ӘОЖ 004.6 **DOI 10.52167/1609-1817-2025-136-1-290-298**

Ж.А. Абитханова, Ж. К. Алимсеитова
Ssatbayev University, Алматы, Қазақстан
Email: zhuldyz_al@mail.ru

ЭЛЕКТРОНДЫҚ ДАУЫС БЕРУ ЖҮЙЕЛЕРІ ҮШІН БЛОКЧЕЙНДІ ҚОЛДАЙТЫН СМАРТ-КЕЛІСІМШАРТТАРДЫ ҚОЛДАНУ МӘСЕЛЕЛЕРІ

Аңдатпа. Дәстүрлі компьютерлендірілген дауыс беру әдістері хакерлер үшін осалдықты, дауыс беруді манипуляциялау және жеке деректерді ұрлау сияқты бірқатар проблемалардан зардап шегеді. Енгізілген өзгермеушілік, ашықтық және қауіпсіздік функцияларының арқасында блокчейн технологиясы смарт-келісімшарттармен бірге сенімді ауыстыруды қамтамасыз етеді. Бұл мақалада электронды дауыс берудің қауіпсіздігі мен тиімділігін арттыру үшін ақылды келісімшарттар бойынша блокчейнге негізделген электронды дауыс беру алгоритмі ұсынылған. Ұсынылған әдіс сонымен қатар мөлдірлікке, өзгермейтіндікке және манипуляцияның төмен ықтималдығына кепілдік береді. Алгоритм дәл қорытындылауды қамтамасыз етеді және келіспеушіліктерді шешу арқылы электрондық дауыс беру үшін берік негіз жасайды. Сайлаушылардың жетілдірілген аутентификациясына көп факторлы аутентификация және эллиптикалық қисық цифрлық қолтаңбалар арқылы қол жеткізіледі, бұл рұқсатсыз қол жеткізу тәуекелдерін азайтады.

Түйінді сөздер. Ақылды келісімшарт, блокчейн, электронды дауыс беру, қауіпсіздік, ашықтық.

Кіріспе.

Blockchain технологиясына негізделген ақылды келісімшарттарды тиімділік, қауіпсіздік және ашықтық сияқты әртүрлі мәселелерді шешу үшін қолдану жақында айтарлықтай қызығушылық тудырды [1]. Ақылды келісімшарттар келісімшарт талаптарын автоматты түрде орындау арқылы делдалдар мен сыртқы мониторинг қажеттілігін жоюға бағытталған. Блокчейнге негізделген ақылды келісімшарттар қауіпсіздіктің жоғарылауы, транзакциялық шығындардың төмендеуі және тиімділіктің жоғарылауы сияқты бірқатар көрсеткіштер бойынша дәстүрлі келісімшарттардан асып түседі [2]. Олардың танымалдылығының артуын олардың тиімділігімен, өзгермейтіндігімен және ашықтығымен түсіндіруге болады. Блокчейнге негізделген ақылды келісімшарттар келісімшартты басқару мен транзакцияны өңдеуді өзгертеді. Ақылды келісімшарттар-бұл екі немесе одан да көп тараптарға үшінші тараптың араласуын қажет етпестен заңды түрде міндетті келісімдер жасауға мүмкіндік беретін өздігінен орындалатын бағдарламаланатын код бөліктері [3]. Олардың ашықтығы, өзгермейтіндігі және қауіпсіздігінің жоғары деңгейі оларды қаржы, жылжымайтын мүлік, Денсаулық сақтау және жабдықтау тізбегін басқару сияқты көптеген салалар үшін тамаша құрал етеді [4]. Электрондық дауыс беру әдістері негізінен блокчейн технологиясына негізделген ақылды келісімшарттарға негізделген. Сайлаудағы алаяқтық, хакерлік шабуылдар және жеке ақпараттарды ұрлау - бұл дәстүрлі компьютерленген дауыс беру әдістеріне бұрыннан кедергі келтірген мәселелердің кейбірі ғана. Blockchain технологиясы осы ұзақ уақытқа созылған қауіпсіздік, адалдық және сайлаудың ашықтығы мәселелерінің ықтимал шешімдерін ұсынады, олар негізгі мәселелер болып табылады.

Электрондық дауыс беруге блокчейн технологиясын енгізу сайлаушылардың құпиялылығын қорғау, дауыстардың қайталануын болдырмау және келісімге тез қол

жеткізу сияқты мәселелерді шешуге мүмкіндік береді. Бұл мәселелерді шешу үшін көптеген балама нұсқалар ұсынылды, соның ішінде озық криптографиялық әдістерді қолдану, тұрақты консенсус алгоритмдерін әзірлеу және қауіпсіз аутентификация процедураларын енгізу.

