

## БЛОКЧЕЙН ЖҮЙЕСІНДЕ АҚПАРАТТЫ ҚОРҒАУ ЖӘНЕ ҚАРЖЫ САЛАСЫНА ЕНГІЗУДІҢ МОДЕЛІ

**Мейрамбек Ұлдана Жалғасбекқызы, Ербаянова Дария Алибековна**  
[uldana.meirambek@mail.ru](mailto:uldana.meirambek@mail.ru), [e.dariya18@mail.ru](mailto:e.dariya18@mail.ru)

Л.Н.Гумилев атындағы ЕҰУ 2 курс магистранты, Нұр-Сұлтан, Қазақстан  
Ғылыми жетекшісі – Қ.Р.Есмханова

Кіріспе

Қазіргі таңда қаржылық қызмет көрсету саласында жаңа технологиялардың пайда болуымен және дамуымен байланысты ақпараттық технологиялар бөлімі шығындарды азайту және қолданыстағы жүйелерді қолдау арқылы тиімділікті арттырып, бірегей инновацияларды дамыту маңызды. Банк жүйесіне инвестициялардың өтелімділігінің барлық арналары бойынша анағұрлым сапалы, мінсіз қызмет көрсетуді, ақпаратты жинау және талдау қабілетін өзгертетін жаңа технологияларды енгізу керек.

Бұл қызметтер блокчейннің жаңа технологияларының пайда болуымен көбейеді. Бүгінде блокчейн бірнеше салада қолданыста, бірақ экономика мен қоғамның әртүрлі салаларында блокчейнді қолдану мүмкіндіктері өте көп. Оны одан әрі дамытып, қолданысқа енгізу қажет.

Блокчейн және криптовалюта тақырыптарына жоғары қызығушылықтың пайда болуы қаржы институттарына да әсер етті. Қазір бұл жаңа технологиялардың банк жүйесіне әсері белсенді зерттелуде.

Қазіргі уақытта банк саласында блокчейнді пайдалану қаржылық операцияларды қорғауды дамытуда және олардың жылдамдығын арттыруда жаңа перспективаларды ашуға көмектеседі деп сеніммен айтуға болады. Әр түрлі елдердің банкирлері осы технологияларды өз қызметтеріне енгізу бойынша жұмысқа көп тартылған.

Мұнда деректерді сақтаудың үлестірілген тізілімі ретінде құрылған блокчейн идеясын еске түсірген жөн, бұл жүйе ішіндегі операцияларды немесе қаржылық делдалдарды пайдалануды үшінші тараптың бақылауын білдірмейді.

Ақпаратты қорғаудың міндеттерінің бірі - деректердің дұрыстығын қамтамасыз ету. Бұл зерттеуде біз RSA асимметриялық шифрлау алгоритмін қарастырамыз. Бұл шифрлау әдісі логистикалық блокчейн жүйелерінде белсенді қолданылады. Математикалық модель келесідей болады:

$$n = b * c \quad (1)$$

$$\phi(n) = (b - 1)(c - 1) \quad (2)$$

$$c * e \text{ mod } \phi(n) = 1 \quad (3)$$

$$d = m^e \text{ mod } n \quad (4)$$

$$m = d^c \text{ mod } n \quad (5)$$

мұндағы  $b, c$  - жай сандар,  $n$  – ашық және жеке кілтке арналған модуль,  $\phi(n)$  - Эйлер функциясы. Жай сандарды таңдағаннан кейін 1-ден  $\phi(n)$ -ге дейінгі  $e$  бүтін саны (ашық экспонента) таңдалады. Келесі (3)- формулаға сәйкес келетін  $c$  саны табылады. Осылайша, жеке кілт  $\{c, n\}$  және жалпыға ашық кілт  $\{d, n\}$  (4) шифрлау және деректерді шифрлау арқылы жасалады.

