АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION AND COMMUNICATION TECHNOLOGIES

ИНФОРМАТИКА
ИНФОРМАТИКА
COMPUTER SCIENCE

DOI 10.51885/1561-4212_2025_2_131
МҒТАА 20.53.19

Н.М. Казиева[1], Р.М. Оспанов[1], Д.Ю. Зернов[2], А.К. Калиев[3]
[1]«Л.Н. Гумилев атындағы Еуразия ұлттық университеті» КеАҚ, Астана қ., Қазақстан
*E-mail: kaziyevanm@gmail.com**
E-mail: ospanovrm@gmail.com
[2]«ҰК «Қазахстан Ғарыш Сапары» АҚ, Астана қ., Қазақстан
E-mail: d.zernov@gharysh.kz
[3]Group 42 Holding Ltd, Әбу Даби, Біріккен Араб Әмірліктері
E-mail: kaliyev.arman@yandex.kz

ТАРАТЫЛҒАН ТІЗІЛІМ ТЕХНОЛОГИЯЛАРЫНА НЕГІЗДЕЛГЕН ГИБРИДТІ БИОМЕТРИЯЛЫҚ ЖҮЙЕЛЕРДІ ЖОБАЛАУДЫҢ ЗАМАНАУИ ТӘСІЛДЕРІ

СОВРЕМЕННЫЕ ПОДХОДЫ К ПРОЕКТИРОВАНИЮ ГИБРИДНЫХ БИОМЕТРИЧЕСКИХ СИСТЕМ, НА ОСНОВЕ ТЕХНОЛОГИЙ РАСПРЕДЕЛЕННОГО РЕЕСТРА

MODERN APPROACHES TO THE DESIGN OF HYBRID BIOMETRIC SYSTEMS BASED ON DISTRIBUTED REGISTRY TECHNOLOGIES

Аңдатпа. *Биометриялық технологияларды таралған реестр технологияларымен, атап айтқанда блокчейн технологиясымен интеграциялау саласындағы зерттеулер қазіргі заманғы гибридтік биометриялық жүйелерді жобалау кезінде қауіпсіздік, құпиялылық және функционалдық үйлесімділікті арттыру жолдарын іздеуге бағытталған. Биометрия және блокчейн технологиялары бір-бірінен тәуелсіз өз артықшылықтары мен әлеуетіне ие. Олардың интеграциясы бұл артықшылықтарды өзара тиімді пайдалану мүмкіндігін береді. Бұл мақала биометрия және блокчейн технологияларын интеграциялаудың әртүрлі аспектілеріне арналған. Блокчейнде идентификация мен қолжетімділікті басқару деңгейінде биометриялық жүйелерді пайдалану мәселесі, әсіресе, биометриялық цифрлық қолтаңбаларды әзірлеу және пайдалану мәселесі қарастырылады. Сондай-ақ, блокчейннің биометриялық деректерді басқаруда, атап айтқанда, блокчейнде биометриялық шаблондарды қауіпсіз сақтау мәселесі қарастырылады.*
Түйін сөздер: *Биометрия, блокчейн, криптография, сандық қолтаңба.*

Аннотация. *Исследования в области интеграции биометрических технологий с технологиями распределенного реестра, в частности с технологией блокчейн, направлены на поиск путей повышения безопасности, конфиденциальности и функциональной совместимости при проектировании современных гибридных биометрических систем. Технологии биометрии и блокчейна независимо друг от друга имеют свои преимущества и потенциал. Их интеграция позволяет взаимовыгодно эти преимущества использовать. Данная статья посвящена различным аспектам интеграции технологий биометрии и блокчейна. Рассматривается вопрос использования биометрических систем на уровне управления идентификацией и доступом в блокчейне, в особенности, вопрос разработки и использования биометрических цифровых подписей. Также рассматривается применение блокчейна в управлении биометрическими данными, в частности, безопасное хранение биометрических шаблонов в блокчейне.*
Ключевые слова: *Биометрия, блокчейн, криптография, цифровая подпись.*

Abstract. *Research in the field of integrating biometric technologies with distributed ledger technologies,*

particularly with blockchain technology, aims to find ways to enhance security, privacy, and functional compatibility in the design of modern hybrid biometric systems. Biometric and blockchain technologies each have their own advantages and potential independently of each other. Their integration allows for the mutually beneficial use of these advantages. This article is dedicated to various aspects of the integration of biometric and blockchain technologies. It discusses the use of biometric systems at the level of identity management and access control in blockchain, especially the development and use of biometric digital signatures. It also examines the application of blockchain in managing biometric data, particularly the secure storage of biometric templates in blockchain

Keywords: *Biometrics, blockchain, cryptography, digital signature.*

Кіріспе. Биометриялық технологияларды, атап айтқанда, блокчейн технологиясымен біріктіру саласындағы зерттеулер заманауи гибридті биометриялық жүйелерді жобалау кезінде қауіпсіздікті, конфиденциалдылықты және функционалдық үйлесімділікті арттыру жолдарын іздеуге бағытталған. Биометрия және блокчейн технологиялары өз алдына артықшылықтары мен потенциалына ие. Оларды біріктіру осы артықшылықтарды өзара тиімді пайдалануға мүмкіндік береді. Блокчейн, бір жағынан, биометрия жүйелеріне тұрақтылық, есеп берушілік, қолжетімділік, әмбебап қолжетімділік сияқты қасиеттерді қамтамасыз ете алады. Бұл қасиеттер биометриядағы басқа қолданбалармен қатар, биометриялық үлгілерді қорғау және биометриялық жүйелерде конфиденциалдылықты қамтамасыз ету үшін өте пайдалы болуы мүмкін. Екінші жағынан, биометрия блокчейнге әртүрлі жолдармен, мысалы, блокчейндегі ағымдағы таралған сандық аутентификация және идентификация схемаларын жақсарту арқылы көмектесе алады (Delgado-Mohatar, et al., 2020; Ghafourian, M.,2023).

Бұл мақала биометрия және блокчейн технологияларын интеграциялаудың әртүрлі аспектілеріне арналған. Біріншіден, биометриялық жүйелерді блокчейндегі идентификациялау және кіруді басқару деңгейінде пайдалану мәселесі, атап айтқанда, биометриялық сандық қолтаңбаларды әзірлеу және пайдалану мәселесі қарастырылады. Екіншіден, блокчейннің биометриялық деректерді басқарудағы қолданылуы, атап айтқанда, биометриялық үлгілерді блокчейнде қауіпсіз сақтау қарастырылады. Үшіншіден, гибридті биометриялық сандық қолтаңбаның жаңа схемасы ұсынылады.

Одан әрі мақала келесі бөлімдерден тұрады. Бірінші тармақта таралған реестр технологияларының архитектурасы қарастырылады. Екінші тармақ жалпы биометриялық жүйелерді сипаттауға арналған. Келесі тармақтарда, тиісінше, блокчейнді биометрияда және биометрияны блокчейнде қолдану мәселелері қарастырылады. Одан әрі келесі тармақта ұсынылған жаңа гибридті биометриялық сандық қолтаңба схемасы қарастырылады.

Таратылған тізілім технологиясының архитектурасы. Таратылған тізілім технологиясының анықтамалық архитектурасы әдетте келесі компоненттерді қамтиды (ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), 2019; International Organization for Standardization. 2022).