Материалдар мен тәсілдер.

Ақылды келісімшарттарды кеңінен енгізу және қолайлылығы олардың қауіпсіздігі мен сенімділігіне байланысты; осылайша, ақауларға, хакерлерге немесе қателіктерге осал ақылды келісімшарттар елеулі қаржылық шығындарға әкелуі, сондай-ақ сенім мен беделге нұқсан келтіруі мүмкін. Бұл мәселені шешу үшін өзгермейтіндігін қамтамасыз ететін, жазбалардың қолдан жасалуын болдырмайтын және жазбалары бар транзакциялардың тұтастығы мен сенімділігін қамтамасыз ететін блокчейнді қолдайтын жеке шешім пайдаланылады. Қауіпсіздік шаралары сайлау өткізу кезінде интеллектуалды электронды дауыс беру жүйелерін пайдалануды жақсарту үшін блокчейн технологиясымен және екі факторлы аутентификациямен біріктіріледі [5]. Дерекқорда таратылған тізілімдердің транзакцияларының қауіпсіздігін қамтамасыз етудің тағы бір қызықты тәсілі пайдаланылады, ол жазбаларды алаяқтық әрекеттерден, тізбек қатысушыларының бұрмалауы мен бұрмалануынан қорғайды [6]. Қосымша нұсқа-ақылды келісімшарттарды құру және енгізу үшін ең жақсы тәжірибелер мен салалық стандарттарды белгілеу [7].

Бірнеше назар аударарлық зерттеулер ақылды келісімшарттар туралы түсініктерді кеңейтуде және оларды блокчейн платформаларында қолдануда шешуші рөл атқарды, осылайша блокчейн технологиясының дамуына ықпал етті. Келесі негізгі жұмыстар осы саланың негізгі аспектілеріне жол ашып, блокчейн туралы білім шегін кеңейтті. Tanwar және т.б. [8] ақылды келісімшарттарды қолдана отырып, Ethereum блокчейнінде орталықтандырылмаған электронды дауыс беру қосымшасын (DApp), сондай-ақ блокчейнге кедергісіз қол жеткізуге арналған интерфейсті құрды. Бұл тәсіл сайлаушыларды толығымен ашық сайлау кезінде жасырын ұстауға бағытталған. Алайда, ұсынылған тәсіл теориялық негізді қамтамасыз етті және блокчейн технологиясын пайдалана отырып, электрондық дауыс беру жүйесін нақты енгізуді қамтамасыз етпеді.

Abuidris және басқалар. [9] электрондық дауыс беру жүйелерін басқару және олардың қауіпсіздігін қамтамасыз ету үшін бірге жұмыс істейтін proof-of-stake және proof-of-stake біріктіретін proof-of-stake консенсус блокчейнінің (PSC-Bchain) гибридті моделін ұсынды. Ақылды келісімшарттар сенімді қоғамдық хабарландыру тақтасын, сондай-ақ дауыс беру нәтижелерінің дұрыстығына кепілдік беретін қауіпсіз есептеу ортасын қамтамасыз ету үшін қолданылады. PSC-bchain гибридті тәсіліне негізделген шардинг технологиясы blockchain негізіндегі электрондық дауыс беру жүйесінің қауіпсіздігін, өткізу қабілеттілігін және тиімділігін арттыру үшін қолданылады.

Emami және т.б. [10] орталықтандырылмаған электронды дауыс беру жүйесін енгізді, ол кең ауқымды сайлауды тиімді басқару үшін дербес нөлдік есептеулерді қолданады, сонымен бірге кіріктірілген жадтың белгіленген көлемін қажет етеді. Ұсынылған стратегия құпиялылықты, әмбебап тексеруді, ашықтықты және бюллетеньдерді қажет етпеуді ынталандырады. Сайлаушылардың транзакциялық шығындарын азайту үшін "дауыс беру жәшіктері"деген жаңа идея ұсынылды. Жоспардың негізгі сипаттамасы-оның блокчейн технологиясының артықшылықтарын пайдалана отырып, жаппай сайлауды бақылау мүмкіндігі. Осы схеманың жүзеге асырылуын тексеру үшін Ethereum тест желісінде тұжырымдаманы тестілеу өткізілді, бұл электрондық дауыс берудің әлеуетті қауіпсіз, масштабталатын және жеке жүйелеріне жол ашты.

