumatların bütövlüyünü yoxlamalı olduğu sistemlərdə etimadı və audit qabiliyyətini artırmaq üçün çox vacibdir (Nair, 2019). zk-STARK -ın tədqiqatı və inkişafı informasiya təhlükəsizliyinin müxtəlif sahələrində geniş təsirlərə malikdir. Tranzaksiyaların bütövlüyü və məxfiliyinin təmin edilməsinin vacib olduğu blokçeyn texnologiyası kontekstində zk-STARK böyük vəd edir. Məxfiliyi qoruyan əməliyyatları və ağıllı müqavilələri işə salmaqla, zk-STARK blokçeyn əsaslı sistemlərin məxfiliyini artıra bilər, eyni zamanda əsas kitabçanın dəyişməzliyini və şəffaflığını təmin edə bilər (Binance Academy, 2009)

Bundan əlavə, zk-STARK həssas məlumatı aşkar etmədən şəxsiyyət və ya icazənin təsdiqlənməsinin vacib olduğu autentifikasiya və girişə nəzarət mexanizmlərində tətbiqlərə malikdir. zk-STARK əsaslı autentifikasiya protokollarından istifadə etməklə, təşkilatlar şəxsiyyət oğurluğu və ya icazəsiz girişlə bağlı riskləri minimuma endirməklə yanaşı, öz təhlükəsizlik mövqelərini gücləndirə bilərlər.

Praktik tətbiqlərinə əlavə olaraq, zk-STARK-ın tədqiqatı kriptoqrafiyanın və hesablama mürəkkəbliyi nəzəriyyəsinin nəzəri əsaslarına töhfə verir. Güclü

təhlükəsizlik zəmanətləri ilə səmərəli ZKP sxemlərinin inkişafı təhlükəsiz rabitə və hesablamaların əsasını təşkil edən fundamental prinsiplər haqqında anlayışımızı genişləndirir və bu sahədə gələcək yeniliklərə yol açır.

Sıfır bilik isbatının informasiya təhlükəsizliyinin təmin edilməsində dəqiq hansı rolu oynadığını nəzərdən keçirək.

✓ **Məlumat Məxfiliyinin Qorunması:** Sıfır bilik isbatının əsas rollarından biri məlumat məxfiliyini təmin etməkdir. Isbat prosesi zamanı heç bir məxfi məlumat tərəflərə açıqlanmır ki, bu da məlumatların sızması və ya ona icazəsiz daxil olma ehtimalını aradan qaldırır. Bu, maliyyə əməliyyatları, tibbi qeydlər və ticarət sirləri kimi məxfiliyin kritik olduğu sahələrdə xüsusilə vacibdir.

✓ **Açıqlanmadan həqiqətin isbatı:** Sıfır bilik isbatı sizə müəyyən ifadə və ya faktın həqiqətini onunla əlaqəli məlumatları açıqlamadan təsdiq etməyə imkan verir. Bu, yoxlama və yoxlama prosesini təhlükəsiz və təhlükəsiz edir, çünki heç bir həssas məlumatın sızma və ya təhlükə altına düşmə riski yoxdur.

✓ **Fırıldaqçılıq risklərini minimuma endirin:** Sıfır bilik isbatından istifadə hakerlik və fırıldaqçılıq risklərini minimuma endirməyə kömək edir. Heç bir həssas məlumat ötürülmədiyi və aydın mətndə saxlanmadığı üçün təcavüzkarlar üçün məlumatlara daxil olmaq və ya isbatlara müdaxilə etmək çətindir. Bu, sistemə təhlükəsizlik və etibar səviyyəsini artırır.

✓ **Şəffaflığın və ardıcıllığın təmin edilməsi:** Sıfır bilik isbatı məlumat mübadiləsində şəffaflığı və ardıcıllığı təşviq edir. Proses riyazi alqoritmlərə və şifrələməyə əsaslandığı üçün isbatın nəticələri obyektiv və insan faktorlarından asılı deyildir. Bu, tərəflər arasında etimad və səmərəli qarşılıqlı fəaliyyət üçün zəmin yaradır.

✓ **Müxtəlif sahələrdə Tətbiq:** Sıfır bilik isbatı maliyyə texnologiyası, tibb, hüquq və blokçeyn texnologiyası da daxil olmaqla müxtəlif sahələrdə geniş tətbiqlərə malikdir. Məlumatların təhlükəsizliyini və məxfiliyini təmin etmək qabiliyyəti onu günümüzün rəqəmsal dünyasında əvəzsiz alətə çevirir.

Nəticə etibarilə, xüsusilə zk-STARK sxemi ilə nümunə verilmiş sıfır bilik isbatlarının rolu informasiya təhlükəsizliyi vəziyyətinin yüksəldilməsində əvəzsizdir.

Miqyaslılıq, şəffaflıq və məxfiliyi qoruyan xassələri vasitəsilə zk-STARK rəqəmsal qarşılıqlı əlaqənin məxfiliyini, bütövlüyünü və etibarlılığını artırmaq üçün güclü alət təklif edir. Bu sahədə tədqiqatlar inkişaf etməyə davam etdikcə biz təhlükəsiz kommunikasiya və hesablamanın gələcəyini formalaşdıran təhlükəsizlik mənzərəsinə daha da dərin təsirləri təxmin edə bilərik. Beləliklə, sıfır bilik isbatı məlumatın məxfiliyinin və etibarlılığının təmin edilməsində mühüm rol oynayır (Petkus, 2018).

1.4. Sıfır bilik isbatında zk-STARK ın əhəmiyyəti

ZKP müasir kriptoqrafiyada təməl daşı kimi ortaya çıxdı və tərəflərə heç bir əsas məlumatı aşkar etmədən məlumatın düzgünlüyünü yoxlamağa imkan verdi. Müxtəlif ZKP sxemləri arasında zk-STARK özünəməxsus xüsusiyyətləri və potensial tətbiqləri sayəsində böyük diqqəti cəlb etmişdir. Bu məqalə zk-STARK -ın sıfır bilik isbatlarında əhəmiyyətini araşdırır, onun texniki aspektlərini, tətbiqlərini və informasiya təhlükəsizliyi üçün təsirlərini araşdırır.

zk-STARK sıfır bilik isbatı sahəsində görkəmli vasitədir. Onun əhəmiyyəti kriptoqrafik protokolların təhlükəsizliyinə və səmərəliliyinə təsir edən bir neçə əsas aspektdə əks olunur.

Birincisi, zk-STARK məxfi məlumatların ötürülməsi zamanı yüksək səviyyədə təhlükəsizlik təmin edir. Sıfır bilik isbatları məlumatların özünü aşkar etmədən iddiaların həqiqətini isbat edə bildiyi üçün, zk-STARK şəxsi və biznes məlumatlarını icazəsiz giriş və istifadədən qoruyaraq məxfiliyi təmin edir.

İkincisi, zk-STARK, zk-STARK kimi alternativ metodlarla müqayisədə əhəmiyyətli dərəcədə genişlənmə və səmərəlilik üstünlüklərinə malikdir. Parametrlərin yaradılmasında açıq şəkildə yoxlanılan təsadüfilikdən istifadə etməklə, zk-STARK etibarlı tərəflərə ehtiyacı aradan qaldıraraq onu geniş istifadə üçün daha açıq və etibarlı edir.

zk-STARK-ın üçüncü mühüm xüsusiyyəti, isbatların yaradılması və yoxlanılması vaxtını artırmadan böyük həcmdə məlumatı emal etmək qabiliyyətidir. Bu, xüsusilə böyük verilənlər bazalarının və ya mürəkkəb hesablama proseslərinin etibarlılığının isbatınu tələb edən sahələrdə faydalıdır.

Bundan əlavə, zk-STARK blokçeyn sistemlərində şəffaflığın və etibarın təmin edilməsində əsas rol oynayır. Blokçeyn texnologiyaları rəqəmsal iqtisadiyyat üçün getdikcə əhəmiyyət kəsb etdikcə, zk-STARK istifadəçilərin əməliyyatların bütövlüyü və təhlükəsizliyinə arxayın ola biləcəyi mərkəzləşdirilməmiş və etibarlı sistemlər yaratmağa imkan verir.

Beləliklə, sıfır bilik isbatında zk-STARK -ın əhəmiyyəti danılmazdır. O, yüksək səviyyəli təhlükəsizlik, səmərəlilik və miqyaslılığı təmin etməklə onu müasir kriptoqrafik protokolların və məlumat təhlükəsizliyi sistemlərinin ayrılmaz hissəsinə çevirir.

zk-STARK sıfır bilik isbatları sahəsində əhəmiyyətli irəliləyişi təmsil edir. Təsdiqləyici və yoxlayıcı arasında çoxlu əlaqə raundları tələb edən interaktiv protokollara əsaslanan bəzi əvvəlki ZKP sxemlərindən fərqli olaraq, zk-STARK qeyri-interaktivliyə nail olmaqla onu daha səmərəli və miqyaslı edir. Bu xüsusiyyət sürət və hesablama resurslarının məhdud olduğu real dünya tətbiqləri üçün çox vacibdir.

Bundan əlavə, zk-STARK şəffaflıq təklif edir, yəni yaradılan isbatlar hesablama gücündən və təcrübəsindən asılı olmayaraq istənilən tərəf tərəfindən qısa və asan yoxlanılır. Bu şəffaflıq xüsusiyyəti bir çox maraqlı tərəfin mərkəzi orqana etibar etmədən əməliyyatların və ya məlumatların bütövlüyünü yoxlamalı olduğu sistemlərdə etibarı və audit qabiliyyətini artırır.

zk-STARK -ın Texniki Aspektləri:

zk-STARK genişlənmə, şəffaflıq və məxfiliyi qoruyan xassələrinə nail olmaq üçün bir neçə kriptoqrafik üsuldan istifadə edir. zk-STARK -ın əsas komponentlərindən biri çoxhədli öhdəliklərin istifadəsidir ki, bu da tərəflərə əmsallarını açıqlamadan hesablama tapşırıqlarını təmsil edən çoxhədlilərə öhdəlik götürməyə imkan verir. Bu, bahalı və resurs tutumlu qarşılıqlı əlaqəyə ehtiyac olmadan hesablamaların səmərəli yoxlanılmasına imkan verir.

Bundan əlavə, zk-STARK yaradılan isbatların düzgünlüyünü və təhlükəsizliyini təmin etmək üçün səhvləri düzəltmək kodlarından və cəbri üsullardan istifadə edir. Bu üsullar zk-STARK-a səmərəliliyi və miqyasını qoruyarkən yüksək səviyyəli

təhlükəsizlik əldə etməyə imkan verir və onu informasiya təhlükəsizliyində geniş tətbiqlər üçün uyğun edir.

zk-STARK tətbiqləri:

zk-STARK tətbiqləri blokçeyn texnologiyası, autentifikasiya mexanizmləri və təhlükəsiz rabitə protokolları da daxil olmaqla müxtəlif domenləri əhatə edir. Blokçeyn kontekstində zk-STARK əməliyyatlarda və ağıllı müqavilələrdə məxfiliyin və məxfiliyin artırılması üçün böyük vədlər verir. Məxfiliyi qoruyan əməliyyatlara və hesablamalara imkan verməklə, zk-STARK blokçeynin bütövlüyünü və şəffaflığını qoruyarkən ictimai kitablarda həssas məlumatların ifşası ilə bağlı narahatlıqları həll edə bilər.

Bundan əlavə, zk-STARK, həssas məlumatları aşkar etmədən şəxsiyyət və ya icazənin təsdiqlənməsinin vacib olduğu autentifikasiya mexanizmlərində tətbiqlərə malikdir. zk-STARK əsaslı autentifikasiya protokollarından istifadə etməklə, təşkilatlar şəxsiyyət oğurluğu və ya icazəsiz girişlə bağlı riskləri minimuma endirməklə yanaşı, öz təhlükəsizlik mövqelərini gücləndirə bilərlər.

İnformasiya təhlükəsizliyinə təsirlər:

1. zk-STARK -ın tədqiqi və inkişafı informasiya təhlükəsizliyi üçün dərin təsirlərə malikdir. Sıfır bilik isbatları üçün səmərəli və genişlənə bilən həllər təmin etməklə, zk-STARK rəqəmsal qarşılıqlı əlaqənin məxfiliyini, bütövlüyünü və etibarlılığını artırır. Onun şəffaflıq xüsusiyyəti etimad və audit qabiliyyətini artırır, maraqlı tərəflərə mərkəzləşdirilmiş orqanlara etibar etmədən əməliyyatların və hesablamaların düzgünlüyünü yoxlamağa imkan verir (Ben-Sasson, Chiesa, Tromer, & Virza 2017).
2. zk-STARK kriptoqrafiya və hesablama mürəkkəbliyi nəzəriyyəsinin nəzəri əsaslarına töhfə verir. Güclü təhlükəsizlik zəmanətləri ilə səmərəli ZKP sxemlərinin inkişafı təhlükəsiz rabitə və hesablamalar haqqında anlayışımızı genişləndirir, informasiya təhlükəsizliyi sahəsində gələcək yeniliklərə yol açır.

Yekun olaraq qeyd edək ki, zk-STARK sıfır bilik isbatları və informasiya təhlükəsizliyi vəziyyətinin inkişafında mühüm rol oynayır. Onun miqyaslılığı, şəffaflığı və məxfiliyi qoruyan xassələri onu rəqəmsal qarşılıqlı əlaqənin məxfiliyini,

bütövlüyünü və etibarlılığını artırmaq üçün güclü alətə çevirir. Bu sahədə tədqiqatlar inkişaf etməyə davam etdikcə biz təhlükəsiz kommunikasiya və hesablamaların gələcəyini formalaşdıracaq gələcək irəliləyişləri gözləyə bilərik. zk-STARK -ın fərqli xüsusiyyətlərinə onun miqyaslılığı və açıqlığı daxildir. zk-STARK -dan fərqli olaraq, zk-STARK -ın isbat yaratma və yoxlama vaxtı şahidin ölçüsü ilə əhəmiyyətli dərəcədə artmır. Bundan əlavə, zk-STARK parametrlər yaradan zaman açıq şəkildə yoxlanılan təsadüfilikdən istifadə edir və onu zk-STARK-dan daha açıq edir. Nəticədə, zk-STARK müəyyən hallarda, məsələn, böyük verilənlər bazalarının isbat edilməsində daha effektiv ola bilər.

II FƏSİL. ZK-STARK IN RİYAZİ ƏSASLARI, TƏTBİQİ TRANZAKSİYA ŞİFRƏLƏMƏ TEXNİKALARI VƏ ƏSAS BLOKÇEYN KONSEPSİYALARI

2.1. zk-STARK ın riyazi əsasları

zk-STARK təsnifatı Alman riyaziyyatçısı Ernst Baruch Zk və Amerika riyaziyyatçısı Corc Stark tərəfindən təklif edilən Xətti cəbrlərinin təsnifatıdır. Onlar bu təsnifatı mürəkkəb ədədlər üzərində sadə Xətti cəbrlərinin strukturunu müəyyən etmək üçün hazırlayıblar.

Xətti cəbrləri nəzəri fizikada, xüsusilə qruplar və simmetriyalar nəzəriyyəsində mühüm rol oynayır. zk-STARK təsnifatı mürəkkəb ədədlər sahəsi üzrə sadə Xətti cəbrlərinin, yəni qeyri-trivial idealları olmayan (cəbrin özü və sıfır idealı istisna olmaqla) Xətti cəbrlərinin təsnifatıdır.

zk-STARK təsnifatına ölçü, kommutasiya əlaqələrinin forması və s. kimi struktur xassələri əsasında təsnif edilən müxtəlif Xətti cəbr növləri daxildir. Bu növlər Xətti cəbrlərinin müxtəlif "ailələrini" təşkil edir.

zk-STARK təsnifatının son məqsədi riyaziyyat və fizikanın müxtəlif sahələrində onların öyrənilməsinə və tətbiqinə kömək edən bütün sadə Xətti cəbrlərini təsvir etmək üçün sistematik bir üsul təqdim etməkdir.

zk-STARK blokçeynlərdə hesablamaların bütövlüyünü və məxfiliyini təmin edən kriptoqrafik isbat sistemidir.

- **Çoxhədli Öhdəliklər:** zk-STARK polinom öhdəlikləri kimi qabaqcıl riyazi konstruksiyalara əsaslanır. Prover, FFT (Fast Fourier Transform) adlı bir texnikadan istifadə edərək bir sıra polinomları öhdəsinə götürür.

zk-STARK kriptoqrafik innovasiyaların önündə dayanır və blokçeynlərdə hesablamaların bütövlüyü və məxfiliyində inqilab etməyi vəd edir. Əsasında, xüsusilə FFT tətbiqi vasitəsilə çoxhədli öhdəliklərin istifadəsi ilə xarakterizə olunan mürəkkəb riyazi çərçivə var.

Polinomial tənlik:

Əgər IF sahə olarsa onda

$$P(x)IF[x] \qquad (2.1.1)$$

Çoxhədli olsun. Əgər

$$x\{x_0,x_1,\ldots x_n\} \qquad (2.1.2)$$

olarsa, onda P(x)=0 olur. Bu da IF də H(x) polinomunun mövcud olduğunu göstərir.

$$P(x) = a_n x^n + a_{n-1} x^{n-1}+\ldots\ldots\ldots\ldots+a_2 x^2 + a_1 x + a_0 \qquad (2.1.3)$$

P(x)- polynomial tənlik.

IF- sahə.

x- polinom tənliyin dəyişənləri.

a- Dəyişənlərin əmsalı.

Loqranj interpoliyasiyası:

IF sahə olsun və $x_0,x_1,\ldots x_n$ IF-dən n+1 fərqli qiymət, $y_0,y_1,\ldots y_n$ n+1 fərqli qiymət olsun. Ən çox n olan P(x) IF[x] polinomları var ki i üçün

$$P(x_i)=y_i \qquad (2.1.4)$$

olsun. Bu Laqranj çoxhədlisi adlanır.

$$P(x):= \qquad (2.1.5)$$

$$(x)== \ldots. \qquad (2.1.6)$$

(x)-laqranj çoxhədlisi.

