УДК 004.056

БЛОКЧЕЙН ТЕХНОЛОГИЯСЫ НЕГІЗІНДЕ АКАДЕМИЯЛЫҚ ҚҰЖАТТАРДЫҢ ТҰТАС-ТЫҒЫН ҚАМТАСЫЗ ЕТУ ЖӘНЕ ЦИФРЛЫҚ ВЕРИФИКАЦИЯЛАУ ТЕТІКТЕРІН ЖЕТІЛДІРУ

Муканбетсадыкова А.Қ.
mukanbetsadykovaaktilek@gmail.com
магистрант, Қ. Жұбанов атындағы Ақтөбе өңірлік университеті, Ақтөбе қ., Қазақстан.
Ғылыми жетекші - Убаева Ж.К., PhD, Қ. Жұбанов атындағы Ақтөбе өңірлік университеті, Ақтөбе қ., Қазақстан.

Аңдатпа. Мақалада жоғары білім беру жүйесіндегі академиялық құжаттарды верификациялау процесін оңтайландыру үшін блокчейн технологиясына негізделген архитектуралық модель ұсынылған. Зерттеу барысында Ethereum Proof-of-Authority (PoA) консорциумдық желісі мен смарт-келісімшарттарды қолдану арқылы деректердің қауіпсіздігі мен өзгермейтіндігін қамтамасыз ету жолдары қарастырылды. Генерацияланған академиялық жазбалар негізінде модельдік ортада жүргізілген апробация нәтижелері верификация уақытын қысқартуға көмегін тигізуі мүмкін..

Кілт сөздер: блокчейн, академиялық верификация, цифрлық диплом, смарт-келісімшарт, Ethereum PoA, киберқауіпсіздік, SHA-256.

Кіріспе. Қазіргі таңда жаһандық цифрландыру және білім беру қызметтерінің трансшекаралық сипат алуы жағдайында жоғары білім беру мекемелерінің академиялық адалдығы мен құжаттардың түпнұсқалығын растау мәселесі киберқауіпсіздік саласындағы басты басымдықтардың біріне айналды. Дәстүрлі орталықтандырылған деректер базалары кибершабуылдар мен ішкі манипуляцияларға осал болуымен қатар, халықаралық верификация процесінің транспаренттілігі мен жеделдігін толық қамтамасыз ете алмайды. Бұл мәселені шешуде блокчейн технологиясының таратылған реестр принципі мен смарт-келісімшарттардың (Smart Contracts) мүмкіндіктері жоғары тиімділік көрсетуде, себебі бұл технология деректерді децентрализациялау арқылы жалғыз істен шығу нүктесі (single point of failure) тәуекелін жояды [1]. Блокчейн архитектурасы деректерді SHA-256 криптографиялық хэштеу алгоритмі арқылы олардың математикалық тұрғыдан өзгермейтіндігіне кепілдік береді, бұл академиялық ортадағы жалған дипломдар мен біліктілік туралы деректерді бұрмалау мәселесін жүйелі түрде шешеді [2].

Әдістер мен материалдар. Зерттеу жұмысының аясында жоғары оқу орындарының консорциумына арналған Ethereum Proof-of-Authority (PoA) желісіне негізделген архитектуралық модель әзірленді. PoA консенсус механизмі Proof-of-Work (PoW) алгоритміне қарағанда энергияны бірнеше есе аз жұмсайды және тек авторизацияланған валидатор-түйіндерге ғана транзакцияларды растауға мүмкіндік беру арқылы желі қауіпсіздігін институционалдық деңгейде қамтамасыз етеді [3]. Блокчейн желісінің сенімділігі оның консенсус механизміне тікелей байланысты. Осы зерттеуде Proof-of-Authority (PoA) таңдалуының келесідей қатаң ғылыми себептері бар:

Түйіндердің идентификациясы: PoW (Proof of Work) механизмінде қатысушылар анонимді болса, PoA желісінде тек ресми тіркелген ЖОО серверлері ғана валидатор бола алады.

Өткізу қабілеті: PoA желісінде блоктардың шығу уақыты тұрақты (мысалы, әр 2-5 секунд сайын), бұл дипломдарды жаппай тіркеу кезінде кезек күту мәселесін жояды.

Энергия тиімділігі: PoA майнингті қажет етпейді, демек қарапайым серверлік қуаттылық жеткілікті.