Блокчейндегі сандық қолтаңбалар ашық кілт криптография әдістеріне негізделген. Екі кілт қолданылады: жеке кілт — сандық қолтаңбаларды қалыптастыру үшін қолданылады және құпия сақталады, ашық кілт — электрондық қолтаңбаны тексеру үшін қажет. Ашық кілт жеке кілт негізінде есептеледі, бірақ кері түрлендіру үлкен есептеуді қажет етеді.

Жеке кілтті таңдауға тырысқанда,  $2^N$  комбинациясын сұрыптау керек, мұндағы  $N$  - кілттің ұзындығы. Брутфорс кілтін таңдау тіпті ең заманауи жоғары өнімді кластерлерде де ұзақ уақыт алады. Мысалы, кілттің ұзындығы 256 бит және секундына 1024 құпия сөзді таңдау жылдамдығы үшін  $1,23 \times 10^{67}$  жыл қажет болады. Осылайша, логистикалық блокчейн жүйелерінде қолданылатын қарастырылған шифрлау әдісі қауіпсіздіктің жоғары деңгейіне ие. Дәстүрлі компьютерлермен салыстырғанда өнімділігі жоғары кванттық компьютерлер қауіп төндіруі мүмкін, алайда қосымша қорғаныс әдістерін қолдану (мысалы, блоктау алгоритмдері) бұл мәселені шешеді. Бұл блокчейн жүйесіндегі ақпаратты қорғаудың негізгі формуласы болып табылады.

Блокчейн технологиясы ең аз шығындармен және орталықтандырылған басқару органына жүгінбестен бірден жүзеге асыруға мүмкіндік береді.

Осыған байланысты көптеген қаржы институттарының осы технологияға деген қорқынышы түсінікті, себебі олар өз бизнестерін бақылаудан айрылудан қорқады. Дегенмен банк жүйесіне блокчейнді бейімдеуге болады

Банктерде жаңа технологияны бірқатар қызметтерге енгізуге мүмкіндік бар:

- клиринг және бағалы қағаздар саудасы;
- консалтинг және анықтамалық мәліметтерді ұсыну;
- клиенттерді сәйкестендіру;
- трансшекаралық және бөлшек төлемдерді өңдеу.

Үлестірілген тіркеу технологиясына негізделген блокчейн транзакцияларға қатысатын барлық тараптар үшін қол жетімді. Технология транзакциялардың барлық деректерін, соның ішінде олардың тарихын блок түрінде сақтауға көмектеседі. Үлестірілген тіркеу бола отырып, блокчейн қаржылық жүйелерге - ашықтықты, қауіпсіздікті, сенімділікті, өзгермейтіндікті, алаяқтықтың алдын - алуды қамтамасыз етуден пайда көреді.

Қаржы институттары блокчейн енгізу арқылы олар келесі артықшылықтарға ие болады:

- Транзакциялық шығындарды азайту (блок - тізбек транзакциялар кезінде тараптар арасында ақпарат алмасу тұжырымдамасына негізделгендіктен, ол банктер арасындағы салыстыру шығындарын және құжаттамалық алаяқтықтар үшін шығындарды үнемдеуге көмектеседі);
- Делдалдардың рөлін барынша азайту (блок - тізбек тең - теңімен транзакциялар қағидаты бойынша жұмыс істейді, кез келген делдалдың, орталық биліктің немесе ақпарат алмасу орталығының рөлі барынша азаяды, бұл транзакцияларды тезірек және тегіс өңдеуге әкеледі);
- Транзакциялар жолын қадағалау (блокчейн алаяқтық пен қара ақшаны бақылауға көмектесетін нақты транзакцияның бүкіл тізбегін бақылай алады).

Блокчейн - ашық әрі сенімді болғандықтан оны қаржы саласына енгізу арқылы ол үлкен әлеуетке ие болады.

Бұл технологияны қаржы саласына енгізудің алғашқы қадамы белгілі бір банктің немесе қаржы тобының ішінде технологияны енгізу болып табылады. Банктер экожүйені құра отырып блокчейнді қаржы институтының сыртқы қатысушыларына оңай тарата алады. Сондай-ақ, олар блокчейнді қаржы саласына енгізуді іске асыру үшін екі кезеңнен тұратын тәсілді пайдалана алады.

