МАТЕМАТИКАЛЫҚ ЖӘНЕ КОМПЬЮТЕРЛІК МОДЕЛЬДЕУ
МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ
MATHEMATICAL AND COMPUTER MODELING

DOI 10.51885/1561-4212_2024_2_144
МҒТАА 81.93.29

Д.Д. Қиноят[1], Р.У. Мукашева[2]
[1]«Сарапшы Плюс» коллекторлық агенттігі, Алматы қ, Қазақстан
E-mail: kdinayadi@gmail.com
[2]Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті,
Өскемен қ., Қазақстан
*E-mail: mukashevaru@mail.ru**

BLOCKCHAIN ТЕХНОЛОГИЯСЫ НЕГІЗІНДЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ КОМПЬЮТЕРЛІК МОДЕЛІН ӘЗІРЛЕУ

РАЗРАБОТКА КОМПЬЮТЕРНОЙ МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИИ BLOCKCHAIN

DEVELOPMENT OF A COMPUTER MODEL FOR ENSURING INFORMATION SECURITY BASED ON BLOCKCHAIN TECHNOLOGY

Аңдатпа. *Цифрлық технологиялар мен ақпараттық қатерлер дәуірінде деректердің қауіпсіздігін қамтамасыз ету басым мәселе болып табылады. Бұл жұмыста қауіпсіз қаржылық операцияларды қамтамасыз қамтамасыз ету және деректермен алмасу мәселесін шешетін транзакцияларды қауіпсіз орындауға мүмкіндік беретін блокчейн технологиясына негізделген инновациялық компьютерлік модель ұсынылған. Blockchain технологиясын және SHA-256 алгоритмін қолдана отырып, модель ақпараттың тұтастығы мен өзгермеуіне кепілдік береді, бұл ақпаратты манипуляциялар мен өзгерістерден қорғайды.Әзірленген бағдарлама мәтіндік ақпараттың хэш мәндерін сенімді есептеу үшін SHA-256 алгоритмін қолданады. Сонымен қатар, жұмыста блокчейн технологиясын практикалық түрде қолдану мысалдары келтірілген, соның ішінде Metamask кибер-әмиянын ашу және Goerli тесттік желісінде шынайы транзакцияларды жасау қарастырылған. Бұл модельді нақты сценарийлерде қалай тиімді қолдануға болатындығын көрсетеді. Зерттеу нәтижелері ақпараттық қауіпсіздікті қамтамасыз етудегі блокчейн технологиясының болашағы мен тиімділігі туралы қорытынды жасауға мүмкіндік береді.Зерттеу нәтижелері ақпараттық қауіпсіздікті қамтамасыз етудегі блокчейн технологиясының болашағы мен тиімділігі туралы қорытынды жасауға мүмкіндік береді.*

Түйін сөздер: *транзакция; блокчейн; крипто-әмиян; Metamask; тесттік желі; Goerli; Ethereum; Эфириум; майнер.*

Аннотация. *В эпоху цифровых технологий и информационных угроз обеспечение безопасности данных является приоритетным вопросом. В данной работе представлена инновационная компьютерная модель, основанная на технологии блокчейн, которая позволяет безопасно совершать транзакции, что решает проблему обеспечения безопасных финансовых операций и обмена данными. Благодаря использованию технологии блокчейн и алгоритма SHA-256, модель гарантирует целостность и неподменность данных, что защищает информацию от манипуляций и изменений. Разработанная программа использует алгоритм SHA-256 для надежного вычисления хэш-значений текстовой информации. Кроме того, в работе представлены примеры практического применения блокчейн-технологии, включая открытие киберкошелька Metamask и проведение реальных транзакций на тестовой сети Goerli.* Это демонстрирует, как модель может быть эффективно применена в реальных сценариях. *Результаты исследования позволяют сделать вывод о перспективности и эффективности технологии блокчейн в обеспечении информационной безопасности.*

Ключевые слова: *транзакция; блокчейн; крипто-кошелек; Metamask; тестовая сеть; Goerli; Ethereum; Эфириум; майнер.*

Abstract. *In the era of digital technologies and information threats, ensuring data security is a priority issue. This paper presents an innovative computer model based on blockchain technology, which allows you to safely make transactions, which solves the problem of ensuring secure financial transactions and data exchange. Thanks to the use of blockchain technology and the SHA-256 algorithm, the model guarantees the integrity and non-substitution of data, which protects information from manipulation and changes.The developed program uses the SHA-256 algorithm for reliable calculation of hash values of textual information. In addition, the paper presents examples of the practical application of blockchain technology, including the opening of the Metamask cyber wallet and conducting real transactions on the Goerli test network. This demonstrates how the model can be effectively applied in real-world scenarios. The results of the study allow us to conclude that blockchain technology is promising and effective in ensuring information security.*

Keywords: *transaction; blockchain; crypto wallet; Metamask; test network; Goerli; Ethereum; Ethereum; miner.*

Кіріспе. Деректер экономикада, әлеуметтік өзара әрекеттесуде және техникалық инновацияларда шешуші рөл атқаратын қазіргі цифрлық технологиялар әлемінде ақпараттың сенімді қорғалуын қамтамасыз ету барған сайын басым міндетке айналуда. Ақпараттық қауіпсіздікке деген қызығушылықтың артуы деректердің құпиялылығын, тұтастығын және сәйкессіздігін қамтамасыз ете алатын инновациялық тәсілдерді үнемі іздеуге әкеледі. Бұл тұргыда, блокчейн технологиясы транзакция қауіпсіздігі мен деректерді сақтаудың ең перспективалы шешімдеріпің бірі ретінде ерекшеленеді.