Желілік деңгей. Бұл желідегі тораптар арасында байланыс пен консенсусты қолдайтын негізгі инфрақұрылым. Осы деңгейде қолданылатын хаттамалар мен алгоритмдер желіні құру және қолдау көрсету, сондай-ақ транзакцияларды дәйекті және тиімді тарату мен жазуды қамтамасыз ету үшін арналған. Ол тең-теңімен желі хаттамалары, консенсус алгоритмдері және желілік топологияларды қамтиды. Тең-теңімен желі хаттамалары (P2P) желідегі тораптар арасында байланыстарды орнату және қолдау үшін қолданылады, бұл оларға деректермен алмасуға мүмкіндік береді. Бұл хаттамалар топтағы басқа тораптармен тиімді ақпарат алмасуға мүмкіндік беретін кеңейтілген және көпадресатты механизмдерді қамтуы мүмкін. Консенсус алгоритмдері желідегі барлық тораптарда реестрдің тұтастығы мен келісімділігін қамтамасыз ету үшін қолданылады. Бұл алгоритмдер реестрде транзакцияларды тексеру және жазу механизмін қамтамасыз етеді және жұмыс дәлелі, үлес

дәлелі және басқа механизмдерді қамтуы мүмкін. Желілік топологиялар блокчейн жүйесінің өнімділігі мен масштабталуына елеулі әсер етуі мүмкін желінің құрылымын білдіреді. Желілік топологиялардың мысалдары толық байланысқан, жартылай байланысқан және иерархиялық құрылымдарды қамтиды. Жалпы, желілік деңгей басқа деңгейлердің негізін құрайды, бұл технологиялардың архитектурасының тиімді және қауіпсіз жұмыс істеуін қамтамасыз етеді.

Тізілім деңгейі. Бұл тізілімнің күйін қолдайтын және желіде жазылған транзакцияларды және деректерді сақтайтын деңгей. Бұл деңгей транзакцияларды және желідегі деректерді жазу мен бақылау үшін қолданылатын деректер моделін, деректер құрылымын және сақтау механизмін қамтиды. Бұл дәстүрлі реляциялық дерекқор, NoSQL дерекқорлары немесе IPFS сияқты таралған файлдық жүйелер болуы мүмкін. Бұл деңгей сонымен қатар деректерге қол жеткізу және оларды басқару функцияларын қамтиды, бұл реестрдегі деректерді сақтау, алу және манипуляциялауға мүмкіндік береді. Тізілім деңгейі желідегі барлық транзакциялар мен деректердің өзгермейтін жазбасын қолдауға жауап береді, бұл ашықтық пен көрінуді қамтамасыз етеді. Бұл сонымен қатар реестрді бірнеше торапта сақтау арқылы желіні орталықтандыруға мүмкіндік береді, яғни бір орталықтандырылған жерде емес. Бұл маңызды деңгей, себебі ол желінің барлық транзакциялар мен деректердің қауіпсіз және ашық жазбасын қолдауға мүмкіндік береді, сонымен қатар желінің децентрализденуіне мүмкіндік береді.

Консенсус деңгейі. Бұл желідегі тораптар арасында консенсусты басқаруға және тізілімнің күйінің барлық тораптармен келісілгенін қамтамасыз етуге арналған деңгей. Бұл деңгей консенсусты орнату және қолдау үшін қолданылатын консенсус хаттамаларын қамтиды, мысалы, жұмыс дәлелі (PoW), үлес дәлелі (PoS), византийская қателікке төзімділік (BFT) және басқалары. Бұл хаттамалар желінің қауіпсіздігін қамтамасыз ету үшін, сондай-ақ реестрдің дәлдігін және рұқсатсыз қол жеткізуден қорғауды қамтамасыз ету үшін қолданылады. Консенсус деңгейі транзакцияларды тексеруге, оларды блоктарға қосуға және желідегі барлық тораптардың реестрдің күйін келісуін қамтамасыз етуге жауап береді. Бұл сонымен қатар желінің зиянкестерден қорғалғанын қамтамасыз етеді, жаңа блоктардың тізбекке тек жеткілікті тораптар блоктың мазмұнымен келісетін кезде ғана қосылуын талап етеді. Бұл маңызды деңгей, себебі ол желінің реестрдің күйі бойынша консенсусты қамтамасыз етуіне мүмкіндік береді, желінің қауіпсіздігін және шабуылдарға төзімділігін қамтамасыз етеді.

Ақылды келісімшарттар деңгейі. Бұл желідегі ақылды келісімшарттардың орындалуын басқаратын деңгей. Бұл деңгейге, мысалы, ақылды келісімшарттар жасау үшін қолданылатын Solidity немесе Vyper сияқты бағдарламалау тілдері, сондай-ақ оларды орындау үшін қолданылатын жұмыс уақыты мен виртуалды машиналар кіреді. Ол сондай-ақ ақылды келісімшарттарды құрастыру, сынау және орналастыру үшін қолданылатын Truffle, Embark немесе Geth сияқты құралдар мен даму орталарын қамтиды. Ақылды келісімшарт деңгейі белгілі бір шарттар орындалған кезде келісімшарт талаптарын автоматты түрде орындауға жауап береді. Бұл мүмкіндік бизнес-процестерді автоматтандыруға және орталықтандырылмаған қосымшаларды (gapps) құруға мүмкіндік береді. Бұл маңызды деңгей, өйткені ол желідегі транзакциялар мен өзара әрекеттесулердің әртүрлі түрлерін автоматтандыру және оңтайландыру үшін пайдалануға болатын сенімсіз және дербес жүйелерді құруға мүмкіндік береді.

Қолданбалы деңгей. Бұл пайдаланушы мен қолданбаның желімен өзара әрекеттесуі үшін интерфейс пен функционалдылықты қамтамасыз ететін деңгей. Оған веб-қосымшалар мен мобильді қосымшалар, сондай-ақ желімен өзара әрекеттесу үшін жасалған басқа пайдаланушы интерфейстері кіреді. Ол сондай-ақ желіге кіру үшін пайдаланылатын API, кітапханалар және SDK, сондай-ақ кітап сұраулары, смарт

келісімшарттарды орналастыру және орындау, шот туралы ақпаратқа қол жеткізу сияқты желі ұсынатын қызметтерді қамтиды. API интерфейстері сыртқы қолданбаларға DLT желісінің функционалдығын қамтамасыз ету үшін пайдаланылады. Бұған тізіліммен өзара әрекеттесу үшін HTTP пайдаланатын RESTful API, сондай-ақ gRPC немесе GraphQL сияқты басқа API стандарттары кіруі мүмкін. SDK және кітапханалар блокчейн желісімен өзара әрекеттесетін қосымшаларды құру процесін жеңілдету үшін қолданылады. Бұл Java, Python немесе JavaScript сияқты танымал бағдарламалау тілдеріне арналған кітапханалар, сондай-ақ iOS немесе Android сияқты платформаларға арналған SDK болуы мүмкін. Бұл деңгей, әдетте, даму орталарын, ақылды келісімшарттарды әзірлеуді, қосымшаларды орналастыруды, әмияндарды, шолғыштарды, бақылау тақталарын, интеграцияланған даму ортасын (IDE) қамтиды.