*1 кезең:* біріншіден, блокчейнді енгізу арқылы ішкі транзакциялар мен экожүйенің басқа да салалары үшін ақпараттарды бақылау және деректерге қол жеткізу жүзеге асырылады. Ірі банктер бүкіл әлем бойынша таратылатын барлық бағыттар бойынша мемлекетаралық операциялар үшін блокчейнді пайдалануға болады.

2 кезең: блокчейн технологиясы бойынша ішкі экожүйені енгізу және тестілеуден кейін, олар басқа блокчейн экожүйелеріне, серіктестеріне қосылуға және басқа қаржы институттарымен өзара әрекеттесуге болады.

Іске асыру кезінде кезеңдер белгілі бір пайдалану міндеттеріне негізделген толқындар ретінде ашылуы керек. Пайдалану жағдайларын сүзу және қысқа мерзімді пайдалану үшін «іске асыру уақыты» және «бизнес құндылығы» ұсынылады. Сондай-ақ, іске асырудың итеративті тәсілін қолдану ұсынылады.

Блокчейнді банктерде үш негізгі жағдайда кезең - кезеңмен қолдануға болады.

КҮС және AML процесі: банктер КҮС Тұтынушы деректерін қолдау үшін блокчейн негізіндегі технологияларды қолдана алады. Бұл шешімдер AML сәйкестігін қамтамасыз етумен қатар банктегі бизнестің әртүрлі салаларында қолданыла алады.

КҮС (Know Your Customer немесе Know Your Client) - қаржы институттары мен букмекерлік кеңселерге, сондай-ақ жеке тұлғалардың ақшасымен жұмыс істейтін басқа компанияларға арналған банктік және биржалық реттеу термині, олар қаржы операциясын жүргізбестен бұрын контрагенттің жеке басын анықтап, анықтауы керек дегенді білдіреді.

AML (Anti-Money Laundering) -занды сипат беру мақсатында ақша қаражатының шығу көзін жасыратын әрекеттер.

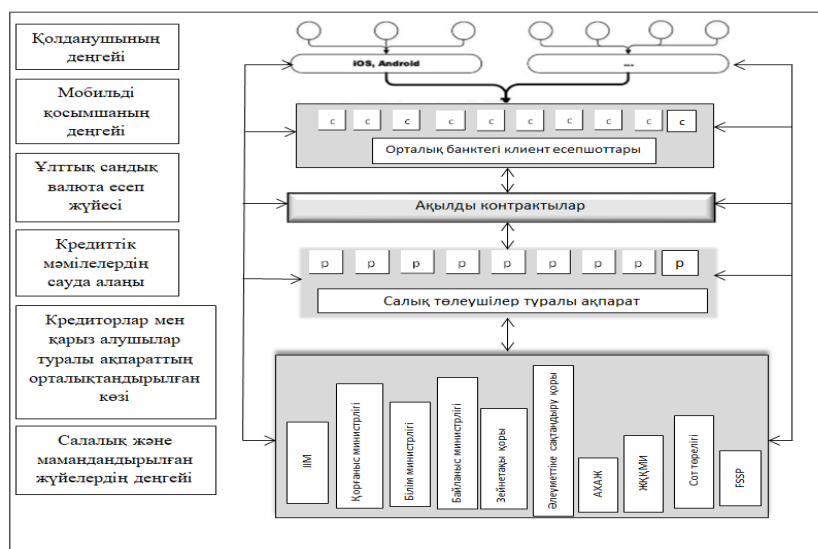
КҮС аяқталғаннан кейін, деректер қайтадан клиент үшін КҮС істеу қажет болған жағдайда, банктің түрлі бөлімдерінің қол жетімді блокчейн жүйесінде сақталуы мүмкін. Бұл шешім банктің әртүрлі бөлімдерінің КҮС-ті аяқтауға кететін уақытын азайтуға көмектеседі.