Бастапқыда криптовалюталардың негізі ретінде құрылған Блокчейн орталықтандырылмаган қаржылық операцияларга арналган инфрақұрылымнан әлдеқайда көп болды. Оның блокчейнге негізделген бірегей құрылымы жогары сенімділік пен мөлдірлікті қамтамасыз етеді. Әрбір транзакция расталады және блокчейнде сақталады, бұл деректерді манипуляциялау және бұрмалау мүмкіндігін жояды. Алайда, blockchain қосымшаларында қауіпсіздікті жүзеге асыру тек осы технологияның негіздерін түсінуді гана емес, сонымен қатар қосымша қорганыс қабатын қамтамасыз ете алатын инновациялық әдістерді әзірлеуді қажет етеді.

Бұл зерттеудің мақсаты транзакциялар кезінде ақпараттың сенімді қорғалуын қамтамасыз ету үшін блокчейн технологиясына негізгі ірге тасы болып табылатын хэштеу операциясын жүзеге асыратын компьютерлік модельді әзірлеу және талдау, сондай-ақ goerli сынақ желісіпің мысалында блокчейн технологиясының практикалық қолданылуын зерттеу болып табылады.

Зерттеудің міндеттеріне компьютерлік модельді әзірлеу, SHA және MD5 алгоритміп қарастыру, Metamask кибер-әмиянын және Goerli сынақ желісін пайдалана отырып, транзакциялардың шынайы мәнінде қалай жүзеге асатынын зерттеу, нәтижелерді талдау және ақпараттық қауіпсіздікті қамтамасыз етудегі блокчейн технологиясының тиімділігіп багалау кіреді.

Зерттеу нысаны: блокчейн технологиясы және оны деректер қауіпсіздігі мен транзакцияларды жүзеге асыруда қолдану.

Зерттеу пәні: блокчейн технологиясына негізделген компьютерлік модель, сонымен қатар Goerli сынақ желісіпің мысалында осы модельдің практикалық қолданылуын талдау.

Бұл тақырыптың өзектілігі блокчейн технологиясына деген қызығушылықтың артуына, оны әртүрлі салаларда қолдануга, сондай-ақ цифрлық қауіптердің қарқынды дамуына байланысты. Бұл зерттеудің практикалық маңызы бар және ақпараттық қауіпсіздікті қамтамасыз етудің тиімді әдістерін дамытуга, сондай-ақ осы салада блокчейннің түсінігі мен әлеуетін ілгерілетуге ықпал етуі мүмкін.

Әдеби шолу. Мақалада [1] Blockchain технологиясы негізінде Бішкек қаласының Ішкі істер бас басқармасының экстремизмге және заңсыз көші-қонға қарсы іс-қимыл қызметінің есепті тұлғаларының деректеріп сақтау және өңдеу үшін таратылған құжат айналымы жүйесін әзірлеу нәтижелері келтірілген. Мақалада [2] жүргізілген зерттеу веб-қосымшалардағы деректердің қауіпсіздігі мен сенімділігін арттырудағы блокчейн технологиясының рөліне багытталган. Жұмыста блокчейнді қолданатын онлайн оқыту платформаларындағы деректердің қауіпсіздігін жақсарту жолдары қарастырылады, блокчейн пайдаланушылардың авторизациясына шабуылдарды қалай болдырмайды, сонымен қатар онлайн курстық платформаларга арналган блокчейн транзакциясының моделі ұсынылган мәселелер талқыланады. Мақала авторлары [3] спутниктік ресурстардың шектеулі болуына байланысты спутниктік байланыс жүйелерінің осалдыгы мәселелерін қарастырады және байланыс қауіпсіздігін жақсарту үшін архитектуралық шешім ұсынады. Бұл схема спутниктер мен жердегі жабдықты біріктіреді, деректерді тіркеу және аутентификация үшін блокчейнді пайдаланады және эксперименттік модельдеу көрсеткендей, деректерді қоргауды айтарлықтай жақсартады. Кітаптың авторы [4] Bitcoin және Blockchain технологиясына егжей-тегжейлі кіріспе береді, сонымен қатар blockchain қауіпсіздігінің негізі болып табылатын криптографияның негіздерін сипаттайды. Жұмыста [5] блокчейннің негізгі тұжырымдамалары мен оның әртүрлі салаларда, соның ішінде киберқауіпсіздік саласында қолданылуы туралы қол жетімді сипаттама берілген. Кітапта [6] блокчейннің экономика мен қогамның әртүрлі секторларына, соның ішінде ақпараттық қауіпсіздік саласына енгізген өзгертулерінің әлеуеті талқыланады. Кітап авторы [7] блокчейнді әртүрлі салаларда, соның ішінде деректердің қауіпсіздігінде блокчейнді практикалық қолданудың нақты мысалдарына назар аударады. Жұмыста [8] блокчейн технологиясының негізгі аспектілеріне, соның ішінде қауіпсіздікке қысқаша, бірақ ақпараттық шолу жасалынган. Кітап [9] блокчейн қауіпсіздігі мәселелерін қарастырады және әртүрлі қауіптер мен шабуыл сценарийлерін, сондай-ақ қорганыс әдістері мен құралдарын талқылайды.

Мақалада [10] автор блокчейн технологиясына негізделген жеке деректерді өңдеудің инновациялық тәсілін сипаттайды. Бұл тәсіл деректерді өңдеудің қауіпсіздігі мен тиімділігін қамтамасыз етуге багытталган бірқатар негізгі аспектілерді қамтиды. Мақаланың авторы [11] негізделген қауіпсіздік әдістерін сипаттау және салыстыру, Bitcoin және Ethereum-да қолданылатын блоктарды бірнеше рет растау, сондай-ақ желіпің таралуы, әртүрлі блок өлшемдері, блоктарды құру аралықтары, тарату механизмі сияқты нақты әлемдегі шектеулерді ескере отырып, майнерлердің жұмыстарына байланысты оңтайлы стратегиялық ақпарат береді.