Сәйкестендіру және қол жеткізуді басқару деңгейі (IAM). Бұл желідегі мүшелерді сәйкестендіруді басқаруға және желіге кіруді бақылауға жауап беретін деңгей. Ол пайдаланушы куәліктерін жасау, басқару және тексеру тетіктерін, сондай-ақ тізілімге және ақылды келісімшарттарға кіруді басқару элементтерін қамтиды. Оған жеке куәлік провайдерлері (IdP), ашық кілт инфрақұрылымы (PKI), рөлге негізделген қол жеткізуді басқару (RBAC) және желіге кіру үшін пайдаланушылар мен қолданбаларды аутентификациялау және авторизациялау үшін пайдаланылатын өзін-өзі сәйкестендіру шешімдері (SSI) сияқты компоненттер кіреді. IDP блокчейн желісіндегі мүшелерді аутентификациялау үшін қолданылады. Бұл дәстүрлі пайдаланушы аты мен құпия сөз аутентификациясын, сондай-ақ көп факторлы аутентификация (MFA) және биометрия сияқты жетілдірілген әдістерді қамтуы мүмкін. PKI блокчейн желісіндегі қатысушылардың сандық сертификаттары мен ашық және жеке кілттерін басқару үшін қолданылады. Бұған цифрлық сертификаттарды беретін және қайтарып алатын сертификаттау орталықтары (ОЖ), сондай-ақ онлайн сертификат мәртебесі хаттамасы (OCSP) және сертификаттарды қайтарып алу тізімі (CRL) сияқты сертификаттарды басқару хаттамалары кіруі мүмкін. RBAC блокчейн желісіндегі мүшелердің рөлдері мен рұқсаттарына негізделген тізілімге және ақылды келісімшарттарға қол жеткізуді басқару үшін қолданылады. Бұл қол жеткізу саясаттарын анықтау және қолдану үшін қол жеткізуді басқару (ACL) және атрибутқа негізделген қол жеткізуді басқару (ABAC) тізімдерін пайдалануды қамтуы мүмкін. SSI-адамдарға жеке сәйкестендіру ақпаратын толық бақылауға мүмкіндік беретін орталықтандырылмаған сәйкестендіруді басқару жүйесі. Блокчейн жүйесіндегі IAM деңгейінің негізгі ерекшеліктерінің бірі-авторизацияланған пайдаланушылар үшін тізілімге және ақылды келісімшарттарға оңай қол жеткізуді қамтамасыз ете отырып, қауіпсіздік пен құпиялылықтың жоғары деңгейін қамтамасыз ету мүмкіндігі. Бұл көп факторлы аутентификация, биометриялық аутентификация, шифрлау және қауіпсіз деректер алмасу сияқты озық қауіпсіздік және криптографиялық технологияларды пайдалануды талап етеді.

Жалпы типтегі биометриялық жүйелер. Биометриялық жүйенің мақсаты – олардың әртүрлі биологиялық және мінез-құлық сипаттамаларына, яғни дене бөліктерінің физикалық қасиеттеріне, денеде жүретін физиологиялық процестерге, дене шығаратын мінез-құлық процестеріне және олардың комбинацияларына негізделген адамдарды автоматты түрде тану (Стандартинформ. 2018. ГОСТ ИСО/МЭК 19794-1-2015). Адамның биологиялық сипаттамаларының мысалдары: папиллярлық сызықтардың құрылымы (саусақ ізі), көздің торлы қабығының суреті, ирис құрылымы, бет геометриясы, алақан пішіні, құлақ пішіні, дене иісі, жүрек соғысы, қолдардағы тамыр үлгісі, ДНҚ құрылымы. Мінез-құлық сипаттамаларының мысалдары: жүру, дауыс, қолжазба, пернетақта қолжазбасы.

Биометриялық тану биометриялық жүйенің келесі функцияларын орындау арқылы

жүзеге асырылады: биометриялық тіркеу, тексеру және сәйкестендіру.

Адаммен өзара әрекеттесу нәтижесінде биометриялық тіркеу кезінде биометриялық жүйе сенсорлардың (биометриялық сканерлердің) көмегімен кескін немесе сигнал түрінде биометриялық сипаттамалардың деректерін алады және тіркейді. Содан кейін тіркелген деректер олардағы кейбір тән биометриялық белгілерді (қайталанатын және айрықша көрсеткіштер) анықтау және кейіннен бөліп көрсету мақсатында өңделеді. Өңделген деректер әрі қарай пайдалануға жарамдылығы тексеріледі және тексеруден өтпеген жағдайда деректерді қайта жинау, тіркеу және өңдеу қажет болуы мүмкін. Қажет болса, тіркелген деректердің сапасын жақсарту жүзеге асырылады. Әрі қарай, өңделген және тексерілген деректер осы адамға арналған биометриялық тіркеудің бақылау үлгісі ретінде сақталады. Сондай-ақ, биометриялық тіркеу кезінде биометриялық тіркеу нәтижесінің одан әрі пайдалану үшін жарамдылығын растау үшін тестілік верификация немесе сәйкестендіру жүргізіледі, ал қанағаттанарлықсыз нәтижелер болған жағдайда биометриялық тіркеуді қайталап көруге рұқсат беріледі.

Тексеру кезінде биометриялық жүйе адаммен өзара әрекеттесу кезінде деректерді алады және тіркейді, содан кейін олар өңделеді және тексеріледі. Әрі қарай үлгінің алынған биометриялық белгілері биометриялық бақылау үлгісімен салыстырылады. Салыстыру нәтижелері бойынша салыстыру нәтижесін бере отырып, адамның деректер жүйесінде болуын растау үшін верификация бойынша шешім қабылданады.

Сәйкестендіру кезінде биометриялық жүйе адаммен өзара әрекеттесу кезінде деректерді алады және тіркейді, содан кейін олар өңделеді және тексеріледі. Содан кейін алынған үлгінің биометриялық белгілерін әр салыстыру үшін салыстыру нәтижесін бере отырып, биометриялық тіркеу дерекқорында сақталған жеке немесе барлық биометриялық бақылау үлгілерімен салыстыру жасалады. Салыстыру нәтижелері бойынша үміткерлердің тізімі жасалады. Кандидаттардың тізімдері негізінде сәйкестендіру бойынша шешім қабылданады.

Жалпы алғанда, биометриялық жүйенің құрылымы келесі компоненттерден тұрады: деректерді жинау ішкі жүйесі, деректерді беру ішкі жүйесі, сигналды өңдеу ішкі жүйесі, деректерді сақтау ішкі жүйесі, деректерді салыстыру ішкі жүйесі, шешім қабылдау ішкі жүйесі, әкімшілік ішкі жүйе, интерфейс.

Деректерді жинаудың ішкі жүйесі сенсорларды (биометриялық сканерлер) қолдана отырып, кескін немесе сигнал түрінде биометриялық сипаттамалардың деректерін алуға және тіркеуге арналған.

Деректердің ішкі жүйесі биометриялық деректерді биометриялық жүйенің әртүрлі ішкі жүйелері арасында биометриялық деректермен алмасудың кейбір стандартты форматында беруге арналған. Сонымен қатар, ақпараттың түпнұсқалығын, тұтастығын және құпиялылығын қамтамасыз ету үшін берілетін деректерге ақпаратты қорғаудың әртүрлі әдістері, соның ішінде қысу және/немесе шифрлау алгоритмдері қолданылуы мүмкін.

Сигналды өңдеудің ішкі жүйесі алынған және тіркелген деректерде анықтауға және кейіннен белгілі бір тән биометриялық белгілерді (қайталанатын және айрықша көрсеткіштер) бөліп көрсетуге арналған. Сондай-ақ, сигналды өңдеудің ішкі жүйесі сапаны бақылауды жүзеге асырады, өңделетін деректерді одан әрі пайдалануға жарамдылығын тексереді және тексеруден өтпеген жағдайда деректерді жинаудың ішкі жүйесіне деректерді басқаруды қайтарады немесе өңдеу параметрлерін өзгертеді. Қажет болса, тіркелген деректердің сапасын жақсарту жүзеге асырылады.