Polinom öhdəlikləri zk-STARK -ın təməl daşı kimi xidmət edir. Bu öhdəliklər tərəflərə onların əsas dəyərlərini açıqlamadan bir sıra polinomlara öhdəlik götürməyə imkan verir. Polinom öhdəliklərindən istifadə etməklə, zk-STARK tərəflərə etibarlı

şəkildə qarşılıqlı əlaqə yaratmağa imkan verir, burada hesablamaların bütövlüyü həssas məlumatları ifşa etmədən yoxlanıla bilər. Bu, əməliyyatların mərkəzləşdirilməmiş və tez-tez rəqib şəraitdə baş verdiyi blokçeyn mühitlərində xüsusilə vacibdir . (Petkus, 2018)

FFT zk-STARK daxilində çoxhədli öhdəliklərin həyata keçirilməsində mühüm rol oynayır. Əvvəlcə 19-cu əsrin əvvəllərində Karl Fridrix Qauss tərəfindən hazırlanmış FFT ardıcıllığın diskret Furye çevrilməsini səmərəli hesablayan hesablama alqoritmidir. zk-STARK kontekstində FFT həm səmərəli, həm də təhlükəsiz şəkildə polinomlarla manipulyasiya və öhdəliyi asanlaşdırır.

Sonda qeyd edək ki, zk-STARK blokçeynlərdə hesablamaların bütövlüyünü və məxfiliyini təmin etmək üçün güclü alət təklif edərək kriptoqrafiya sahəsində əhəmiyyətli irəliləyişi təmsil edir. Polinom öhdəlikləri, FFT və sıfır bilik isbatlarından istifadə edərək, zk-STARK istifadəçi məxfiliyini qoruyarkən hesablamaların şəffaf şəkildə yoxlanılmasını təmin edir. Texnologiya inkişaf etməyə davam etdikcə, zk-STARK innovasiyaları təşviq etmək və müxtəlif sənayelərdə mərkəzləşdirilməmiş sistemlərə inamı gücləndirmək potensialına malikdir.

- **Mark Ağacları:** zk-STARK kriptoqrafiyada fundamental konsepsiya olan Mark ağaclarından istifadə edir.

Mark ağaclarının zk-STARK -ın riyazi çərçivəsinə inteqrasiyası bu əsaslı kriptoqrafik isbat sisteminə daha bir mürəkkəblik və təhlükəsizlik qatını əlavə edir. Kriptoqrafiyada fundamental konsepsiya olan Mark ağacları zk-STARK tətbiqlərinin bütövlüyü və səmərəliliyinin təmin edilməsində mühüm rol oynayır.

Özündə Mark ağacı fərdi məlumat blokları dəstindən yaranan heş dəyərlərinin iyerarxik düzülüşündən ibarət məlumat strukturudur. Ağacdakı hər bir yarpaq qovşağı məlumat blokunu təmsil edir, daxili qovşaqlar isə onların uşaq qovşaqlarının heşlərinin birləşməsindən hesablanmış heşləri ehtiva edir. Bu iyerarxik struktur, bütün verilənlər toplusunu endirməyə ehtiyac qalmadan tərəflərə xüsusi məlumat bloklarının həqiqiliyini yoxlamağa imkan verməklə məlumat bütövlüyünün səmərəli yoxlanılmasına imkan verir.

Mark ağacları binar ağaclardır və verilənlərin heş funksiyaları ilə təmsil edilməsi əsasında qurulur.

Addım 1: Verilənlərin Yarpaqlara Bölünməsi

Verilənlər ardıcıllıqla yarpaqlara bölünür. Məsələn, verilənlər şəklində olsun.

Addım 2: Yarpaq Heşlərinin hesablanması

Hər yarpaq heş funksiyası ilə şifrələnir. Bir heş funksiyası *H* istifadə edilərək, hər yarpaq üçün heş aşağıdakı kimi hesablanır:

(2.1.7)

Addım 3: Daxili Düyünlərin Heşlərinin hesablanması

Mark ağacının içindəki hər iki ardıcıl hash birləşdirilir və onların hash-i hesablanır:

(2.1.8)

Burada iki yarpaq düyününün birləşmiş hash-idır və || stringlərin birləşdirilməsi operatorudur.

Bu proses ağacın bütün səviyyələri boyunca təkrarlanır və hər səviyyədəki heş-lar birləşdirilərək yeni heş-lar hesablanır.

Addım 4: Mark Kökünün Hesablanması

Mark ağacının yuxarı səviyyəsində əldə edilən son heş, Mark kökü adlanır. Bu kök heş bütün ağacın xülasəsidir və ağacın bütün məlumatlarının doğruluğunu təmsil edir:

(2.1.9)

zk-STARK kontekstində Mark ağacları sistemin ümumi təhlükəsizliyinə və səmərəliliyinə töhfə verən çoxsaylı məqsədlərə xidmət edir. zk-STARK -da Mark ağaclarının əsas tətbiqlərindən biri böyük məlumat dəstlərinin qısa və yoxlanıla bilən təsvirlərinin qurulmasıdır. Məlumatları Mark ağacı formatında təşkil etməklə, zk-STARK bu verilənlər dəstləri üzərində aparılan hesablamaların etibarlılığını təsdiq

edən yığcam isbatlar yarada bilər. Bu lakoniklik zk-STARK -ın miqyasını qorumaq üçün çox vacibdir ki, bu da mürəkkəb hesablamaların həddindən artıq hesablama xərcləri olmadan səmərəli yoxlanılmasına imkan verir.

Bundan əlavə, Mark ağacları zk-STARK isbatlarının şəffaflığını və yoxlanılabilirliyini artırır. Mark ağacları əsas məlumatlardan deterministik şəkildə qurulduğundan, ağacın kök heşinə çıxışı olan hər kəs müstəqil olaraq bütün verilənlər bazasının bütövlüyünü yoxlaya bilər. Bu şəffaflıq maraqlı tərəflərin mərkəzləşdirilmiş orqanlara etibar etmədən əməliyyatların və hesablamaların düzgünlüyünü yoxlaya bildiyi blokçeyn ekosistemlərində etimadı artırır.

Məlumatların təşkili və yoxlanılmasındakı rolundan əlavə, Mark ağacları zk-STARK-ın məxfiliyi qoruyan xüsusiyyətlərinə də töhfə verir. Tərəflərə məlumatların qalan hissəsini gizlətməklə ağacın daxilindəki spesifik budaqları və ya yolları seçmə şəkildə açıqlamağa imkan verməklə, Mark ağacları hesablamaların düzgünlüyünü yoxlamaq üçün yalnız zəruri məlumatları aşkar edən sıfır bilik isbatlarının qurulmasını asanlaşdırır. Bu seçmə açıqlama mexanizmi həssas məlumatların məxfi qalmasını təmin edir, eyni zamanda hesablamaların şəffaf şəkildə yoxlanılmasına imkan verir.

zk-STARK-da Mark ağaclarının istifadəsi kompüter elmləri, riyaziyyat və informasiya nəzəriyyəsindən əsas götürərək kriptoqrafiyanın fənlərarası xarakterini vurğulayır. Polinom öhdəlikləri və sıfır bilik isbatları kimi digər kriptoqrafik üsullarla yanaşı Mark ağaclarından istifadə edərək, zk-STARK məxfilik, miqyaslılıq və yoxlanılabilirlik arasında incə tarazlığa nail olur və onu geniş tətbiqlər üçün cəlbedici həll edir.

Çoxsaylı üstünlüklərinə baxmayaraq, Mark ağaclarının zk-STARK-a inteqrasiyası da müəyyən problemlər və mülahizələr yaradır. Belə problemlərdən biri səmərəlilik və təhlükəsizlik baxımından optimallaşdırmaq üçün Mark ağacının strukturunu diqqətlə tərtib etmək ehtiyacıdır. Heşing alqoritmlərinin seçimi, ağacın dərinliyi və budaqlanma faktoru Mark ağacının performansına və dayanıqlığına təsir göstərə bilər. Bundan əlavə, zk-STARK tətbiqləri Mark ağac konstruksiyalarının əsas

məlumatların bütövlüyünü poza biləcək toqquşma və ya əvvəlcədən təsvir hücumları kimi hücumlara davamlı olmasını təmin etməlidir.

Üstəlik, Mark ağacları məlumatların səmərəli və yoxlanıla bilən təqdimatını təmin etsə də, onlar müəyyən növ hücumlara qarşı immun deyillər. Məsələn, kifayət qədər hesablama resurslarına malik olan zərərli aktor sistemi etibarsız məlumatlarla doldurmaqla xidmətdən imtina hücumu təşkil edə bilər və bununla da zk-STARK yoxlamasının performansını aşağı sala bilər (Gennaro, Gentry, Parno,& Raykova 2013). Bu riskləri azaltmaq üçün zk-STARK tətbiqləri möhkəm doğrulama mexanizmlərini özündə birləşdirməli və zərərli davranışın qarşısını almaq üçün işin isbatı və ya riskin isbatı kimi üsullardan istifadə etməlidir.

Yekun olaraq, Mark ağaclarının zk-STARK-a inteqrasiyası sistemin bütövlüyünü, səmərəliliyini və məxfiliyi qoruyan xüsusiyyətlərini artıraraq kriptoqrafiya sahəsində əhəmiyyətli irəliləyişi təmsil edir. Mark ağaclarını digər kriptoqrafik üsullarla birlikdə istifadə edərək, zk-STARK şəffaflıq və məxfilik arasında zərif tarazlığa nail olur və onu blokçeynlərdə və digər mərkəzləşdirilməmiş sistemlərdə hesablamaların təhlükəsizliyini və məxfiliyini təmin etmək üçün güclü alətə çevirir. zk-STARK inkişaf etməyə davam etdikcə, Mark ağacları, şübhəsiz ki, müxtəlif sənaye və tətbiqlərdə davamlı uğurunda və qəbulunda mərkəzi rol oynayacaqdır.

- **İnteraktiv Oracle Proofs:** zk-STARK İOP (Interactive Oracle Proofs) istifadə edir.

İOP zk-STARK arxitekturasına daxil edilməsi kriptoqrafik protokollar sahəsində əhəmiyyətli irəliləyişə işarə edir, sistemin blokçeynlərdə və digər mərkəzləşdirilməmiş platformalarda təhlükəsiz və özəl hesablamaları təmin etmək qabiliyyətini daha da artırır. İOP effektivliyi və miqyaslılığı qoruyarkən yoxlanıla bilənliyə və məxfiliyə nail olmaq üçün güclü mexanizm təklif edir.

Özündə, İOP kriptoqrafik protokoldur ki, o, isbat edən şəxsə bir sıra oracle sorğuları ilə qarşılıqlı əlaqə yaratmaqla ifadənin düzgünlüyünə təsdiqləyicini inandırmağa imkan verir. Bu sorğular vasitəçi kimi xidmət edir, bunun vasitəsilə isbat edən hər hansı həssas məlumatı açıqlamadan etibarlı isbat haqqında bilik nümayiş

etdirə bilər. İOP istifadə etməklə, zk-STARK qısa və yoxlana bilən hesablama isbatları qura bilir və bununla da istifadəçi məxfiliyini qoruyarkən mürəkkəb hesablamaların şəffaf yoxlanılmasını təmin edir.

İOP-un əsas üstünlüklərindən biri onların sıfır bilik xüsusiyyətlərinə nail olmaq qabiliyyətidir, yəni isbat edilən ifadənin etibarlılığından kənar heç bir məlumatı aşkar etmir. Bu əmlak həssas məlumatların icazəsiz girişdən qorunmalı olduğu mərkəzləşdirilməmiş sistemlərdə məxfiliyin qorunması üçün vacibdir. İOP-dan istifadə etməklə, zk-STARK hesablamaların heç bir məxfi məlumatı açıqlamadan yoxlanılmasını təmin edir, beləliklə, istifadəçi məxfiliyini və məxfiliyini qoruyur.

Bundan əlavə, İOP hesablamaların effektiv yoxlanılmasına imkan verməklə zk-STARK-ın miqyasına kömək edir. Mürəkkəb hesablamaları yoxlamaq üçün geniş hesablama resursları tələb edə bilən ənənəvi kriptoqrafik protokollardan fərqli olaraq, İOP bir sıra oracle sorğuları vasitəsilə qısa və səmərəli yoxlamaya imkan verir. Bu miqyaslılıq zk-STARK-ın təhlükəsizlik və ya performansdan ödün vermədən mərkəzləşdirilməmiş tətbiqlərin və platformaların artan tələblərini dəstəkləməsini təmin etmək üçün çox vacibdir.

İOP-un digər mühüm cəhəti onların sağlamlığa və tamlığa zəmanət vermək qabiliyyətidir. Sağlamlıq isbat edir ki, isbat edən yalançı ifadənin təsdiqləyicisini inandıra bilməz, tamlıq isə isbat edənin doğru ifadənin yoxlayıcısını yüksək ehtimalla inandıra bilməsinə zəmanət verir. Bu xüsusiyyətlər kriptoqrafik protokollara etibar yaratmaq üçün vacibdir, çünki onlar sistemin gözlənildiyi kimi davranmasını və zərərli aktorlar tərəfindən asanlıqla manipulyasiya oluna bilməməsini təmin edir (Gennaro, 2013).

İOP-un zk-STARK-a inteqrasiyası da sistemin şəffaflığına və audit oluna bilənliyinə kömək edir. İOP sübut edən və yoxlayıcı arasında bir sıra qarşılıqlı əlaqə vasitəsilə qurulduğundan, sübuta çıxışı olan hər kəs onun düzgünlüyünü müstəqil şəkildə yoxlaya bilər. Bu şəffaflıq, maraqlı tərəflərin mərkəzləşdirilmiş orqanlara etibar etmədən hesablamaların bütövlüyünü yoxlaya biləcəyi qeyri-mərkəzləşdirilmiş ekosistemlər daxilində etibarı artırır.

Çoxsaylı üstünlüklərinə baxmayaraq, İOP da müəyyən çətinliklər və mülahizələr yaradır. Belə problemlərdən biri hücumlar və ya zəifliklər riskini minimuma endirmək üçün qarşılıqlı əlaqə protokolunu diqqətlə tərtib etmək ehtiyacıdır. Oracle sorğularının, rabitə kanallarının və kriptoqrafik primitivlərin seçimi isbat protokolunun təhlükəsizliyinə və səmərəliliyinə təsir edə bilər. Bundan əlavə, İOP qeyri-interaktiv protokollarla müqayisədə əlavə hesablama resursları tələb edə bilər ki, bu da onların resurs məhdud mühitlərdə tətbiqini potensial olaraq məhdudlaşdırır.

Bundan əlavə, İOP dizaynı və tətbiqi sövdələşmə və ya rəqib davranış potensialını nəzərə almalıdır. İOP sübut edən və yoxlayıcı arasında bir sıra qarşılıqlı əlaqəyə əsaslandığından, zərərli aktyorlar təsdiqləyicini aldatmaq və ya sübutun bütövlüyünü pozmaq üçün protokoldakı boşluqlardan istifadə etməyə cəhd edə bilərlər. Bu riskləri azaltmaq üçün zk-STARK tətbiqləri möhkəm doğrulama mexanizmlərini özündə birləşdirməli və təhlükəsizlik və dayanıqlığı artırmaq üçün çoxtərəfli hesablama və ya eşik kriptoqrafiyası kimi üsullardan istifadə etməlidir. İOP-un zk-STARK-a inteqrasiyası mərkəzləşdirilməmiş sistemlər üçün kriptoqrafik protokolların inkişafında əhəmiyyətli bir mərhələni təmsil edir. İOP-dan istifadə etməklə, zk-STARK yoxlanıla bilənlik, məxfilik və miqyaslılıq arasında incə tarazlığa nail olur və onu blokçeynlərdə və digər mərkəzləşdirilməmiş platformalarda hesablamaların təhlükəsizliyini və bütövlüyünü təmin etmək üçün güclü alətə çevirir. zk-STARK təkamül etməyə davam etdikcə, İOP , şübhəsiz ki, onun davamlı uğurunda və müxtəlif sənaye və tətbiqlərdə qəbulunda mərkəzi rol oynayacaqdır (Zaghloul, Li, Mutka, & Ren, 2020).

- **Arifmetizasiya:** STARK-lar üçün hesablama sahəsi kriptoqrafik çətin problemdən müstəqildir və buna görə də bu sahə performansı optimallaşdırmaq üçün xüsusi olaraq seçilə bilər.

zk-STARK kontekstində hesablama konsepsiyası kriptoqrafik protokol dizaynında əsas dəyişikliyi təmsil edir, konkret kriptoqrafik çətin problemlərlə bağlı olmadan performans və səmərəliliyi optimallaşdırmaq üçün yeni yanaşma təklif edir. Arifmetizasiya zk-STARK-ın qurulmasında mərkəzi rol oynayır, mürəkkəb

hesablama tapşırıqlarını səmərəli şəkildə emal edilə və yoxlana bilən cəbri tənliklərə çevirməyə imkan verir. Bunu sadə bir numunə ilə izah edək.

