УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ“ ВО СКОПЈЕ

ФАКУЛТЕТ ЗА ЕЛЕКТРОТЕХНИКА И ИНФОРМАЦИСКИ ТЕХНОЛОГИИ

Авни Рустеми

ДИЗАЈН НА БЕЗБЕДЕН СИСТЕМ ЗА ГЕНЕРИРАЊЕ И ПРОВЕРКА НА АКАДЕМСКИ ДОКУМЕНТИ БАЗИРАН НА BLOCKCHAIN-ТЕХНОЛОГИЈА

Докторски труд

Скопје, 2024

Докторанд:
Авни Рустеми
Тема: Дизајн на безбеден систем за генерирање и проверка на академски документи базиран на blockchain-технологија

Ментор:
проф. д-р Владимир Атанасовски,
Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

Комисија за одбрана:
проф. д-р Александар Ристески, претседател
Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

проф. д-р Владимир Атанасовски, ментор
Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

проф. д-р Перо Латкоски, член
Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

проф. д-р Валентин Раковиќ, член
Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

проф. д-р Фисник Далипи, член
Универзитет „ Линеус“ во Калмар, Шведска, Технолошки факултет
Катедра за информатика

Лектор: Лилјана Пандева

Научна област:
Електротехника и информациски технологии

Датум на одбрана:

Авни Рустеми

ДИЗАЈН НА БЕЗБЕДЕН СИСТЕМ ЗА ГЕНЕРИРАЊЕ И ПРОВЕРКА НА АКАДЕМСКИ ДОКУМЕНТИ БАЗИРАН НА BLOCKCHAIN-ТЕХНОЛОГИЈА

— Апстракт —

Дигитализацијата на услугите е предизвик со кој се соочуваат сите јавни и приватни институции, вклучително и високообразовните установи (ВОУ). Blockchain-технологијата има потенцијал да го револуционизира образовниот систем преку обезбедување на поединци со иновативни и ефективни начини за учење, како и со менување на начинот на кој професорите и студентите работат заедно. Дигитализацијата на услугите на ВОУ, особено за генерирање и проверка на дипломи, е многу важно прашање, бидејќи пред сè мора да се гарантира непроменливоста, приватноста и безбедноста на податоците.

ВОУ во денешно време се соочуваат со различни предизвици: недостиг на дигитализација на услугите, а особено генерирање и проверка на многу академски документи во физичка форма, вклучувајќи ги и дипломите; недостиг од дигитализација на услугите поврзани со оценувањето на студентите и флексибилност на часовите на наставата; долго чекање за добивање на дипломата, долго чекање за проверка на академските документи, вклучувајќи ги и дипломите; не постои платформа што ќе ја гарантира приватноста на студентите, транспарентноста на услугите, класификацијата на услугите на јавни и приватни, недостаток на ефикасни методи за идентификација на студентите и на другите актери во сегашните системи, сите податоци се чуваат во централизирани бази на податоци со кои лесно може да се манипулира од страна на системските администратори; недостиг на долгорочна стратегија во однос на квалитетот на образованието и ефикасни методи за подобрување на процесот на учење. Blockchain-технологијата се гледа како единствена надеж за решавање на овие проблеми во областа на образованието, иако и таа се соочува со различни предизвици во практиката.

Со докторската дисертација, за прв пат се прави систематска анализа на сите blockchain-имплементации што имаат врска со генерирање и проверка на академски документи, особено на дипломите. Врз основа на оваа систематска анализа, ќе бидат дизајнирани функционалните и нефункционалните барања на системот заснован на blockchain, вклучувајќи дијаграми за случаи на употреба и сценарија за случаи на употреба за сите вклучени актери. Врз основа на сите неодамнешни истражувања, за прв пат дизајнираме концептуален модел на blockchain-систем, создавајќи јасно дефинирана архитектура, при што дадовме големо значење на безбедноста, на енкрипцијата, на механизмите за консензус и на сите други субјекти неопходни за функционирање на системот. Ќе се дизајнира систематската архитектура на процесот на генерирање и проверка на дипломи, архитектурата на функционирањето на паметните договори, и можноста за имплементација на вештачка интелигенција во предложениот модел. На крај, со создавање прототип на предложениот модел, го потврдуваме системот и покажуваме дека blockchain-системите имаат многу предности во генерирањето и проверка на дипломи и други академски документи. За имплементацијата на blockchain-системи во ВОУ, пред сè, мора да бидат усогласени и правни прашања поврзани со високото образование.