Zhang және оның авторлары [11] блокчейнді (BEV) қолдана отырып дауыс беру механизмін жасады. Әзірлеу барысында ауқымдылығы, тексерілуі және сенімділігін қоса алғанда, тоғыз маңызды талап айқындалды. Бұдан басқа, BEV жүйесінің құнын төмендету

үшін авторлар тез аутентификациялау үшін Блум есептеу сүзгісі мен Меркл хэш-ағашын біріктіретін гибридті деректер құрылымын әзірледі.

Panja және Bimal [12] құпия дауыс беруді тексеруге рұқсат етілген криптографиялық әдісті ұсынды. Ұсынылған әдіс жеке электронды тікелей тіркеу құрылғыларының (DRE) нәтижелерін ашпай, соңғы санау нәтижелерін жариялау арқылы бюллетеньдерге шабуыл жасауға жол бермейді. Бұл бюллетеньдерді сақтау үшін екі механизм қолданылды: блокчейн және бұлтты серверлер. Алайда, олар ұсынған тәсілді қолдана отырып алынған нәтижелерді прототип ретінде тексеру және енгізу қиын болды.

de Farias және т.б. [13] киберқауіпсіздік пен деректердің құпиялылық қажеттіліктерін анықтау үшін процестерді теориялық-жүйелік талдауды (STPA) және оның кеңейтімдерін, сондай-ақ электронды дауыс берудің негізгі жүйесі үшін шешім жасау үшін блокчейн технологиясын қолданатын тәсілді енгізді. Деректердің киберқауіпсіздігі мен құпиялылығын қамтамасыз ету үшін тұжырымдамалық шешім әзірленді және сыналды.

Adeniyi және т.б. [14] электронды дауыс беруге арналған блокчейнді ұсынды. Дауыс берудің анонимділігін қамтамасыз ету үшін биометрияға негізделген криптография енгізілді. Биометриялық деректер әрбір сайлаушының жеке кілтін жасауға негіз ретінде енгізілді, ал ашық кілт сайлаушыны сәйкестендіру үшін жасалды. Әрбір адамның биометриялық деректері жеке және қолдан жасалуы мүмкін болмағандықтан, сайлаушыны сәйкестендіру қорғалды. Берілген ашық кілтті жеке кілтпен сәйкестендіру мүмкін болмады, сондықтан сайлаушының жеке басы жасырын болды.

Liao және Cheng [15] бедел мен дауыс беруге (RVC) негізделген консенсус әдісін ұсынды. Сәйкестендіру процесіне кететін уақытты азайту үшін RVC күрделі хэш есептеулерін қажет етпейтін және жетілдірілген есептеулерді де, дәйекті блокчейн әрекеттерін де ескеретін беделді бағалау әдісін қолдана отырып, блоктауды ұсынатын қатысушыларды таңдайды. Алаяқтық түйіндердің консенсусқа келуіне жол бермеу үшін зиянды әрекеттерді көрсететін түйіндерді анықтайтын және сүзетін RVC сүзу алгоритмі жасалды.

Бұл зерттеулер жиынтығында блокчейн-платформаларда ақылды келісімшарттарды қолданудың артықшылықтары, шектеулері мен мүмкіндіктері туралы құнды ақпарат береді. Әрбір зерттеу саланың қазіргі жағдайы мен болашақ даму бағыттары туралы жан-жақты түсінік бере отырып, ақылды келісімшарттардың нақты аспектілерін және оларды жүзеге асыруды қарастырады.

Жоғарыда келтірілген талдау нәтижелерін ескере отырып, Ethereum негізіндегі электронды қауіпсіз дауыс беру алгоритмі ұсынылады.

Ethereum - бұл әзірлеушілерге смарт-келісімшарттар мен орталықсыздандырылған қосымшаларды (dApps) жасау және өрістету үшін Solidity бағдарламалау тілін пайдалануға мүмкіндік беретін блокчейнге негізделген орталықсыздандырылған бастапқы платформа [16]. Ethereum орталықсыздандырылған тораптар желісінде жұмыс істейтін жаһандық компьютердің тұжырымдамасына негізделген, олардың әрқайсысы транзакцияларды, келісімшарттарды және dApps қосымшаларын орындайды және тексереді. Ethereum ең маңызды ерекшеліктерінің бірі оның делдалдарды немесе орталық органдарды пайдаланбай сенімді және ашық транзакциялар мен келісімшарттарды қамтамасыз ету қабілеті болып табылады; бұған криптографиялық хаттамалардың, консенсус әдістерінің және орталықсыздандырылған басқару жүйелерінің көмегімен қол жеткізіледі. Solidity-ақылды келісімшарттар жасау үшін Ethereum платформасында қолданылатын негізгі бағдарламалау тілі; бұл әзірлеушілерге Ethereum виртуалды машинасында (EVM) жұмыс істей алатын қауіпсіз және тиімді ақылды келісімшарттар жасауға көмектесуге арналған жоғары деңгейлі, келісімшартқа бағытталған бағдарламалау тілі. Ethereum және Solidity банктік қызметтен бастап жеткізілім тізбегін басқаруға және