Деректерді сақтаудың ішкі жүйесі биометриялық тіркеу деректерін сақтауға арналған, мүмкін кейбір стандартты биометриялық алмасу форматында. Оның негізгі бөлігі сәйкесінше биометриялық тіркеу дерекқоры болып табылады. Сонымен қатар, белгілі бір деректерді биометриялық сканердің өзінде, кейбір портативті медиада (мысалы, смарт-

карта), Дербес компьютерде сақтауға болады.

Деректерді салыстыру ішкі жүйесі алынған және тіркелген деректерден оқшауланған биометриялық белгілерді деректерді сақтау ішкі жүйесінде сақталған бір немесе бірнеше биометриялық бақылау үлгілерімен салыстыруға арналған. Ол салыстыру нәтижелерін шешім қабылдаудың ішкі жүйесіне береді. Тексеру кезінде жүйе әр сұрау үшін бір салыстыру нәтижесін береді. Сәйкестендіру кезінде жүйе көптеген салыстыруларды орындайды және әр салыстыру үшін нәтиже береді.

Шешім қабылдаудың ішкі жүйесі верификация немесе сәйкестендіру кезінде қорытынды нәтиже беруге арналған. Ол деректерді салыстыру ішкі жүйесімен алынған салыстыру нәтижелерін пайдаланады. Бұл нәтижелерді бір немесе бірнеше әрекеттен кейін алуға болады.

Ішкі басқару жүйесі биометриялық жүйені жалпы басқаруға арналған. Ол заңнамалық, құқықтық және қоғамдық шектеулер мен талаптарды ескере отырып, биометриялық жүйенің жалпы әдістемесін, мінез-құлқын және қолданылуын басқарады.

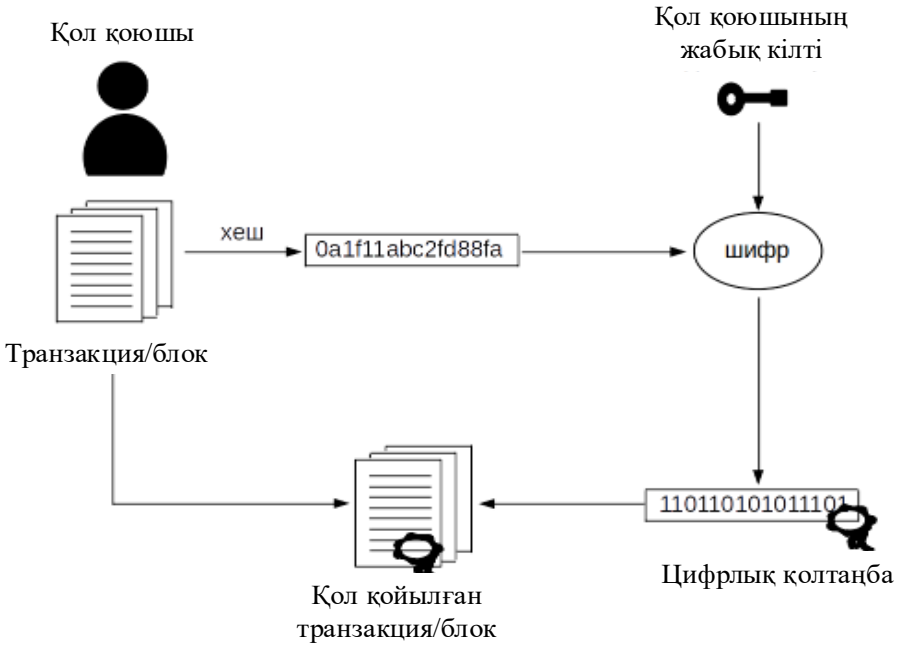
Интерфейс биометриялық жүйенің сыртқы қосымшалармен немесе жүйелермен өзара әрекеттесуіне арналған. Ол мұндай өзара әрекеттесуді қолданбалы бағдарламалық интерфейс, аппараттық интерфейс немесе хаттама интерфейсі арқылы жүзеге асырады.

Блокчейн жүйелерінде биометрияны қолдану. Блокчейндегі биометрияны қолданудың негізгі бағыттарының бірі – сәйкестендіру және қол жеткізуді басқару деңгейінде биометриялық жүйелерді пайдалану. Атап айтқанда, бірқатар артықшылықтары бар биометриялық цифрлық қолтаңбаларды әзірлеу және пайдалану мәселесі өзекті.

Жалпы алғанда, цифрлық қолтаңба схемасы келесі жалпы мақсатты көздейтін алгоритмдердің жиынтығы болып табылады. Кейбір бастапқы алғышарттар орындалған кезде жарамды цифрлық қолтаңба хабарламаны алушыға алынған хабарламаны белгілі жіберуші жасағанына және хабарлама жіберілген кезде өзгертілмегеніне, сондай-ақ жіберуші хабарламаға қол қою фактісінен бас тартпайтынына сенімді болуға мүмкіндік береді. Басқаша айтқанда, цифрлық қолтаңба схемасының мақсаты – хабарламалардың түпнұсқалығын, тұтастығын, сондай-ақ бас тартпауды қамтамасыз ету (Menezes, A., et al., 1997).

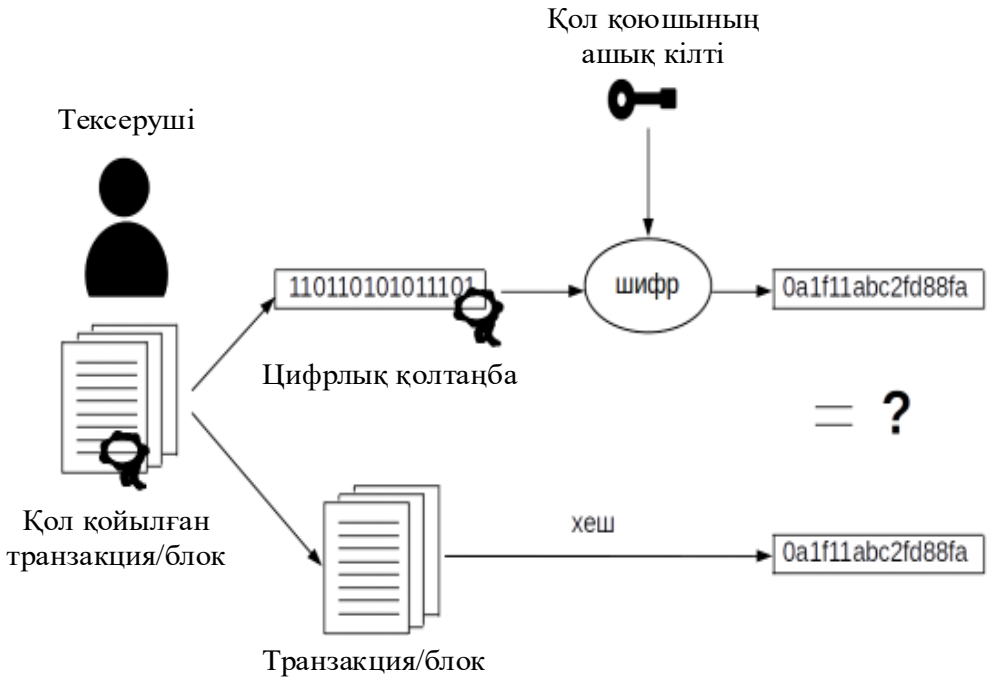
Цифрлық қолтаңба схемасы кем дегенде негізгі жұпты қалыптастыру алгоритмін, цифрлық қолтаңбаны қалыптастыру алгоритмін, цифрлық қолтаңбаны тексеру алгоритмін қамтиды. Негізгі жұпты құру алгоритмінің кірістері, мысалы, қауіпсіздік параметрі, кейбір математикалық параметрлер, қолданылатын криптографиялық хэш функциясының сипаттамасы болуы мүмкін ғаламдық ақпарат болып табылады. Алгоритмнің жұмысының нәтижесінде ашық және жеке кілттер жұбы алынады. Цифрлық қолтаңбаны қалыптастыру алгоритмінің кірістері хабарлама, ғаламдық ақпарат, жеке кілт болып табылады. Алгоритмнің жұмысының нәтижесінде қол қойылған хабарлама алынады. Сандық қолтаңбаны тексеру алгоритмінің кірістері ашық кілт, хабарлама және қолтаңба болып табылады. Алгоритмнің жұмысының нәтижесінде қолтаңба, егер ол жарамды болса немесе басқаша қабылданбаса қабылданады.