Клучни зборови: проверка, генерација, диплома, архитектура, нов дизајн, blockchain-систем, систематска архитектура.

Avni Rustemi

THE APPLICATION OF THE BLOCKCHAIN SYSTEM IN HIGHER EDUCATION INSTITUTIONS FOR THE GENERATION AND VERIFICATION OF DIPLOMAS

—Abstract—

Digitalization of services is a challenge that all public and private institutions are facing, including higher education institutions. Blockchain technology has the potential to revolutionize the educational system by providing individuals with innovative and cost-effective ways to learn, as well as by altering the way teachers and students work together. Digitization of HEI services, especially for the generation and verification of diplomas, is a very important issue, because the immutability, privacy, and security of data must be guaranteed above all.

High education institutions nowadays face various challenges: lack of digitization of services, and especially the generation and verification of many academic documents in physical form, including diplomas; lack of digitization of services related to student evaluation and flexibility of teaching hours; long wait for receiving the diploma, long wait for verification of academic documents, including diplomas; there is no platform that will guarantee the privacy of students, the transparency of services, the classification of services into public and private, the lack of efficient methods for identifying students and other actors in the current systems, all data are stored in centralized databases that can be easily manipulated by system administrators; lack of a long-term strategy regarding the quality of education and efficient methods for improving the learning process. Blockchain technology is seen as the only hope for solving these problems in the field of education, although it also faces various challenges in practice.

Through the doctor's dissertation, for the first time, a systematic analysis of all blockchain implementations that are related to the generation and verification of academic documents, especially diplomas. Based on this systematic analysis, the functional and non-functional requirements of the blockchain-based system will be designed, including use-case diagrams and use-case scenarios for all actors involved. Based on all the recent research, for the first time we design the conceptual model of the blockchain system, creating a clearly defined architecture, where we gave great importance to security, encryption, consensus mechanisms and all other entities necessary for the system to function. The systematic architecture of the process of generating and verifying diplomas, the architecture of the functioning of smart contracts, and the possibility of implementing artificial intelligence in the proposed model will be designed. Finally, by creating a prototype of the proposed model, we validate the system and show that blockchain systems have many advantages in generating and verifying diplomas and other academic documents. The implementation of the blockchain system in HEI, first of all, must be agreed with legal issues related to higher education.

Keywords: verification, generation, diploma, architecture, new design, blockchain system, systematic architecture.

Благодарност **до моето семејство и менторот**

Изјавувам дека докторскиот труд е оригинален труд што го имам изработено самостојно.

Своерачен потпис на докторандот

Изјавувам дека електронската верзија на докторскиот труд е идентична со отпечатениот докторски труд.

Потпис на авторот, с.р.

СОДРЖИНА

1. ВОВЕД 12
1.1. Мотивација за изработка на докторската дисертација 17
1.2. Предмет на истражување и хипотеза 18
1.3. Цели и придобивки од истражувањето 20
1.4. Структура на докторската дисертација 21
1.5. Очекуван научен придонес и примена на резултатите од истражувањето 22
2. ЗНАЧЕЊЕ, КАРАКТЕРИСТИКИ И КЛУЧНИ ЕЛЕМЕНТИ НА BLOCKCHAIN 23
2.1. Безбедност, доверба и приватноста во blockchain-технологијата 23
2.2. Blockchain-алгоритми и употреба 23
2.3. Карактеристики на blockchain 25
2.4. Вовед во blockchain-системите за генерирање и проверка на дипломи 26
3. ПОДОБРУВАЊЕ НА АКАДЕМСКИТЕ АКРЕДИТИВИ: СИНЕРГИЈА НА BLOCKCHAIN И ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА 28
3.1. Интеграција на blockchain и вештачка интелигенција 28
3.2. Поврзана литература 30
3.3. Придобивки од споредување на blockchain и ВИ 32
3.4. Предизвици, импликации и препораки 35
4. СИСТЕМАТСКИ ПРЕГЛЕД НА ЛИТЕРАТУРА ЗА СИСТЕМИ БАЗИРАНИ НА BLOCKCHAIN ЗА ПРОВЕРКА НА АКАДЕМСКИ ДОКУМЕНТИ 37
4.1. Историјат и поврзана работа 37
4.2. Безбедност, транспарентност и предизвици на blockchain во ВОУ 40
4.3. Поврзани истражувања во врска со примена на blockchain во ВОУ 44
4.4. Дизајн на истражувањето 46
4.4.1. Стратегија на пребарување и собирање податоци 47
4.4.2. Избор на релевантни студии 49
4.4.3. Ограничувањата за имплементирање blockchain во ВОУ 51
4.5. Тематска анализа 51
4.5.1. Тип на blockchain (класификација) 52
4.5.2. Автоматско генерирање дипломи 53
4.5.3. Безбедност и транспарентност 54