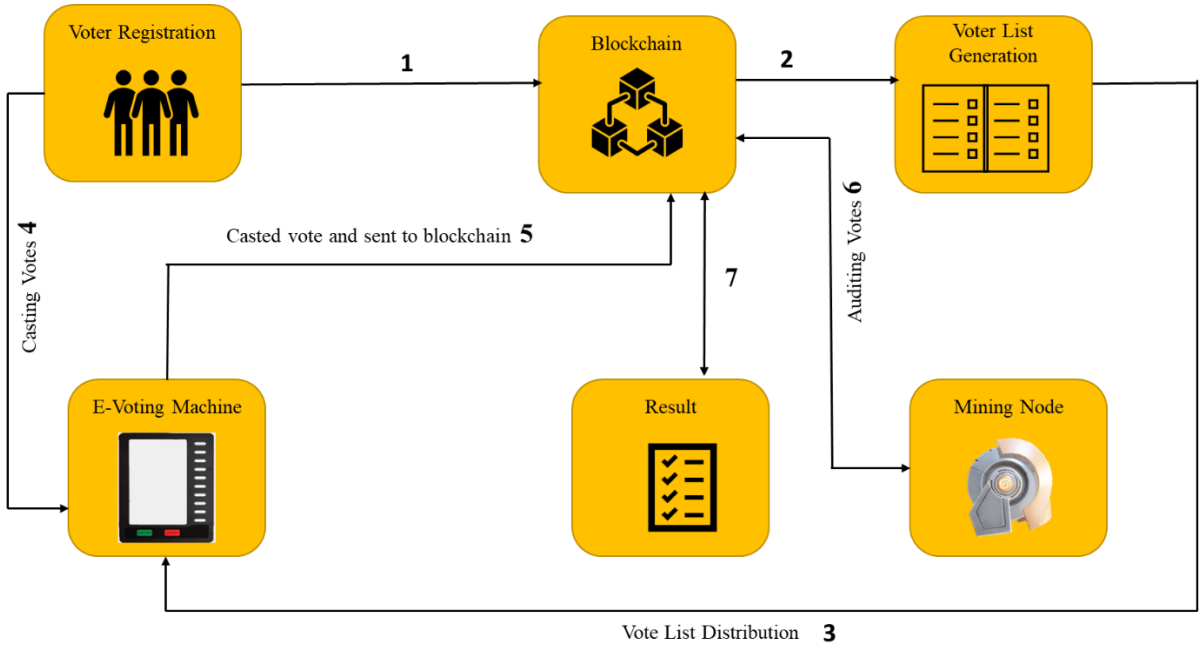
денсаулық сақтауға дейінгі әртүрлі салалардағы сенім, ашықтық және басқару идеяларын өзгертті. Ұсынылған алгоритм және блокчейнге негізделген ақылды келісімшарттар жүйесі үш кезеңге бөлінеді:

- Pdpos көмегімен электронды дауыс беру блоктарын құру процесі.
- Электрондық дауыс беруге арналған ақылды келісімшарттардың ашық орындалуы.

Электрондық дауыс беру қорытындысын шығару.

Нәтижелер.

Қауіпсіз, тиімді және инклюзивті келісімшарттық экожүйені құруда ынтымақтаса отырып, блокчейн негізіндегі ақылды келісімшарттардың әлеуетін толық іске асыруға болады. 1-суретте блокчейнге негізделген электронды дауыс беру үшін ақылды келісімшарттың қалай жасалғаны көрсетілген.



1 сурет - Электрондық дауыс беруге арналған блокчейнге негізделген ақылды келісімшарттың жалпы архитектурасы