Банк блокчейн клиенттері үшін КҮС дерекқорын орнатқаннан кейін, ол басқа банктер мен басқа қаржы институттары жүйесінен жеке кілт арқылы тұтынушы туралы мәліметтермен жұмыс жасай алады. Мысалы, компания өз қызметтерін ұсынбас бұрын клиент үшін КҮС процесін аяқтауға мәжбүр болады. Бұл компания клиенттің КҮС толтыра алады, жабық кілт арқылы банктің блокчейн жүйесіне оңай және тез қол жеткізе алады; банк өз кезегінде сенімді деректер көзін ұсынғаны үшін фирмаларға қызмет үшін комиссия ала алады. Бұл барлық тараптар үшін жеңіске жететін жағдай:

- банк қолда бар деректерді монетизациялай алады;
- фирма КҮС процесін сенімді деректер көзі арқылы тез жүзеге асыра алады;
- клиент жұмыс істейтін әрбір банк/коммуналдық фирмада КҮС процесіне кететін уақытты үнемдейді.

## **БЛОКЧЕЙН ТЕХНОЛОГИЯСЫНА НЕГІЗДЕЛГЕН ОРТАЛЫҚТАНДЫРЫЛМАҒАН НЕСИЕ ЖҮЙЕСІНІҢ МОДЕЛІ**

Жоғарыда айтылғандарды ескере отырып, блокчейн технологиялары негізінде ұлттық есеп жүйелерін құру кезінде көп деңгейлі өзара әрекеттесуді ұйымдастыру бойынша ұсыныстарды ескере отырып, орталықтандырылмаған несие жүйесін құрудың мүмкін нұсқаларының бірі 1-суретте көрсетілген.



**Сурет 1.** Блокчейн-технологиялар негізіндегі орталықтандырылмаған кредиттік жүйе

Блокчейн технологиясына негізделген орталықтандырылмаған несие жүйесінің бұл моделінде қаржы нарығының қатысушыларын тексеру үшін жеке емес мәліметтер қолданылады, бірақ сонымен бірге несие өтей алу қабілеттілігін максималды тексеру қамтамасыз етіледі.

Диаграммада көрсетілген өзара әрекеттесу деңгейлері (сурет 1):

- пайдаланушылардың өтініштері орталықтандырылмаған мобильді немесе онлайн қосымшалар арқылы жүзеге асырылуы мүмкін;
- орталық банк блокчейннің мүшесі бола отырып, бір жағынан ұлттық криптовалютаны шығарады және есепке алады, екінші жағынан, несие тарихы бюросының қызметін бақылайды, бұл қаржы нарығына қатысушылардың несие тарихын тексеруге мүмкіндік береді;
- жүйенің деңгейлерінің бірі клиенттер сауданы өздерінің криптовалюталық шоттарынан тікелей жүзеге асыратын сауда алаңы болып табылады; шарттарды жасасу және орындау смарт - келісімшарттар арқылы автоматты түрде жүзеге асырылады;
- қаржы нарығына қатысушылар туралы орталықтандырылған ақпарат көзі – Қазақстан Республикасының салық қызметі – қажет болған жағдайда ведомствоаралық өзара іс - қимыл жүйесі арқылы қосымша ақпарат көздеріне -салалық және мамандандырылған ақпараттық жүйелерге, мемлекеттік тізілімдерге және тіркелімдерге тексеру жүргізеді;
- блокчейнде контрагенттерді верификациялау мен тексерулерден сәтті өткен жағдайда смарт - келісімшарттың жасалуы расталады, содан кейін шарттың орындалуы басталады.

Ұсынылған модельде үлестірілген тіркеу технологиясын қолдану қажеттілігі блокчейннің қасиеттерімен негізделген.

Блокчейн негізіндегі орталықтандырылмаған несие жүйесінің сенімділігі транзакциялар туралы ақпараттың өзгермейтіндігі және деректерді жоғалту мүмкін еместігі арқылы қол жеткізіледі. Блокчейннің барлық қатысушыларының компьютерлерінде транзакциялар тізілімін сақтау келісімшарттар, жүргізілген операциялар, тексеру нәтижелері туралы ақпараттың жоғалуын болдырмайды. Компьютерлік техниканың немесе ақпараттық-телекоммуникациялық жабдықтың жекелеген бірліктерінің істен шығуы тұтастай алғанда жүйенің жұмыс қабілеттілігін бұзбайды.