Біздің жұмысымызда деректерді хэштеуді SHA және MD5 алгоритмдері арқылы жүзеге асыратын компьютерлік модель, хештеу және транзакциялар алгоритмдері, сондай-ақ goerli сынақ желісі арқылы блокчейндегі транзакцияларды зерттеу қарастырылады.

Материалдар және зерттеу әдістері. Жұмысты орындау барысында келесі теориялық материалдар мен әдістер қолданылды: криптография негіздері, транзакция деректеріп талдау, блокчейн технологиясы, Goerli сынақ желісі, Metamask киберкошелегі, SHA-256, SHA-512 алгоритмі, статистикалық әдістер, транзакция деректеріп қоргау әдістері мен құралдары, сынақ желісіндегі транзакцияларды талдау әдістері.

Жұмыс аясында қолданылган багдарламалар және багдарламалау тілдері: Microsoft Visual Studio, Windows PowerShell, MetaMask, C#.

Нәтижелері және оларды талқылау. Бұл бөлімде хэштеу арқылы деректерді қоргау, блокчейндегі транзакцияларды тесттік желісінің мысалында зерттеу, хэштеуді жүзеге асыратын компьютерлік модель құру сұрақтарын қарастырамыз.

Хэштеу арқылы деректерді қорғау: SHA және MD5 негізіндегі хэштерді есептеудің бағдарламалық моделі. Хэш – ақпаратты қоргау үшін қажетті шифрлау талаптарына жауап беретін функция. Хэш функциясы еркін ұзындықтагы кірістер мәнді хэш коды немесе хэш мәні деп аталатын тұрақты ұзындықтагы шыгыс мәніне түрлендіреді. Хэш функцияларының негізгі қасиеттерінің бірі – оның бірегейлігі: әртүрлі хэш мәндері әртүрлі кіріс мәндеріне сәйкес келуі керек. Хэш функциялары деректердің тұтастыгын тексеру, аутентификация және деректерді іздеу үшін ақпараттық қауінсіздікте кеңінен қолданылады. Олар сондай-ақ ақпаратты тиімді сақтау және іздеу үшін хэш кестелері сияқты деректер құрылымдарында қолданылады [12].

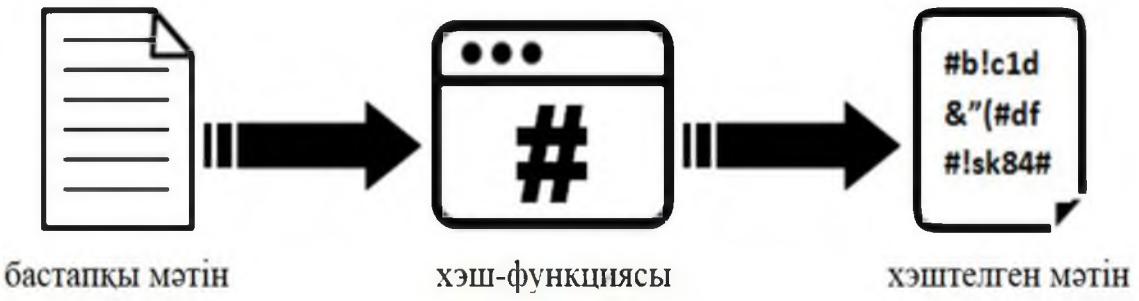
Хэш функциялары қазіргі криптографияда маңызды рөл атқарады. Олар әртүрлі мақсаттарда қолданылады, соның ішінде деректердің тұтастыгын тексеру, цифрлық қолтаңбалар, құпия сөздерді сақтау және кілттерді шыгару. Сонымен қатар, хэш функциялары бір багытта тез есептелетіндей етіп жасалган, бірақ керісінше есептеу мүмкін емес, бұл оларга сүйенетін криптографиялық схемалардың қауінсіздігін қамтамасыз етеді [13].

Бірдей деректер әрқашан бірдей хэштелген мәнді береді. Блокта жазылган ақпараттың бір символы гана өзгерсе, онда хэш сомасы түбегейлі өзгеріске ұшырайды.

Блокчейн жүйесінде әрбір блокта өзіне дейінгі блокта жазылган ақпараттың хешінің бір бөлігі сақталынады, сол себепті де блоктар бір-бірімен әрдайым тыгыз байланыста болады.

Хэштеу алгоритмі төмендегі 1-суреттегідей жүзеге асырылады, ягни бастапқы мәтінге арнайы хэштеу функциясы қолданылады, кейіннен белгілі бір бекітілген ұзындықтагы хештелген мәтін алынады [14].

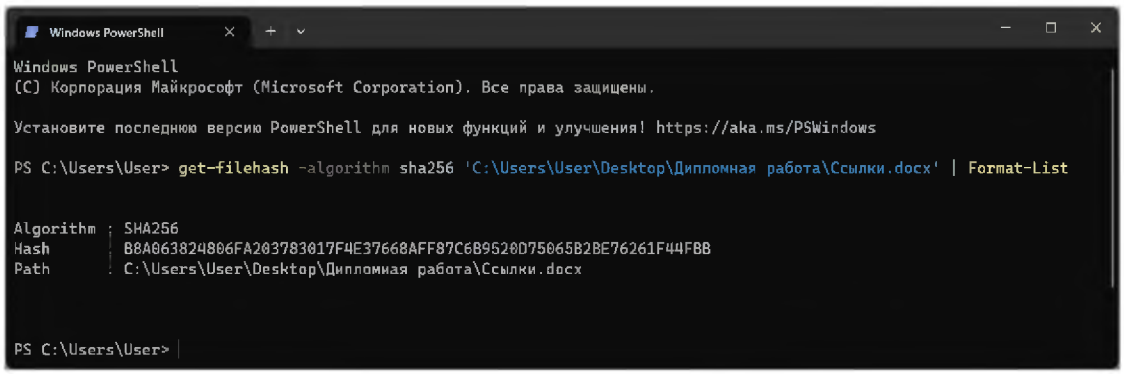
Құжаттарды басқару үшін деректерді аутентификациялауга арнайы хэштеу алгоритмдері қолданылады. Яғни, бүкіл құжат хэштелінеді. Осы ретте хэш – мақұлдау мөрі сынды жұмыс жасайтын болады. Құжатты алушы да деректерді хэштеп, оны түпнұсқамен салыстыра алады. Егер де, хештің екі нұсқасы да бірдей болса, онда деректер шынайы болып тұжырымдалады. Ал керісінше жагдай орын алса, онда құжат өзгеріске ұшырады деген сөз.