Блокты құру-бұл блокчейн технологиясындағы негізгі процесс, оның негізгі функциясы блокчейн желісіндегі транзакциялар жиынтығын мұқият жазатын жаңа блокты құруды жеңілдету болып табылады. Осылайша, жасалған әрбір блок алдыңғы блоктың криптографиялық хэшін қамтитын негізгі құрылым ретінде қызмет етеді, осылайша бұзуға немесе рұқсат етілмеген модификацияларға жол бермейтін үзілмейтін жазбалар тізбегін жасайды. Дауыс беру транзакцияларының құпиялылығына, тұтастығына және қауіпсіздігіне кепілдік беру үшін біз бірнеше маңызды криптографиялық әдістерді қолданамыз. SHA-256 алгоритмі деректердің нақты сандық ізін жасай отырып, дауыс берудің әрбір транзакциясын хэштеу үшін пайдаланылады. Дауыс беру транзакциясы деректерінің кез келген өзгеруі нақты хэштің алынуына әкелетіндігіне кепілдік бере отырып, бұл хэштеу деректердің тұтастығын сақтайды. Криптографиялық кілттерді құру және дауыс беру транзакцияларының қауіпсіздігін қамтамасыз ету үшін біз эллиптикалық қисық криптографияны (ECC) қолданамыз [17]. Әдеттегі криптографиялық әдістермен салыстырғанда, ECC кілттердің аз мөлшері кезінде қауіпсіздіктің неғұрлым жоғары деңгейін қамтамасыз етеді, бұл оны біздің электрондық дауыс беру жүйеміз сияқты

шектеулі ресурстары бар қосымшаларға қолайлы етеді. Сайлаушының жеке кілті әр дауыс беру операциясына сандық қол қою үшін қолданылады.

Бұл цифрлық қолтаңба дауыстың авторландырылған сайлаушымен берілгеніне және өзгертілмегеніне кепілдік бере отырып, аутентификацияны қамтамасыз етеді. Қолтаңбаның түпнұсқалығын тексеру үшін тиісті ашық кілт қолданылады. Блоктағы дауыс беру операцияларының дұрыстығын тиімді және сенімді тексеру үшін біз Меркл ағаштарын қолданамыз [18]. Меркла ағашында әрбір соңғы торап дауыс беру транзакциясының хэшін білдіреді, ал әрбір соңғы емес торап өзінің еншілес тораптарының хэшін білдіреді. Мұндай құрылым электрондық дауыс беру жүйесін қауіпсіз және тез тексеруге мүмкіндік береді. Әрбір блокты құру бүкіл блокчейн желісінің қауіпсіздігі мен тұтастығын сақтау үшін бірінші кезектегі мәнге ие.

Дауыс беру сайлау комиссиясы тобының тарапынан растауды және бақылауды талап етеді. Елдің түкпір-түкпірінен келген сайлаушылар өз дауыстарын электронды түрде береді. Әрбір дауыс тіркеледі және оны ресми түрде қабылдағанға дейін сайлау комиссиясы растауы керек. Егер дауыс беру нәтижелерімен комиссия мүшелерінің кемінде 25% келіссе, оларды мақұлдау жеткілікті.

Төменде қауіпсіз және тиімді электрондық дауыс беру жүйесіне арналған Ethereum блокчейніне негізделген алгоритм берілген

Algorithm 1: Ethereum блокчейніне негізделген электрондық дауыс беру жүйесі

1. **Initialization:** {B_{et}: Ethereum blockchain; S_c: Smart contract; Vt: Votes; V_c: Vote collection; Vtr: Voters;V_v: Verified votes; V_I: Verified integrity; V_A: Verified authenticity; C_s : Consensus state; V_e: Velocity; γ: Fine tune; M_e: Mechanism; S_{pr}: State parameters; V_d: Voting dynamic; Bl: Block; Bl_c: Block creation; $\ddot{\omega}$: Tamper proof; ζ: Criteria of security; V_n: Voters in network; γ: Efficient}
2. **Input**: { $Vt; Vtr$}
3. Output: { $\gamma; Bl_c; C_s$}
4. **Set** B_{et}
5. **Deploy** S_c
6. **Compute** $Vt = S_c + V_c$
7. **Authorize** $Vt \rightarrow Vtr$
8. **For** $Vtr = 1;\ Vtr \leq Vt;\ Vtr++$
9. Compute $V_v = (V_I + V_A)V_I$
10. **End-For**
11. **Evaluate** C_s
12. **Adjust** C_s
13. **Update** $V_e \rightarrow \gamma(C_s)$
14. **Adapt** $(M_e) \cong V_e$
15. **Update** $S_{pr} \in V_e$
16. **Adapt** $B_{et} \cong V_d$
17. **Compute** $Bl = Bl_c \cup V_v$
18. **Ensure** $Bl \in \ddot{\omega}$
19. **Validate** $Bl_c \subseteq C_s$
20. **If** $Bl_c = \zeta$ then
21. Broadcast $Bl_c \rightarrow V_n$
22. Confirm $Bl_c \subseteq \gamma$
23. **End-If**