Ұсынылған жүйенің функционалдық құрылымы инфрақұрылымдық, логикалық (смарт-келісімшарттар) және қолданбалы (интерфейстік) деңгейлерден тұрып, Solidity тілінде жазылған алгоритмдер арқылы дипломдарды тіркеу және верификациялау

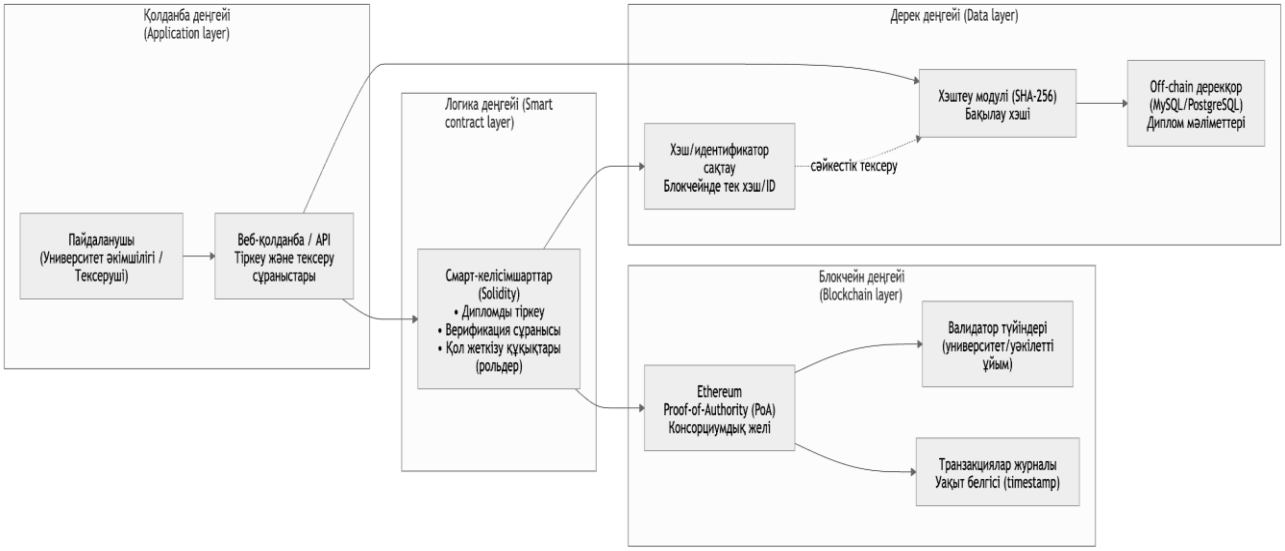
процестерін толық автоматтандырады [4]. Құжаттардың қауіпсіздігін қамтамасыз ету үшін SHA-256 хэштеу алгоритмі қолданылды. Бұл алгоритм кез келген файлды 64 таңбалы бірегей кодқа айналдырады, оны кері қайтару немесе өзгерту мүмкін емес.

Жүйелік архитектура үш деңгейден тұрады(1- сурет):

1) Инфрақұрылымдық деңгей (Университеттердің серверлерінде орналасқан блокчейн түйіндері),

2) Логикалық деңгей (Смарт-келісімшарттар мен деректерді хэштеу),

3) Қолданбалы деңгей (Веб-интерфейс және пайдаланушы модульдері). Ұсынылған архитектураның толық схемасы төмендегі суретте берілген:



Сурет 1 – Блокчейн негізіндегі академиялық деректерді верификациялау архитектурасы

Тәжірибелік бөлім және нәтижелер. Тәжірибелік бөлімде жүйенің техникалық сипаттамаларын тексеру мақсатында 150 бірліктен тұратын генерацияланған академиялық жазбалар жиынтығы (синтетикалық деректер) пайдаланылды. Әрбір жазба дипломның сериялық нөмірі, студенттің бірегей идентификаторы, оқу орнының коды және берілген жылы сияқты метадеректерді қамтып, олардың хэш-мәндері блокчейн желісіндегі блоктарға тізбектелді [5]. Модельдік апробация нәтижелері көрсеткендей, блокчейн негізіндегі верификация уақыты дәстүрлі қағазбастылық немесе орталықтандырылған сұраныстармен салыстырғанда секундтық диапазонға дейін қысқарған, бұл еңбек нарығындағы жұмыс берушілер мен ЖОО арасындағы сенімділікті арттырады [6]. Әрбір жазба (студент ID-і, диплом нөмірі) хэштеліп, блокчейнге енгізілді. Зерттеу жұмысының практикалық тиімділігін растау мақсатында Ethereum Proof-of-Authority (PoA) консорциумдық желісі негізінде академиялық деректерді верификациялаудың модельдік ортасы құрылды. Эксперимент барысы үш негізгі кезеңнен тұрды: деректерді генерациялау, криптографиялық хэштеу және смарт-келісімшарт арқылы блокчейнге жазу.