(2.1.10)

(2.1.10) formasında verilmiş tənlik üzərindəki hesablamalara baxaq.

$$x \cdot x = x_2 \quad (2.1.11)$$

$$x_2 \cdot x = x_3 \quad (2.1.12)$$

$$x_3 \cdot x = x_4 \quad (2.1.13)$$

$$x_4 - 10 \cdot x_3 = tmp_1 \quad (2.1.14)$$

$$tmp_1 + 35 \cdot x_2 = tmp_2 \quad (2.1.15)$$

$$tmp_2 - 50 \cdot x = tmp_3 \quad (2.1.16)$$

$$tmp_3 + 24 = out \quad (2.1.17)$$

Əsasında hesablama hesablamaların sonlu sahələr üzərində cəbri ifadələr kimi təqdim edilməsini nəzərdə tutur və bununla da kriptoqrafik protokollara cəbri üsulların tətbiqinə imkan verir. Böyük tam ədədlərin faktorinqi və ya diskret loqarifmlərin hesablanması kimi xüsusi riyazi problemlərin sərtliyinə əsaslanan ənənəvi kriptoqrafik yanaşmalardan fərqli olaraq, zk-STARK üçün arifmetizasiya bu kriptoqrafik fərziyyələrdən asılı olmayaraq işləyir. Bu müstəqillik əsas arifmetik sahənin seçimində daha çox çevikliyə imkan verir və bununla da xüsusi istifadə halları üçün performans və səmərəliliyi optimallaşdırır.

zk-STARK-da arifmetizasiyanın əsas üstünlüklərindən biri onun təhlükəsizliyə xələl gətirmədən miqyaslılığa nail olmaq qabiliyyətidir. Hesablamaları cəbri tənliklər kimi təqdim etməklə, zk-STARK çoxhədli manipulyasiya və qiymətləndirmə üçün səmərəli alqoritmlərdən istifadə edə bilər ki, bu da minimal hesablama yükü ilə mürəkkəb hesablamaların yoxlanılmasına imkan verir. Bu genişlənmə, hesablamaların həcminin və mürəkkəbliyinin artmaqda davam etdiyi mərkəzləşdirilməmiş tətbiqlərin və platformaların artan tələblərini dəstəkləmək üçün çox vacibdir (Zaghloul, Li, Mutka, & Ren, 2020).

Bundan əlavə, hesablama zk-STARK-a məxfilikdən ödün vermədən şəffaflığa və audit edilə bilənliyə nail olmağa imkan verir. Cəbri tənliklər mahiyyət etibarilə şəffaf və yoxlanıla bilən olduğundan, zk-STARK sübutuna çıxışı olan hər kəs əsas hesablamaların düzgünlüyünü müstəqil şəkildə yoxlaya bilər. Bu şəffaflıq, maraqlı tərəflərin mərkəzləşdirilmiş orqanlara etibar etmədən əməliyyatların və ağıllı müqavilələrin bütövlüyünü yoxlaya biləcəyi qeyri-mərkəzləşdirilmiş ekosistemlərdə etimadı artırır. Eyni zamanda arifmetizasiya zk-STARK-a yoxlama prosesi zamanı həssas məlumatların məxfi qalmasını təmin etməklə istifadəçi məxfiliyini qorumağa imkan verir.

zk-STARK-da hesablamanın digər üstünlüyü onun müvafiq hesab sahəsini seçməklə performansı optimallaşdırmaq qabiliyyətidir. Arifmetik sahənin seçimi zk-STARK tətbiqlərinin səmərəliliyinə və miqyasına əhəmiyyətli dərəcədə təsir göstərə bilər, çünki müxtəlif sahələr hesablama mürəkkəbliyi və təhlükəsizlik arasında müxtəlif güzəştlər təklif edir. Arifmetizasiyanı xüsusi kriptoqrafik çətin problemlərdən ayırmaqla, zk-STARK xüsusi proqramların hesablama tələblərinə uyğunlaşdırılmış hesab sahələrini seçə bilər və bununla da performans və səmərəliliyi maksimuma çatdırır.

Çoxsaylı üstünlüklərinə baxmayaraq, hesablama müəyyən çətinliklər və mülahizələr də yaradır. Belə çətinliklərdən biri hesablamaları təmsil etmək üçün istifadə olunan cəbri tənlikləri diqqətlə tərtib etmək və təhlil etmək ehtiyacıdır. zk-STARK sübutlarının səmərəliliyi və təhlükəsizliyi cəbri təsvirin seçimindən çox asılıdır, çünki zəif tərtib edilmiş tənliklər sistemdə zəifliklər və ya səmərəsizliklər yarada bilər. Bundan əlavə, arifmetik sahələrin seçilməsi hesablama mürəkkəbliyi, kosmik səmərəlilik və kriptoqrafik hücumlara qarşı müqavimət kimi amillərin diqqətlə nəzərdən keçirilməsini tələb edir.

Bundan əlavə, zk-STARK üçün hesablamanın həyata keçirilməsi cəbri hücumlar və ya arifmetik təsvirdəki zəifliklərdən istifadə edən optimallaşdırma üsulları potensialını həll etməlidir. zk-STARK sübutun qurulmasında istifadə olunan cəbri tənliklərin düzgünlüyünə və təhlükəsizliyinə güvəndiyi üçün zərərli aktorlar yoxlayıcını aldatmaq və ya sübutun bütövlüyünü pozmaq üçün bu tənlikləri

manipulyasiya etməyə cəhd edə bilərlər (Gennaro, Gentry, Parno, & Raykova, 2013). Bu riskləri azaltmaq üçün zk-STARK tətbiqləri ciddi yoxlama mexanizmlərini özündə birləşdirməli və təhlükəsizlik və dayanıqlığı artırmaq üçün sıfır bilik sübutları və ya çoxtərəfli hesablama kimi üsullardan istifadə etməlidir.

Nəticə olaraq, arifmetizasiya zk-STARK tətbiqlərində performansı və səmərəliliyi optimallaşdırmaq üçün güclü alətdir və mürəkkəb hesablamaların səmərəli şəkildə işlənilə və yoxlana bilən cəbri ifadələrə çevrilməsinə imkan verir. Arifmetizasiyanı xüsusi kriptoqrafik çətin problemlərdən ayırmaqla zk-STARK təhlükəsizlikdən ödün vermədən miqyaslılığa, şəffaflığa və məxfiliyə nail olur. zk-STARK təkamül etməyə davam etdikcə, arifmetizasiya, şübhəsiz ki, onun davamlı uğurunda və müxtəlif sənaye və tətbiqlərdə mənimsənilməsində mərkəzi rol oynayacaqdır (Яковлев & Сычева, 2017).

- **Post-Kvant Təhlükəsizlik:** STARK sübut sistemində yeganə kriptoqrafik tərkib hissəsi toqquşmaya davamlı heş funksiyasıdır. Nəticə etibarilə, sübut sistemi heş funksiyasının ideallaşdırılmış modeli altında sübut oluna bilər ki, post-kvantdır.

zk-STARK kontekstində kvantdan sonrakı təhlükəsizlik konsepsiyası kriptoqrafik protokol dizaynında paradiqma dəyişikliyini təmsil edir və kvant kompüterlərinin ənənəvi kriptoqrafik sistemlərə yaratdığı potensial təhlükəyə qarşı möhkəm müdafiə təklif edir. Yalnız toqquşmaya davamlı heş funksiyalarına güvənərək, zk-STARK həm klassik, həm də kvant düşmənlərinin hücumlarına qarşı davamlı olan təhlükəsizlik səviyyəsinə nail olur.

Kvant kompüterləri, miqyasda həyata keçirildiyi təqdirdə, Shor alqoritmi kimi kvant alqoritmlərinə xas zəifliklərindən istifadə edərək, bir çox mövcud kriptoqrafik alqoritmləri köhnəlmək potensialına malikdir. Bu alqoritmlər böyük tam ədədlərin faktorinqi və ya diskret loqarifmlərin hesablanması kimi geniş istifadə olunan kriptoqrafik sxemlərin əsasını təşkil edən riyazi məsələləri səmərəli həll edə bilər. Nəticədə, kriptoqrafik cəmiyyətdə kvant hesablamalarının inkişafı fonunda mövcud kriptoqrafik sistemlərin təhlükəsizliyi ilə bağlı artan narahatlıq var.

Bu təhlükəyə cavab olaraq, zk-STARK sübut sistemində yeganə kriptoqrafik tərkib hissəsi kimi toqquşmaya davamlı heş funksiyalarından istifadə etməklə

cəlbedici həll təklif edir. Toqquşmaya davamlı heş funksiyası ixtiyari ölçülü giriş məlumatlarını sabit ölçülü çıxışa uyğunlaşdıran kriptoqrafik primitivdir ki, eyni heş dəyərini yaradan iki fərqli girişi tapmaq hesablama baxımından qeyri-mümkündür. Bu xüsusiyyət xüsusi riyazi problemlərin sərtliyinə əsaslanmadan məlumatların bütövlüyü və həqiqiliyinin yoxlanılmasını təmin edir.

zk-STARK -ın toqquşmaya davamlı heş funksiyalarına etibar etməsinin əsas üstünlüklərindən biri onun heş funksiyasının ideallaşdırılmış modeli altında sübut edilə bilən post-kvant təhlükəsizliyidir. Kvant hücumlarına qarşı həssas ola bilən ənənəvi kriptoqrafik sxemlərdən fərqli olaraq, zk-STARK-ın təhlükəsizlik zəmanətləri hətta kvant düşmənlərinin mövcudluğunda da qorunur. Bu xüsusiyyət, kvant hücumları təhlükəsinin adi kriptoqrafik sistemlərə nisbətən daha böyük olduğu yeni yaranan kvant texnologiyaları kontekstində xüsusilə qiymətlidir.

Bundan əlavə, zk-STARK-ın toqquşmaya davamlı heş funksiyalarına etibarı səmərəlilik və sadəlik baxımından əlavə üstünlüklər təklif edir. Mürəkkəb riyazi əməliyyatlar və ya xüsusi avadanlıq tələb edə bilən digər kriptoqrafik primitivlərdən fərqli olaraq, heş funksiyaları nisbətən sadə və effektivdir. Bu sadəlik hesablama xərclərinin azaldılmasına və resurs tələblərinin azaldılmasına çevrilərək zk-STARKı geniş tətbiqlər üçün praktik və miqyaslana bilən həllə çevirir (CoinDesk, 2009).

zk-STARK-ın toqquşmaya davamlı heş funksiyalarına etibar etməsinin digər üstünlüyü onun mövcud kriptoqrafik standartlar və infrastrukturla uyğunluğudur. Heş funksiyaları kriptoqrafik protokollarda və tətbiqlərdə geniş istifadə olunduğundan, zk-STARK əhəmiyyətli dəyişikliklər və ya təkmilləşdirmələr tələb etmədən mövcud sistemlərə problemsiz şəkildə inteqrasiya edə bilir. Bu uyğunluq zk-STARK-ın real dünya ssenarilərində asanlıqla yerləşdirilməsini təmin edir və təşkilatlara geniş yenidənqurma səylərinə məruz qalmadan təhlükəsizliyini və məxfiliyi qoruyan xassələrindən istifadə etməyə imkan verir.

Çoxsaylı üstünlüklərinə baxmayaraq, zk-STARK-ın toqquşmaya davamlı heş funksiyalarına etibar etməsi də müəyyən problemlər və mülahizələr yaradır. Belə problemlərdən biri əsas heş funksiyasının həyata keçirilməsinin təhlükəsizliyini və bütövlüyünü təmin etmək ehtiyacıdır. Klassik kriptoqrafik fərziyyələr altında

toqquşmaya davamlı heş funksiyaları geniş şəkildə öyrənilsə və təhlükəsiz hesab edilsə də, kvant hesablamalarının ortaya çıxması diqqətlə həll edilməli olan yeni problemlər və təhlükələr yaradır.

Üstəlik, zk-STARK-ın toqquşmaya davamlı heş funksiyalarına etibar etməsi onu bütün növ hücumlara qarşı immunitetli etmir. Məsələn, kifayət qədər güclü kvant kompüteri potensial olaraq heş funksiyasının toqquşma müqaviməti xüsusiyyətini poza bilər və bununla da zk-STARK-ın təhlükəsizliyinə xələl gətirir. Bu riskləri azaltmaq üçün zk-STARK tətbiqləri kvant hesablamasındakı irəliləyişləri izləməli və təhlükəsizlik mexanizmlərini müvafiq olaraq uyğunlaşdırmalıdır (Petkus M , 2018).

zk-STARK-ın toqquşmaya davamlı heş funksiyalarına etibarı kriptoqrafik protokollarda post-kvant təhlükəsizliyinə nail olmaq üçün perspektivli bir yol təqdim edir. Öz sübut sistemində yeganə kriptoqrafik tərkib hissəsi kimi heş funksiyalarından istifadə etməklə, zk-STARK hətta kvant düşmənlərinin mövcudluğunda belə sübut edilə bilən təhlükəsizlik zəmanətlərinə nail olur. Bu xüsusiyyət, zk-STARK-ın effektivliyi, sadəliyi və mövcud kriptoqrafik infrastruktura uyğunluğu ilə birlikdə onu getdikcə kvantın aktivləşdiyi dünyada hesablamaların təhlükəsizliyini və məxfiliyini təmin etmək üçün cəlbedici həll yolu kimi yerləşdirir. zk-STARK təkamül etməyə davam etdikcə, kvant hesablama inkişafının yaratdığı təhlükələrə qarşı möhkəm müdafiəni təmin edərək, post-kvant kriptoqrafiyasının təməl daşı olmaq potensialına malikdir (Горячев, 2011).

- **Etibarlı Quraşdırma yoxdur:** İctimai parametrlər yaratmaq üçün etibarlı quraşdırma məsələlərinə güvənən ənənəvi zk-SNARK-lardan fərqli olaraq, STARK-ların etibarlı quraşdırması yoxdur və buna görə də kriptoqrafik zəhərli tullantılar yoxdur.

zk-STARK-da etibarlı quraşdırmanın olmaması, sıfır bilik sübutları sahəsində misilsiz təhlükəsizlik və etibarsızlıq səviyyəsini təklif edən ənənəvi kriptoqrafik protokollardan əhəmiyyətli dərəcədə uzaqlaşma deməkdir. İctimai parametrlər yaratmaq üçün etibarlı quraşdırma məsələlərinə əsaslanan zk-SNARK-lardan fərqli olaraq, zk-STARK belə bir məsələlərə ehtiyacı aradan qaldırır, bununla da

kriptoqrafik zəhərli tullantılarla bağlı potensial risklərdən qaçır və sübut sisteminin bütövlüyünü və şəffaflığını təmin edir.

zk-STARK-lar kimi ənənəvi sıfır bilik sübut sistemlərində sübutların yoxlanılması üçün vacib olan ictimai parametrləri yaratmaq üçün etibarlı quraşdırma məsələlərindən istifadə edilir. Bu məsələlər zamanı bir qrup etibarlı şəxs bu parametrləri kollektiv şəkildə yaradır və dərc edir, sonra sistemdəki bütün iştirakçılar tərəfindən sübutları yoxlamaq üçün istifadə olunur. Bu yanaşma praktikada geniş şəkildə istifadə edilsə və qəbul edilsə də, bir sıra potensial risklər və zəifliklər təqdim edir.

Etibarlı quraşdırma məsələləri ilə bağlı əsas narahatlıqlardan biri iştirakçılar arasında sövdələşmə və ya kompromis riskidir. İctimai parametrlərin yaradılması bir çox şəxslərin əməkdaşlığına əsaslandığından, bu şəxslərin bəzilərinin sübut sisteminin təhlükəsizliyinə xələl gətirəcək şəkildə parametrləri manipulyasiya etmək və ya güzəştə getmək üçün əlbir ola bilməsi ehtimalı həmişə mövcuddur. İştirakçıların ziddiyyətli maraqları və ya təşviqləri ola biləcəyi ssenarilərdə bu risk xüsusilə narahatdır (Ishai, Mahmoody, Sahai, & Xiao, 2012).

Quraşdırma məsələləri ilə bağlı başqa bir narahatlıq kriptoqrafik zəhərli tullantıların olmasıdır ki, bu da məxfi məlumatlara istinad edir ki, bu, təhlükəyə məruz qaldıqda bütün sistemin təhlükəsizliyini pozmaq üçün istifadə edilə bilər. zk-SNARK kontekstində, etibarlı quraşdırma məsələləri zamanı yaradılan ictimai parametrlər kriptoqrafik zəhərli tullantıları ehtiva edir, çünki onlar yalnız iştirakçılara məlum olan məxfi məlumatlardan əldə edilir. Bu məxfi məlumat sızdırılarsa və ya ələ keçirilərsə, bu, potensial olaraq təcavüzkarın yalan sübutlar yaratmasına və ya sistemin məxfilik zəmanətlərini pozmasına icazə verə bilər.

zk-STARK-da etibarlı quraşdırmanın olmaması bu narahatlıqları aradan qaldırır və sübut sisteminin bütövlüyünü və şəffaflığını təmin edir. Etibarlı quraşdırma məsələlərinə ehtiyac olmadan zk-STARK sövdələşmə, kompromis və kriptoqrafik zəhərli tullantılarla bağlı risklərin qarşısını alır və bununla da protokolun təhlükəsizliyini və etibarlılığını artırır. Etibarlı şəxslər qrupu tərəfindən yaradılan ictimai parametrlərə etibar etmək əvəzinə, zk-STARK mahiyyət etibarilə təhlükəsiz

və yoxlanıla bilən sübutlar yaratmaq üçün polinom öhdəlikləri və səhvləri düzəltmə kodları kimi kriptoqrafik üsullardan istifadə edir.

zk-STARK-ın etibarlı quraşdırma yanaşmasının əsas üstünlüklərindən biri onun şəffaflığı və yoxlanılabilirliyidir. zk-STARK sübutları heç bir məxfi məlumat və ya etibarlı tərəflərə güvənmədən qurulduğundan, sübuta çıxışı olan hər kəs onun düzgünlüyünü və bütövlüyünü müstəqil şəkildə yoxlaya bilər. Bu şəffaflıq, maraqlı tərəflərin mərkəzləşdirilmiş orqanlara və ya etibarlı vasitəçilərə etibar etmədən əməliyyatların və hesablamaların etibarlılığını yoxlaya biləcəyi qeyri-mərkəzləşdirilmiş ekosistemlər daxilində etibarı artırır.

Bundan əlavə, zk-STARK-da etibarlı quraşdırmanın olmaması protokolun yerləşdirilməsini və qəbulunu asanlaşdırır, çünki o, mürəkkəb və potensial riskli məsələlərin əlaqələndirilməsi və icrasına ehtiyacı aradan qaldırır. Etibarlı quraşdırma məsələlərləri ilə əlaqəli logistik problemlər və təhlükəsizlik problemləri olmadan, zk-STARK mövcud sistemlərə və tətbiqlərə daha asanlıqla inteqrasiya oluna bilər, bu da təşkilatlara geniş yenidənqurma səylərinə məruz qalmadan təhlükəsizlik və məxfiliyi qoruyan xassələrindən istifadə etməyə imkan verir (Zaghloul, Li , Mutka, & Ren, 2020).

