Manba va foydalanilgan adabiyotlar ro‘yxati:

1. *Ярыгина И.З. Банковская система Канады: решение современных вызовов. // США и Канада: экономика, политика, культура. 2017. № 2 (566). С. 87.*
2. *Ahmed Zebal M., M. Saber H. Market orientation in Islamic banks–a qualitative approach. // Marketing Intelligence & Planning. 2014. Т. 32. №. 4. С. 495-527.*
3. *Ghayad R. Corporate governance and the global performance of Islamic banks. // Humanomics. 2008. Т. 24. №. 3. С. 207-216.*
4. *Abdel Karim R.A. The nature and rationale of a conceptual framework for financial reporting by Islamic banks. // Accounting and business research. 1995. Т. 25. №. 100. С. 285-300.*
5. *Karim R.A.A. International accounting harmonization, banking regulation, and Islamic banks. // The International Journal of Accounting. 2001. Т. 36. №. 2. С. 169-193.*
6. *Шовхалов Ш.А. Привлечение заемных средств на условиях совместного партнерства согласно исламским правилам. // Проблемы экономики и юридической практики. 2014. №. 2. С. 55-59.*
7. *Мазурина Т. Ю., Шарипов Ш. Ф. Банковское регулирование и надзор в традиционных и исламских финансах: сравнительный анализ и особенности реализации. // Вестник университета. 2020. №. 6. С. 144-151.*
8. *Абдоров С. (2023). Banklar faoliyatida xulq-atvor iqtsodiyotining ahamiyati. Economics and Innovative Technologies, 11(3), 12-20.*
9. *Alessandro Carretta, Franco Fiordelisi (2000). Competition E Regulation In The Banking And Quasi-Banking Industries: Evidence From Italy Journal of Political Economy, 87.*
10. *https://gadebate.un.org/sites/default/files/gastatements/64/64_SG_en.pdf*
11. *https://www.japantimes.co.jp/opinion/2008/10/05/commentary/world-commentary/eu-financially-vulnerable-when-confidence-collapses/*
12. *https://morb.bsp.gov.ph/instruction-to-users/*
13. *Rossiya Fuqarolik kodeksining 82-moddasi, 3-bandi.*
14. *Тарасенко О.А. Квазибанки в банковской системе России. // Законы России: опыт, анализ, практика. 2013. № 7 (299). С. 82-86.*
15. *Rusakovich, V.I. Ko‘rfaz mamlakatlari milliy iqtisodiyotini diversifikatsiya qilish yo‘nalishlari: Bahrayn Qirolligining alyuminiy sanoati. // Iqtisodiyot va tadbirkorlik. 2017-yil. 8-2 (85)-son. 185-bet.*
16. *Alam N., Gupta L., Shanmugam B. Islamic Finance. A Practical Perspective. – N.Y.: Springer, 2017. P. 9.*
17. *Журавлев А.Ю. Концептуальные начала исламской экономики. // Исламские финансы в современном мире. Экономические и правовые аспекты. / под.ред. Р.И.Беккина. – М.: УММА, 2004. С.14.*
18. *Глоссарий. // Исламские финансы в современном мире. Экономические и правовые аспекты. / Под ред. Р.И. Беккина. – М.: УММА, 2004. С. 270.*
19. *Жданов С.В. Исламская экономика: ретроспективный анализ. // Финансовый бизнес. 2000. № 5. С. 35-41.*
20. *Ибадов Э.С., Шмырева А.И. Этапы развития исламского банковского дела, характеристика и мировой опыт. // Вестник Томского государственного университета. 2015. №. 390. С. 152.*
21. *Shkvarya L.V., Tirkba X.V. Xalqaro kapital migratsiyasi jarayonidagi global o‘zgarishlar va rivojlanayotgan bozorlarga ega mamlakatlarning roli. // Iqtisodiyot va tadbirkorlik. 2017 yil. 8-3 (85)-son. 75-bet.*

KREDITLASH SOHASINI RAQAMLASHTIRISH VA RAQAMLI TRANZAKSIYALARINI RIVOJLANTIRISHDA BLOKCHEYN TRANZAKSIYALARINI IMZOLASH USULLARINI TAKOMILLASHTIRISH

Raximberdiyev Quvonchbek Bakhtiyorovich
Toshkent davlat iqtisodiyot universiteti
Iqtisodiyotda matematik metodlar kafedrasi o‘qituvchisi

https://doi.org/10.55439/ECED/vol25_iss1/a11

Annotatsiya. *Ushbu maqolada, blokcheyn tranzaktsiyalarini shakllantirish jarayonlari tadqiq etilgan. Shuningdek, kreditlash blokcheyni tranzaksiyalarini imzolash mexanizmlari va ularning nazariy asoslar ko‘rib chiqilgan. Mazkur ilmiy tadqiqot davomida kreditlash blokcheyni tranzaksiyalarini imzolash imzolash va imzoni tekshirish jarayonini o‘z ichiga oluvchi model taklif etilgan. Taklif etilgan modelda tranzaktsiyalarni imzolashda ECDSA (Ellipti Curve Digital Signature Algortihm) elliptik egri chiziqlarga asoslangan elektron raqamli imzo algoritmi tadbiq etilgan bo‘lib, elliptik egri chiziqlarning umumiy modeli, samarali elliptik egri chiziqlarni tanlash hamda uni DSA elektron raqamli imzo algoritmiga tadbiqi keltirilgan.*