1-қадам алгоритмге қажетті айнымалыларды анықтайды. 2-қадам нәтиже алу үшін 3-қадамда өңделетін деректерді береді. 4-қадам Ethereum блокчейн архитектурасын инициализациялаудан басталады. 5-қадам-сайлау жүйесінің қауіпсіздігі мен ашықтығын қамтамасыз ететін дауыс беру процесін бақылау үшін арнайы әзірленген ақылды келісімшартты енгізу. 6-қадам дауыстарды қауіпсіз жинау үшін кеңейтілген ақылды келісімшартты пайдалануды көздейді. 7-қадам тек тіркелген сайлаушылардың дауыс беруге қатысып, өз дауыстарын бере алатындығына көз жеткізу үшін қатаң тексеру процедураларын қамтиды. 8-қадам әр берілген дауыстың дұрыстығы мен тұтастығын растау үшін озық криптографиялық технологияларды қолданады. 9-қадамда блокчейн желісінде келісу процесі үнемі тексеріледі. 10-қадамда ағымдағы бағаларға сәйкес келісу тетігінің тиімділігін барынша арттыру үшін әртүрлі элементтер серпінді өзгереді. 11-қадам жүйенің жалпы өнімділігін арттыру үшін консенсустың жаңару жылдамдығын реттейді. 12-қадамда сәйкестендіру процесі өзгеретін дауыс беру сценарийлері мен желілік жағдайларға бейімделе алады. 13-қадам нақты уақыт режимінде күй параметрлерін жаңарту үшін ағымдағы жұмыс жылдамдығын пайдаланады. 14-қадам блокчейн жүйесінің икемді болып қалуын және дауыс беру динамикасы мен тенденцияларының өзгеруіне жауап беруін қамтамасыз етеді. 15-қадам расталған дауыстары бар жаңа блокты қосу арқылы тізілімді нығайтады. 16-қадам әрбір блокчейн блогының өзгермейтіндігіне кепілдік беретін қатаң шектеулерді енгізеді. Желінің тұтастығын сақтау үшін 17-қадамда алдын-ала жасалған келісілген әдісті қолдана отырып, әрбір жаңа блокты тексеру жүргізіледі. 18-қадам деректердің дәлдігі мен сенімділігін қамтамасыз етеді, өйткені әрбір блок блокчейнге жүктелмес бұрын алдын ала белгіленген стандарттарға сәйкес келеді. 19-қадам желінің барлық мүшелеріне жаңа ғана сертификатталған блоктарды тарату арқылы дауыс беру процесінің ашықтығы мен синхрондалуын қамтамасыз етеді. 20-қадам бүкіл желі бойынша блокчейн жазбаларының дәйектілігін қолдайды, осылайша дауыс беру процесінің тұтастығы мен сенімділігін қамтамасыз етеді.

Талқылау.

Блокчейн технологиясы адам өмірінің әртүрлі салаларына көбірек енуде. Мамандардың болжамы бойынша жақын арада блокчейн қызметтің ажырамас бөлігіне айналады. Қазақстанда әзірге блокчейн көп таралған жоқ, бірақ бұл болашақта оны пайдаланбаймыз дегенді білдірмейді. Блокчейнді пайдалану ұсынылатын бағыттардың бірі-қауіпсіз электрондық дауыс беру.

Қазіргі уақытта дауыс беруді өткізу үшін түрлі технологиялар қолданылады, бірақ көп жағдайда Қазақстанда электрондық дауыс беру жүргізілмейді. Сондықтан оған көптеген қаржылық және еңбек шығындары жұмсалады. Сайлау учаскелері құрылады, бюллетеньдер басылады, байқаушылар шақырылады және т.б. дауыс берудің қауіпсіздігі, ашықтығы, дауыстарды санау және қорытындылау сайлау комиссияларына жүктеледі, яғни адами факторға негізделеді. Электрондық дауыс беруге көшу кезінде қаржылық және еңбек шығындары да болады, сайлау комиссиялары құрылады, бірақ мұнда қауіпсіздікке, ашықтыққа, дауыстарды автоматты және жылдам санауға кепілдік беріледі.

Авторлар ұсынған алгоритм Ethereum блокчейнін қолдана отырып, электронды дауыс беру жүйесіне қатысушылар үшін блоктар құру процесін сипаттайды. Ол әрбір қатысушының жаңа блокты құру шығындарын жабу үшін жеткілікті Ethereum балансына ие болуын және блокты құру процесі адал және тиімді жүзеге асырылатынын қамтамасыз етеді. Осы алгоритмге сүйене отырып, электронды дауыс беру жүйесі блокчейннің тұтастығын сақтай алады және барлық қатысушылардың блок құру процесіне қатысуға тең мүмкіндіктерге ие болуын қамтамасыз етеді.