1-сурет. Хэштеу алгоритмі

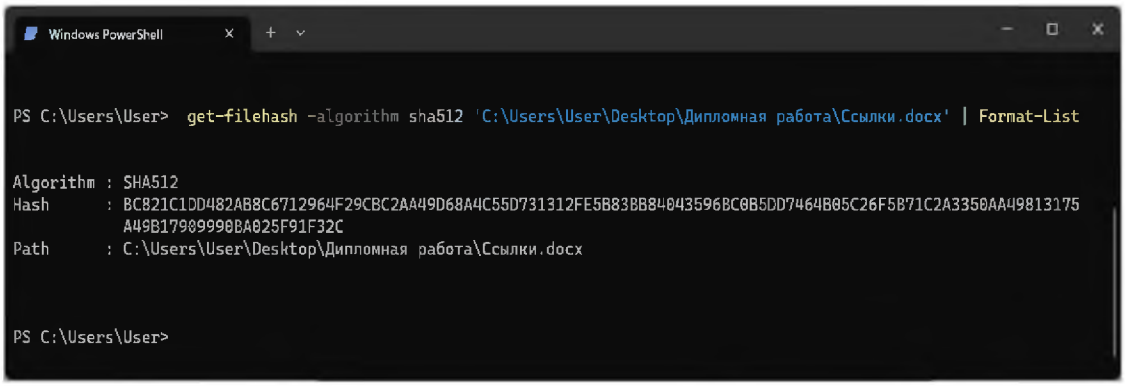
Құжатты хэштеуді Windows операциялық жүйесінде Windows PowerShell багдарламасы арқылы жүзеге асыруга болады. Бұл қосымша арнайы командаларды қолдана отырып, компьютер жадында орыналасқан кез-келген файлды SHA-256 және SHA-512 хештеу алгоритмдеріне түрлендіруге мүмкіндік береді.

Керекті файлдың SHA-256 хэш мәнін есептеу үшін келесі команданы қолдану керек: get-filehash -algorithm sha256 'filename' | Format-List [15].



2-сурет. Файлдың SHA-256 хэш мәнін есептеу

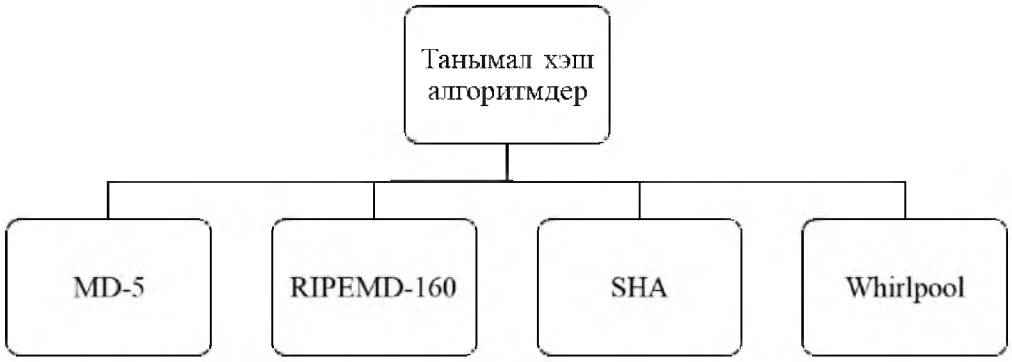
Керекті файлдың SHA-512 хэш мәнін есептеу үшін келесі команданы қолдану керек: get-filehash -algorithm sha512 'filename' | Format-List [15].



3-сурет. Файлдың SHA-512 хэш мәнін есептеу

Керекті команданы жазғаннан кейін бағдарлама алгоритм (Algorithm), құжаттың хэші (Hash) және файлдың орналасқан жері (Path) сынды деректерді көрсетеді.

Төмендегі 1-сызбада ең танымал деген хэш алгоритмдер көрсетілген.



1-Сызба. Танымал хэш алгоритмдері

MD5 (HMAC) хештеу алгоритмі – кеңінен мақұлданған алғашқы алгоритмдердің бірі болып табылады, 1991 жылы жасалған және сол кезде таңқаларлықтай қауіпсіз деп саналған болатын, сол уақыттан бері тіпті ондаған жылдар өтсе де, әлі де танымал алгоритмдердің бірі болып есептелінеді.

Бағдарламаны жасау үшін C# объектіге бағытталған бағдарламалау тілі және Microsoft Visual Studio 2013 интеграцияланған бағдарламалау ортасы пайдаланылды.

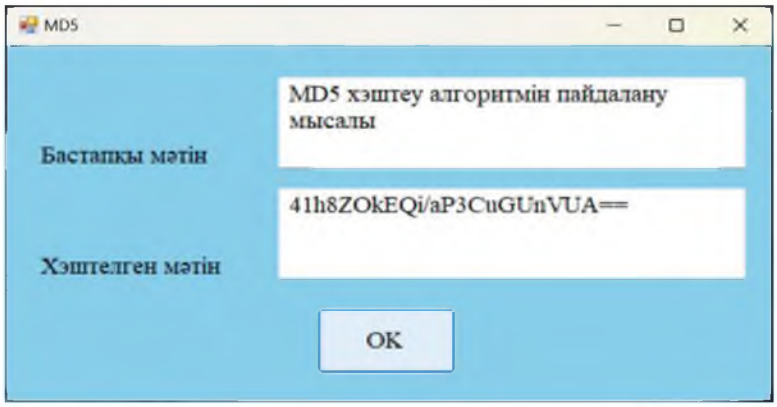
4-суретте MD5 хэштеу алгоритміпің бағдарламалық бейнесі көрсетілген, бұл терезеден бастапқы мәтінді және бағдарлама есептен шығарған хэштелген мәтінде байқауға болады.