Қол қою схемасы блокчейнде транзакцияға қол қою үшін қолданылады, демек, жіберушінің болжамды аутентификациясы және транзакцияның тұтастығын, сондай-ақ жіберушінің бас тартпауын қамтамасыз ету. Көптеген қолтаңба схемалары блокчейнде тұтастық пен анонимділікті қамтамасыз ету үшін кеңінен қолданылады (Bellaj, B., et al., 2022). Сандық қолтаңба – бұл блокчейнді көпшілік алдында тексерілетін және қол жетімді консенсусқа айналдыратын маңызды криптографиялық примитивтердің бірі. Қолтаңба схемалары барлық дерлік блокчейндерде қолданылады. 1-суретте блокчейн пайдаланушысы (қол қоюшы) өзінің жеке кілтін пайдаланып транзакцияны немесе цифрлық қолтаңба блогын қалай жасайтынының жалпы мысалы келтірілген.



1-сурет. ЭЦҚ арқылы транзакция (блок) құру
Ескерту – автормен құрастырылған немесе (Menezes, A., et al., 1997) негізінде құрастырылған

Сонымен қатар, 2-суретте басқа блокчейн түйіндері (тексерушілер) транзакциядағы немесе блоктағы қолтаңбаның жарамды немесе қол қоюшының ашық кілтін пайдаланбағанын қалай тексеретінін көрсетеді.



2-сурет. Транзакцияның (блоктың) ЭЦҚ-ны тексеру
Ескерту – автормен құрастырылған немесе (Menezes, A., et al., 1997) негізінде құрастырылған

Блокчейн құпиялылық, анонимділік және байланыстырылмау сияқты қосымша мүмкіндіктерді қамтамасыз ету үшін әртүрлі қол қою схемаларын пайдаланады.

Блокчейндегі дәстүрлі цифрлық қолтаңбалар криптографиялық кілттерге негізделген, олар тиімді болғанымен ұрлануы, жоғалуы немесе бұзылуы мүмкін. Биометриялық цифрлық қолтаңбалар қауіпсіздіктің қосымша деңгейін қосады, себебі олар саусақ ізі немесе бет үлгісі сияқты адамның бірегей физикалық немесе мінез-құлық қасиеттеріне байланысты. Бұл рұқсат етілмеген қол жеткізу және алаяқтық транзакциялар қаупін айтарлықтай төмендетеді (Hassen O, A., et al., 2020; Kaga, Y., et al., 2017).

Биометриялық цифрлық қолтаңбалар аутентификацияның күшті дәлелін береді. Пайдаланушы биометрикасын пайдаланып транзакцияға немесе құжатқа қол қойғанда, бұл олардың жеке басын растап қана қоймайды, сонымен қатар олардан бас тартуға болмайтындығына кепілдік береді. Бұл пайдаланушының транзакцияға қатысуын кейіннен бас тарта алмайтынын білдіреді, бұл биометриялық қолтаңбаны заңды және нормативтік талаптарға сәйкестік үшін құнды етеді.

Құпия сөздер немесе PIN кодтары сияқты дәстүрлі аутентификация әдістерімен салыстырғанда, биометриялық аутентификация пайдаланушылар үшін ыңғайлы. Ол сондай-ақ күрделі құпия сөздерді есте сақтау қиынға соғатын адамдар үшін қолжетімділікті жақсарта алады.

Биометриялық цифрлық қолтаңбаларды жобалау биометриялық деректерден криптографиялық кілттерді генерациялауға негізделген. Негізгі материалдың көзі ретінде биометриялық деректерді пайдаланудың артықшылықтарына биометриялық мүмкіндіктердің бірегейлігі, қайталануы және тұрақты қолжетімділігі, сонымен қатар ыңғайлылық, икемділік, әртүрлі мүмкіндіктердің үйлесімділігі және үнемділігі жатады. Бұл ретте оларды пайдалануда кейбір мәселелер бар екенін ескеру қажет. Биометриялық технологиялар бастапқыда бірінші типтегі қателердің (немесе FAR, жалған қабылдау, жалған мақұлдау) және екінші типтегі қателердің (немесе FRR, жалған қабылдамау, жалған бас тарту) болуын болжайды. Биометриялық ақпаратты дәл және сенімді қайта шығару мүмкін емес және ықтималдықтың біркелкі таралуына бағынбайды. Оның үстіне биометриялық деректер құпия емес және адамның физикалық және эмоционалдық жағдайына байланысты өзгеруі мүмкін.

Биометриялық деректерден криптографиялық кілттерді генерациялау, өз кезегінде, биометриканы кодқа түрлендіру әдістеріне негізделген, олар «Меншікті» анық емес, анық емес биометриялық параметрлердің векторларын анық, бірмәнді кілттік (пароль) кодтарға түрлендіруге және жауап беруге қабілетті. Көптеген «Меншікті» кескіндерге жатпайтын кездейсоқ кіріс векторларының әсеріне кездейсоқ шығыс кодтары. «Биометрикадан кодқа» түрлендіргіштер екі түрге бөлінеді: анық емес экстракторлар және «биометрикадан кодқа» нейрондық желі түрлендіргіштері (Казанцев, Е.И., & Иванов, А. И. 2019; Стандартинформ. 2020. ГОСТ Р 52633.0-2006).

Бұлыңғыр экстрактор – бұл өзін-өзі түзететін артық кодтарды пайдалана отырып, кіріс деректеріндегі өзгерістер мен қателерге сенімді бола отырып, шулы немесе сенімсіз шикі биометриялық кіріс деректерінен бір мағыналы криптографиялық кілт кодын жасайтын алгоритм. Бұлыңғыр экстракторлар әдетте екі негізгі құрамдас бөліктен тұрады: тіркеу кезеңі, онда биометриялық деректер жиналады және анықтамалық үлгіні жасау үшін пайдаланылады және биометриялық деректер қайтадан жиналып, анықтамалық үлгімен салыстырылады. криптографиялық кілт (Казанцев, Е.И., & Иванов, А. И. 2019).

Нейрондық желі «биометрика-код» түрлендіргіштері – «Меншікті» кіріс биометриялық параметрлерінің ішінара кездейсоқ векторын бірмәнді криптографиялық кілт кодына (ұзын пароль) түрлендіретін және кез келген басқа түрлендіретін кірістер мен шығыстардың үлкен саны бар алдын ала дайындалған жасанды нейрондық желілер. Кездейсоқ шығыс

кодына енгізілген деректердің кездейсоқ векторы (Стандартинформ. 2020. ГОСТ Р 52633.0-2006). Нейрондық желі жаттығу кезінде биометриялық деректерден тиісті мүмкіндіктерді алуды үйренеді және оларды дәйекті көрініске түсіреді.