Çoxsaylı üstünlüklərinə baxmayaraq, zk-STARK-da etibarlı quraşdırmanın olmaması da müəyyən çətinliklər və mülahizələr yaradır. Belə çətinliklərdən biri sübutların qurulması üçün istifadə olunan kriptoqrafik üsulların təhlükəsizliyini və bütövlüyünü təmin etmək ehtiyacıdır. zk-STARK etibarlı quraşdırma məsələlərləri ilə bağlı riskləri aradan qaldırsa da, sübut sisteminin möhkəmliyini təmin etmək üçün hələ də təhlükəsiz kriptoqrafik primitivlərə və alqoritmlərə etibar etməlidir.

zk-STARK-da etibarlı quraşdırmanın olmaması, etibarlı quraşdırmanın zəruri və ya arzuolunan hesab edildiyi müəyyən ssenarilərdə onun tətbiqini məhdudlaşdıra bilər. Məsələn, iştirakçıların tanındığı və güvəndiyi tətbiqlərdə etibarlı quraşdırma məsələləri əlavə təminat və təhlükəsizlik təminatları verə bilər. Belə hallarda, zk-STARK tətbiqin xüsusi tələblərinə cavab vermək üçün əlavə mexanizmlər və ya protokollarla gücləndirilməlidir.

Bu təsnifat zk-STARK-ın əsasını təşkil edən riyazi və kriptoqrafik prinsiplərin yüksək səviyyəli icmalını təqdim edir. Sadə zk-STARK sübutunu daha ətraflı öyrənmək üçün Berentsen, Lenzi və Nyffenegger-nin işinə müraciət edə bilərsiniz.

Yekun olaraq, zk-STARK-da etibarlı quraşdırmanın olmaması, ənənəvi kriptoqrafik protokollarla müqayisə olunmayan təhlükəsizlik, şəffaflıq və etibarsızlıq səviyyəsini təklif edən sıfır bilik sübutları sahəsində əhəmiyyətli irəliləyişdir. Etibarlı quraşdırma mərasiminə ehtiyacı aradan qaldıraraq, zk-STARK sövdələşmə, kompromis və kriptoqrafik zəhərli tullantılarla bağlı risklərin qarşısını alır və bununla da protokolun bütövlüyünü və etibarlılığını artırır. zk-STARK inkişaf etməyə davam etdikcə, onun heç bir etibarlı quraşdırma yanaşması müxtəlif sənaye və tətbiqlərdə mərkəzləşdirilməmiş sistemlərə innovasiya və inamı gücləndirmək potensialına malikdir (Chainlink Community, 2009).

2.2. zk-STARK tranzaksiyaların şifrələnməsi üçün tətbiq metodları

Bu sistem hesablamalarda istifadə edilən girişlər haqqında heç bir məlumatı aşkar etmədən hesablamaların yoxlanılmasına imkan verir. Burada zk-STARK əməliyyatlarının şifrələnməsi üçün tətbiq üsullarını araşdırırıq.

- **Blokçeyn şəbəkələri**

zk-STARK-ların əsas tətbiqlərindən biri blokçeyn şəbəkələrindədir. Blokçeyn texnologiyası şəffaflıq və təhlükəsizliyə əsaslanır və zk-STARK-lar şəxsi əməliyyatları və qorunan ağıllı müqavilələri təmin etməklə bu aspektləri təkmilləşdirə bilər. Blokçeyn şəbəkəsində istifadəçi əməliyyatın və ya müqavilənin təfərrüatlarını gizli saxlayaraq əməliyyat həyata keçirə və ya ağıllı müqavilə icra edə bilər. Bu, şəbəkəyə əməliyyatın və ya müqavilənin konkret detalları bilmədən düzgünlüyünü yoxlamağa imkan verən zk-STARK-lardan istifadə etməklə əldə edilir. (Яковлев & Сычева, 2017).

- **Maliyyə Təhlükəsizliyi Tətbiqləri**

zk-STARK-ların maliyyə təhlükəsizliyində də tətbiqləri var. Məsələn, əməliyyatların məxfiliyini və təhlükəsizliyini təmin etmək üçün blokçeyn əsaslı ödəniş sistemlərində istifadə edilə bilər. zk-STARK-lardan istifadə etməklə,

əməliyyatın təfərrüatları şifrələnmiş qala bilər, lakin hələ də etibarlı kimi təsdiqlənə bilər. Bu, ödəniş sisteminin ümumi təhlükəsizliyini artırmaqla təhlükəsiz və şəxsi maliyyə əməliyyatlarına imkan verir.

- **Şəxsiyyətin doğrulanması**

zk-STARK-ların başqa bir tətbiqi şəxsiyyət yoxlama sistemlərindədir. Belə sistemlərdə istifadəçi müəyyən xidmətlərə və ya məlumatlara daxil olmaq üçün öz şəxsiyyətini sübut etməli ola bilər. Bununla belə, həssas şəxsiyyət məlumatlarının açıqlanması məxfilik riskləri yarada bilər. zk-STARK bu sistemlərdə heç bir həssas məlumatı açıqlamadan şəxsiyyətini sübut etmək üçün istifadə edilə bilər. Bu, istifadəçinin məxfiliyinin qorunmasını təmin edir, eyni zamanda effektiv şəxsiyyətin yoxlanılmasına imkan verir.

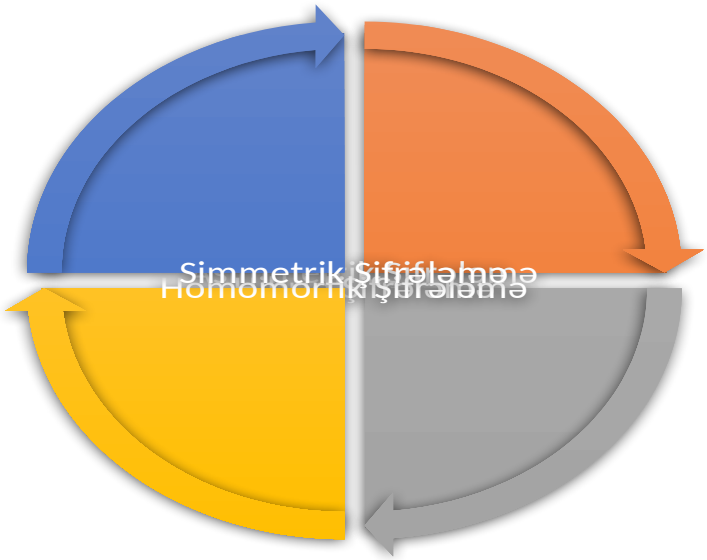
Şəkil 2.1: Zk-stark tranzaksiyalarda şəxsiyyət doğrulaması nümunəsi

- **zk-Rollup Proqramları**

zk-STARK-lar zk-Rollup proqramlarında da istifadə edilə bilər. zk-Rollup birdən çox köçürməni bir tranzaksiyada birləşdirən Layer 2 miqyaslı həlldir. Bu, zəncirdə saxlanmalı olan məlumatların miqdarını azaldır və bununla da blokçeynin miqyasını yaxşılaşdırır. zk-STARK-lar paketləşdirilmiş əməliyyatların məxfiliyini və bütövlüyünü təmin etmək üçün bu proqramlarda istifadə edilə bilər.

zk-STARK-da əməliyyatların şifrələnməsi həssas məlumatların məxfiliyini təmin etməklə yanaşı, əməliyyatların etibarlılığının şəffaf şəkildə yoxlanılmasına imkan verir. Bu proses təhlükəsizlik, məxfilik və yoxlanılabilirlik arasında düzgün tarazlığı yaratmaq üçün müxtəlif şifrələmə üsulları və üsullarının diqqətlə nəzərdən

keçirilməsini tələb edir (Abdolmaleki, Baghery, Lipmaa, & Zajac, 2019). Biz həm simmetrik, həm də asimmetrik şifrələmə yanaşmalarını, həmçinin onların məxfilik, səmərəlilik və təhlükəsizlik üçün təsirlərini nəzərə alaraq zk-STARK əməliyyatlarının şifrələnməsi üçün bəzi tətbiq üsullarını araşdıracağıq.(Şəkil 2.2)



Şəkil 2.2: zk-STARK əməliyyatlarının şifrələnməsi üçün bəzi tətbiq üsulları

✓ **Simmetrik Şifrələmə**

Simmetrik şifrələmə məlumatların həm şifrələnməsi, həm də deşifrə edilməsi üçün bir açardan istifadəni nəzərdə tutur. zk-STARK əməliyyatları kontekstində simmetrik şifrələmə sadəlik və səmərəlilik təklif edərək, onu böyük həcmli məlumatların şifrələnməsi üçün praktik seçim edir (Ümumi bir simmetrik şifrələmə alqoritmi, təhlükəsizliyi və performansı üçün geniş istifadə olunan AES (Advanced Encryption Standard).

zk-STARK əməliyyatlarında əməliyyat məbləğləri, göndərici və alıcı ünvanları və hər hansı digər həssas məlumat kimi daxilolma məlumatlarını şifrələmək üçün simmetrik şifrələmə tətbiq oluna bilər. Şifrələnmiş məlumatlar daha sonra zk-STARK sübutuna daxil edilə bilər ki, bu da yoxlayıcılara əsas açıq mətn məlumatlarını aşkar etmədən əməliyyatın düzgünlüyünü təsdiq etməyə imkan verir (Елистратов, Маршалко, & Светушкин, 2019).

Bununla belə, simmetrik şifrələmə ilə bağlı problemlərdən biri əsas idarəetmədir. Eyni açar həm şifrələmə, həm də şifrənin açılması üçün istifadə edildiyi

üçün şifrələnmiş məlumatlara icazəsiz girişin qarşısını almaq üçün şifrələmə açarlarını təhlükəsiz şəkildə yaymaq və idarə etmək çox vacibdir. Bu, şifrələmə prosesinin təhlükəsizliyini təmin etmək üçün möhkəm açar idarəetmə protokollarının və infrastrukturun tətbiqini tələb edə bilər.

✓ **Asimmetrik Şifrələmə**

Açıq açar şifrələməsi kimi də tanınan asimmetrik şifrələmə bir cüt açarın istifadəsini nəzərdə tutur: şifrələmə üçün açıq açar və şifrənin açılması üçün şəxsi açar. Bu yanaşma simmetrik şifrələmə ilə müqayisədə daha güclü təhlükəsizlik təminatları təklif edir, çünki o, şifrələmə açarlarını tərəflər arasında paylaşmaq ehtiyacını aradan qaldırır.

zk-STARK əməliyyatlarında, alıcının açıq açarından istifadə edərək həssas məlumatları şifrələmək üçün asimmetrik şifrələmədən istifadə edilə bilər. Bu, yalnız müvafiq şəxsi açara malik olan nəzərdə tutulan alıcının açıq mətn məlumatlarını deşifrə edə və əldə edə biləcəyini təmin edir. Asimmetrik şifrələmə daha yüksək səviyyəli məxfilik və məxfilik təmin edir, çünki şifrələmə açarının tərəflər arasında bölüşdürülməsinə ehtiyac yoxdur (Zaghloul, Li, Mutka, & Ren, 2015).

Tez-tez istifadə olunan asimmetrik şifrələmə alqoritmi Rivest-Şamir-Adleman (RSA) alqoritmidir ki, bu da təhlükəsiz rabitə və məlumatların şifrələnməsi üçün geniş şəkildə tətbiq edilir. ECC (Elliptic Curve Cryptography) kimi digər alternativlər daha kiçik açar ölçüləri ilə oxşar təhlükəsizlik xassələri təklif edir ki, bu da onları resurs məhdud mühitlər üçün yaxşı uyğunlaşdırır (Sun, Yu, Zhang, Sun, Xie, & Peng, 2021).

RSA alqoritmi ilə asimmetrik şifrələmənin riyazi təsviri belədir. Açar cütlərinin yaradılması:

İki böyük ədədi seçin, və q. Bunlar sadə ədədlər olmalıdır.

$$n=p \qquad (2.1.18)$$

hesablayın. Bu, modulyus kimi istifadə olunur.

(2.1.19)

olan bir ədədi seçin, belə ki, qarşılıqlı sadə olsun.

d belə bir ədədi hesablayın ki,

(2.1.20)

Nəticədə, açıq açar (*e*,*n*) və gizli açar (*d*,*n*) olacaq.

Şifrələmə:

Məlumatın mətni olmalıdır.

Şifrələnmiş mətn *C* belə hesablanır:

(2.1.21)

Deşifrələmə:

Şifrələnmiş mətn C-ni, gizli açar (*d*,*n*) istifadə edərək deşifrə etmək:

$$M = \bmod n \qquad (2.1.22)$$

C- şifrələnmiş mətn.

e- açıq açar.

d- gizli açar.

və *q*- sadə açar.

Bununla belə, asimmetrik şifrələmə simmetrik şifrələmə ilə müqayisədə əlavə hesablama xərclərini təqdim edə bilər, çünki adətən şifrələmə və şifrənin açılması əməliyyatlarını yerinə yetirmək üçün daha çox hesablama resursları tələb olunur. Bu əlavə məsrəf zk-STARK tranzaksiyalarının səmərəliliyinə və miqyasına təsir edə bilər, xüsusən də yüksək əməliyyat həcmi və ya məhdud hesablama resursları olan ssenarilərdə.

✓ **Hibrid Şifrələmə**

Hibrid şifrələmə məlumatları şifrələmək üçün simmetrik şifrələmə və şifrələmə açarını təhlükəsiz şəkildə paylaşmaq üçün asimmetrik şifrələmədən istifadə etməklə simmetrik və asimmetrik şifrələmənin üstünlüklərini birləşdirir. Bu yanaşma böyük həcmli məlumatların şifrələnməsi üçün simmetrik şifrələmənin səmərəliliyindən

istifadə etməklə yanaşı, əsas idarəetmə üçün asimmetrik şifrələmənin təhlükəsizlik zəmanətlərindən faydalanır.

zk-STARK əməliyyatlarında təsadüfi yaradılan simmetrik şifrələmə açarından istifadə edərək həssas məlumatları şifrələmək üçün hibrid şifrələmə tətbiq oluna bilər. Simmetrik olaraq şifrələnmiş məlumatlar, alıcının açıq açarı ilə birlikdə zk-STARK sübutuna daxil edilə bilər. Təsdiq edildikdən sonra, alıcı simmetrik şifrələmə açarının şifrəsini açmaq üçün şəxsi açarından istifadə edə və sonra şifrələnmiş məlumatı deşifrə edə bilər.

Hibrid şifrələmə təhlükəsizlik, səmərəlilik və miqyaslılıq arasında praktiki uzlaşma təklif edir və onu zk-STARK əməliyyatları üçün yaxşı uyğunlaşdırır. Məlumatların şifrələnməsi üçün simmetrik şifrələmədən və açarların idarə edilməsi üçün asimmetrik şifrələmədən istifadə etməklə hibrid şifrələmə zk-STARK əməliyyatlarının məxfiliyini və bütövlüyünü təmin etmək üçün möhkəm və səmərəli həll yolu təqdim edir.

✓ **Homomorfik Şifrələmə**

Homomorfik şifrləmə, şifrənin açılmasına ehtiyac olmadan şifrələnmiş verilənlər üzərində hesablamaların aparılmasına imkan verən şifrələmə sxeminin xüsusi növüdür. Bu xüsusiyyət əsas məlumatların məxfiliyini qoruyarkən tərəflərə şifrələnmiş zk-STARK əməliyyatları üzrə hesablamalar aparmağa imkan verir.

zk-STARK tranzaksiyalarında, əməliyyat məbləğlərinin yoxlanılması və ya toplama əməliyyatlarının yerinə yetirilməsi kimi şifrələnmiş əməliyyat məlumatlarında hesablamaların aparılması üçün homomorfik şifrələmə tətbiq oluna bilər. Homomorfik şifrələmədən istifadə etməklə tərəflər əsas məlumatların məxfiliyinə xələl gətirmədən zk-STARK əməliyyatlarını təhlükəsiz şəkildə emal edə və təhlil edə bilərlər.

Homomorfik Şifrələmə Üsulları

Cəmi saxlayan homomorfik şifrələmə:

Şifrələnmiş məlumatlar üzərində toplama əməliyyatını dəstəkləyir.

$$E(a)+E(b)=E(a+b) \qquad (2.1.23)$$

Vurmanı saxlayan homomorfik şifrələmə:

Şifrələnmiş məlumatlar üzərində vurma əməliyyatını dəstəkləyir.

$$E(a)\cdot E(b)=E(a\cdot b) \tag{2.1.24}$$

Tam homomorfik şifrələmə:

Həm toplama, həm də vurma əməliyyatlarını dəstəkləyir.

$$E(a+b)=E(a)\oplus E(b) \tag{2.1.25}$$

$$E(a\cdot b)=E(a)\otimes E(b) \tag{2.1.26}$$

Burada E(a) – a məlumatının şifrələnmiş forması

Burada E(b) – b məlumatının şifrələnmiş forması

Bununla belə, homomorfik şifrələmə sxemləri hesablama baxımından intensiv ola bilər və zk-STARK əməliyyatlarına əlavə mürəkkəblik gətirə bilər. Bundan əlavə, homomorfik şifrələmə sxemləri adətən yerinə yetirilə bilən hesablama növləri üzrə məhdudiyyətlərə malikdir və bu, zk-STARK əməliyyatlarının çevikliyinə və funksionallığına təsir göstərə bilər.

zk-STARK əməliyyatlarının şifrələnməsi əməliyyatların məxfiliyini, bütövlüyünü və yoxlanılmasını təmin etmək üçün müxtəlif şifrələmə üsul və üsullarının diqqətlə nəzərdən keçirilməsini nəzərdə tutur. Simmetrik şifrələmə sadəlik və səmərəlilik təklif edir, lakin möhkəm açar idarəetmə protokollarını tələb edir. Asimmetrik şifrələmə daha güclü təhlükəsizlik təminatları təmin edir, lakin hesablama yükü əlavə edə bilər (Sun, Yu, Zhang, Sun, Xie, & Peng, 2021). Hibrid şifrələmə təhlükəsizlik və səmərəlilik arasında praktiki uzlaşma üçün simmetrik və asimmetrik şifrələmənin üstünlüklərini birləşdirir. Homomorfik şifrləmə, şifrələnmiş məlumatların şifrəsini açmadan hesablamaları yerinə yetirməyə imkan verir, təkmilləşdirilmiş məxfilik və məxfilik təklif edir. Nəhayət, şifrələmə metodunun seçimi təhlükəsizlik, səmərəlilik və funksionallıq arasında mübadiləleri tarazlayan zk-STARK əməliyyat mühitinin xüsusi tələblərindən və məhdudiyyətlərindən asılıdır.