Несие беру шартының талаптары ақылды келісімшартта жазылады, ол автоматты түрде орындалады: несие бойынша қаражат аударылады, шартта көрсетілген кезеңділікпен несие өтеу және пайыздарды төлеу жүзеге асырылады. Осылайша, ақылды келісімшарт түрінде несие беру шартын жасасу қарыз алушының шоттарында қаражат болған кезде несие бойынша төлемеуді болдырмайды, ал олар болмаған жағдайда банкроттық рәсімін

жеңілдетеді. Блокчейнде барлық транзакциялар туралы мәліметтер бар: несие алу, несие беру туралы ұсыныстардың түсуі, қарыз алушы мен кредиторды тексеру процедурасы, несие шартын жасасу, несие алу, несие төлемдері.

Блокчейн негізінде жұмыс істейтін қаржылық қызметтерді ұсынуға арналған орталықтандырылмаған қосымшалар пайдаланушыларға өз қаржыларын делдалдарсыз тікелей басқаруға мүмкіндік береді, бұл операциялық шығындардың төмендеуіне әкеледі.

Біздің өміріміздің әртүрлі салаларында блокчейн технологияларын жаппай енгізу уақыты келіп жатыр. Блокчейн технологиялар негізіндегі жүйелі шешімдер олардың салалық, өңірлік және ұлттық деңгейде интеграциялануын талап ететін кемелдік пен қажеттілік деңгейіне ие болады.

Жетекші мемлекеттердің шешімдерін енгізу мен интеграциялаудың табысты мысалдары технологияны жаңа деңгейге шығаруға және мемлекеттік билік органдарының халықпен және бизнеспен өзара іс-қимыл форматтарына айтарлықтай әсер етуге қабілетті. Сондықтан бұл жүйені еліміздің экономикасын одан әрі дамыту мақсатында тезірек қолданысқа енгізгеніміз дұрыс.

Бірнеше жылдар ішінде компьютерлік технологиялар мен блокчейн желілерін енгізуге негізделген компьютерлендіру блокчейн технологиясының көптеген жаңа мүмкіндіктерін қалыптастырды және оны дамыту жалғаса түспек. Дегенмен банктер реттеу мен масштабталу проблемаларына тап болады, бірақ бұл кез-келген жаңа даму сияқты уақытша шешілетін шектеулер. Сондай-ақ, компаниялар бағдарламалық жасақтама мен басқа да ұқсас заманауи технологияларды қалыпқа келтіріп, күмәнмен қарамауы үшін техникалық білімді мәдениетті дамытуы керек.

#### **Пайдаланылған әдебиеттер:**

1. Ашба, А.А. Особенности конкурентного поведения коммерческих банков в условиях цифровизации экономики (на примере Сбербанка России) // Социальные науки. 2018. № 4 С. 17-21
2. Воронин В.П., Федосова С.Н. Деньги, кредит, банки: Учеб.пособие [Текст]. – М.: Юрайт-Издат, 2017. – 352 с.
3. Vorick D., Champine L. Sia: simple decentralized storage. Security and Privacy Workshops (SPW). 2014.
4. Цыпкин Ю.А., Кудряшов Ю.Н. Применение блокчейн-технологий в информационных системах в сфере кадастрового учета и регистрации прав на недвижимое имущество // Землеустройство, кадастр и мониторинг земель. 2018. № 4 (159). С. 38-42.
5. Лаврушин О.И. Новые явления в развитии кредита и институциональной структуре банковского сектора // Банковское дело. 2017. № 2. С. 14-19.
6. Peters G. W., Efstathios P. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money // Banking Beyond Banks and Money. Springer, Cham. 2016. pp. 239-278.
7. Hassani, H., Huang, X., Silva, E.S. Banking with blockchained big data//Journal of Management Analytics. 2018. № 5 (4). pp. 256-275.