Kalit so‘zlar: *raqamli banking, kreditlash, raqamli transformatsiya, blokcheyn texnologiyalari, kriptovalyuta, tranzaksiya, elektron raqamli imzo, kriptografik algoritm, Bitcoin, Ethereum, Litecoin, elektron tijorat.*

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ПОДПИСАНИЯ БЛОКЧЕЙН-ТРАНЗАКЦИЙ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВИЗАЦИИ И ЦИФРОВОЙ ТРАНСФОРМАЦИИ КРЕДИТНОЙ ОТРАСЛИ

Рахимбердиев Кувончбек Бахтиёрович
Ташкентский государственный экономический университет
Преподаватель кафедры математических методов в экономике

Аннотация. *В данной статье исследуются процессы формирования транзакций блокчейна. Также рассмотрены механизмы подписания кредитных блокчейн-транзакций и их теоретические основы. В ходе исследования была предложена модель, включающая процесс подписания и проверки подписи кредитных транзакций блокчейна. В предлагаемой модели для подписания транзакций применяется алгоритм электронной цифровой подписи ECDSA (Elliptic Curve Digital Signature Algorithm), основанный на эллиптических кривых.Общая модель эллиптических кривых, выбор эффективных эллиптических кривых и ее применение к алгоритму электронной цифровой подписи DSA представлены.*

Ключевые слова: *цифровой банкинг, кредитование, цифровая трансформация, технология блокчейн, криптовалюта, транзакция, электронная цифровая подпись, криптографический алгоритм, Биткойн, Ethereum, Litecoin, электронная коммерция.*

IMPROVING THE METHODS OF SIGNING BLOCKCHAIN TRANSACTIONS IN THE DEVELOPMENT OF DIGITIZATION AND DIGITAL TRANSFORMATION OF THE LENDING INDUSTRY

Rakhimberdiev Kuvonchbek Bakhtiyorovich
Tashkent state university of economics
Teacher of the department of mathematical methods in economics

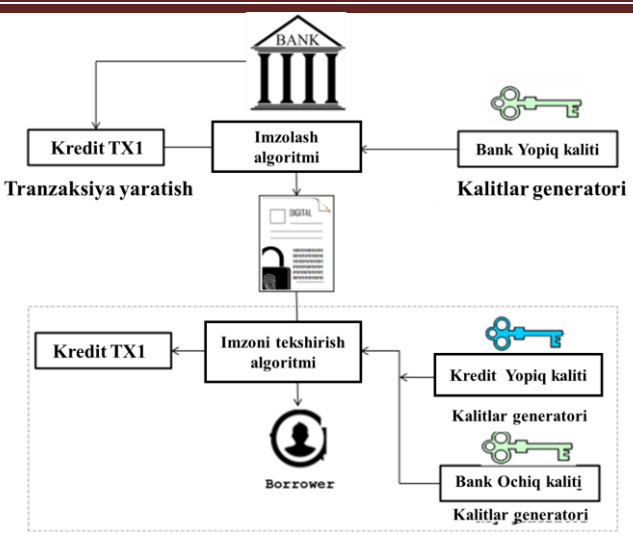
Annotation. *In this article, the processes of forming blockchain transactions are explored. Mechanisms for signing lending blockchain transactions and their theoretical foundations are also considered. During this research, a model was proposed that includes the process of signing and verifying the signature of credit blockchain transactions. In the proposed model, ECDSA (Elliptic Curve Digital Signature Algorithm) electronic digital signature algorithm based on elliptic curves is applied for signing transactions. The general model of elliptic curves, the selection of effective elliptic curves and its application to the DSA electronic digital signature algorithm are presented.*

Keywords: *digital banking, lending, digital transformation, blockchain technology, cryptocurrency, transaction, electronic digital signature, cryptographic algorithm, Bitcoin, Ethereum, Litecoin, e-commerce.*

Kirish. Hozirda mavjud bo‘lgan moliyaviy blokcheynlarda (Bitcoin, Ethereum, Litecoin va h.k.) elliptik egri chiziqlar nazariyasiga asoslangan asimmetrik kalitli kriptografik algoritmlardan foydalaniladi (1-rasm). Asimmetrik kriptotizimlarga asoslangan elektron raqamli imzo algoritmlarini tadqiq qilish va foydalanishda (1)-(2) tenglamalarda ifodalangan holda elektron raqamli imzo usullari ishlab chiqiladi. Elektron raqamli imzo algoritmlari kreditlash tranzaksiyani amalga oshirgan kredit oluvchilarni tasdiqlash va axborot almashinuvini shakllantirishda qo‘llaniladi (2-rasm)[5].