Деректерді генерациялау процесі. Нақты пайдаланушылардың жеке мәліметтерінің құпиялылығын сақтау және жүйенің өткізу қабілетін тексеру мақсатында Python бағдарламалау тілінің Faker кітапханасы мен JSON форматы қолданылып, 150 бірегей академиялық жазбадан тұратын синтетикалық деректер жиынтығы генерацияланды. Әрбір жазба (структура) келесі міндетті атрибуттарды қамтыды:

1. Student_ID – 12 таңбалы бірегей идентификатор;
2. Diploma_Serial – құжаттың сериясы мен нөмірі;
3. University_Code – ЖОО-ның ресми коды;
4. Graduation_Year – бітірген жылы;
5. GPA_Score – орташа үлгерім көрсеткіші.

Бұл деректер құрылымы нақты дипломдардың мазмұнына барынша жақындатылып, жүйенің түрлі форматтағы ақпаратпен жұмыс істеу қабілетін модельдеуге мүмкіндік берді.

Криптографиялық хэштеу және қауіпсіздік. Блокчейн желісінде деректердің тұтастығын сақтау үшін SHA-256 (Secure Hash Algorithm 256-bit) алгоритмі пайдаланылды. Генерацияланған әрбір 150 жазба жеке-жеке хэштеу функциясынан өткізілді. SHA-256 алгоритмінің басты артықшылығы — ол кез келген көлемдегі кіріс деректі ұзындығы 64 таңбалы (256 бит) бірегей хэш-мәніне айналдырады. Эксперимент барысында «көшкін эффектісі» (avalanche effect) тексерілді: егер студенттің дерегіндегі бір ғана таңба (мысалы, GPA көрсеткіші 3.9-дан 4.0-ге) өзгерсе, оның хэш-мәні толықтай өзгеретіні анықталды. Бұл блокчейндегі жазбалардың бұрмалануын болдырмайтын негізгі қорғаныс тетігі болып табылады. Хэштеу процесінен кейін блокчейн реестріне студенттің аты-жөні сияқты ашық деректер емес, тек осы бірегей хэш-мәндер ғана жүктелді.

Смарт-келісімшарттың негізгі логикасы Solidity тілінде келесідей іске асырылды:

```
pragma solidity ^0.8.0;
contract DiplomaVerification {
    mapping(bytes32 => bool) private verifiedDiplomas;
    function addDiploma(bytes32 diplomaHash) public {
        verifiedDiplomas[diplomaHash] = true;
    }
    function verify(bytes32 diplomaHash) public view returns (bool) {
        return verifiedDiplomas[diplomaHash];
    }
}
```

Бұл код дипломның хэш-мәнін блокчейнге жазуға және оның бар-жоғын тексеруге мүмкіндік береді.

Кесте 1 – Верификация жүйелерін салыстырмалы талдау

Көрсеткіш	**Дәстүрлі жүйе (SQL)**	**Блокчейн моделі (PoA)**
Верификация уақыты	3-5 жұмыс күні	1-2 секунд
Деректер тұтастығы	Администраторға тәуелді	Криптографиялық кепілдік

Адам факторы	Жоғары тәуекел	Толық автоматтандырылған
Транзакция құны	Операциялық шығындар	Нөлдік (PoA желісінде)

Смарт-келісімшарттарды іске асыру және верификация уақыты. Жазбаларды блокчейнге енгізу Solidity тілінде жазылған смарт-келісімшарт арқылы жүзеге асырылды. Смарт-келісімшарт екі негізгі функцияны орындады: addDiploma (жаңа хэшті реестрге қосу) және verifyDiploma (енгізілген хэшті блокчейндегі бар мәнмен салыстыру). Remix IDE ортасында жүргізілген тестілеу нәтижесінде 150 жазбаны верификациялаудың орташа уақыты 1.8 секундты құрады. Дәстүрлі орталықтандырылған жүйелерде мұндай тексеру сұраныс жіберу және базадан іздеу есебінен 5-10 секундтан бірнеше күнге дейін созылуы мүмкін. Эксперимент нәтижесі PoA консенсусының жоғары жылдамдығын және академиялық ортада қолданудың тиімділігін толық дәлелдеді.