4.5.4. Приспособливост 55
4.5.5. Потребни технологии 56
4.5.6. Концептуални модели и рамки 57
4.6. Наоди од систематскиот преглед на литературата 58
4.7. Дискусии и импликации 62
4.7.1. Идентификувани празнини 62
4.7.2. Препораки и идни насоки за истражување 64
5. КОНЦЕПТУАЛЕН МОДЕЛ НА BLOCKCHAIN-СИСТЕМ ЗА АВТОМАТСКО ГЕНЕРИРАЊЕ АКАДЕМСКИ ДИПЛОМИ: СЛУЧАИ ЗА УПОТРЕБА И СЦЕНАРИЈА 66
5.1. Значењето на паметните договори 66
5.2. Тестирање и распоредување паметни договори 67
5.3. Предизвиците за усвојување blockchain во ВОУ 69
5.4. Определување на барањата 72
5.5. Случаи за употреба и сценарија 74
6. ДИАР (DIAR): СИСТЕМ ЗАСНОВАН НА BLOCKCHAIN ЗА ГЕНЕРИРАЊЕ И ПРОВЕРКА НА АКАДЕМСКИ ДИПЛОМИ 78
6.1. Поврзана литература 78
6.1.1. Blockchain-решение за ВОУ 80
6.1.2. Предизвици на blockchain во ВОУ 83
6.2. Предложен blockchain-систем за генерирање и проверка на академски дипломи 86
6.2.1. Системска архитектура на blockchain-систем 90
6.2.2. Процес на издавање диплома 93
6.2.3. Процес на верификација на дипломата 95
6.2.4. Архитектура на паметни договори 96
6.3. Дискусија за предложениот систем 98
7. ИМПЛЕМЕНТАЦИЈА НА ПРОТОТИП ЗА ГЕНЕРИРАЊЕ И ПРОВЕРКА НА ДИПЛОМИ 102
7.1. Создавање системски прототип за генерирање и проверка на дипломи на централизиран начин 103
7.2. Имплементација на blockchain-прототип за генерирање и проверка на дипломи 111
7.3. Вметнување податоци во blockchain системот и генерирање дипломи 115
7.4. Проверка на дипломи преку blockchain-системот 122
7.5. Валидација на системот 126

7.6. Повеќекратни регресивни предвидливи анализи за проверка на диплома 135
7.7. Законски прашања во врска со спроведувањето на систем заснован на blockchain во ВОУ 139
8. ПРИДОНЕСИ ОД ДОКТОРСКАТА ДИСЕРТАЦИЈА..... 141
9. ЗАКЛУЧОК И ПОНАТАМОШНА РАБОТА..... 144
10. ТРУДОВИ ОБЈАВЕНИ ОД ДОКТОРСКАТА ДИСЕРТАЦИЈА 147