Nəticə olaraq, zk-STARK müxtəlif tətbiqlərdə, xüsusən də blokçeyn texnologiyasında məxfiliyin və bütövlüyün qorunması üçün möhkəm həll təklif edir. Onların hesablamalarda istifadə edilən girişlər haqqında heç bir məlumat vermədən hesablamaları yoxlamaq qabiliyyəti onları bugünkü rəqəmsal əsrdə əvəzolunmaz alətə çevirir. Bu sahədə tədqiqat və inkişaf davam etdikcə, gələcəkdə zk-STARK-ların daha da innovativ tətbiqlərini görəcəyimizi gözləyə bilərik.

2.3. Blokçeyn və zk-STARK ın əsas konseptləri

ZKP bir tərəfə (təsdiq edən) digər tərəfi (təsdiq edən) heç bir əlavə məlumat vermədən ifadənin doğru olduğuna inandırmağa imkan verən kriptoqrafik bir texnikadır. Başqa sözlə, ZKP sizə biliyin özünü üzə çıxarmadan bir şey haqqında biliyi sübut etməyə imkan verir.

Nümunə üçün deyək ki, adınızı və ya pasport nömrənizi açıqlamadan kimməsə vətəndaşlığınızı sübut etmək istəyirsiniz. ZKP identifikasiya həlli ilə siz şəxsi məlumatlarınızı açıqlamadan vətəndaşlığınızı təsdiq edə bilərsiniz.

İdentifikasiya ilə yanaşı, ZKP-lər müxtəlif sistemlərin məxfiliyini, təhlükəsizliyini və səmərəliliyini artırmaq üçün müxtəlif sahələrdə istifadə olunur. (Şəkil 2.3)

Şəkil 2.3: zk-STARK-ın əsas xüsusiyyətləri

zk-STARK-ın əsas xüsusiyyətlərinin açıqlaması aşağıdakılardır:

1.**Təkmilləşdirilmiş Təhlükəsizlik:** zk-STARK daha yüksək səviyyəli təhlükəsizlik təmin edən qabaqcıl kriptoqrafik üsullardan istifadə edir. Bu, blokçeyn texnologiyasında həssas tətbiqlər üçün xüsusilə vacibdir.

2.**Daha Yüksək Ölçmə qabiliyyəti:** zk-STARK miqyaslılığı əhəmiyyətli dərəcədə təkmilləşdirir, geniş yayılmış blokçeyn tətbiqləri üçün vacib olan böyük əməliyyat həcmlərinin səmərəli işlənməsinə imkan verir.

3.**Şəffaflıq və Etibarlılıq:** zk-STARK etibarlı konfiqurasiya tələb etmir, bu da sistemin potensial kompromislərə qarşı həssaslığını azaltmaqla istifadəçilər arasında şəffaflığı və etibarı artırır.

4.**Kvant Müqaviməti:** zk-STARK -lar kvant hesablama hücumlarına davamlı olmaq üçün nəzərdə tutulmuşdur və texnologiyanın gələcək mümkün təhlükələrdən qorunmasını təmin edir.

Blokçeyn, yarandığı gündən bəri böyük populyarlıq və əhəmiyyət qazanmış inqilabi bir texnologiyadır. Özündə blokçeyn bir çox kompüterlər arasında əməliyyatları təhlükəsiz, şəffaf və dəyişməz şəkildə qeyd edən mərkəzləşdirilməmiş, paylanmış kitabdır. Texnologiya əvvəlcə kriptovalyutalar, xüsusən Bitcoin üçün əsas çərçivə kimi ortaya çıxdı, lakin onun potensial tətbiqləri rəqəmsal valyutalardan çox kənara çıxır.

Blokçeynin əsas prinsiplərindən biri mərkəzsizləşdirmədir, yəni heç bir qurum bütün şəbəkəyə nəzarət edə bilməz. Bunun əvəzinə əməliyyatlar konsensus mexanizmi vasitəsilə təsdiqlənir və blokçeynə əlavə olunur, adətən işin sübutu və ya mədənçilər və ya validatorlar kimi tanınan şəbəkə iştirakçılarının iştirak etdiyi payın sübutudur.

Blokçeyn, hər bir iştirakçının və ya qovşaqın bütün kitabçanın surətini saxladığı peer-to-peer şəbəkəsində işləyir. Bu, şəffaflığı təmin edir və bir nöqtədə uğursuzluq və ya manipulyasiya riskini azaldır. Bundan əlavə, blokçeyn əməliyyatların təhlükəsizliyini təmin etmək üçün kriptoqrafik üsullardan istifadə edir, əməliyyat qeydə alındıqdan sonra onun şəbəkədən konsensus olmadan dəyişdirilə və ya silinə bilməyəcəyini təmin edir.

Blokçeyn texnologiyasının potensial tətbiqləri geniş və müxtəlifdir. Kriptovalyutalardan başqa, blokçeyn təchizat zəncirinin idarə edilməsi, şəxsiyyətin yoxlanılması, səsvermə sistemləri, səhiyyə qeydlərinin idarə edilməsi və sair üçün istifadə edilə bilər. Onun əməliyyatların saxta və şəffaf qeydini təmin etmək qabiliyyəti onu əməliyyatlarında təhlükəsizliyi, səmərəliliyi və etibarı artırmaq istəyən sənayelər üçün ideal həll edir.

zk-STARK və Blokçeyn Əlaqəsi:

zk-STARK bir tərəfə hər hansı əlavə məlumatı açıqlamadan ifadənin doğru olduğunu digər tərəfə sübut etməyə imkan verən kriptoqrafik üsuldur. zk-STARK əvvəlki həllərlə müqayisədə miqyaslılığı və şəffaflığı artıraraq, sıfır bilik sübutları konsepsiyasına əsaslanır.

zk-STARK və blokçeyn arasındakı əlaqə rəqəmsal əməliyyatlarda məxfiliyi, təhlükəsizliyi və səmərəliliyi artırmaq kimi ortaq məqsədlərindən ibarətdir. Blokçeyn kontekstində zk-STARK əməliyyat məxfiliyi, genişlənmə və qarşılıqlı fəaliyyət kimi əsas problemləri həll etmək üçün müxtəlif istifadə hallarına tətbiq edilə bilər.

Blokçeyndə zk-STARK-ın əsas tətbiqlərindən biri əməliyyat məxfiliyini artırmaqdır. Bitcoin və ya Ethereum kimi ictimai blokçeyndə əməliyyatlar istifadəçilərin məxfiliyinə xələl gətirərək şəbəkədəki hər kəsə görünür. zk-STARK, blokçeynin bütövlüyünü təmin edərkən əməliyyatın təfərrüatlarının gizlədildiyi şəxsi əməliyyatlar yaratmağa imkan verir (Habr, 2009).

Bundan əlavə, zk-STARK tranzaksiyaların yoxlanılması üçün tələb olunan hesablama əlavə xərclərini azaltmaqla blokçeyn şəbəkələrinin miqyasını yaxşılaşdıra bilər. İşin sübutu kimi ənənəvi konsensus mexanizmləri resurs tutumlu ola bilər, əməliyyatların ötürülməsini məhdudlaşdırır. zk-STARK tətbiq etməklə, blokçeyn şəbəkələri təhlükəsizliyi itirmədən daha yüksək əməliyyat ötürmə qabiliyyətinə nail ola bilər.

Üstəlik, zk-STARK fərqli platformalarda əməliyyatları yoxlamaq üçün standartlaşdırılmış metod təqdim etməklə müxtəlif blokçeyn şəbəkələri arasında

qarşılıqlı əlaqəni asanlaşdırır. Bu qarşılıqlı fəaliyyət müxtəlif şəbəkələr arasında aktivlərin və məlumatların mübadiləsinə imkan verən qüsursuz və bir-biri ilə əlaqəli blokçeyn ekosisteminin inkişafı üçün vacibdir.

zk-STARK -ın blokçeyn-də tətbiqi:

✓ Artırılmış əməliyyat məxfiliyi: zk-STARK sizə məlumatların məxfi saxlanılmasını və əməliyyatın bütövlüyünün yoxlanılmasını təmin edərək, blokçeyn şəbəkələrində şəxsi əməliyyatlar həyata keçirməyə imkan verir.

✓ Ağıllı Müqavilələr: Artan səmərəlilik və təhlükəsizlik ilə zk-STARK ağıllı müqavilələrin performansını və etibarlılığını əhəmiyyətli dərəcədə yaxşılaşdıra bilər.

✓ Çarpaz Zəncirli Birlikdə İşləmələk: zk-STARK müxtəlif blokçeyn şəbəkələri arasında təhlükəsiz və səmərəli qarşılıqlı əlaqəni asanlaşdırır, blokçeyn ekosistemində qarşılıqlı fəaliyyətə kömək edir.

zk-STARK -ın əsas anlayışları:

Sıfır Bilik isbatları: zk-STARK sıfır bilik sübutlarına, bir tərəfə (təsdiq edənə) sirri digər tərəfə (təsdiqləyici) açıqlamadan sirr haqqında məlumatı nümayiş etdirməyə imkan verən kriptoqrafik texnikaya əsaslanır. Bu, məxfiliyi və məxfiliyi təmin edir, eyni zamanda proverin iddiasının yoxlanılmasına imkan verir.

Miqyaslılıq: zk-STARK yüksək miqyaslana bilən, böyük həcmdə əməliyyatları səmərəli şəkildə idarə etmək üçün nəzərdə tutulmuşdur. Performans məhdudiyyətlərindən əziyyət çəkə biləcək bəzi digər sıfır bilik sübut sistemlərindən fərqli olaraq, zk-STARK təkmilləşdirilmiş miqyaslılıq təklif edir, bu da onu geniş miqyaslı blokçeyn şəbəkələrində və yüksək ötürmə qabiliyyəti tələb edən digər tətbiqlərdə istifadə üçün uyğun edir.

Şəffaflıq və Yoxlanılabilirlik: zk-STARK sübut yaratma prosesində şəffaflıq və yoxlanıla bilənliyi təmin edir. Bu o deməkdir ki, hər kəs proverin məxfi məlumatlarına giriş tələb etmədən zk-STARK sübutunun etibarlılığını yoxlaya bilər. Bu şəffaflıq sistemin bütövlüyünə inamı və inamı artırır (Gennaro, 2013).

Kvant Hesablamalarına Müqavimət: zk-STARK ənənəvi kriptoqrafik sistemlər üçün potensial təhlükə yaradan kvant kompüterlərinin hücumlarına davamlı

olmaq üçün nəzərdə tutulmuşdur. Qabaqcıl kriptoqrafik üsullardan istifadə etməklə, zk-STARK hətta kvant hesablamalarından irəli gələn təhdidlər qarşısında möhkəm təhlükəsizlik təklif edir.

Universal Tətbiq: zk-STARK blokçeyndən kənar tətbiqləri olan çox yönlü kriptoqrafik vasitədir. O, rəqəmsal əməliyyatlar və məlumatların idarə edilməsində məxfilik, təhlükəsizlik və səmərəliliyi artırmaq üçün kibertəhlükəsizlik, maliyyə, səhiyyə və daha çox kimi müxtəlif sahələrdə istifadə oluna bilər (Abdolmaleki, Baghery, Lipmaa, & Zajac, 2019).

Nəticə olaraq, blokçeyn və zk-STARK müxtəlif sənayelərdə inqilab etmək üçün böyük vədlər verən iki təməlqoyma texnologiyasını təmsil edir. Mərkəzsizləşdirmə, şəffaflıq və kriptoqrafik təhlükəsizlik prinsiplərindən istifadə etməklə bu texnologiyalar bugünkü rəqəmsal mənzərənin bəzi ən aktual problemlərinə həllər təklif edir. Blokçeyn inkişaf etməyə və əhatə dairəsini genişləndirməyə davam etdikcə və zk-STARK miqyaslılıq və istifadəyə yararlılıq baxımından irəlilədikcə, bir çox sektorda yenilik və pozulma potensialı sonsuzdur.

zk-STARK ilə gələcək:

zk-STARK-ın tətbiqi blokçeyn texnologiyası sahəsində əhəmiyyətli irəliləyişi təmsil edir. Miqyaslılıq, təhlükəsizlik və məxfiliyin əsas problemlərini həll etməklə, zk-STARK-lar daha etibarlı, səmərəli və təhlükəsiz rəqəmsal əməliyyatlar üçün yol açır. Blokçeyn texnologiyası inkişaf etdikcə, mərkəzləşdirilməmiş rəqəmsal qarşılıqlı əlaqənin gələcəyinin formalaşmasında zk-STARK-ın rolu mühüm olaraq qalır.

III FƏSİL. SIFIR BİLİK İSBATININ SSENARİ MEXANİZMİNİN TƏHLİLİ

3.1. Kriptovalutada zk-STARK ın rolu

Kriptovalyutalar əməliyyatlar və məlumatların saxlanması üçün mərkəzləşdirilməmiş və təhlükəsiz həllər təklif edərək, maliyyə və texnologiya mənzərəsini dəyişdirdi. Bununla belə, məxfilik, miqyaslılıq və təhlükəsizlik kimi problemlər davam edir və onların geniş yayılmasına mane olur. zk-STARK kriptoqrafik texnika bu problemləri həll etmək üçün perspektivli həll yolu kimi ortaya çıxdı. Bu dissertasiya zk-STARK -ın kriptovalyutadakı rolunu araşdırır, onun məxfiliyə, genişlənməyə və təhlükəsizliyə verdiyi töhfələrə diqqət yetirir. Kriptovalyuta dünyasında STARK-lar əməliyyatların yoxlanılması zamanı məxfiliyin təmin edilməsində mühüm rol oynayır. Bu kriptoqrafik alətlər əməliyyatın göndəricisinə ünvanlar və ya əməliyyat məbləğləri kimi həssas detalları açıqlamadan kifayət qədər vəsaitə və düzgün şəxsi açara malik olmaq kimi bütün zəruri şərtlərin yerinə yetirildiyini sübut etməyə imkan verir. Bu, müəyyən blokçeyn qaydalarını starka kodlaşdırmaqla əldə edilir (Zaghloul, Li, Mutka, & Ren, 2020).

zk-STARK mahiyyətcə, bir sıra transformasiyalar vasitəsilə orijinal hesablamanı çox xüsusi riyazi formata çevirməklə müəyyən hesablamanın baş verdiyini yoxlayır. Məsələn, parolun mülkiyyətinin sübutunda faktiki ifadə hashing alqoritmindən istifadə edərək parolun aydın mətndə ötürülməsinin funksional ekvivalentinə çevrilir. Bu çevrilmə prosesi vacibdir, çünki o, funksiyanı orijinal məlumatları aşkar etmədən effektiv şəkildə yoxlanıla bilən formata çevirir.

Onları yaratmaq üçün prover kriptoqrafik tapmacalar kimi xidmət edən çoxhədli tənliklər yaradır. Bu tənliklər onlarda mühüm rol oynayır və məlumatı aşkar etmədən ötürmək üçün təhlükəsiz üsul yaradır. Təsadüfilik bu prosesdə böyük əhəmiyyət kəsb

edir, çünki o, hər bir sübuta özünəməxsus cəhət əlavə edir və əks mühəndisliyin qarşısını alır (Petkus, 2018).

Rəqəmsal imzalar STARK-ın fəaliyyətində də mühüm rol oynayır. Prover açar cütü (ictimai və özəl) yaradır və əməliyyatı imzalamaq üçün şəxsi açardan istifadə edir. Bu əməliyyat daha sonra onun etibarlılığının riyazi sübutunu təmin edən STARK-a kodlanır. Bu sübut açıq açarla birlikdə validatora göndərildikdə, əməliyyat haqqında əlavə məlumat almadan əməliyyatın etibarlılığını tez və səmərəli şəkildə yoxlaya bilər.

Bundan əlavə, zk-STARK post-kvant təhlükəsizliyini təmin edir, yəni bir çox ənənəvi kriptoqrafik üsullar üçün təhlükə yaradan kvant kompüterlərinin mövcudluğunda belə təhlükəsiz olaraq qalır. Bu xüsusiyyətlər zk-STARK-ı kriptovalyutaların məxfiliyini, genişlənməsini və təhlükəsizliyini artırmaq üçün cəlbedici bir həll edir.

Məxfilik kriptovalyuta əməliyyatlarında əsas narahatlıq doğurur, çünki ənənəvi blokçeyn şəbəkələri çox vaxt həssas əməliyyat təfərrüatlarını ictimaiyyətə açıqlayır. zk-STARK məxfi əməliyyatlar və özəl ağıllı müqavilələr kimi məxfiliyi artıran xüsusiyyətlərin həyata keçirilməsinə imkan verir.

Məxfi əməliyyatlar əməliyyatların məbləğlərini və ya göndərən/qəbuledici ünvanlarını açıqlamadan əməliyyatların etibarlılığını sübut etmək üçün zk-STARK-dan istifadə edir. Bu, tranzaksiya təfərrüatlarının məxfi qalmasını təmin edir, eyni zamanda şəbəkə iştirakçıları tərəfindən təhlükəsiz yoxlamaya imkan verir.