Келесі танымал хэштеу алгоритмі бұл – SHA криптографиялық хэш функциялары тобы.

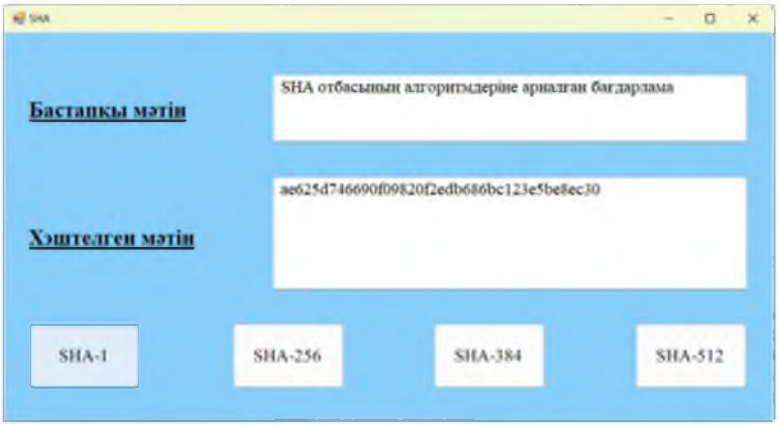
Төмендегі 5-суретте C# объектіге бағытталған бағдарламалау тілінің арнайы кітапханасын қолдана отырып жасалынған қосымша терезесі бейнеленген. Бұл бағдарлама енгізілген бастапқы мәтінді SHA отбасының 4 түрлі алгоритмдерін пайдалана отырып, хэштеуге қабілетті.

SHA топтағы ең көп қолданылатын алгоритмдердің бірі SHA-1 болып табылады.

SHA-1 айнымалы ұзындықты енгізуді қабылдайды және 160 бит тұрақты ұзындық хэш мәнін жасайды. Алгоритмде соқтығысуға төзімділік және бір бағыттылық қасиеттері бар, бұл оны әртүрлі қолданбаларда деректер тұтастығын тексеру және қауіпсіздік үшін пайдалы етеді [16].



4-сурет. MD5 алгоритмінің бағдарламалық көрінісі



5-сурет. SHA-1 алгоритмінің бағдарламалық көрінісі

Блокчейндегі транзакцияларды тесттік желісінің мысалында зерттеу. Блокчейн – белгілі бір ережелерге сәйкес құрылған деректерді ұйымдастыру жүйесі, егер де агылшын тілінен сөзбе-сөз, тура магынада аударса, онда «блоктар тізбегі» деген магына береді.

Блокчейн жүйесінде әрбір транзакция жүйе мүшелерінің көпшілігінің консенсусы арқылы тексеріледі. Бір рет енгізілгеннен кейін ақпаратты ешқашан өшіруге болмайды. Блокчейнде әрбір жасалган транзакция туралы нақты және тексерілетін жазба бар.

Транзакция деп қарапайым сөзбен бір шоттан екінші шотқа ақша аударудан тұратын операцияны атайды. Бұл криптовалюталарга негізделген блокчейн технологиясының негізгі құрылыс материалы. Әрбір транзакцияга меншік құқыгын тексеру және транзакцияның тұтастыгын қамтамасыз ету үшін жіберуші криптографиялық түрде қол қояды.

Крипто-әмияндар сіздің жеке кілттеріңізді – криптовалюталарыңызга кіруге мүмкіндік беретін құпия сөздерді – қауінсіз және қол жетімді етіп сақтайды, бұл сізге Bitcoin және Ethereum сияқты криптовалюталарды жіберуге және алуга мүмкіндік береді [17].

Нақты қолма-қол ақшаны сақтай алатын кәдімгі әмияннан айырмашылыгы, крипто әмияндар қолданушының криптовалюталарын техникалық түрде емес, блокчейн желісінде сақтайды, дегенмен де активтерге тек жеке кілт арқылы гана қол жеткізуге болады. Қолданушының кілттері оның сандық ақшаларына меншік құқыгын растай отырып, транзакциялар жасауга да мүмкіндік береді. Егер де пайдаланушы жеке кілттерін жогалтқан, немесе ұмытқан жагдай орын алса, онда активтеріне қайтадан қол жеткізуі екі талай. Сондықтан да, криптовалютаны жогалтып алмас үшін крипто әмиянның қауінсіздігін қамтамасыз ету немесе сенімді әмиян түрін пайдалану керек, мысалы – Metamask [18].

MetaMask – бұл Ethereum блокчейнімен өзара әрекеттесу үшін қолданылатын криптовалюталық багдарламалық әмиян, әлемдегі ең көп сұранысқа ие криптовалюта әмияндарының бірі.