Kreditlash blokcheyni tranzaksiyalarni imzolashda elektron raqamli imzodan foydalanish bo‘yicha 2.3.11-rasmda taklif etilayotgan model tranzaksiyalarni imzolash va imzoni tekshirish qismlaridan iborat bo‘lishi lozim. Bunda, ochiq va yopiq kalitlardan foydalaniladi. Ochiq va yopiq kalitlarni hosil qilishda kalitlarni generatsiya qilish algoritmlaridan foydalanish mumkin. Ushbu modelga ko‘ra, Bank-kreditlash tashkiloti tomonidan kreditlash tranzaksiyasi bajarilgandan so‘ng uning yopiq kaliti yordamida imzolash algortimi bajariladi. Tranzaksiyaga qo‘ilgan imzoni tekshirish jarayonida kredit oluvchi mijoz yopiq kaliti, bank-kreditlash tashkiloti ochiq kalitidan foydalaniladi[15].

Hozirgi kunda, keng tarqalgan Bitcoin blokcheyni platformasida tranzaksiyalarni imzolashda ECDSA (Elliptic Curve Digital Signature Algorithm) va ECRSA[13] algoritmlari qo‘llaniladi[14]. Elliptik egri chiziqlar, Veyershtrass tenglamasining xususiy holi sifatida aniqlanuvchi (63) ko‘rinishidagi egri chiziqqa aytiladi, bu yerda $a,b \in F_p$, F_p - biror chekli maydon bo‘lib, ushbu maydondagi nuqtalar sonini anglatadi. Mazkur egri chiziq parametrlarini hisoblagan holda samarali elliptik egri chiziqlarni tanlash mumkin.



2-rasm. Bank kreditlash tashkilotlarida tranzaksiyalarni imzolash va imzoni tekshirish jarayoni

Manba: *taklif etilgan blokcheyn va intellektual texnologiyalar asosidagi kreditlash jarayoni modeli asosida muallif ishlanmasi.*

(63) ko‘rinishda keltirilgan egri chiziqni DSA (Digital Signature Algorithm) elektron raqamli imzo algoritmiga tadbiq etgan holda, ECDSA algoritmini takomillashtirish mumkin[6].

$$y^2 = x^3 + ax + b \qquad (1)$$

Tadqiq etilayotgan ECDSA algoritmning asosiy xarakteristikasi p-tub sondan tuzilgan chekli maydonda aniqlangan (63) tenglama ko‘rinishidagi E- elliptik egri chiziq hamda ushbu egri chiziqga tegishli bo‘lgan katta tub tartibga ega bo‘lgan $G \in E(F_p)$ - bazaviy nuqta hisoblanadi. Ta’kidlash joizki, elliptik egri chiziq ko‘rinishi uning $a,b \in F_p$ parametrlariga bog’liq holda o‘zgaradi. Shuningdek, elliptik egri chiziq tenglamasining ahamiyatli parametrlaridan biri diskriminanti bo‘lib, u quyidagicha keltiriladi[7]:

$$D = -16(4a^3 + 27b^2) \qquad (2)$$

ko‘rinishida bo‘lib uning invarianti sifatida $j = \frac{1728(4a)^3}{D}$ keltiriladi. Ushbu j invariantdan foydalangan holda (2) tenglamaning a,b parametrlari koyfitsientlarini quyidagicha aniqlaymiz:

$$k \equiv \frac{j}{1728-j} (\text{mod } p), \quad j \neq 0, j \neq 1728'$$

$$\begin{cases} a \equiv 3k (\text{mod } p) \\ b \equiv 2k (\text{mod } p) \end{cases} \qquad (3)$$

(65) taqqoslamalar orqali keltirilgan parametr koyfitsientlari, elliptik egri chiziqning G bazaviy nuqtasi $F_p : G = (x_G, y_G)$ chekli maydonda olingan (x_G, y_G) elementlar juftligi bilan aniqlanadi[12].

Mavzuga oid adabiyotlar tahlili. Hozirgi kunda butun dunyoda iqtisodiyotni raqamlashtirish jarayoni jadal rivojlanmoqda. Ko‘pchilik iqtisodiy jarayonlarni amalga oshirishda raqamli va axborot texnologiyalari qo‘llanilishi yuqori iqtisodiy samaradorlikka olib kelmoqda. Bank-kreditlash sohalari iqtisodiyotning muhim bo‘g’inlaridan biri hisoblanadi. Ushbu sohalarda raqamlashtirish jarayonini samarali tashkil etish iqtisodiy samaradorlikning ortishida ahamiyatli hisoblanadi. Shu boisdan, bank-kreditlash jarayonlarini raqamlashtirishda blokcheyn, su’iy intellekt, IOT, bulutli texnologiyalar va boshqa texnologiyalarni qo‘llash masalalari dunyo olimlari tomonidan dolzarb hisoblanmoqda.