Şəxsi ağıllı müqavilələr zk-STARK-dan istifadə edərək şifrlənmiş məlumatlar üzərində mürəkkəb hesablamaları yerinə yetirir və tərəflərə həssas məlumatları bir-birinə və ya ictimaiyyətə açıqlamadan qarşılıqlı əlaqə yaratmağa imkan verir. Bu, müxtəlif sənayelərdə mərkəzləşdirilməmiş tətbiqlər üçün yeni imkanlar açaraq, ağıllı müqavilə əməliyyatlarının məxfiliyini və məxfiliyini artırır.

Onu kriptovalyuta protokollarına inteqrasiya etməklə tərtibatçılar istifadəçi məxfiliyini artıra, fərdlər və müəssisələr arasında daha çox inam və qəbulu gücləndirə bilər (Ethereum Foundation, 2009).

Ənənəvi blokçeyn şəbəkələri bütün şəbəkə iştirakçılarından hər bir tranzaksiyanı yoxlamağı tələb edir və bu, şəbəkə böyüdükcə miqyaslılıq problemlərinə səbəb olur. zk-STARK ilə əməliyyatlar daha tez və effektiv şəkildə yoxlanıla bilər ki, bu da blokçeyn şəbəkələrinə təhlükəsizlik və ya mərkəzsizləşdirmədən ödün vermədən əməliyyatların daha yüksək ötürmə qabiliyyətini emal etməyə imkan verir.

Bundan əlavə, zk-STARK şəbəkə iştirakçılarının ümumi hesablama yükünü azaldaraq, çoxsaylı əməliyyatları bir sübutda birləşdirməyə imkan verir. Bu aqreqasiya mexanizmi blokçeyn şəbəkələrinin miqyasını artırır və onları ödəniş emalı və mərkəzləşdirilməmiş mübadilələr kimi yüksək əməliyyat qabiliyyəti tələb edən tətbiqlər üçün daha uyğun edir.

Ondan istifadə etməklə, kriptovalyuta layihələri genişlənmə məhdudiyyətlərini aradan qaldıra, müxtəlif sənayelərdə daha geniş qəbul və istifadə hallarına yol aça bilər.

Kriptovalyuta sistemlərində təhlükəsizlik hər şeydən üstündür, çünki hər hansı zəifliklər və ya zəifliklər vəsaitlərin itirilməsinə və ya şəbəkənin bütövlüyünə xələl gətirə bilər. zk-STARK həm klassik, həm də kvant düşmənlərinin hücumlarına müqavimət göstərən güclü kriptoqrafik primitivlər təmin etməklə təhlükəsizliyi artırır.

2022-ci ilin iyul ayında StarkWare, mərkəzləşdirilməmiş idarəetmədə və ekosistemin saxlanmasında əsas rol oynayacaq bir layihə idarəetmə tokeni buraxmaq niyyətini təsdiqlədi. Token emissiyasının həcmi hələ müəyyən edilməyib. StarkWare ilkin olaraq Ethereum şəbəkəsində 10 milyard ERC-20 tokeni buraxacaq və bunlar aşağıdakı kimi paylanacaq:

1. 30% - Layihəni həyata keçirən StarkWare şirkətinə, layihənin inkişafını dəstəkləmək və bütün ekosistemi inkişaf etdirmək üçün.

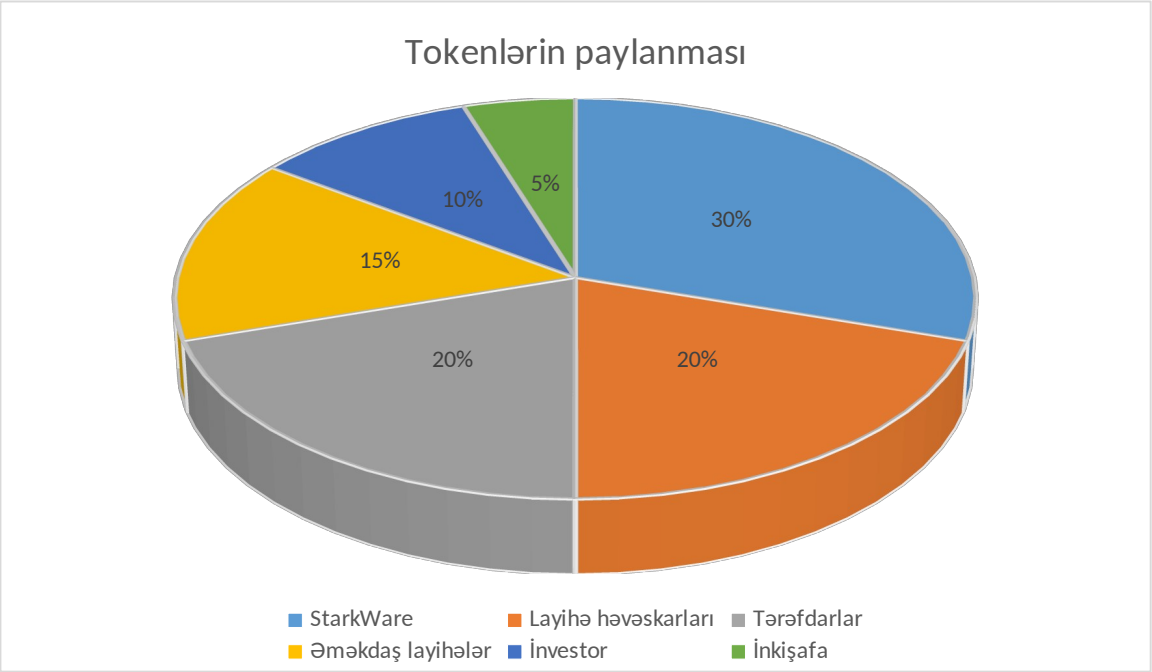
2. 20% - StarkWare tərəfindən təyin olunan layihə həvəskarları və digər tərəfdarlar üçün, layihədən əldə ediləcək gəlirlərin böyük bir hissəsinin paylaşılması üçün.

3. 20% - StarkWare ekosisteminin tərəfdarları, həyata keçirilən layihələrdən əldə ediləcək gəlirlərin paylaşılması üçün.

4. 15% - Layihəni inkişaf etdirmək və birləşmələri və alqı-satqıları dəstəkləmək üçün StarkWare ilə əməkdaşlıq edən layihələr üçün.

5. 10% - İnvestorlar, bazar tərəfdarları və təşəbbüskarlar üçün paylaşılacaq.

6. 5% - Protokol təhlükəsizliyi, kəşfiyyatı və inkişafı üçün StarkWare tərəfindən idarə ediləcək.(Şəkil 3.1)



Şəkil 3.1: Tokenlərin paylanması

İnvestorlara və komandaya paylanan bütün tokenlər 1 il ərzində kilidlənəcək və növbəti 4 il ərzində xətti olaraq açılacaq.

- STRK tokeni üç əsas funksiyanı yerinə yetirəcək:
- Şəbəkənin idarə edilməsində iştirak;
- StarkNet-də əməliyyatlar üçün komissiyaların ödənilməsi;
- Konsensus mexanizmində və əməliyyatların işində iştirak.
- Kripto aktivin 2022-ci ilin oktyabrında buraxılmışdır.

Bir çox ənənəvi kriptoqrafik üsullardan fərqli olaraq, zk-STARK kvantdan sonrakı təhlükəsizlik təklif edir, yəni kvant kompüterlərinin mövcudluğunda belə təhlükəsiz olaraq qalır (Bowe, 2013). Bu, kriptovalyuta şəbəkələrinin uzunmüddətli təhlükəsizliyini qorumaq üçün çox vacibdir, xüsusən kvant hesablama texnologiyası irəliləməyə davam edir.

Bundan əlavə, zk-STARK-ın şəffaflığı və etibarlı quraşdırma mərhələsinin olmaması zərərli aktyorlar tərəfindən istifadə oluna biləcək potensial zəifliklərin və ya arxa qapıların riskini azaldır. zk-STARK-ın güclü təhlükəsizlik xüsusiyyətlərindən istifadə etməklə kriptovalyuta layihələri istifadəçilər və investorlar arasında inam yaradaraq, daha möhkəm və etibarlı sistemlər qura bilər.

zk-STARK kriptovalyuta sistemlərində məxfiliyin, genişlənmənin və təhlükəsizliyin artırılması üçün çoxsaylı üstünlüklər təklif etsə də, bir sıra problemlər və mülahizələrə diqqət yetirilməlidir (Bowe, 2013).

Çətinliklərdən biri zk-STARK sübutlarının yaradılması və yoxlanması ilə əlaqəli hesablama xərcləridir, bu, resurs tutumlu ola bilər və xüsusi avadanlıq tələb edir. Bununla belə, davam edən tədqiqat və optimallaşdırma səyləri bu problemləri azaltmaq və zk-STARK tətbiqlərinin səmərəliliyini artırmaq məqsədi daşıyır.

STARK-ın mövcud kriptovalyuta protokollarına inteqrasiyası şəbəkə infrastrukturunda və konsensus mexanizmlərində əhəmiyyətli dəyişikliklər tələb edə bilər. Tərtibatçılar, mədənçilər və digər şəbəkə iştirakçıları arasında koordinasiya zk-STARK texnologiyasının düzgün inteqrasiyasını və qəbulunu təmin etmək üçün vacibdir.

Müxtəlif kriptovalyuta layihələrində zk-STARK-ın qəbulu üçün mövcud blokçeyn standartları ilə qarşılıqlı fəaliyyətin və uyğunluğun təmin edilməsi çox vacibdir. Standart qurumlar və sənaye əməkdaşlığı zk-STARK inteqrasiyası üçün ümumi çərçivələrin və protokolların işlənib hazırlanmasında mühüm rol oynayır.

STARK kimi məxfiliyi artıran texnologiyalarla bağlı tənzimləmə və uyğunluq problemlərinin həlli ümumi qəbul üçün vacibdir. Məxfilik hüquqlarını tənzimləyici tələblərlə balanslaşdıran aydın təlimatlar və qaydalar kriptovalyuta sistemlərində onun məsuliyyətli istifadəsini asanlaşdıra bilər.

Sonda, zk-STARK kriptovalyuta sistemlərində məxfilik, genişlənmə və təhlükəsizlik üçün transformativ faydalar təklif edən kriptoqrafik üsullarda əhəmiyyətli irəliləyişdir. zk-STARK-dan istifadə etməklə kriptovalyuta layihələri istifadəçi məxfiliyini artıra, əməliyyatların miqyasını yaxşılaşdıra və şəbəkə

təhlükəsizliyini gücləndirə, müxtəlif sənayelərdə daha geniş qəbul və istifadə hallarına yol açа bilər. (Nair, 2019).

Problemlər və mülahizələr mövcud olsa da, davam edən tədqiqat, inkişaf və əməkdaşlıq səyləri kriptovalyuta ekosistemlərində zk-STARK texnologiyasının inteqrasiyasına və qəbuluna təkan verir. Kriptovalyuta mənzərəsi inkişaf etməyə davam etdikcə, zk-STARK mərkəzləşdirilməmiş maliyyə və rəqəmsal aktivlərin gələcəyinin formalaşmasında mühüm rol oynamağa hazırlaşır.

Beləliklə, o kompleks riyazi çevrilmələri, çoxhədli tənlikləri və rəqəmsal imzaları birləşdirərək blokçeyn şəbəkələrində əməliyyatların təhlükəsiz və özəl yoxlanılmasını təmin edir. Bu texnologiya kriptovalyuta əməliyyatlarının məxfiliyini yaxşılaşdırmaqla yanaşı, təhlükəsiz və etibarlı hesablamalar üçün yeni imkanlar açır. (Елистратов, Маршалко, & Светушкин, 2019).

3.2. zk-STARK və zk-STARK-ın müqayisəli tədqiqi

Məxfiliyi qoruyan texnologiyalar, heç bir məxfi məlumatı üzə çıxarmadan yoxlanıla bilən hesablamalara icazə verərkən həssas məlumatları qorumaq qabiliyyətinə görə əhəmiyyətli diqqət qazanmışdır. ZKP bir tərəfə (təsdiq edənə) digər tərəfi (təsdiq edəni) ifadənin etibarlılığından kənar hər hansı əlavə məlumatı açıqlamadan ifadənin doğruluğuna inandırmağa imkan verən kriptoqrafik protokollardır. Geniş öyrənilmiş iki ZKP konstruksiyası zk-SNARK və zk-STARK-dır, hər biri özünəməxsus üstünlüklər və güzəştlər təklif edir (Ning, Zhen, Shi, & Daneshmand, 2020).

zk-SNARK Eli Ben-Sasson və digərləri tərəfindən təqdim edilmiş qısa, interaktiv olmayan sıfır bilik sübut sistemidir.

zk-STARK, sıfır bilik sübutu, məzmununu açıqlamadan müəyyən məlumatın sahibliyini sübut etməyə imkan verən qeyri-interaktiv arqumentasiyaya əsaslanır. Doğrulayıcı və sübut edən arasında qarşılıqlı əlaqə minimaldır və sübut millisaniyələr ərzində yoxlanıla bilər və hətta böyük proqramlar üçün də ölçüsü cəmi bir neçə yüz baytdır.

zk-SNARK sübutları JP Morgan Chase-in blokçeyn əsaslı ödəniş sistemi olan Zcash kriptovalyutasında və serverlərdə müştərilərin etibarlı autentifikasiyası vasitəsi kimi istifadə olunur. Zcash kontekstində zk-SNARK xüsusi maraq doğurur. Zcash tərəfindən təmin edilən güclü məxfilik zk-SNARK sübutlarından istifadə edərək şəbəkənin konsensus qaydalarına qarşı yoxlanılması şərti ilə blokçeyndən istifadə edərək qorunan əməliyyatları tam şifrələmək qabiliyyətinə əsaslanır. (Ben-Sasson, Chiesa, Tromer, & Virza, 2014)

Hal-hazırda, zk-SNARK sübutları Zcash-da parametr yaratma mərasimi adlanan ictimai parametrlərin ilkin təyin edilməsindən asılıdır. Əvvəlcədən konfiqurasiya mərhələsi kritik bir prosedurdur, çünki təcavüzkarın parametr yaratma mexanizminə giriş əldə etmək qabiliyyəti saxta sübutların yaradılmasına səbəb ola bilər. Bu, təcavüzkarın saxta sikkələrdən istifadə edə biləcəyi Zcash üçün xüsusilə təhlükəli ola bilər. Bu ssenarinin qarşısını almaq üçün Zcash mürəkkəb çoxqatlı proses vasitəsilə ictimai parametrlər yaradır.

O, isbat edən şəxsə heç bir əsas məlumatı aşkar etmədən yığcam, effektiv şəkildə yoxlanıla bilən şəkildə ifadənin etibarlılığına təsdiqləyicini inandırmağa imkan verir. zk-SNARK-ın qurulması bir neçə əsas komponenti əhatə edir:

a.**Quraşdırma mərhələsi:** Bu mərhələdə etibarlı tərəf sübut sistemi üçün tələb olunan ümumi istinad sətirləri CRS (Common Reference Strings) yaradır.

b.**İsbat mərhələsi:** Prover CRS və girişdən istifadə edərək ifadənin etibarlılığını təsdiq edən qısa sübut qurur.

c.**Doğrulama mərhələsi:** Təsdiqləyici CRS, bəyanat və sübutun özündən istifadə edərək isbatın etibarlılığını yoxlayır.

zk-SNARK-lar blokçeyn texnologiyası (məsələn, Zcash), autentifikasiya protokolları və təhlükəsiz çoxtərəfli hesablamalar da daxil olmaqla müxtəlif domenlərdə tətbiq edilmişdir. Bununla belə, zk-SNARK-ların etibarlı quraşdırma tələbləri və nisbətən yüksək hesablama xərcləri daxil olmaqla nəzərə çarpacaq məhdudiyyətləri var.

- **Təhlükəsizlik:** Həm zk-SNARK, həm də zk-STARK güclü kriptoqrafik təhlükəsizlik zəmanətlərini təmin edir. Bununla belə, zk-SNARK etibarlı

quraşdırmaya əsaslanır və quraşdırma parametrləri pozulduğu təqdirdə potensial zəifliklər yaradır. Bunun əksinə olaraq, zk-STARK post-kvant təhlükəsizliyinə nail olur və etibarlı quraşdırma ehtiyacını aradan qaldıraraq hücumlara davamlılığını artırır.

- **Şəffaflıq:** zk-STARK mahiyyətcə şəffafdır, çünki isbat yaratma prosesi heç bir gizli parametrləri əhatə etmir. Bu şəffaflıq, xüsusən mərkəzləşdirilməmiş sistemlərdə inamı və audit qabiliyyətini artırır. Digər tərəfdən, zk-SNARK etibarlı quraşdırma tələb edir ki, bu da quraşdırma iştirakçılarının bütövlüyü ilə bağlı narahatlıq yarada bilər.
- **Miqyaslılıq:** zk-STARK zk-SNARK ilə müqayisədə üstün miqyaslılıq nümayiş etdirir. zk-STARK-da isbat ölçüsü hesablamanın mürəkkəbliyi ilə xətti olaraq böyüyərək onu geniş miqyaslı tətbiqlər üçün uyğun edir. Bunun əksinə olaraq, zk-SNARK-ın isbat ölçüsü hesablamanın mürəkkəbliyindən asılı olmayaraq sabit qalır və onun miqyasını məhdudlaşdırır.
- **Performans**: zk-SNARK adətən kiçik və orta ölçülü hesablamalar üçün zk-STARK ilə müqayisədə daha sürətli isbat və yoxlama vaxtları təklif edir. Bununla belə, zk-STARK-ın performansı xətti miqyaslılığı və etibarlı quraşdırma tələbinin olmaması səbəbindən mürəkkəb hesablamalar üçün daha rəqabətli olur (Bowe, 2013).