Биометриялық негізделген цифрлық қолтаңба схемаларының әртүрлі мысалдары бар. Мысалы, (Burnett, A., et al., 2007) жұмысы анық емес экстракторлар негізінде ашық кілтті және сәйкес жабық кілтті және эллиптикалық қисық нүктелер арқылы деректерді көрсету әдісін генерациялау үшін биометриялық деректерді пайдаланатын цифрлық қолтаңба схемасын сипаттайды (Janbandhu, P.K., & Siyal, M.Y. 2001). RSA және DSA бар және кеңінен қолданылатын екі цифрлық қолтаңба алгоритмдерін пайдалана отырып, шатыраш қабық көз тануға негізделген екі биометриялық қолтаңба схемасын ұсынады. RSA және DSA алгоритмдері жеке кілтті жасау үшін 512 байт шатыраш қабық көз биометриялық үлгісімен пайдаланылады. (Kwon, T., & Lee, J. 2004) инфрақұрылымын өзгертпей RSA сияқты бар криптографиялық алгоритмді пайдаланып тексеруге арналған биометриялық цифрлық қолтаңба схемасын ұсынады. (Takahashi, K., et al., 2019) мақалада жеке кілт ретінде биометриялық деректер сияқты шулы жолды пайдаланатын, бірақ қолтаңбаны генерациялау үшін пайдаланушыға арналған көмекші деректерді (сонымен қатар анық емес экстракторлар контекстінде көмекші жол деп те аталады) қажет етпейтін цифрлық қолтаңба схемасын ұсынады. Сондай-ақ мақалада биометриялық деректердің өзін жалпы биометриялық инфрақұрылым (PBI) деп аталатын криптографиялық кілт ретінде пайдаланатын биометриялық негізделген PKI енгізу үшін анық емес қолтаңба схемаларын қалай пайдалануға болатыны талқыланады. (Shan, X., You, L., & Hu, G. 2021)-да эллиптикалық қисық топтарға негізделген биометриялық деректерді пайдалана отырып, цифрлық қолтаңба үшін BioFIBS және Bio-IBS екі дизайны әзірленген. Жоба (Nagpal, R., & Nagpal, S. 2002) биометриялық деректер негізінде цифрлық қолтаңба үшін кілттерді генерациялау схемасын құрудың тұжырымдамалық негізін ұсынады. Бұл схемада жеке кілт құжатқа немесе жазбаға қол қою қажет болған сайын жасалады. Дегенмен, нақты алгоритмдер анықталмаған. (slam, S. H., Das, A. K., & Khan, M. K. 2016) мақалада анық емес экстракторды және екі сызықты эллиптикалық қисық жұптастыруды пайдалана отырып, биометриялық негізделген сандық көп қолтаңбалы схеманы (BIO-IDMS) ұсынады.

Биометриялық жүйелерде блокчейнді қолдану. Бөлінген кітап технологияларын, атап айтқанда блокчейнді қолдану биометриялық деректерді басқару және құпия жеке ақпаратты өңдеудің қауіпсіз және ашық әдісін қамтамасыз ету, биометриялық деректерді сақтау және аутентификациямен байланысты кейбір мәселелерді шешу болып табылады. Биометриялық жүйелер бірқатар шабуылдарға осал екені белгілі (Delgado-Mohatar, et al., 2020) және биометриядағы блокчейннің маңызды қолданбаларының бірі биометриялық үлгілерді қорғау болып табылады. Биометриялық үлгілерді блокчейнде сақтау дерекқордағы үлгілерді өзгерту және дерекқор мен деректерді жинау ішкі жүйесі арасындағы деректерді ұстап алу арқылы шабуылдардың алдын алуға мүмкіндік береді. Бірақ биометриялық деректер иелерінің құпиялылығын барынша қорғау және биометриялық үлгілердің қайтымсыздығы, байланыссыздығы және жаңартылу мүмкіндігінің қажетті қасиеттеріне қол жеткізу үшін биометриялық үлгілерді қорғаудың күрделі схемалары қолданылады. Биометриялық үлгілерді қорғау әдістерін (Delgado-Mohatar, et al., 20201) ретінде жіктеуге болады:

1) жойылатын биометрия (Mohamed, S., et al., 2017) (мысалы, кездейсоқ проекция, биохэшинг, биоконволюция, қайтымсыз трансформация);

2) биометриялық криптожүйелер (Patel, V.M., et al., 2015) (бұлыңғыр сақтау, анық емес міндеттеме, қауіпсіз эскиздер);

3) шифрланған түрдегі биометрия (гомоморфты шифрлау, бұрмаланған схемалар).

Биометриялық жүйелерде блокчейнді қолдану бірқатар артықшылықтарға ие. Биометриялық деректер өте сезімтал және қауіпсіз сақтауды қажет етеді. Блокчейннің өзгермейтіндігі деректер жазылғаннан кейін оны із қалдырмай өзгертуге болмайтындығына кепілдік береді. Бұл биометриялық жазбаларға рұқсатсыз араласудың немесе манипуляцияның алдын алады. Дәстүрлі орталықтандырылған дерекқорлар бір ғана сәтсіздіктер мен ымыраға келу нүктелеріне осал. Блокчейн желісінде биометриялық деректерді сақтау деректерді бірнеше түйіндер бойынша таратады, бұл барлық деректерді бұзатын бір бұзу қаупін азайтады. Блокчейн пайдаланушыларға биометриялық деректерін көбірек бақылауға мүмкіндік береді. Қажет болса, пайдаланушылар толық биометриялық профилін көрсетпестен белгілі бір атрибуттарға уақытша рұқсат бере алады. Блокчейндегі ақылды келісімшарттар келісімді басқаруды жеңілдетеді. Пайдаланушылар өздерінің биометриялық деректеріне кім және қандай жағдайларда қол жеткізе алатынын басқара алады, бұл дұрыс құпиялылықты басқаруды қамтамасыз етеді. Блокчейн аудитті және ашықтықты қамтамасыз етеді: блокчейндегі әрбір транзакция жазылады және бақыланады. Бұл пайдаланушыларға деректеріне кім және қашан қол жеткізгенін бақылауға мүмкіндік беретін аудит мақсатында пайдалы болуы мүмкін. Блокчейн әртүрлі платформалар мен ұйымдар арасында биометриялық деректерді қауіпсіз алмасу үшін стандартталған хаттаманы қамтамасыз ете алады, өзара әрекеттесуді жақсартады. Қауіпсіз көп факторлы аутентификация процесін жасау үшін блокчейн негізіндегі биометриялық аутентификацияны құпия сөздер немесе таңбалауыштар сияқты аутентификацияның басқа әдістерімен біріктіруге болады. Блокчейн орталықтандырылған органдарды қажет етпейақ қауіпсіз трансшекаралық аутентификацияны және жеке басын растауды жеңілдетеді. Блокчейнде сақталған биометриялық деректер технологияның криптографиялық сипатына байланысты жеке басын куәландыратын ұрлыққа және алаяқтыққа өте төзімді. Банктер сияқты жеке басын растауы қажет ұйымдар биометриялық деректердің түпнұсқалығын тексеру және тұтынушыны қосу процестерін жеңілдету үшін блокчейнді пайдалана алады.

Сонымен бірге, биометрияға блокчейнді қолдану кезінде ескеру қажет бірқатар мәселелер бар. Блокчейндегі үлкен көлемдегі биометриялық деректерді сақтау және басқару масштабтауға әсер етуі мүмкін. Офлайн сақтау немесе бүйірлік тізбектер сияқты шешімдер қажет болуы мүмкін. Блокчейн құпиялылықты жақсартса да, құпия биометриялық ақпаратты жалпыға қолжетімді немесе реттелмейтін блокчейнде сақтауға байланысты ықтимал құпиялылық мәселелерін шешу маңызды. Құпиялылық пен құпиялылық ережелерін сақтау, әсіресе денсаулық сақтау және қаржы салаларында, биометриялық деректермен жұмыс істеу кезінде өте маңызды. Блокчейн желісін құру және қолдау бастапқы шығындар мен техникалық инфрақұрылым талаптарын қамтуы мүмкін.