Jumladan, moliyaviy tizimlarga blokcheyn texnologiyasini tadbiq etish bo‘yicha dastlabki tadqiqotlar yaponiyalik olim Satoshi Nakamoto ilmiy ishlarida keltirilgan bo‘lib, unda dastlabki kriptovalyuta modelini va tranzaksiyalarni shakllantirish jarayonlarini amalga oshirish bo‘yicha takliflari keltirilgan hamda ushbu modellar asosida bitcoin kriptovalyutasi ishlab chiqilgan. W.Frank va Y.N.Sotskovlarning ilmiy tadqiqotlari kreditlash sohasini iqtisodiy matematik modellashtirishga yo‘naltirilgan bo‘lib, ular ushbu sohani raqamlashtirishda matematik modellashtirish va dasturlash lozimligini ilgari suradilar[1].

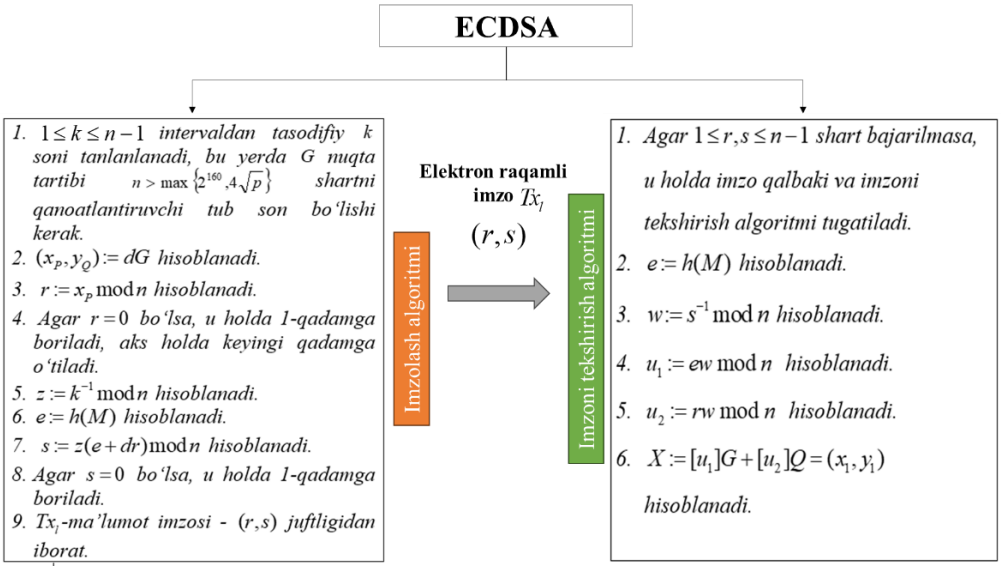
C.Lin, D.He, S.Zeadally, N.Kumar ilmiy ishlari natijalariga ko‘ra, kreditlash tizimlariga blokcheyn texnologiyasining qo‘llanilishi bank tashkilotlarida axborot almashinuv jarayonini 30% oshishiga olib kelganligini ko‘rish mumkin[2]. Ammo, Muxi Li fikrlariga ko‘ra, blokcheyn asosida elektron tijorat tizimlarini ishlab chiqish, ma’lumotlar bazasi sifatida foydalanishdan samarali

hisoblanadi[3]. Shuning ilan bir qatorda, ushbu masalalar bo‘yicha mamlakatimiz olimlari ham izhil tadqiqotlar olib bormoqdalar. Jumladan, G.U.Jurayev ilmiy ishlarida, blokcheyn bloklarini yaratishda zarur bo‘lgan kriptografik algoritmlar tadqiq etilgan. S.Gulyamov va M.Q.Abdullayevlarning ilmiy ishlari blokcheyn texnologiyasining raqamli iqtisodiyotni takomillashtirishda qo‘llanilishiga bag’ishlangan[4].

Mazkur ilmiy tadqiqotlar natijalari va ilmiy xulosalariga tayangan holda blokcheyn tranzaksiyalarining konfedentsialligini ta’minlashda elektron raqamli imzo algoritmlari ahamiyatli ekanligini anglash mumkin.

Tadqiqot metodologiyasi. Ushbu ilmiy tadqiqot davomida, elliptik egri chiziqlarni shakllantirish usullari, elekron raqamli imzoni takomillashtirishda asimmetrik kriptografik usullar foydalanilagan. Kreditlash blokcheyni tranzaksiyalarini imzolashda takomillashtirigan ECDSA elektron raqamli imzo algoritmi qo‘llanilgan.