Ұсынылатын алгоритмде дауыс беруді өткізу процесі электрондық дауыс беруге және тіпті әлеуетті зиянды тораптар болған кезде де процестің тұтастығын қамтамасыз етуге арналған қауіпсіз және масштабталатын платформаның көмегімен тексеріледі және расталады. Бұл көп факторлы аутентификация және криптографиялық қорғау үшін эллиптикалық қисық цифрлық қолтаңба алгоритмі арқылы рұқсатсыз қол жеткізу қаупін азайту арқылы сайлаушылардың аутентификациясының тиімділігін арттырады. Сонымен қатар, әр сайлаушы үшін бірегей сәйкестендіру нөмірлерін пайдалану сайлаудың адалдығы мен анонимділігін қамтамасыз етеді.

Қорытынды.

1. Электрондық дауыс беру жүйесі үшін блокчейнге негізделген ақылды келісімшарттарды енгізу үшін жаңа архитектура ұсынылады, ол қолданыстағы жүйелердің шектеулерін жояды және олардың функционалдығын кеңейтеді. Меншік құқығын растау ақылды келісімшарттардағы қол жетімділік пен құпиялылықты басқару үшін қолданылады және осылайша электронды дауыс беру жүйесіне рұқсатсыз кіруден үлкен икемділік пен қорғауды қамтамасыз етеді.

2. Дауыс берудің икемділігіне, тексерудің тиімділігіне, адалдығына және дауыс беру процесін жеделдетуге кепілдік беріледі.

3. Дауыс беруді өткізу процесі қауіпсіз, сайлаушылардың жасырын болуы, дауыс беру процесінің ашықтығы, қорытындылардың жылдам шығарылуы қамтамасыз етіледі.

ӘДЕБИЕТТЕР

[1] Hewa, Tharaka, Mika Ylianttila, and Madhusanka Liyanage. "Survey on blockchain based smart contracts: Applications, opportunities and challenges." Journal of network and computer applications 177 (2021): 102857.

[2] Peng, Xiangzhen, Zhiyao Zhao, Xiaoyi Wang, Haisheng Li, Jiping Xu, and Xin Zhang. "A review on blockchain smart contracts in the agri-food industry: Current state, application challenges and future trends." Computers and Electronics in Agriculture 208 (2023): 107776.

[3] Benabdallah, Ali, Antoine Audras, Louis Coudert, Nour El Madhoun, and Mohamad Badra. "Analysis of blockchain solutions for E-voting: A systematic literature review." IEEE Access (2022).

[4] Liu, Y., Guo, T., Chen, Z., & Jiang, X. Efficient Attribute-Based Smart Contract Access Control Enhanced by Reputation Assessment. Future Generation Computer Systems, 126,(2021) 182-192.

[5] Ajao, Lukman Adewale, Buhari Ugbede Umar, Daniel Oluwaseun Olajide, and Sanjay Misra. "Application of crypto-blockchain technology for securing electronic voting systems." In Blockchain Applications in the Smart Era, pp. 85-105. Cham: Springer International Publishing, 2022.

[6] Ajao, Lukman Adewale, James Agajo, Emmanuel Adewale Adedokun, and Loveth Karngong. "Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry." J 2, no. 3 (2019): 300-325.

[7] Gupta, S., & Manjunath, C. R. (n.d.). Blockchain-based Preferential E-Voting System DApp using Smart Contract(2021).

[8] Tanwar, Sarvesh, Neelam Gupta, Prashant Kumar, and Yu-Chen Hu. "Implementation of blockchain-based e-voting system." Multimedia Tools and Applications 83, no. 1 (2024): 1449-1480.

[9] Abuidris, Yousif, Rajesh Kumar, Ting Yang, and Joseph Onginjo. "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding." Etri Journal 43, no. 2 (2021): 357-370.

[10] Emami, Ashkan, Habib Yajam, Mohammad Ali Akhaee, and Rahim Asghari. "A scalable decentralized privacy-preserving e-voting system based on zero-knowledge off-chain computations." Journal of Information Security and Applications 79 (2023): 103645.

[11] Zhang, Shufan, Lili Wang, and Hu Xiong. "Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability." International Journal of Information Security 19 (2020): 323-341.

[12] Panja, Somnath, and Bimal Roy. "A secure end-to-end verifiable e-voting system using blockchain and cloud server." Journal of Information Security and Applications 59 (2021): 102815.