Гибридті биометриялық цифрлық қолтаңба схемасының мысалы. Жаңа гибридті биометриялық цифрлық қолтаңба схемасын қарастырамыз, ол XMSS (eXtended Merkle Signature Scheme) схемасына негізделген, қазіргі заманғы кванттық тұрақты схема, Меркл ағаштарын және WOTS+ (Winternitz One-Time Signature) бір реттік қолтаңбаларын қолданады (Buchmann, J., Dahmen, E., & Huelsing, A. (2011). Биометрияны кілттерді генерациялау процесіне интеграциялау, сондай-ақ блокчейн технологиясымен интеграциялау ұсынылады. Кілт жұбын қалыптастыру алгоритмі (құпия (жабық) кілт SK және ашық кілт PK генерациясы) келесідей анықталады.

Алдымен, кілт жұбын генерациялау үшін бет биометриясы қолданылады. Ол үшін пайдаланушының биометриялық деректерін жинау жүргізіледі. Камера немесе арнайы қабылдау құрылғысы арқылы бет сканерленеді, содан кейін жеке бет ерекшеліктерін сипаттайтын тұрақты ерекшелік векторын алу үшін ерекшеліктерді шығару алгоритмы қолданылады. Алынған шаблон коррекция әдістері арқылы қосымша өңдеуден өтеді, бұл криптографиялық есептеулер үшін жарамды биометриялық ақпараттың тұрақты көрінісін

қамтамасыз етеді. Бұл өңдеудің нәтижесі – криптографиялық хеш-функция арқылы биометриялық шаблонның хеш-мәнін bioH есептеу.

Келесіде SEEDprv мәні криптографиялық тұрғыдан тұрақты псевдослучайлы сандар генераторы арқылы сгенерленген r мәні мен bioH мәнінің конкатенациясынан хеш ретінде есептеледі. Бұл генерацияланатын кілттерді пайдаланушының бірегей биометриялық деректерімен байланыстыруға мүмкіндік береді, олардың нақты тұлғаға байланысын арттырады.

Сондай-ақ, криптографиялық тұрғыдан тұрақты псевдослучайлы сандар генераторы арқылы SK_PRF және SEEDpub мәндері алынады.

Алгоритмнің қалған компоненттері, мысалы, WOTS+ бір реттік қолтаңба схемасы үшін бір реттік құпия кілттер массивін (wots_sk) генерациялау және root хешін treeHash процедурасы арқылы есептеу, принципиалды өзгеріссіз қалады, тек SEEDprv қосымша биометриялық энтропияны қамтиды. Сол сияқты, индекс (idx) бір реттік кілттердің қолданылуын бақылау функциясын орындауды жалғастырады, биометрияға тәуелді болмайды. Сонымен қатар, OID (Object Identifier) – бұл XMSS алгоритмының параметрлерін анықтайтын бірегей идентификатор (мысалы, таңдалған хеш-функция, ағаштың биіктігі, WOTS+ параметрлері және т.б.). Ол ашық кілтке енгізіледі, осылайша кейіннен осы кілтпен жұмыс істейтін параметрлер мен стандарттармен нақты түсіну мүмкін болады, бұл әсіресе үйлесімділік пен қолтаңбаларды дұрыс тексеру үшін маңызды.

Бұл схемада блокчейн технологиясын интеграциялауға ерекше назар аударылады, ол ашық кілттер мен қолтаңбаларды таралған ортада сенімді сақтау мен тексеруді қамтамасыз етеді. Кілт жұбы қалыптасқаннан кейін, OID, root, SEEDpub-тан тұратын ашық кілт блокчейн желісінде тіркеледі, онда ол өзгермейтін реестрде сақталады. Мұндай тіркеу қолтаңбалардың шынайылығын тексеру үшін қолжетімді децентрализованное ашық кілттер қоймасын құруға мүмкіндік береді, бұл жүйенің қауіпсіздігі мен ашықтығын айтарлықтай арттырады. Блокчейнге енгізілген ақпарат тіркелу уақыты, транзакция идентификаторлары және басқа қызметтік деректер туралы метадеректерді қамтиды, бұл өзгерістер тарихын бақылауға және алаяқтық әрекеттерді болдырмауға мүмкіндік береді.

Осылайша, құпия кілт SEEDprv, idx, wots_sk, SK_PRF, root, SEEDpub-ты қамтиды, яғни SK=SEED‖prvidx‖wots_sk‖SK_PRF‖root‖SEEDpub, ал ашық кілт OID, root, SEEDpub-тан тұрады, яғни PK=OID‖root‖SEEDpub.

Осылайша, биометриялық деректерді алгоритмге интеграциялау SEED бастапқы мәндерін қалыптастыру кезеңінде жүзеге асырылады, бұл генерацияланатын кілттердің нақты пайдаланушыға байланысын арттырады. Бұл криптографиялық схеманың тұрақтылығын сақтай отырып, қосымша аутентификация деңгейіне қол жеткізуге мүмкіндік береді. Бет биометриясын интеграциялау генерацияланатын кілттердің нақты пайдаланушыға байланысын арттырады, бұл мүмкін.

Қорытынды. Биометрия мен блокчейннің интеграциясы биометриялық деректердің қауіпсіздігі мен тұтастығын қамтамасыз етуге көмектеседі, бұл рұқсатсыз кіруге және бұрмалауға жол бермейді. Блокчейнде бухгалтерлік кітапқа қосылған деректерді тексеріп, кітапқа қосқаннан кейін өзгерту немесе жою мүмкін емес. Бұл өзгермейтіндікке криптографиялық хэштеу және консенсус механизмдері арқылы қол жеткізіледі. Нәтижесінде блокчейнде сақталған биометриялық деректер рұқсатсыз кіруден және рұқсат етілмеген өзгертулерден қорғалған. Биометриялық деректерді криптографиялық хэштеу алгоритмдері арқылы бекітілген өлшемді таңбалар жолына (хэш) түрлендіруге болады. Бұл хэштер бастапқы деректердің бірегей көрінісі болып табылады және іс жүзінде қайтымсыз. Бұл хэштерді нақты биометриялық деректердің орнына блокчейнде сақтау тиімді тексеру мен аутентификацияға мүмкіндік бере отырып, құпия ақпараттың ашылмауын қамтамасыз етеді. Блокчейнде сақталған биометриялық деректерге қол жеткізуді криптографиялық