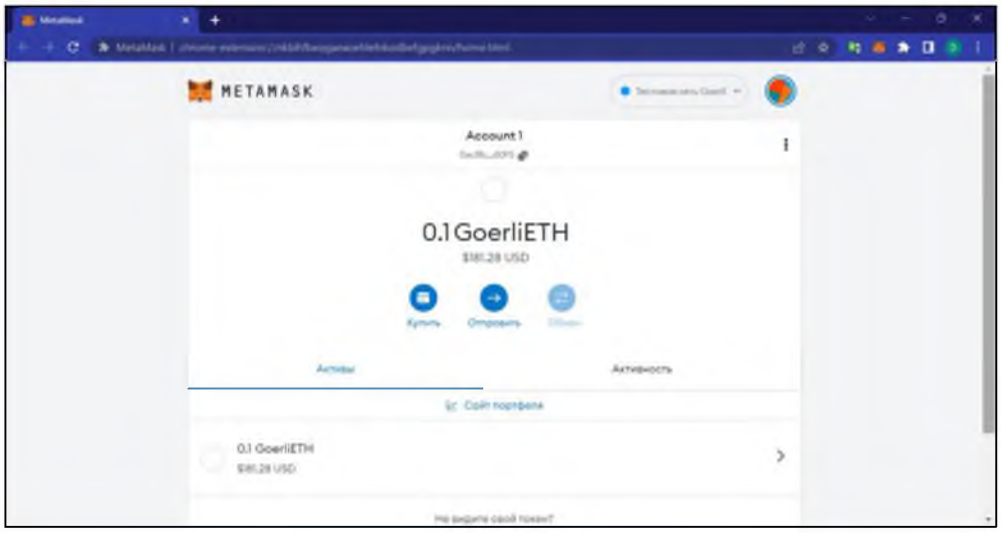
Шынайы транзакцияның қалай жүргізілетінін білу мақсатында Metamask крипто-әмияндагы екі аккаунт қолданылды. Айта кететін жайт, транзациялар жасау үшін шынайы “Ethereum Mainnet” желісін емес, “Goerli” деп аталатын тесттік желіні пайдаланылды.

Тесттік желілер – бұл Эфириум желісіне ұқсайтын және Эфириум сияқты жұмыс жасайтын желілер, алайда олар шынайы ақшамен жұмыс жасамайды және көбінесе багдарламашылардың өздерінің қосымшаларын тексерулері үшін қолданылады.

“Goerli” тесттік желісінде жұмыс жасау үшін “GoerliETH”, ягни “Goerli эфирлары” қажет болады, ал бұны алу үшін goerlifaucet.com деп аталатын сайтқа кіру керек.

7-сурет. Goerli Faucet сайтының көрінісі

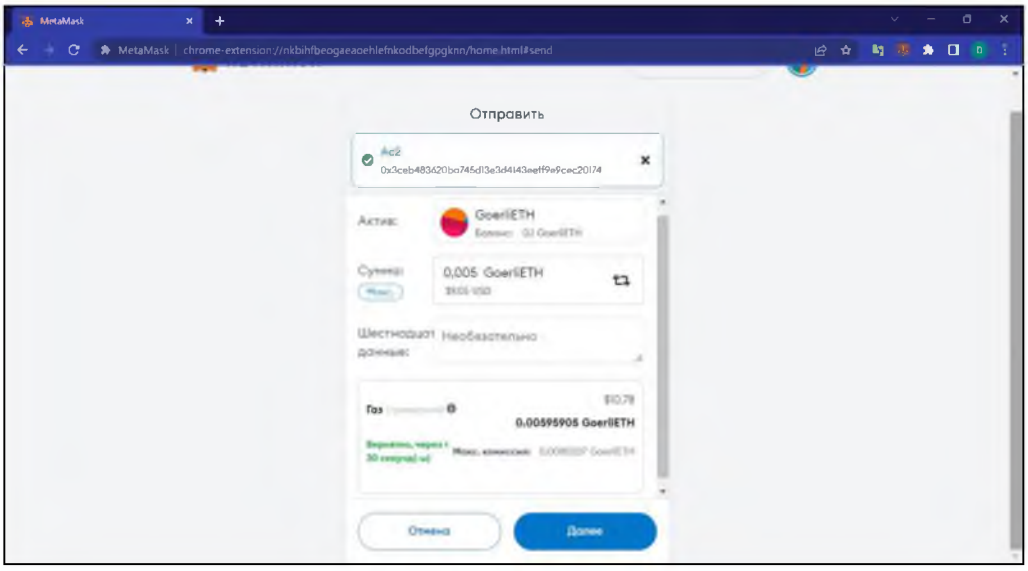
Арнайы шарттарын орындап, “Send Me ETH” батырмасын басса, бірер секундтардан кейін крипто-әмиянға сайтта көрсетілгендей мөлшердегі “GoerliETH” келіп түседі.



8-сурет. Крипто-әмиян

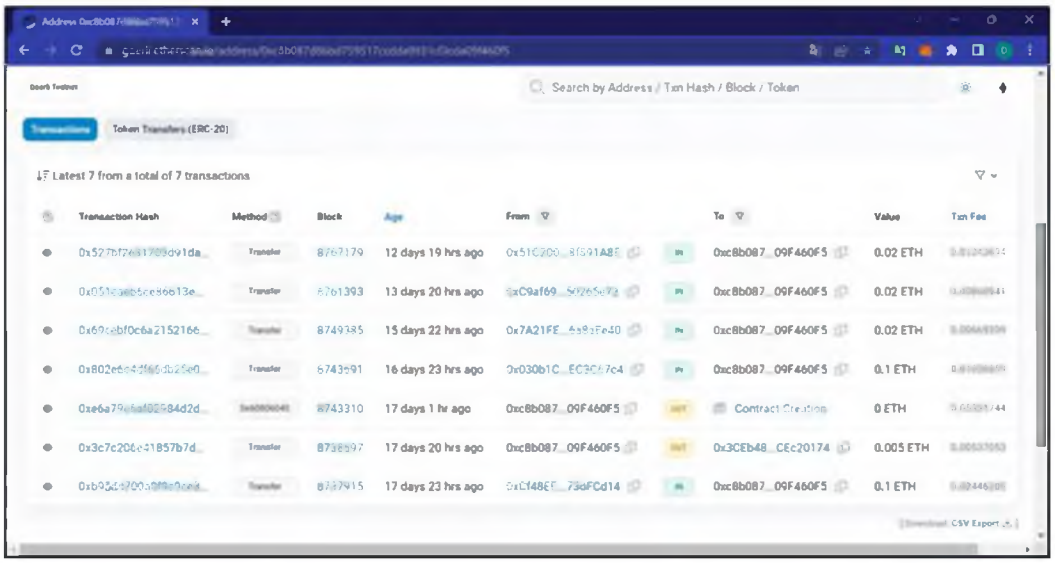
Енді шынайы транзакцияларды да жүргізе берсе болады. Ол үшін «отправить» батырмасын басып, төмендегі 9-суретте көрсетілгендей жіберетін сумма енгізіледі. Бұл жерде айта кететін жайт – газ бағасын да есептеу керек.