Həm zk-SNARK, həm də zk-STARK müxtəlif domenlərdə tətbiqlər tapır, o cümlədən:

- **Kriptovalyutalar:** zk-SNARK məxfi əməliyyatları təmin etmək üçün Zcash kimi məxfiliyə yönəlmiş kriptovalyutalarda istifadə edilmişdir. zk-STARK etibarlı quraşdırma və genişlənmə ilə bağlı narahatlıqları həll edərkən oxşar məxfilik xüsusiyyətləri təklif edir.
- **Doğrulama Protokolları:** Sıfır bilik isbatları autentifikasiya protokollarında mühüm rol oynayır, həssas məlumatları açıqlamadan təhlükəsiz və məxfiliyi qoruyan autentifikasiyaya imkan verir.
- **Mərkəzləşdirilməmiş Maliyyə (DeFi):** DeFi-nin inkişaf edən sahəsində zk-SNARK və zk-STARK məxfiliyi qoruyan əməliyyatları, aktivlərin köçürülməsini və ağıllı müqavilənin icrasını asanlaşdıra bilər.

- **Təchizat Zəncirinin İdarə Edilməsi:** Sıfır bilik isbatları məxfi məlumatları açıqlamadan yoxlanıla bilən hesablamalara imkan verməklə tədarük zəncirinin idarəetmə sistemlərinin məxfiliyini və bütövlüyünü artıra bilər.
- **Səsvermə Sistemləri:** zk-SNARK və zk-STARK səsvermə prosesinin bütövlüyünü və məxfiliyini təmin edən təhlükəsiz və anonim səsvermə sistemlərində potensial tətbiqlər təklif edir.

Çağırışlar və Gələcək İstiqamətlər:

Əhəmiyyətli irəliləyişlərinə baxmayaraq, zk-SNARK və zk-STARK səmərəliliyin artırılması, isbat yaratma vaxtlarının azaldılması və mövcud sistemlərlə uyğunluğun artırılması kimi problemlərlə üzləşir. Gələcək tədqiqat istiqamətlərinə yeni kriptoqrafik üsulların tədqiqi, isbat yaratma alqoritmlərinin optimallaşdırılması və bu texnologiyaların daha geniş şəkildə mənimsənilməsini asanlaşdırmaq üçün istifadəyə yararlılıq problemlərinin həlli daxil ola bilər.

Həm SNARK, həm də STARK-ın öz üstünlükləri var və onların arasında seçim onların istifadəsi üçün xüsusi istifadəçi tələblərindən asılıdır. Qeyd etmək vacibdir ki, hər iki texnologiya fəal şəkildə tədqiq olunan ən qabaqcıl sıfır bilikli isbat üsullarıdır və onlar arasında müqayisələr bu sahədə mövcud irəliləyişlərdən və kəşflərdən asılı ola bilər.

SNARK-ların tərəfdarları onları daha səmərəli və daha sürətli hesab edirlər, çünki onların isbatlarını yoxlamaq yalnız bir neçə millisaniyə çəkə bilər. Bununla belə, bu səmərəlilik baha başa gəlir, çünki bəzi SNARK-lar potensial olaraq həssas etibarlı quraşdırma mərasiminə əsaslanır. Bu o deməkdir ki, isbatda istifadə olunan ilkin parametrlər təhlükəsiz mühitdə yaradılmalıdır və bu parametrlərə güzəştə getmək təhlükəsizlik risklərinə səbəb ola bilər.

STARK-lar etibarlı quraşdırma ehtiyacını aradan qaldırmaqla artan təhlükəsizlik səviyyəsini təmin edə bilər, lakin yoxlama daha uzun çəkə bilər və buna görə də daha az effektiv hesab edilə bilər. STARK isbatları SNARK isbatlarından daha böyükdür, bu da daha uzun yoxlama vaxtları və daha yüksək qaz sərfiyyatı tələb edir. Bununla belə, STARK isbatları xarici parametrlərə etibar etmədən yoxlanıla bilər ki, bu da

onları daha sınaqdan keçirməyə imkan verir, baxmayaraq ki, bu tətbiqdən asılı ola bilər. Əksər SNARK-lardan fərqli olaraq, STARK-lar kvant davamlı heş funksiyalarından istifadə edirlər.

Etibarlı quraşdırma mərasimi ilə bağlı potensial təhlükəsizlik zəifliklərinə baxmayaraq, SNARK-ların əvvəlcə STARK-lardan daha geniş şəkildə qəbul edilməsinin bir neçə səbəbi var. SNARK-lar STARK-dan 6 il əvvəl hazırlanmışdır ki, bu da onlara tətbiq prosesində üstünlük verir (Mazze, 2009).

Aşağıdakı cədvəldə zk-STARK və zk-SNARK arasındakı bəzi fərqlərə diqqət yetirək.(Cədvəl 3.1)

Cədvəl 3.1: zk-STARK və zk-SNARK-ın müqayisəsi

Xüsusiyyət	**ZK-SNARK**	**ZK-STARK**
Etibarlı Quraşdırma	Tələb edilir	Tələb Yoxdur
Sübut ölçüsü	Kiçik	Daha böyük
Doğrulama sürəti	Yavaş	Sürətli
Miqyaslılıq	Məhdud	Yüksək
Şəffaflıq	Aşağı (etibarlı quraşdırmaya görə)	Yüksək
Təhlükəsizlik	Yüksək, lakin quraşdırma pozulursa, pozula bilər	Yüksək
Hesablama Tələbləri	İntensiv, çoxlu hesablama resursları tələb edir	İntensiv, lakin daha səmərəli
Vəziyyətləri istifadə edin	Zcash, JP Morgan Chase-in blokçeyn əsaslı ödəniş sistemi və s.	Çarpaz zəncirli məxfilik təbəqələri, müxtəlif blokçeyn şəbəkələrində qarşılıqlı fəaliyyət və s.
Həssaslığı	Etibarlı quraşdırmanın ilkin parametrləri pozulursa, pozuntulara qarşı həssasdır	Etibarlı quraşdırma olmadığı üçün pozuntulara daha az həssasdır

Yekun olaraq, zk-SNARK və zk-STARK fərqli xüsusiyyətlər və güzəştlər təklif edərək, məxfiliyi qoruyan texnologiyalarda əsaslı irəliləyişləri təmsil edir. zk-SNARK etibarlı quraşdırma ilə səmərəli isbatlar təqdim edərkən, zk-STARK etibarlı quraşdırma tələb etmədən şəffaflıq, genişlənmə və post-kvant təhlükəsizliyi təklif edir. zk-SNARK və zk-STARK arasında seçim xüsusi tətbiq tələblərindən, təhlükəsizlik mülahizələrindən və performans məhdudiyyətlərindən asılıdır. Hər iki konstruksiya məxfilik və məxfiliyi qoruyarkən yoxlanıla bilən hesablamalara imkan verməklə kriptovalyutalardan tutmuş təchizat zəncirinin idarəçiliyinə qədər müxtəlif domenlərdə inqilab etmək potensialına malikdir (DZone, 2009).

3.3. Blokçeyn texnologiyasında zk-STARK-ın ssenari üzərində tədqiqi

İndiki vaxtda rəqəmsallaşma ilə kriptovalyutalar ənənəvi maliyyə sistemlərinə alternativ olaraq getdikcə daha çox əhəmiyyət qazanır. Bununla belə, bu rəqəmsal valyutaların istifadəsi ilə təhlükəsizlik və məxfilik problemləri də yaranır. Bu ssenaridə Alis və Bob adlı iki istifadəçi şəxsi və təhlükəsiz ödəniş sistemi yaratmaq üçün zk-STARK protokolundan istifadə edir.

Alis onlayn sənət qalereyası işlədir və Bob adlı müştərisi var. Bob Alisın qalereyasında sənət əsəri almaq istəyir və kriptovalyuta ilə ödəməyə üstünlük verir. Bununla belə, bu əməliyyatı yerinə yetirərkən həm Bob, həm də Alisın məxfiliyi vacibdir.

Addım-addım Proses:

✓ **Addım 1:** Protokolun Seçilməsi və Hazırlanması

Alis və Bob əməliyyatlarını həyata keçirmək üçün zk-STARK protokolunu seçirlər. Əvvəlcə o, qalereya veb-saytı vasitəsilə Alisın Boba satmaq istədiyi sənət əsərinin qiymətini müəyyənləşdirir.

✓ **Addım 2:** Əməliyyat Təfərrüatları və Məxfilik

Alis Boba satmaq istədiyi sənət əsərinin kriptovalyuta növünü və miqdarını müəyyənləşdirir. Lakin bu detalları açıq şəkildə paylaşmır. Bunun əvəzinə, zk-STARK protokolundan istifadə edərək əməliyyatın düzgünlüyünü təsdiq edən sıfır bilik isbatını yaradır.

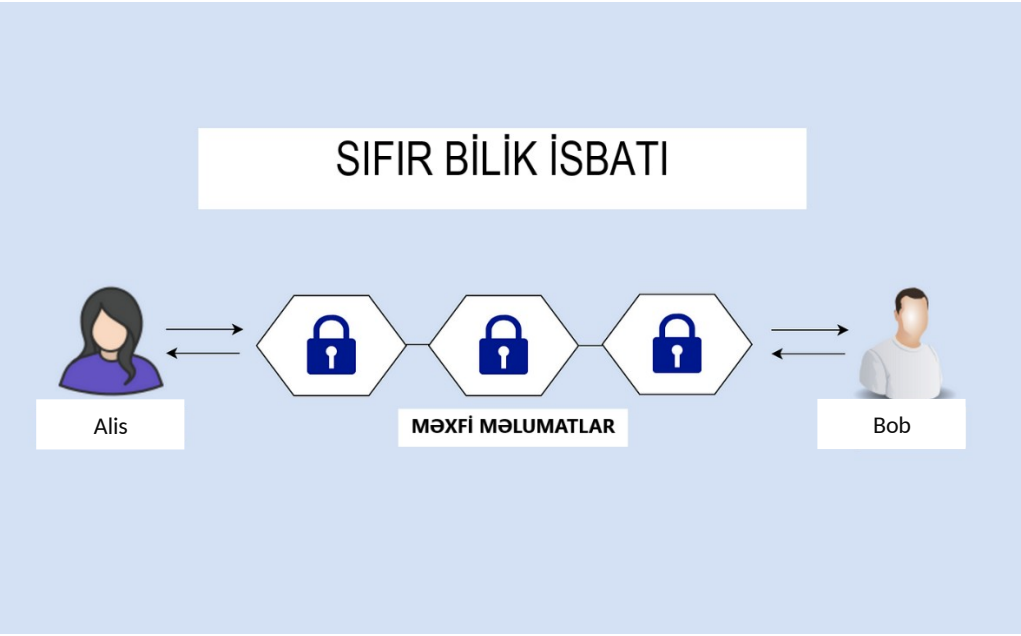
ZKP bir isbata lazımsız məlumatları açıqlamadan bir ifadənin doğruluğunu təsdiqləyəni inandırmağa imkan verən kriptoqrafik üsullardır. Onlar blokçeyn kontekstində autentifikasiya da daxil olmaqla müxtəlif sahələrdə məxfiliyin və təhlükəsizliyin artırılmasında əsas rol oynayırlar. ZKP texnologiyalarının iki əsas kateqoriyası var: interaktiv və qeyri-interaktiv.

İnteraktiv ZKP Protokolları: Bu tip protokollarda isbat edən və yoxlayıcı ifadənin etibarlılığını təsdiqləmək üçün iterativ mübadilə aparır. Hər təkrarlama zamanı prover məxfi məlumatları açıqlamadan yoxlayıcını ifadənin doğruluğuna inandırmağa çalışır. İnteraktiv təbiət sorğuların və cavabların mübadiləsini nəzərdə tutur ki, bu da qarşılıqlı əlaqənin bir neçə mərhələsinə ehtiyac yaradır.

Qeyri-interaktiv ZKP protokolları: Bu protokollar etibar edən tərəfə isbat edən tərəflə birbaşa əlaqə yaratmadan məlumatın autentifikasiyasına imkan verir. Bu tip ZKP ikitərəfli əlaqə tələb etmir və birbaşa əlaqənin mümkün olmadığı ssenarilərdə xüsusilə təsirlidir.

✓ **Addım 3:** Sıfır Bilik isbatının yaradılması

Alis əməliyyatın etibarlılığını isbat edən sıfır bilik isbatı yaratmaq üçün zk-STARK protokolundan istifadə edir. Bu isbat əməliyyatın həyata keçirilmə qaydasını, məbləği və digər zəruri məlumatları ehtiva edir, lakin bu məlumatı açıqlamır.

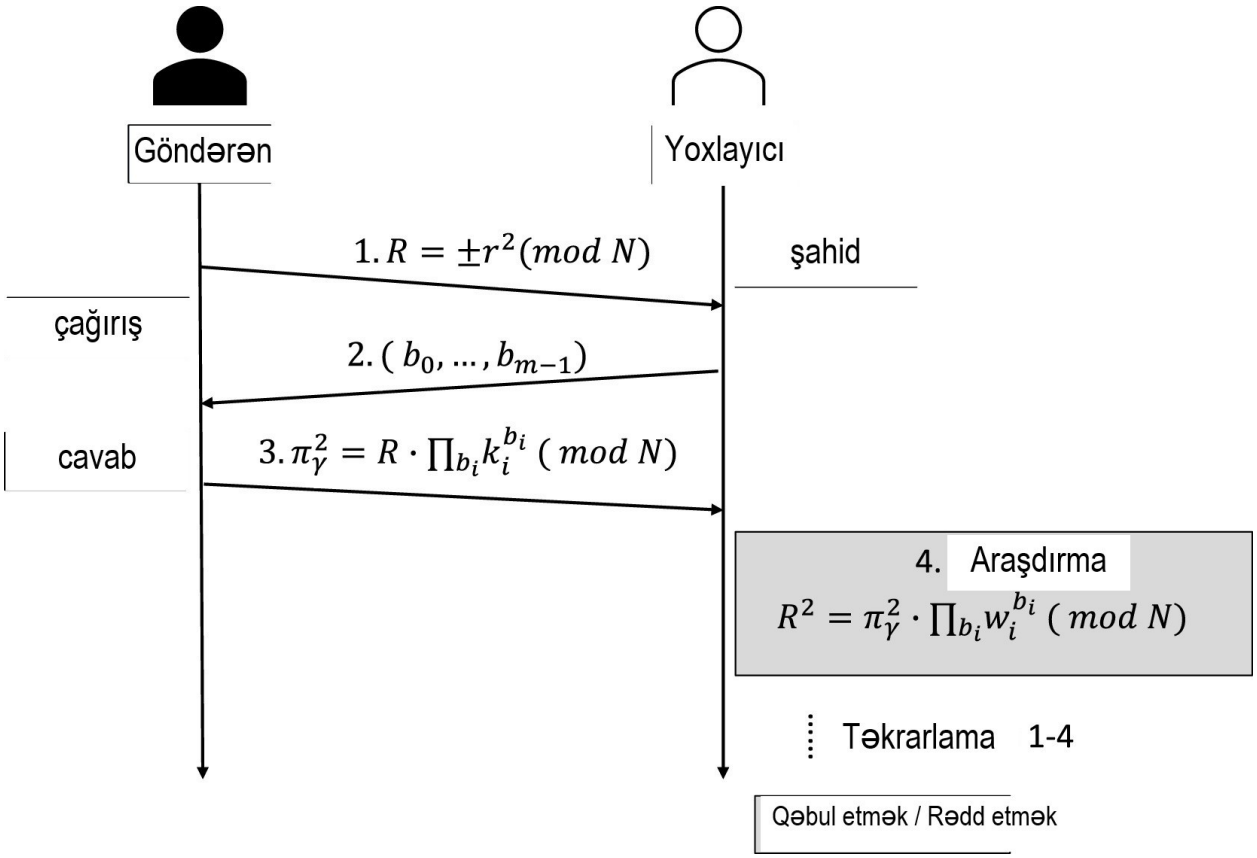


Şəkil 3.2: Zk-stark protokol üzrə sıfır bilik isbatı nümunəsi

✓ **Addım 4:** İsbatı təqdim edin və yoxlayın

Alis yaratdığı sıfır bilik isbatını Boba göndərir. Bu isbatdan istifadə edərək, Bob əməliyyatın etibarlılığını yoxlayır. Beləliklə, Alis göndərdiyi kriptovalyutanın miqdarını və digər detalları bilmədən əməliyyatın təhlükəsiz olduğunu yoxlaya bilər.

ZKP alqoritminin strukturu aşağıdakı Şəkil 3.3-də göstərilmişdir və aşağıdakı addımları əhatə edir:



Şəkil 3.3 :Sıfır bilik İsbatının təqdim edilib və yoxlanılması prosesi

✓ **Addım 5:** Prosesin Tamamlanması

Aldığı sıfır bilik isbatından istifadə edərək əməliyyatın etibarlı olduğunu təsdiqlədikdən sonra Bob sənət əsərinin pulunu kriptovalyuta ilə ödəyir. Ödənişi aldıqdan sonra Alis sənət əsərini Boba çatdırır və əməliyyat tamamlanır.

Nəticə: Təhlükəsiz və Şəxsi Əməliyyat

Bu ssenaridə Alis və Bob zk-STARK protokolundan istifadə edərək təhlükəsiz və özəl şəkildə kriptovalyuta ilə ticarət edirdilər. Bu protokol onlara əməliyyatın təfərrüatlarını gizli saxlamaqla təhlükəsiz əməliyyatlar aparmağa imkan verdi. Beləliklə, hər iki tərəf məxfiliyini qoruyaraq etibarlı əməliyyat həyata keçirə bildi.

Məxfiliyi artırmaq üçün sıfır bilik isbatı protokollarının ZKP blokçeyn sistemlərinə inteqrasiyası dəyərli dərslər və irəliləyişlər gətirdi. İstifadəçilərin əməliyyatlarının və şəxsi məlumatlarının məxfiliyinin qorunması ilə bağlı müxtəlif tədqiqatlardan aşağıdakı dərslər və potensial problemlər öyrənilib (Chainlink Education Hub, 2009).

Öyrənilmiş dərslər:

1.Müxtəlif Tətbiqlər: ZKP-ni dəstəkləyən blokçeyn sistemləri maliyyə, səhiyyə, əşyaların interneti və təhsil kimi müxtəlif sahələrdə tətbiq oluna biləcəyini nümayiş etdirib. Bu, müxtəlif ssenarilərdə məxfilik məsələlərini həll etmək üçün bu üsulların potensialını vurğulayır.