Tahlil va natijalar muhokamasi. ECDSA elektron raqamli imzo algoritmi umumiy algoritmi quyidagicha keltiriladi: 2.3.2-jadvalda keltirilgan Tx_l-imzolanishi tranzaktsiya ma’lumoti bo‘lib, shu tranzaksiyaga (r,s) sonlar juftligidagi imzo hisoblanishi kerak (2-rasm)[7].



3-rasm. ECDSA elektron raqamli imzo algoritmining imzolash va imzoni tekshirish algoritmi

Manba: *muallif ishlanmasi.*

3-rasmda keltirilgan ECDSA elektron raqamli imzo algoritmi imzolash va imzoni tekshirish modullaridan iborat bo‘ladi. Imzolash jarayoni kiruvchi dastlabki 256 bitlik, $hash(Tx_l)$ xesh qiymatga ega bo‘lgan tranzaksiyani imzolaydi va imzo sifatida (r,s) juftlik qabul qilinadi hamda tekshiruvchiga (Bank–kreditor tashkilot) jo‘natiladi. Tekshiruvchi tomonidan imzoni tekshirish jarayonida, Tx_l tranzaksiya, imzoni tekshirish kaliti hamda Tx_l tranzaksiyasi imzosi kabi asosiy parametrlar tekshiriladi. Natijada, $r = x_1 \bmod n$ shart bajarilsa, imzo haqiyqiy aks holda imzo qalbaki kabi qaror qabul qilinadi hamda imzoni tekshirish jarayoni algoritmi tugaydi[8].

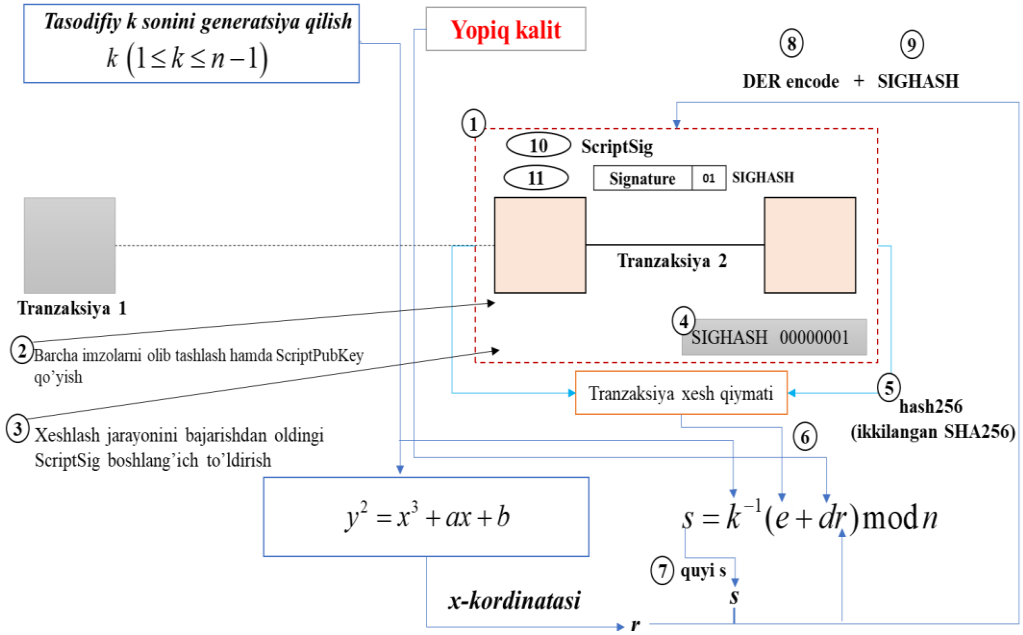
Endi, biz (2) tenglikda keltirilgan 2-jadvaldagi tranzaksiyaning $hash(Tx_l)$ xesh qiymatini 3-rasmda keltirilgan elektron raqamli imzo algoritmidan foydalangan holda imzolaymiz. Kreditlash tranzaksiyalarini imzolashning umumiy modeli quyidagicha taklif etiladi (4-rasm).

Ushbu taklif etilayotgan kreditlash tranzaksiyalarini imzolashning umumiy modeli quyidagicha amalga oshiriladi:

1-qadam: Tranzaksiya (4-rasm) (45) va (46) tenglamalardagi kirish va chiqishlar yaratiladi. Ushbu jarayon tangalar (coin) harakatini ifodalaydi (3-jadval);

2-qadam: Tranzaksiyalarni imzolashda biz tangalar (coin)lar harakatini ifodalovchi ma’lumotlar imzolanadi. Shu boisdan, oldin imzolangan boshqa kirishlar uchun **scriptSigs** yaratilgan bo‘lsa, ushbu script vaqtinchalik olib tashlanadi. Agarda, dastlabki kirish qulfdan chiqarilayotgan bo‘lsa, ushbu scriptni olib tashlash shart emas;

3-qadam: Kirishning oldingi qulflash (locking) scripti **Scriptpubkey** imzo qo‘yilishi lozim bo‘lgan joyga **Scriptsig** qilish. Ushbu holda, tranzaksiya ma’lumotiga ko‘ra 76a9144299ff317fcd12ef19047df66d72454691797bfc88ac qiymatga ega P2PKH qulflash skripti mavjudligi aniqlanadi.