Газ – бұл майнерлерге (валидаторларға) транзакцияны блокқа қосу үшін қанша эфир төлеу керектігін анықтайтын блокчейн желісіндегі жұмыс өлшемі. Газ транзакциялар үшін "отын" ретінде қызмет етеді. Блокчейн бір уақытта тонналаған аударымдарды жүзеге асырады. Газ бағасы оны берілген уақыт аралығында қаншалықты көп қолданушылар пайдаланатынына байланысты өзгеріп тұрады.



9-сурет. Транзакция жасау

Блокчейннің ең негізгі қасиеттерінің бірі бұл – ашықтық, биткойн немесе эфириум секілді криптовалюта желілерін алып қарасақ, олардың арнайы сайтына кіру арқылы кез келген транзакция жайлы мәліметтерді оңай білуге болады.



10-сурет. Транзакциялар тарихы

Қолданушыға транзакциялар тарихы жазылған сайттың көмегімен белгілі бір крипто-эмиян арқылы жасалынған барлық тразакциялар жайлы әртүрлі деректерді білуге болады:

– Transaction Hash – жасалынған транзакцияның хеші;

– Method – аударым жасалынған әдіс түрі;

– Block – блок номері;

– Age – транзакцияның жасы, дәлірек айтсам, аударымның қанша уақыт бұрын жасалынғанын көрсетеді;

– From – қандай адрестен аударым жасалынды; бұл жерде айта кететін жайт – “From” және “To” екі кестенің отасында орналасқан сары және жасыл түсті белгілер аударымның жасалынған бағытын көрсетеді, яғни, “IN” – эмиянға жасалынған (кірген) транзакцияны көрсетсе, “OUT” – эмияннан жасалынған (шыққан), яғни қолданушының басқа адреске жіберген аударымын білдіреді;

– To – қандай адреске транзакция жасалынды;

– Value – көлем, қанша эфир жіберілді, соны көрсетеді;

– Txn Fee – криптовалюта транзакцияның жүзеге асырылуы үшін жасалатын міндетті төлемнің түрі, ол крипто-транзакцияларды орындау кезінде аударымдарды өңдеу мақсатында пайдаланушылардан комиссия ретінде алынады.

Транзакцилярдың жұмыс жасау алгоритмі мына әрекеттерді құрайды:

– транзакциялар іске асу үшін, алгоритм бойынша, ең алдымен пайдаланушы көрсеткен деректер құрылымы хабар тарату үшін P2P желілеріне, яғни блокчейннің орталықтандырылмаған желілеріне жіберіледі;

– кейіннен ол деректер міндетті түрде арнайы тексерістен өту керек, егер де тексеріс кезінде қандай да бір бұзушылықтар байқалынса, онда транзакция жасалынбай қалады;

– келесі кезекте желідегі басқа да тексерістен өткен транзакциялардың барлығы біріғіп, жаңа блокты құрайды;

– блок құрылымы – валидациядан, ягни өзге бір тексерістен өтеді. Блоктың валидациясы – блок құрылымының дұрыстығын, оны құру уақытын, оның алдыңғы блокпен үйлесімділігін, сонымен қатар транзакциялық қолтаңбаларды және транзакциялардың блокчейн деректеріне сәйкестігін тексеру;

– тексеріс аяқталғаннан кейін, егер де блок валидациядан сәтті өтсе, онда блоктар тізбегіне келесі жаңа блок ретінде қосылады, ал керісінше жағдайда блок жай ғана жарамсыз деп танылады. Жаңа блок жарамсыз деп табылса, онда блокты барлық түйіндер бірден қабылдамай қояды, және де, нәтижесінде блок жойылады, ал желі түйіндері транзакция деректерін өңдеуді жалғастырады немесе жаңа блоктың хэш-пазлын аяқтайды. Жарамсыз блокты жіберген түйін марапатталмайды.

Қорытынды. Жұмыс барысында ақпараттық қауінсіздікті қамтамасыз ету мақсатында блокчейн технологиясына негізделген компьютерлік модель жасалынды. Бұл модель транзакцияларды жүзеге асыруға және деректерді блокчейнде сақтауға мүмкіндік бере отырып, ақпаратты қоргаудың жогары деңгейіне кепілдік береді. Сонымен қатар, жұмыс аясында SHA және MD5 алгоритмдерін қолдана отырып, енгізілген мәліметтің хэш мәндерін есептеу багдарламасы жасалынды, және де файлдардың хэш мәндерін есептеу жолы көрсетілді. Бұл хэштеу алгоритмдері ақпараттық қауінсіздік саласында кеңінен қолданылатын және кеңінен танылган құралдар болып табылады. SHA алгоритмін әзірленген блокчейн моделіне енгізу жүйенің қауінсіздігін толықтырады және деректердің тұтастыгын растайды.

Сондай-ақ, жұмыста блокчейннің құрылымын, блоктардың негізгі элементтерін, блокчейннің әртүрлі салаларда қолданылуын және оның биткоин және эфириум сынды криптовалюталармен байланысын қарастыратын блокчейн технологиясына кең теориялық шолу берілген. Сонымен қатар, Metamask кибер-әмиянын ашу проңесі және goerli тесттік желісінде шынайы транзакциялардың нақты қалай жүзеге асырылатыны көрсетілген. Бұл блокчейнмен және криптовалюталармен жұмыс істеудің нақты қадамдарымен және проңестерімен танысуга мүмкіндік бере отырып, әзірленген модельді тереңірек түсінуге және оны практикалық қолдануга ықпал етеді.