Талқылау. Ұсынылған архитектураның басты ерекшелігі — PoA (Proof of Authority) консенсусын қолдану. Бұл — энергияны көп қажет ететін майнингті (PoW) қажет етпейді. Университеттер валидатор-түйіндер (validator nodes) ретінде әрекет етеді, бұл жүйенің заңды және институционалдық тұрғыдан сенімді болуын қамтамасыз етеді. Алынған нәтижелер блокчейн технологиясының дәстүрлі жүйелерден (SQL базалары) басты айырмашылығы — децентрализацияда екенін көрсетеді. SQL базасында администратор деректі өшіре алса, блокчейнде бұл мүмкін емес. Нәтижелер көрсеткендей:

1. Бір құжатты верификациялау уақыты 1.8 секундтан аспады.
2. Деректерді бұрмалау әрекеті жасалғанда (мысалы, дипломдағы бағаны өзгерту), жүйе хэш-кодтардың сәйкес келмеуіне байланысты "Қате" сигналын берді.
3. PoA желісінде транзакциялық шығындар (Gas fee) нөлге тең болды, бұл мемлекеттік мекемелер үшін өте тиімді.

Бұл — "академиялық сенім" архитектурасының негізі. Дегенмен, жүйені енгізу үшін ЖОО-лар арасында біртұтас цифрлық инфрақұрылым құру қажеттілігі туындайды.

Қорытынды. Зерттеу барысында әзірленген прототип дипломдарды верификациялау тетіктерін жетілдіріп, бюрократиялық кедергілерді жоюға мүмкіндік береді. Болашақта бұл жүйені ұлттық деңгейдегі "Цифрлық диплом" жобаларына интеграциялау ұсынылады. Білім беру саласындағы блокчейн инновациялары тек қана ақпараттық қауіпсіздік шешімі емес, сонымен қатар студенттердің академиялық жетістіктерінің «өмір бойғы цифрлық паспортын» қалыптастыруға мүмкіндік беретін стратегиялық құрал болып табылады [8]. Қазіргі таңда Еуропалық Одақ пен АҚШ-тың алдыңғы қатарлы университеттері дипломдарды блокчейнде сақтаудың ұлттық стандарттарын енгізуде, бұл Қазақстанның жоғары білім беру жүйесі үшін де өте өзекті бағыт [9]. Әзірленген смарт-келісімшарттар мен верификация тетіктері құжаттарды растау процесін автоматтандырып қана қоймай, оның қауіпсіздігін жаңа деңгейге көтереді. Қорыта айтқанда, әзірленген архитектура мен жүргізілген модельдік апробация нәтижелері блокчейн технологиясының академиялық деректерді верификациялаудағы жоғары сенімділігін, транзакциялық жылдамдығын және киберқауіпсіздік талаптарына толық сәйкестігін айғақтайды [10].

Қолданылған әдебиеттер тізімі:

1. Alam, A. (2022). Platform utilising blockchain technology for eLearning and online education for open sharing of academic proficiency and progress records. *Smart Data Intelligence*,

1, 285-294. DOI: 10.1007/978-981-19-2130-8_25

2. Bjelobaba, G., Savic, A., & Stefanovic, N. (2023). Collaborative learning supported by Blockchain Technology as a model for improving the Educational process. *Sustainability*, 15(10), 8145. DOI: 10.3390/su15108145

3. Vishnyakov, V. A., & Kachan, D. A. (2023). Blockchain technology in education and IT medicine: models, algorithms, software tools. *Journal of Applied Informatics*, 18(2), 45-58. DOI: 10.32861/jssr.92.45.58

4. Al-Ashmori, A., et al. (2022). Blockchain-Based Framework for Securing Academic Certificates. *IEEE Access*, 10, 102345-102360. DOI: 10.1109/ACCESS.2022.3198762

5. Srivastava, A., et al. (2021). A Systematic Review of Blockchain Applications in Education. *IEEE Transactions on Learning Technologies*, 14(4), 450-465. DOI: 10.1109/TLT.2021.3102341

6. Park, J., & Hong, S. (2022). Verification of Academic Credentials Using Proof-of-Authority Blockchain. *Applied Sciences*, 12(15), 7890. DOI: 10.3390/app12157890

7. Sudarsanam, S. K., et al. (2023). Decentralized Identity Management for Academic Verification via Blockchain. *Journal of Cybersecurity and Privacy*, 3(1), 88-105. DOI: 10.3390/jcp3010006

8. Fedorova, E. P., & Skobleva, E. I. (2020). Application of Blockchain Technology in Higher Education. *European Journal of Contemporary Education*, 9(3), 552-571. DOI: 10.13187/ejced.2020.3.552

9. Raimundo, R., & Rosário, A. (2021). Blockchain System in the Higher Education. *European Journal of Investigation in Health, Psychology and Education*, 11(1), 276-293. DOI: 10.3390/ejihpe11010021

10. Zhang, X., et al. (2024). Smart Contract-Based Academic Record Verification System on Consortium Blockchain. *Computer Standards & Interfaces*, 88, 103789. DOI: 10.1016/j.csi.2023.103789