ЛИСТА НА СЛИКИ

Слика 3.1. Интеграција помеѓу blockchain и вештачката интелигенција
Слика 3.2. Интероперабилност помеѓу ВИ и системи базирани на blockchain
Слика 3.3. Предизвици за интегрирање на вештачката интелигенција и blockchain во академските акредитиви
Слика 4.1.Таксономија со главните теми и поттеми
Слика 4.2. Предизвиците за имплементација на blockchain-системот во ВОУ
Слика 4.3. ПРИСМА (PRISMA)-методологија за пребарување
Слика 4.4. Дистрибуција на истражувачки трудови во академски складишта
Слика 4.5. Број на собрани трудови од конференции и списанија во периодот 2018-2022 година
Слика 5.1. Етерскен (Etherscan) пример за успешна трансакција
Слика 5.2. Поедноставена архитектура на предложениот blockchain-систем
Слика 5.3. Дијаграм на кориснички случаи за студентот
Слика 5.4. Дијаграм на кориснички случаи за професорите
Слика 5.5. Дијаграм на кориснички случаи за издавачот
Слика 5.6. Дијаграм на кориснички случаи за проверувачот
Слика 5.7. Дијаграм на кориснички случаи за администраторот
Слика 6.1. Концептуален модел на предложениот blockchain-систем
Слика 6.2. Графикон на тек на издавање и потврда на диплома
Слика 6.3. Архитектура на blockchain-систем
Слика 6.4. Детален процес на издавање диплома
Слика 6.5. Детален процес на проверка на диплома
Слика 6.6. Архитектура на паметни договори
Слика 7.1. Blockchain-мрежа на blockchain-системот за повеќе ВОУ
Слика 7.2. Поедноставен приказ на работата на централизираниот систем
Слика 7.3. Вметнување, ажурирање и бришење податоци преку системот
Слика 7.4. Дневник на администраторите
Слика 7.5. Генерирање дипломи во ПДФ или Ексел
Слика 7.6. Организација на улоги на blockchain-системот
Слика 7.7. Процесот на blockchain за реализација на трансакција (диплома)
Слика 7.8. Интерфејс на регистрирање и логирање на blockchain-системот
Слика 7.9. Пример за потпишување на дипломата при вметнување
Слика 7.10. Интерфејс за управување со студенти
Слика 7.11. Интерфејс за управување со предметите
Слика 7.12. Опис на процесот на шифрирање и дешифрирање на дипломата
Слика 7.13. Блок-дијаграм за процесот на генерирање диплома
Слика 7.14. Опис на процесот на проверка на диплома
Слика 7.15. Процесот на креирање на blockchain-мрежата од вметнување на податоците
Слика 7.16. Време и големина на блокови, и нови адреси на Етериум (Ethereum), (17 март- 17 април 2024)
Слика 7.17. Успешно извршување паметен договор во Ремикс ИДЕ (Remix IDE)
Слика 7.18. Проценет надоместок за трансакцијата, во очекување на потврда од паричникот на Метамаск

Слика 7.19. Процес на тестирање паметни договори и вклучување интелигентни агенти во Ремикс ИДЕ
Слика 7.20. Транспарентност на паметните договори во Етерскен (Etherscan)
Слика 7.21. Тестирање на паметниот договор во Етерскен
Слика 7.22. Потврда на диплома врз основа на студентски ИД (ID) и број на диплома

ЛИСТА НА ТАБЕЛИ

Табела 1. Класификација на предизвиците за примена на blockchain во ВОУ
Табела 2. Резиме на минати поврзани прегледи
Табела 3. Низа за пребарување (прашања)
Табела 4. Трудови пронајдени во различни академски складишта
Табела 5. Резиме на идентификуваните трудови и нивната корелација со RQs
Табела 6. Теми и нивната поврзаност со релевантните трудови
Табела 7. Резиме на blockchain образовните платформи за проверка на дипломи
Табела 8. Идентификувани празнини поврзани со прашањата за истражување
Табела 9. Ограничувања и решение за blockchain-системи за ВОУ
Table 10. Резиме на најсовремени карактеристики на blockchain-решенија
Табела 11. Функционални и нефункционални барања, практични предизвици на системот ДИАР (DIAR)
Табела 12. Опис на карактеристиките на системите базирани на blockchain вклучувајќи го и ДИАР-системот
Табела 13. Цена на Етериум (Ethereum) за проверка на диплома за една година (симулирани податоци)
Табела 14. Повеќекратни техники на регресија за проверка на дипломи (податоци од Табела 13)

ЛИСТА НА СКРАТЕНИЦИ

(Сите скратеници во трудот се транскрибирани на македонски јазик според Правописот на македонскиот јазик)