кілттер арқылы басқаруға болады. Пайдаланушылар өздерінің деректерімен өзара әрекеттесу үшін қажет жеке кілттерін толық бақылауға алады. Рұқсат етілмеген тұлғалар сәйкес жеке кілттерсіз деректерге қол жеткізе алмайды, бұл қауіпсіздікті арттырады. Бұзушылықтарды анықтау да қамтамасыз етіледі: блокчейнде сақталған биометриялық деректерді өзгерту әрекеті барлық кейінгі блоктардағы деректерді өзгертуді талап етеді, бұл блокчейннің бөлінген сипатына және оның консенсус механизмдеріне байланысты есептеу мүмкін емес. Кез келген бұзу әрекеттерін желі оңай анықтап, қабылдамайды. Блокчейн желілері кітаптың күйін тексеру және келісу үшін консенсус механизмдеріне сүйенеді. Бұл таратылған салыстыру процесі деректердің қауіпсіздігі мен тұтастығын одан әрі жақсартады. Деректерге өзгертулер желі қатысушыларының көпшілігі келіскен жағдайда ғана мүмкін болады. Биометриялық деректерді блокчейн желісіндегі түйіндер арасында таратуға болады, бұл бір сәтсіздік нүктесінің қаупін азайтады. Бұл таратылған жад деректердің жоғалуынан қорғаудың қосымша қабатын қосады. Биометриялық тексеру қажет болғанда, деректерді блокчейннен қауіпсіз түрде алуға және криптографиялық әдістерді қолдана отырып, түпнұсқа үлгімен салыстыруға болады. Үлгінің өзі ашылмағандықтан, процесс дәл тексеруді қамтамасыз ете отырып, құпиялылықты сақтайды. Блокчейн технологиясының мөлдір және бақыланатын сипаты биометриялық деректермен барлық өзара әрекеттесулерді егжей-тегжейлі тексеруге мүмкіндік береді. Бұл аудит мүмкіндігі сәйкестік, есеп беру және кез келген күдікті әрекетті тексеру үшін пайдалы болуы мүмкін.

Мүдделер қақтығысы. Авторлар мүдделер қақтығысының жоқтығын айтады.

Алғыс. Жұмыс ҚР ҰҚМ ҒК, № AP19678000 «Биометрия есептері мен оның қосымшаларына, соның ішінде блокчейн технологиясы үшін QR кодтарды пайдаланудың қауіпсіз әдістері мен алгоритмдердің әзірлеу» қаржылық қолдауымен орындалды.

Әдебиеттер тізімі

Delgado-Mohatar, O., Fierrez, J., Tolosana, R., & Vera-Rodriguez, R. (2020). Blockchain meets biometrics: Concepts, application to template protection, and trends. arXiv:2003.09262 (cs.CV). https://doi.org/10.48550/arXiv.2003.09262

Ghafourian, M., Sumer, B., Vera-Rodriguez, R., Fierrez, J., Tolosana, R., Moralez, A., & Kindt, E. (2023). Combining blockchain and biometrics: A survey on technical aspects and a first legal analysis. arXiv:2302.10883 (cs.CV). https://doi.org/10.48550/arXiv.2302.10883

ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT). (2019). Technical specification FG DLT D3.1. Distributed ledger technology reference architecture.

International Organization for Standardization. (2022). ISO 23257:2022. Blockchain and distributed ledger technologies. Reference architecture. ISO/TC 307.

Стандартинформ. (2018). ГОСТ ИСО/МЭК 19794-1-2015. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура (ИСО/МЭК 19794-1:2011, Информационные технологии. Форматы обмена биометрическими данными. Часть 1: Структура, IDT). Москва.

Menezes, A., van Oorschot, P., & Vanstone, S. (1997). Handbook of applied cryptography. CRC Press.

Bellaj, B., Ouaddah, A., Bertin, E., Crespi, N., & Mezrioui, A. (2022). SOK: A comprehensive survey on distributed ledger technologies. In 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-16). IEEE. https://doi.org/10.1109/ICBC54727.2022.9805533

Hassen O, A., Abdulhussein A., Darwish S., Othman Z.A., Tiun S., & Lotfy Y. (2020). Towards a secure signature scheme based on multimodal biometric technology application for IoT blockchain network. Symmetry, 12(10), 1699. https://doi.org/10.3390/sym12101699

Kaga, Y., Fujio, M., Naganuma, K., Takahashi, K., Murakami, T., Ohki, T., & Nishigaki, M. (2017). A secure and practical signature scheme for blockchain based on biometrics. In Proceedings of the 3rd International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2017) (pp. 877-891). Springer. http://dx.doi.org/10.1007/978-3-319-72359-4_55

Казанцев, Е.И., & Иванов, А.И. (2019). Обзор средств создания крипторических ключей из биометрии пользователя. Инжиниринг и технологии, 4(1), 1–3. https://doi.org/10.21685/2587-7704-2018-4-1-14

Стандартинформ. (2020). ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации.

Требования к средствам высоконадёжной биометрической аутентификации. Москва.
Burnett, A., Byrne, F., Dowling, T., & Duffy, A. (2007). A biometric identity based signature scheme. International Journal of Network Security, 5(3), 317–326. https://doi.org/10.6633/IJNS.200711.5(3).08
Janbandhu, P.K., & Siyal, M.Y. (2001). Novel biometric digital signatures for Internet-based applications. Information Management & Computer Security, 9(5), 205-212. https://doi.org/10.1108/09685220110408022
Kwon, T., & Lee, J. (2004). Practical digital signature generation using biometrics. In A. Laganá, M.L. Gavrilova, V. Kumar, Y. Mun, C.J.K. Tan, & O. Gervasi (Eds.), Computational science and its applications – ICCSA 2004 (Lecture Notes in Computer Science, vol. 3043, pp. 85-94). Springer. https://doi.org/10.1007/978-3-540-24707-4_85
Takahashi, K., Matsuda, T., Murakami, T., Hanaoka, G., & Nishigaki, M. (2019). Signature schemes with a fuzzy private key. International Journal of Information Security, 18, 581–617. https://doi.org/10.1007/s10207-019-00428-z
Shan, X., You, L., & Hu, G. (2021). Two efficient constructions for biometric-based signature in identity-based setting using bilinear pairings. IEEE Access, 9, 25973-25983. https://doi.org/10.1109/ACCESS.2021.3057064
Nagpal, R., & Nagpal, S. (2002). Biometric based digital signature scheme. Internet-Draft, draft-nagpal-biometric-digital-signature-00.txt.
Islam, S. H., Das, A. K., & Khan, M. K. (2016). Design of a provably secure identity-based digital multi-signature scheme using biometrics and fuzzy extractor. Security and Privacy in Communication Networks, 9, 3229–3238. https://doi.org/10.1002/sec.1528
Mohamed, S., Soltane, M., Messikh, L., & Zaoui, A. (2017). A review regarding the biometrics cryptography challenging design and strategies. BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 41–64.
Patel, V.M., Ratha, N.K., & Chellappa, R. (2015). Cancelable biometrics: A review. IEEE Signal Processing Magazine, 32(5), 54–65. https://doi.org/10.1109/MSP.2015.2434151
Buchmann, J., Dahmen, E., & Huelsing, A. (2011). XMSS – A practical forward secure signature scheme based on minimal security assumptions. In Lecture Notes in Computer Science (Vol. 7071, pp. 1–17). Springer. https://doi.org/10.1007/978-3-642-25405-5_8

Information about authors

Kaziyeva Nazym – acting associate professor, NJSC "L. N. Gumilyov Eurasian National University", Astana, Kazakhstan, kaziyevanm@gmail.com, ORCID: 0000-0002-7559-1795, Phone: +7 7017951787

Ospanov Ruslan – doctoral student, NJSC "L. N. Gumilyov Eurasian National University", Astana, Kazakhstan, ospanovrm@gmail.com, ORCID 0000-0002-0771-575x, Phone: +7 701 816 7966

Zernov Dmitry – chief engineer, JSC " NC "Kazakhstan Garysh Sapary", Astana, Kazakhstan, Astana, Kazakhstan, d.zernov@gharysh.kz, Phone: +7 701 657 8807

Kaliyev Arman – Chief Engineer, Group 42 Holding Ltd, Abu Dhabi, United Arab Emirates,ORCID ID: 0000-0001-8399-8379, kaliyev.arman@yandex.kz, +971 52 500 7989