4-rasm. Kreditlash blokcheyni tranzaksiyalarini imzolashning umumiy sxemasi

Manba: *muallif ishlanmasi.*

4-qadam: Kriptografik xesh funksiya scriptlarini tanlash
0x01 = SIGHASH_ALL
0x02 = SIGHASH_NONE
0x03 = SIGHASH_SINGLE
0x81 = SIGHASH_ANYONECANPAY | SIGHASH_ALL
0x82 = SIGHASH_ANYONECANPAY | SIGHASH_NONE
0x83 = SIGHASH_ANYONECANPAY | SIGHASH_SINGLE

Ushbu keltirilgan scriptlar, (56), (57), (58) tenglamalarda keltirilgan SHA256 xesh funksiya algoritmining mantiqiy funksiyalari modifikatsiyalari hisoblanadi. **0x01** = SIGHASH_ALL scripti moliyaviy blokcheynlarda keng qo'llaniladi. Bu imzo tranzaksiyadagi barcha kirish va chiqishlarni qamrab olish xususiyatida ega bo'lib, keyinchalik hech blokcheyn ishtirokchisi ushbu tranzaksiyaga o'zgartirish kirita olmaydi.

5-qadam: Tranzaksiya ma'lumotlarini xeshlash jarayoni bajariladi. Ushbu jarayon keltirilgan tranzaksiya va xesh qiymatni hisoblashni o'z ichiga oladi. Bunda, xesh qiymat (62) ifodalanadi.

6-qadam: Xesh qiymatga ega bo'lgan tranzaksiya imzolanadi. Imzolash jarayonida ECDSA (4-rasm) algoritmidan foydalangan holda tranzaksiyaning ***hash256*** imzolanadi (1-jadval).

1-jadval

Kreditlash tranzaksiyasining *hash256* xesh qiymatini imzolash jarayoni natijasi

Tasnifi	Parametr	Qiymati
*Kiruvchi tranzaksiyaning dastlabki **hash256** xesh qiymati*	***z***	5aaed19ed368ea9bfe7906c2d7f7134cfec4b24099c0847c2d4dd003d4dc1c7a
Tasodifiy tub son	***k***	107568050855228206237571377334021880498481855579694043643564007384972320063445
Yopiq kalit	***d***	284048500822635664737325869314968134570578953930508005459491872485805252331 91
Elliptik egri chiziqning ***x*** parametri	***Qx***	860066480943774524817233469458318409489888870151531327745182902905155816263 57
Elliptik egri chiziqning ***y*** parametri	***Qy***	111220451801836815752761950666039345724628276023112743763294530346407684221124
Elektron imzoning *r parametri qiymati*	***r***	102696466851757881019097172617257171819969511844070700622413115324830381805181
Elektron imzoning *s parametri qiymati*	***s***	381377847271346087934541754008182708525048502855071720168034133300330640055 22

Manba: *hisoblash natijasi asosida muallif ishlanmasi.*

Ushbu jadvaldagi *k, d, Qx, Qy, r, s* parametrlari o‘nlik sanoq sistemasi (decimal) keltirilgan bo‘lib, *hash256* xesh qiymati ***z*** imzolangan. Bunda, raqamli imzo juftligi

(r,s)=545138A0D5B5C6667EA84987D97A7C71E
F21F9D71943B901427FF2228073C
F92E30C23F1010ADFDDEFA061BFA542B
89CBD427DA181439A88C39CECA71DC48E7D

teng bo‘ladi[9,10].

7-qadam: ECDSA electron raqamli imzo algoritmida imzoning *s* parametri *“high”* yuqori va *“low”* quyi qiymatlarga ega bo‘ladi. Ushbu imzo qiymatlari uchun *BIP62* qoidasi bajarilishi lozim, aks holda tranzaksiya blokcheyn tugunlari tomonidan uzatilmaydi. Bizning holatimizda *“low”* quyi s qiymati talab etiladi. Agarda, s qiymati “high” bo‘lsa, *n-s* hisoblash bajariladi. Bunda, *n*-modul, *s*-imzo parametri[11].