Зерттеудің нәтижелері мен қорытындылары академиялық және кәсіби қауымдастық үшін маңызды үлес болып табылады және оларды одан әрі қолдану біздің барган сайын цифрлық және байланысқан әлемімізде қауіпсіздікті жақсартуга көмектеседі.

Әдебиеттер тізімі

1. Исроилов, С.Г., & Верзунов, С.Н. (2021). Разработка защищенной системы электронного документооборота на основе блокчейн-технологии. Проблемы автоматики и управления, (2), 61-76. извлечено от http://pau.imash.kg/index.php/pau/article/view/204
2. Aliya, B., Olga, U., Yenlik, B., & Sogukpinar, I. (2023). Ensuring Information Security of Web Resources Based on Blockchain Technologies. International Journal of Advanced Computer Science and Applications, 14(6).
3. Li, C., Sun, X., & Zhang, Z. (2021). Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology. IEEE Access, 9, 113558-113565.
4. Antonopoulos A.M. Mastering Bitcoin: unlocking digital cryptocurrencies. – " O'Reilly Media, Inc.", 2017. – 109 pp.
5. Kube N. Daniel Drescher: Blockchain basics: a non-technical introduction in 25 steps: Apress, 2017, 255 pp, ISBN: 978-1-4842-2603-2. – 2018.
6. Comert O. Blockchain Revolution: How the Technology behind Bitcoin and Other Cryptocurrencies Is Changing the World. – 2020.
7. Bahga A., Madisetti V. Blockchain applications: a hands-on approach. – Vpt, 2017.
8. "Blockchain Basics: A Primer for Professionals" by Consensus
9. Jacki Foseid. Blockchain Security: A Comprehensive Guide for Beginners to Advanced

10. Козин И.С. Метод обеспечения безопасной обработки персональных данных на основе применения технологии блокчейн // Научно-технический вестник информационных технологий, механики и оптики. 2019.Т. 19. № 5. С. 892 – 900 doi: ISSN: 2226-1494
11. Gervais A., Karame O., Wust K., Glykantzis V., Ritzdorf H., Capkun S. On the Security and Performance of Proof of Work Blockchains (URL: https://ethz.ch/content/dam/ethz/specialinterest/infk/inst-infsec/system-security-group-dam/research/publications/pub2016/ccs16_gervais.pdf)
12. Cormen, Thomas H., et al. Introduction to Algorithms. MIT Press, 2009.
13. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996.
14. URL: https://www.okta.com/identity-101/hashing-algorithms/
15. URL: https://support.industry.siemens.com/cs/document/109483101/how-do-you-determine-the-sha-256-or-sha-512-checksum-of-a-file-?dti=0&lc=en-AE
16. Douglas Stinson, Rafael Osso. Cryptography: Theory and Practice. CRC Press, 2005
17. Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2014.
18. URL: https://www.coinbase.com/ru/learn/crypto-basics/what-is-a-crypto-wallet

References

1. Isroilov, S.G., & Verzunov, S.N. (2021). Razrabotka zashchishchennoj sistemy ehlektronnogo dokumentooborota na osnove blokchejn-tekhnologii. Problemy avtomatiki i upravleniya, (2), 61-76. izvlecheno ot http://pau.imash.kg/index.php/pau/article/view/204
2. Aliya, B., Olga, U., Yenlik, B., & Sogukpinar, I. (2023). Ensuring Information Security of Web Resources Based on Blockchain Technologies. International Journal of Advanced Computer Science and Applications, 14(6).
3. Li, C., Sun, X., & Zhang, Z. (2021). Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology. IEEE Access, 9, 113558-113565.
4. Antonopoulos A.M. Mastering Bitcoin: unlocking digital cryptocurrencies. – " O'Reilly Media, Inc.", 2017. – 109 rp.
5. Kube N. Daniel Drescher: Blockchain basics: a non-technical introduction in 25 steps: Apress, 2017, 255 pp, ISBN: 978-1-4842-2603-2. – 2018.
6. Comert O. Blockchain Revolution: How the Technology behind Bitcoin and Other Cryptocurrencies Is Changing the World. – 2020.
7. Bahga A., Madisetti V. Blockchain applications: a hands-on approach. – Vpt, 2017.
8. "Blockchain Basics: A Primer for Professionals" by Consensus
9. Jacki Foseid. Blockchain Security: A Comprehensive Guide for Beginners to Advanced
10. Kozin I.S. Metod obespecheniya bezopasnoj obrabotki personal'nykh dannykh na osnove primeneniya tekhnologii blokchejn // Nauchno-tekhnicheskij vestnik informacionnykh tekhnologij, mekhaniki i optiki. 2019. – T. 19. – № 5. – S. 892-900. doi: ISSN: 2226-1494
11. Gervais A., Karame O., Wust K., Glykantzis V., Ritzdorf H., Capkun S. On the Security and Performance of Proof of Work Blockchains (URL: https://ethz.ch/content/dam/ethz/specialinterest/infk/inst-infsec/system-security-group-dam/research/publications/pub2016/ccs16_gervais.pdf)
12. Cormen, Thomas H., et al. Introduction to Algorithms. MIT Press, 2009.
13. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996.
14. URL: https://www.okta.com/identity-101/hashing-algorithms/
15. URL: https://support.industry.siemens.com/cs/document/109483101/how-do-you-determine-the-sha-256-or-sha-512-checksum-of-a-file-?dti=0&lc=en-AE
16. Douglas Stinson, Rafael Osso. Cryptography: Theory and Practice. CRC Press, 2005
17. Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2014.
18. URL: https://www.coinbase.com/ru/learn/crypto-basics/what-is-a-crypto-wallet