2.Təkmilləşdirilmiş Məxfilik: ZKP metodları istifadəçilərin əməliyyatlarının və şəxsi məlumatlarının məxfiliyini effektiv şəkildə artırır. Tranzaksiya atributlarını gizlətməklə və identifikasiyaedici məlumatları seçərək aşkar etməklə, istifadəçilər blokçeynlə qarşılıqlı əlaqə qurarkən daha yüksək məxfilik səviyyəsini qoruya bilərlər.

3.Mərkəzsizləşdirmə və Etibarsızlıq: ZKP-ni dəstəkləyən blokçeyn sistemləri əməliyyatları yoxlamaq və ya şəxsiyyətləri təsdiqləmək üçün etibarlı vasitəçilərə ehtiyacı aradan qaldırır. Bu, blokçeyn texnologiyasında mərkəzsizləşdirmə və etibarsızlığın əsas prinsiplərinə uyğundur.

4.Çevik Atributların Mühafizəsi: Tədqiqatlar göstərdi ki, ZKP metodları xüsusi atributların qorunmasında çeviklik təmin edir, lazım olduqda seçmə açıqlamaya imkan verir. Bu, məxfilik və şəffaflıq arasında balans yaradır.

5.Effektiv Sıfır Bilik isbatları: zk-SNARK və zk-STARK kimi ZKP texnologiyalarında irəliləyişlər sistem performansına xələl gətirmədən məxfiliyin artırılmasına imkan verən daha səmərəli və genişlənə bilən həllərə gətirib çıxardı.

Potensial problemlər:

1.Miqyaslılıq: Blokçeyn şəbəkələri genişləndikcə, ZKP-yə imkan verən sistemlərin miqyasını təmin etmək kritik hala gəlir. Sıfır bilik isbatlarının blokçeyn performansına mane olmamasını təmin etmək üçün davamlı araşdırma və optimallaşdırma lazımdır.

2.İstifadə qabiliyyəti və tətbiqi: ZKP texnologiyasının mövcud blokçeyn sistemlərinə inteqrasiyası son istifadəçilər üçün istifadə problemi ilə üzləşə bilər. Geniş tətbiq üçün sadələşdirilmiş istifadəçi təcrübəsi və məxfilik xüsusiyyətlərinin qüsursuz inteqrasiyası lazımdır.

3.Məxfilik və Tənzimləmə: Məxfiliyin qorunması və tənzimləyicilərə uyğunluq arasında tarazlıq olmalıdır. ZKP metodları zəruri hallarda qanuni girişi təmin etməlidir.

4.Mürəkkəblik: ZKP metodlarının tətbiqi mürəkkəb və resurs tutumlu ola bilər. Düzgün və təhlükəsiz həyata keçirmək üçün onların kriptoqrafik incəliklərini başa düşmək lazımdır.

5.Etibarlı quraşdırma və audit: Bəzi ZKP metodları etibarlı quraşdırma tələb edir. Bu quraşdırmanın bütövlüyünü təmin etmək və zəifliklərin qarşısını almaq üçün müntəzəm yoxlamalar aparmaq vacibdir.

6.Qarşılıqlı işləmə qabiliyyəti: Müxtəlif blokçeynlər və köhnə sistemlər arasında qarşılıqlı fəaliyyətin qurulması çətin ola bilər. Məlumat mübadiləsini asanlaşdırmaq üçün standartlar və protokollar lazımdır.

7.Məxfilik Zəmanəti: ZKP metodlarının hücumlara və zəifliklərə qarşı effektiv olmasını təmin etmək davamlı təkmilləşdirmə tələb edir.

8.Resurs Tələbləri: Sıfır bilik isbatlarının yaradılması və yoxlanması əhəmiyyətli hesablama resursları tələb edə bilər.

9.Təhsil və Maarifləndirmə: İstifadəçiləri və tərtibatçıları ZKP-nin aktivləşdirdiyi sistemlərin faydaları və riskləri haqqında maarifləndirmək vacibdir.

10.Yeni təhdidlər: ZKP-nin yayılması ilə yeni təhlükəsizlik təhdidləri yarana bilər. Ayıq qalmaq və yeni təhlükəsizlik çağırışlarına uyğunlaşmaq vacibdir.

Beləliklə, ZKP ilə blokçeyn sistemləri məxfiliyi əhəmiyyətli dərəcədə yaxşılaşdıra bilər. Bununla belə, onların potensialından tam istifadə etmək üçün miqyaslılıq, istifadəyə yararlılıq, tənzimləmə və mürəkkəbliklə bağlı problemlər həll edilməlidir. Blokçeyn icması daxilində innovasiya və əməkdaşlığa sadiqlik bu problemləri həll etməyə və məxfilik, mərkəzsizləşdirmə və təhlükəsizliyi birləşdirən möhkəm həllər yaratmağa kömək edəcək.

NƏTİCƏ

Bu dissertasiyada ZKP və zk-STARK texnologiyasının informasiya təhlükəsizliyi, məxfilik, və kriptovalyuta sahələrindəki rolunu təhlil edərək bir sıra mühüm nəticələr əldə edilmişdir:

- Sıfır bilik isbatlarının nə olduğunu və onların əsas iş prinsipini ətraflı izah edərək, bu texnologiyanın informasiya təhlükəsizliyi sahəsində necə tətbiq edildiyini və hansı üstünlükləri təmin etdiyini göstərmək mümkün olmuşdur. Bu texnologiya, digər kriptoqrafiya metodları ilə müqayisədə daha təhlükəsiz və effektivdir.
- zk-STARK texnologiyasının əsas riyazi prinsipləri və sıfır bilik isbatlarında mühüm rol oynadığı izah edilmişdir. Riyazi modellərin və alqoritmlərin təhlili, bu texnologiyanın kriptovalyuta və blokçeyn sahələrində effektiv tətbiq metodlarını qiymətləndirmək imkanı vermişdir.
- zk-STARK texnologiyasının tranzaksiya şifrələmə üçün tətbiq olunduğu metodların nə qədər effektiv olduğunu təhlil etmək, bu texnologiyanın blokçeyn ekosistemində təhlükəsizliyi və məxfiliyi artırmaqda necə təsirli olduğunu nümayiş etdirmişdir.
- zk-STARK və zk-SNARK texnologiyalarının müqayisəli tədqiqi aparılaraq, onların üstünlük və çatışmazlıqları müəyyən edilmişdir. Bu texnologiyaların müxtəlif tətbiq sahələrində effektivliyi müqayisə edilmişdir.
- Blokçeyn texnologiyasında zk-STARK texnologiyasının müxtəlif ssenarilər üzərində tətbiqi və bu tətbiqlərin nəticələri təhlil edilmişdir. Kriptovalyuta əməliyyatlarında zk-STARK texnologiyasının məxfiliyi və təhlükəsizliyi necə təmin etdiyi izah olunmuşdur.
- Blokçeyn texnologiyasında əsas konseptlərin və zk-STARK texnologiyasının qarşılıqlı təsiri araşdırılmış və bu konseptlərin informasiya təhlükəsizliyi sahəsində nə qədər mühüm rol oynadığı göstərilmişdir.

- Gələcək tədqiqat istiqamətləri və potensial tətbiq sahələri müəyyən edilmişdir. Bu texnologiyaların informasiya təhlükəsizliyi və məxfilik sahələrində yeni imkanlar yarada biləcəyi göstərilmişdir.

Bu nəticələr göstərir ki, sıfır bilik isbatları və zk-STARK texnologiyaları informasiya təhlükəsizliyi, məxfilik və kriptovalyuta sahələrində mühüm potensiala malikdir və bu sahələrdə tədqiqatlar və tətbiqlər üçün geniş imkanlar açır. Bu dissertasiya bu texnologiyaların daha dərindən araşdırılması və genişləndirilməsi üçün baza rolunu oynayacaqdır.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT

Abdolmaleki, B., Baghery, K., Lipmaa, H., & Zając, M. (2017). A subversion-resistant SNARK. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 10626 LNCS, pp. 3–33). Springer Verlag. https://doi.org/10.1007/978-3-319-70700-6_1

Bai, T., Hu, Y., He, J., Fan, H., & An, Z. (2022). Health-zkIDM: A healthcare identity system based on fabric blockchain and zero-knowledge proof. *Sensors*, *22*(20), 144-231.

Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2014). Succinct non-interactive zero knowledge for a von Neumann architecture. In *Proceedings of the 23rd USENIX Security Symposium* (pp. 781–796). USENIX Association.

Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2017). Scalable zero knowledge via cycles of elliptic curves. *Algorithmica*, *79*(4), 1102–1160. https://doi.org/10.1007/s00453-016-0221-0

Bowe, S., et al. (2013). Zcash protocol specification. Retrieved September 24, 2019, from https://z.cash

Gennaro, R., Gentry, C., Parno, B., & Raykova, M. (2013). Quadratic span programs and succinct NIZKs without PCPs. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 7881 LNCS, pp. 626–645). Springer. https://doi.org/10.1007/978-3-642-38348-9_37

Green, M. (2014). Zero knowledge proofs: An illustrated primer. *A Few Thoughts on Cryptographic Engineering*. Retrieved from https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-an-illustrated-primer/

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, *19*(5), 653–659.

Nair, G. R. (2019). Blockchain technology: Centralized ledger to distributed ledger. *International Research Journal of Engineering and Technology (IRJET)*, 650-745.

Ning, H., Zhen, Z., Shi, F., & Daneshmand, M. (2020). A survey of identity modeling and identity addressing in internet of things. *IEEE Internet of Things Journal*, *7*(6), 46-86.

Petkus, M. (2018, January 3). Game-changing year for private blockchains. *Chronicled*. https://blog.chronicled.com/game-changing-year-for-private-blockchains-5b91eec0a0e4

Pop, C. D., Antal, M., Cioara, T., Anghel, I., & Salomie, I. (2020). Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy. *Sensors*, *20*(19), 567.

Saket, R., Singh, N., Dayama, P., & Pandit, V. (2020). Smart contract protocol for authenticity and compliance with anonymity on Hyperledger Fabric. In *IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020)*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICBC48266.2020.9169401

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network*, *35*(4), 198-205.

Vural, Y., & Sağiroğlu, Ş. (2010). Veritabanı yönetim sistemleri güvenliği: Tehditler ve korunma yöntemleri. *Journal of Polytechnic*, *13*(2), 71-81. https://doi.org/10.6633/IJNS.201709.19(5).01

Ishai, Y., Mahmoody, M., Sahai, A., & X., D. (2012). On zero-knowledge PCPs: Limitations, simplifications, and applications. *Theory of Cryptography*, 151-168.

Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and blockchain: Security and privacy. *IEEE Internet of Things Journal*, *7*(10), 102-108.

Горячев, А. А. (2011). Методические аспекты изложения протоколов с нулевыми знаниями: толкование термина «нулевое разглашение» в дисциплине «Криптографические протоколы». *Современное образование: содержание, технологии, качество*, *2*, 238-240.

Елистратов, А., Маршалко, Г., & Светушкин, В. (2019). Подводные камни сертификации блокчейн-решений. *Открытые системы СУБД*, (1), 86-98.

Салий, В. Н. (2019). Неприводимые расширения графов (доказательства с нулевым разглашением). *Известия ТРТУ*, *4*(33), 271-273.

Яковлев, А. В., & Сычева, Т. С. (2017). Динамическая модель протокола идентификации с нулевым разглашением тайны. *Актуальные проблемы деятельности подразделений УИС: «Научная книга»*, 170-173.

İNTERNET RESURSLARI

Binance Academy. (2009). ZK-STARKs. Binance Academy. https://academy.binance.com/ru/glossary/zk-starks

Ethereum Foundation. (2009). Zero-Knowledge Proofs. Ethereum. https://ethereum.org/ru/zero-knowledge-proofs/#non-interactive-zero-knowledge-proofs

Habr. (2009). Введение в Zero-Knowledge Proofs. Habr. https://habr.com/ru/articles/94901/

Chainlink Community. (2009). Medium. https://medium.com/chainlink-community/

CoinDesk. (2009). Trend Towards Blockchain Privacy: Zero-Knowledge Proofs. CoinDesk. https://www.coindesk.com/trend-towards-blockchain-privacy-zero-knowledge-proofs

Mazze. (2009). How ZK-STARKs Work. Mazze. https://docs.mazze.io/zk-proofs-integration/how-zk-starks-work

Chainlink Education Hub. (2009). Zero-Knowledge Proof Use Cases. Chainlink. https://chain.link/education-hub/zero-knowledge-proof-use-cases

DZone. (2009). Blockchain vs Database: Replace or Enhance? DZone. https://dzone.com/articles/blockchain-vs-databasereplace-or-enhance

XÜLASƏ

Zk-stark sıfır bilik isbatı sxemi üzrə tədqiqatlar ötürülmə və emal zamanı məlumatların məxfiliyini və təhlükəsizliyini təmin etməyə yönəlmiş müasir kriptoqrafiyanın əsas sahəsini təmsil edir. Bu sxemin əsas məntiqi məlumatların özünü və ya onun haqqında məlumatı açıqlamağa ehtiyac olmadan müəyyən əməliyyatların və ya ifadələrin düzgünlüyünü isbat etmək bacarığıdır. Bu addımlar riyazi isbatların yaradılmasını əhatə edir, daha sonra digər iştirakçıları həssas məlumatları aşkar etmədən ifadələrin doğru olduğuna inandırmaq üçün istifadə olunur.

zk-STARK sıfır biliklə isbat sxeminin tədqiqi məlumatların məxfiliyini və bütövlüyünü, habelə icazəsiz girişdən və məlumatın saxtalaşdırılmasından qorunmağı təmin etməkdir. O, müxtəlif sahələrdə, o cümlədən maliyyə əməliyyatları, tibbi məlumatlar və blokçeyn əməliyyatları üzrə məlumat mübadiləsi zamanı yüksək inam və təhlükəsizlik səviyyəsinə nail olmağa imkan verir.

Həmin sxemin dəyəri məlumatın ötürülməsi və yoxlanılmasında yüksək səviyyəli təhlükəsizlik, miqyaslılıq və səmərəlilik təmin etmək qabiliyyətidir. zk-STARK riyazi təsnifatı spesifik tətbiqlərin spesifik tələblərindən və xüsusiyyətlərindən asılı olaraq bu sxemin həyata keçirilməsi üçün müxtəlif növ və yanaşmaları ehtiva edir.

Əməliyyatlarının şifrlənməsi üçün tətbiq olunan üsullar blokçeyn texnologiyasında maliyyə əməliyyatları həyata keçirərkən anonimliyi və təhlükəsizliyi təmin etmək üçün istifadə olunur. Bu texnologiya kriptovalyutada mühüm rol oynayır, isbat edilə bilən təhlükəsiz əməliyyatlar və fırıldaqçılıqdan qorunma təmin edir.

Sözügedən isbat sxeminin blokçeyn texnologiyası ssenarilərində tətbiqi rəqəmsal aktivlərin ötürülməsi, səsvermə və şəxsiyyətin idarə edilməsi kimi müxtəlif əməliyyatlar üçün təhlükəsiz və səmərəli mərkəzləşdirilməmiş sistemlərin yaradılmasına imkan verir.

SUMMARY

Research on the zk-STARK zero-knowledge proof scheme represents a key area of modern cryptography aimed at ensuring privacy and security of data during transmission and processing. The main logic of this scheme is the ability to prove the correctness of certain operations or statements without the need to reveal the data itself or information about it. These steps involve creating mathematical proofs, which are then used to convince other participants that statements are true without revealing sensitive information.

The study of the zk-STARK zero-knowledge proof scheme is to ensure data privacy and integrity, as well as protection against unauthorized access and data falsification. It allows to achieve a high level of trust and security when exchanging information in various fields, including financial transactions, medical data and blockchain transactions.

The value of that scheme is its ability to provide a high level of security, scalability and efficiency in data transmission and verification. zk-STARK mathematical classification includes different types and approaches for implementing this scheme, depending on the specific requirements and characteristics of specific applications.

The methods used to encrypt transactions are used to ensure anonymity and security when conducting financial transactions in blockchain technology. This technology plays an important role in cryptocurrency, providing provably secure transactions and fraud protection.

The application of the said proof scheme in blockchain technology scenarios allows for the creation of secure and efficient decentralized systems for various operations such as digital asset transfer, voting and identity management.

РЕЗЮМЕ

Исследование схемы доказательства с нулевым разглашением zk-STARK представляет собой ключевую область современной криптографии, направленную на обеспечение конфиденциальности и безопасности данных во время передачи и обработки. Основная логика этой схемы — возможность доказать правильность тех или иных операций или утверждений без необходимости раскрытия самих данных или информации о них. Эти шаги включают в себя создание математических доказательств, которые затем используются, чтобы убедить других участников в истинности утверждений без раскрытия конфиденциальной информации.

Исследование схемы доказательства с нулевым разглашением zk-STARK направлено на обеспечение конфиденциальности и целостности данных, а также защиту от несанкционированного доступа и фальсификации данных. Это позволяет достичь высокого уровня доверия и безопасности при обмене информацией в различных сферах, включая финансовые транзакции, медицинские данные и блокчейн-транзакции.

Ценность этой схемы заключается в ее способности обеспечить высокий уровень безопасности, масштабируемости и эффективности передачи и проверки данных. Математическая классификация zk-STARK включает в себя различные типы и подходы реализации этой схемы в зависимости от конкретных требований и особенностей конкретных приложений.

Методы шифрования транзакций используются для обеспечения анонимности и безопасности при проведении финансовых операций в технологии блокчейн. Эта технология играет важную роль в криптовалюте, обеспечивая доказуемо безопасные транзакции и защиту от мошенничества.

Применение указанной схемы доказательства в сценариях технологии блокчейн позволяет создавать безопасные и эффективные децентрализованные системы для различных операций, таких как передача цифровых активов, голосование и управление идентификацией.