8-qadam: Shakllantirilgan elektron raqamli imzoni formatlash bajariladi. Kreditlash blokcheyni imzoni kodlashda DER encoding foydalanish mumkin. DER encoding (r, s) imzo juftligi ma’lumotiga baytlar qo‘shishni anglatadi. Bunda, baytlar uzuligi 0x80 dan oshmasligi talab etiladi. DER encoding (r, s) imzo juftligi quyidagicha[12]:

r=*08f4f37e2d8f74e18c1b8fde2374d5f28402fb8ab7fd1cc5b786aa40851a70cb*
s= *1f40afd1627798ee8529095ca4b205498032315240ac322c9d8ff0f205a93a58*

9-qadam: Imzoning xesh funksiya turi DER kodlangan imzoga qo‘shiladi. Natijada, s imzo parametrining yangi qiymati quyidagicha:

s=*3044022008f4f37e2d8f74e18c1b8fde2374d5f28402fb8ab7fd1cc5b786aa40851a70cb02201f40afd162*
7798ee8529095ca4b205498032315240ac322c9d8ff0f205a93a5801

10-qadam: unlocking scriptni yaratish. Bunda, P2PKH locking script standarti amalga oshiriladi. Natijada, Scriptpubkey va Scriptsig psevdokodi quyidagicha:

Scriptpubkey:

Publickey:*024aeaf55040fa16de37303d13ca1dde85f4ca9baa36e2963a27a1c0c1165fe2b1*
Signature:*3044022008f4f37e2d8f74e18c1b8fde2374d5f28402fb8ab7fd1cc5b786aa40851a70cb02201f*
40afd1627798ee8529095ca4b205498032315240ac322c9d8ff0f205a93a5801

Scriptsig:

hex:473044022008f4f37e2d8f74e18c1b8fde2374d5f28402fb8ab7fd1cc5b786aa40851a70cb02201f
40afd1627798ee8529095ca4b205498032315240ac322c9d8ff0f205a93a580121024aeaf55040fa16d
e37303d13ca1dde85f4ca9baa36e2963a27a1c0c1165fe2b1

bunda, tranzaksiyaga **Publickey**-ochiq kalitdan foydalangan holda **Scriptsig** imzo qo‘yildi.

11-qadam: Ishlab chiqilgan unlocking scripti tranzaksiyani qulflash scripti ishga tushuriladi. Barcha hisoblash qadamlarini umumiylashtirgan va kreditlash blokcheyni tranzaksiya kirish(lar) va chiqish(lar) modeliga mos holda quyidagicha jadvalni shakllantiramiz (1-jadval):

1-jadval

Kreditlash blokcheyni tranzaksiyasi umumiy ko‘rinishi rasmiy protokol spetsifikatsiyasi ko‘rinishida ifodalanishi

version		01 00 00 00
kirishlar soni		01
kirish(lar)	oldingi tranzaksiya xeshi	5aaed19ed368ea9bfe7906c2d7f7134cfec4b24099c 0847c2d4dd003d4dc1c7a
	oldingi tranzaksiya chiqishi tartib raqami	00 00 00 00
	skript uzunligi	6a
	scriptSig	473044022008f4f37e2d8f74e18c1b8fde2374d5 f28402fb8ab7fd1cc5b786aa40851a70cb02201f 40afd1627798ee8529095ca4b20549803231524 0ac322c9d8ff0f205a93a580121024aeaf55040fa 16de37303d13ca1dde85f4ca9baa36e2963a27a1 c0c1165fe2b1
	sequence	ff ff ff ff
chiqishlar soni		01
chiqish(lar)	qiymat	983a000000000000
	skript uzunligi	19
	scriptPubKey	024aeaf55040fa16de37303d13ca1dde85f4ca9b aa36e2963a27a1c0c1165fe2b1
blokirovka qilish vaqti		00 00 00 00

Manba: *muallif ishlanmasi.*

Ushbu jadvalda kreditlash blokcheyni tranzaksiyasi maxsus protokol spetsifikatsiyasi ko‘rinishida ifodalandi. Bunda, UzBCS kreditlash blokcheyni tranzaksiyasi imzolandi. Endi ushbu jadvaldagi barcha ma’lumotlarni ketma-ketga yozgan holda UzBCS kreditlash blokcheyn tarmog’iga uzatish uchun tranzaksiyanni shakllantiramiz.

Transaction:*01000000015aaed19ed368ea9bfe7906c2d7f7134cfec4b24099c0847c2d4dd003d4dc1c7a000000006a473044022008f4f37e2d8f74e18c1b8fde2374d5f28402fb8ab7fd1cc5b786aa40851a70cb02201f40afd1627798ee8529095ca4b205498032315240ac322c9d8ff0f205a93a580121024aeaf55040fa16de37303d13ca1dde85f4ca9baa36e2963a27a1c0c1165fe2b1ffffffff01983a00000000000019024aeaf55040fa16de37303d13ca1dde85f4ca9baa36e2963a27a1c0c1165fe2b100000000*

Xulosa va takliflar. Xulosa qilib aytganda, ushbu ilmiy tadqiqot davomida tranzaktsiyalarni imzolashda ECDSA elektron raqamli imzo algoritmi qo‘llanildi. Natijada, kreditlash blokcheyn platformasi tranzaksiyasining SHA256 xesh funksiya algoritmi asosidagi qiymatidan foydalangan holda imzolash va imzoni tekshirishchu ochiq va yopiq kalitla ishlab chiqildi. Ushbu hisoblashlar davomida, ECDSA electron raqamli imzo algoritmi EL-Gamal, RSA, DSA, GOST va boshqa algoritmlarga qaragnda blokcheyn tranzaksiyalarini imzolashda samarali ekanligi aniqlandi.