[13] de Farias, Júlio César Leitão Albuquerque, Andrei Carniel, Juliana de Melo Bezerra, and Celso Massaki Hirata. "Approach based on STPA extended with STRIDE and LINDDUN, and blockchain to develop a mission-critical e-voting system." Journal of Information Security and Applications 81 (2024): 103715.

[14] Adeniyi, Jide Kehinde, Sunday Adeola Ajagbe, Emmanuel Abidemi Adeniyi, Pragasen Mudali, Matthew Olusegun Adigun, Tunde Taiwo Adeniyi, and Ojo Ajibola. "A biometrics-generated private/public key cryptography for a blockchain-based e-voting system." Egyptian Informatics Journal 25 (2024): 100447.

[15] Liao, Zhuofan, and Siwei Cheng. "RVC: A reputation and voting based blockchain consensus mechanism for edge computing-enabled IoT systems." Journal of Network and Computer Applications 209 (2023): 103510.

[16] Alhijawi, Bushra, Mutaz Abo Alrub, and Mustafa Al-Fayoumi. "Generalized Ethereum Blockchain-based recommender system framework." Information Systems 111 (2023): 102113.

[17] Adeniyi, Jide Kehinde, Sunday Adeola Ajagbe, Emmanuel Abidemi Adeniyi, Pragasen Mudali, Matthew Olusegun Adigun, Tunde Taiwo Adeniyi, and Ojo Ajibola. "A biometrics-generated private/public key cryptography for a blockchain-based e-voting system." Egyptian Informatics Journal 25 (2024): 100447.

[18] Kuznetsov, Oleksandr, Alex Rusnak, Anton Yezhov, Kateryna Kuznetsova, Dzianis Kanonik, and Oleksandr Domin. "Merkle Trees in Blockchain: A Study of Collision Probability and Security Implications." Internet of Things (2024): 101193.

Zhadyra Abitkhanova, doctoral student, Satpayev University, Almaty, Kazakhstan, zh.abitkhanova@satbayev.university

Zhuldyz Alimseitova, PhD, associate professor, Satpayev University, Almaty, Kazakhstan, zhuldyz_al@mail.ru

ISSUES OF USING SMART CONTRACTS WITH BLOCKCHAIN SUPPORT FOR ELECTRONIC VOTING SYSTEMS

Abstract. Traditional computerized voting methods suffer from a number of problems, including vulnerability to hackers, vote manipulation, and identity theft. With built-in features of immutability, transparency, and security, blockchain technology provides a reliable replacement in combination with smart contracts. This article presents a blockchain-based algorithm for electronic voting on smart contracts to improve the security and efficiency of electronic voting. The proposed method also guarantees transparency, immutability and a low probability of manipulation. The algorithm ensures accurate summing up and creates a solid foundation for

electronic voting, settling differences. Improved voter authentication is achieved through multi-factor authentication and digital signatures with an elliptical curve, which minimizes the risks of unauthorized access.

Keywords. Smart contract, blockchain, electronic voting, security, transparency.

Жадыра Абитханова, докторант, Satpayev University, Алматы, Казахстан, zh.abitkhanova@satbayev.university
Жулдыз Алимсеитова, PhD, ассоциированный профессор, Satpayev University, Алматы, Казахстан, zhuldyz_al@mail.ru

ВОПРОСЫ ПРИМЕНЕНИЯ СМАРТ-КОНТРАКТОВ С ПОДДЕРЖКОЙ БЛОКЧЕЙНА ДЛЯ СИСТЕМ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Аннотация. Традиционные компьютеризированные методы голосования страдают от ряда проблем, включая уязвимость для хакеров, манипулирование голосованием и кражу личных данных. Благодаря встроенным функциям неизменности, прозрачности и безопасности технология блокчейн обеспечивает надежную замену в сочетании со смарт-контрактами. В этой статье представлена основанный на блокчейне алгоритм электронного голосования по смарт-контрактам для повышения безопасности и эффективности электронного голосования. Предлагаемый метод также гарантирует прозрачность, неизменность и низкую вероятность манипуляций. Алгоритм обеспечивает точное подведение итогов и создают прочную основу для электронного голосования, улаживая разногласия. Усовершенствованная аутентификация избирателей достигается за счет многофакторной аутентификации и цифровых подписей с эллиптической кривой, что сводит к минимуму риски несанкционированного доступа.

Ключевые слова. Смарт-контракт, блокчейн, электронное голосование, безопасность, прозрачность.

****

Редакцияға түсті / Поступила в редакцию / Received 05.09.2024
Жариялауға қабылданды / Принята к публикации / Accepted 04.02.2025