Bundan,quydagicha ilmiy asoslangan natijalarga asoslangan holda taklilar ishlab chiqildi:

- raqamli iqtisodiyot sharoitida kreditlash tizimlariga zamonaviy moliyaviy va blokcheyn texnologiyalarini joriy etish hamda ular asosida tranzaksiyalar xavfsizligini taminlashning konseptual modellar asoslash mumkin;

- kreditlash tranzaksiyalari xavfsizligini ta’minlash va imzolashda SHA256 xesh funksiya hamda ECDSA elektron raqamli imzo algoritmlaridan foydalanish metodologiyalari taklif etiladi.

Manba va foydalanilgan adabiyotlar ro‘yxati:

1. *Frank Werner and Yuri N. Sotskov «Mathematics of Economics and Business» First published 2006 by Routledge, 52 Vanderbilt Avenue, New York, NY 10017, USA, pp. 536.*
2. *Балтаев.Д.Р., Рақамли иқтисодиёт экотизими. Ривожланишда тутган ўрни, "Science and Education" Scientific Journal/ISSN 2181-0842,June 2022. 1-9 bet.*
3. *Chen, Chiu-Chin; Liao, Chia-Chun (September 15, 2021). "Research on the development of Fintech combined with AIoT". 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). IEEE. pp. 1–2.*
4. *Van Loo, Rory (February 1, 2018). "Making Innovation More Competitive: The Case of Fintech". UCLA Law Review. 65 (1): 232.*
5. *C. Lin, D. He, S. Zeadally, N. Kumar, K.-K.R. Choo, SecBCS: a secure and privacy-preserving blockchain-based crowdsourcing system, Sci. China Inf. Sci. 63 (3) (2020), 1 – 14 pp.*
6. *A. M.Antonopoulos, "Mastering Bitcoin," in Mastering Bitcoin, OREILLY , 2015, pp. 121.*
7. *Ganiev S.K., Karimov M.M., Tashev K.A., Axborot xavfsizligi. Axborot kommunikaцion tizimlar xavfsizligi.– T.: «Fan va texnologiя», 2022, -407 bet*
8. *Berdimurodov M.Q., Raximberdiyev Q.B., Statistik echimlar nazariyasini maksimal haqiqatga yaqinlashuvchanlik kripto analiz usuliga qo‘llash, O‘zbekiston Respublikasi Fanlar Akademiyasining Qoraqalpog’iston bo‘limi Axborotnomasi, 2020 yil 3-son, ISSN-2091-508X Nukus 2020 y., 5-11 bb.*
9. *Berdimuratov M.Q., Raximberdiyev Q.B., Yuldashev A., Kriptografik algoritmlarning kripto mustahkaligini tekshirishda kriptoanaliz usullarining ahamiyati, Berdaq nomidagi Qoraqalpoq davlat universiteti, «Tabiiy fanlarni rivojlantirishda axborot-kommunikatsiya texnologiyalarining o‘rni». Respublika ilmiy-amaliy konferensiyasi maqolalar to‘plami. Nukus, «Qaraqalpaqstan» nashriyoti, 2021, 205-207b.*
10. *Raximberdiyev Q.B., Effective digital signature algorithms for bank lending platforms based on blockchain technology in the digital economy, Xorazm ma’mun akademiyasi axborotnomasi –6/2-2023, Xiva 2023, 97-105 bb.*
11. *Raximberdiev Q.B., PRCA intelektual tizimlar asosidagi uzbcs blokcheyn kreditlash platformasi uchun samarali xesh funksiya algoritmini tanlash, Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali, Vol. 1 No. 2 (2023), 33-42 bb.*
12. *Berdimuratov M., Raximberdiyev Q.B., Kriptografik algortimlarning kriptobardoshliligini oshirishda elliptik egri chiziqlar nazariyasining qo‘llanilishi, Вестник КГУ им. Бердаха. № 4 (57) Nukus 2022,1-8 bb.*
13. *Rakhimberdiev K.B., Mathematical modeling of logic blockchain technology on the basis of RSA algorithm, Science and Education in Karakalpakstan 2021 №3, pp.12-18.*
14. *Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Date Written: Bitcoin.org, August 21, 2008, pp.1-9.*
15. *Rakhimberdiev K.B., Application of blockchain technologies in ensuring the security of lending transactions in the digital economy, “Iqtisodiyot va innovatsion texnologiyalar” (Economics and Innovative Technologies) ilmiy elektron jurnali, 2/2023, mart-aprel (№ 00064), 340-352 bb.*