BFT – Byzantine Fault Tolerance
EVM – Ethereum Virtual Machine
GDPR – General Data Protection Regulation
IPFS – InterPlanetary File System
IoT – Internet of Things
P2P – Peer-to-peer
BFT- Byzantine Fault Tolerance
PBFT – Practical Byzantine Fault Tolerance
SHA – Secure Hash Algorithm
SSI – Self-Sovereign Identity
ZKP – Zero-knowledge proof
MOOC - Massive Open Online Course
PoA – Proof-of-Authority
PoET – Proof-of-Elapsed-Time
PoS – Proof-of-Stake
PoW – Proof-of-Work
POS- Proof-of-Space
DoS – Denial of Service
KSI- Keyless Signature Infrastructure
DNS- Domain Name System
HTTP - Hypertext Transfer Protocol
RPCA - Robust Principal Component Analysis
UNL- Unique Node List
ABCI - Application Blockchain Interface
BSM- Blockchain State Machine
API - Application Programming Interface
SDN - Software-Defined Networking
PRISMA- Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RQ- Research Question
UML- Unified Modeling Language
CSS- Cascading Style Sheets
DLT- Distributed Ledger Technology
ETH- Ether
QR -Quick Response
HIPAA- Health Insurance Portability and Accountability Act
FL- Federated Learning
ML- Machine Learning
PoL- Proof-of-Learning
OCR- Optical Character Recognition

1. ВОВЕД

Дигитализацијата на услугите во јавните институции, вклучувајќи ги и образовните институции, освен што помага многу процеси да се генерираат по електронски пат, без потреба од долго чекање, исто така влијае и на намалување на непотребните административни трошоци, бидејќи најголемиот дел од работата ја завршува самиот систем, и нема потреба од вклучување на администрацијата. Некои високообразовни установи (ВОУ) имаат системи за управување со податоците, се обидуваат да ги дигитализираат услугите, да избегнат разни проблеми и можни злоупотреби, но многу процеси што се однесуваат на приватноста, безбедноста на податоците, трансферот и обработката во реално време, како што е генерирањето и проверката на академските документи, вклучувајќи ги и дипломите, како најважни документи во овие институции, сè уште не нашле решение да се дигитализираат, и да можат на електронски начин да се генерират за студентите што дипломирале во соодветни научни програми.

Во ерата на дигитална трансформација, образованието се менува, како и начинот на кој поединците учат и комуницираат со образовните институции. Исто така, со напредокот на општествениот живот, побарувачката за подобрување на човечкото знаење драстично се зголемува. Од дипломирани студенти до докторанти, сè повеќе и повеќе поединци во денешно време користат онлајн-алатки за да учат и да ги подобрат своите вештини. Како и да е, како резултат на недостиг на доверба во заедницата, вредноста на многу сертификати добиени на интернет се намалува со текот на времето [1, 2], затоа што може да има нивна злоупотреба на истите. Бројот на ученици до кои стигнаа МООК (Масивни отворени онлајн-курсеви) се зголеми од 300.000 на 220 милиони помеѓу 2011 и 2021 година. Растечката побарувачка за онлајн, дигитализирани курсеви носи предизвици, но исто така отвора огромни нови можности за образовните институции. Според една неодамнешна студија на Форбс [3], се проценува дека индустријата за сертификати генерира седум (7) милијарди долари годишно ширум светот во лажни документи и записници.

Следствено, со цел да се избегне дополнително негативно влијание врз општеството, овој проблем мора да се спречи. Бидејќи е предизвик да се направи разлика помеѓу автентични и лажни сертификати без специјализирана опрема и експертиза, што може да ги обезбеди само издавачот на сертификатот, сертификатите традиционално се проверуваат од органот што го издава. Во последниве години, Blockchain се појави како ветувачка технологија што автоматски ги снима и ги потврдува трансакциите [4]. Во едноставни термини, blockchain е криптографски безбеден протокол за создавање непроменлива структура на дигитални податоци што се користат за следење на трансакциите со средства помеѓу членовите на јавна или

приватна peer-to-peer (P2P) мрежа. Клучните карактеристики на blockchain вклучуваат транспарентност, доверба, брзина и елиминација на единствената точка на неуспех на централизираниот систем. И покрај вистинската употреба на blockchain во бизнисот и финансиите, неговите апликации во доменот на образованието добија влечење во последно време [5].

Blockchain-технологијата има потенцијал да го револуционизира образовниот систем со воведување попристапни и достапни опции за учење и менување на динамиката помеѓу образовните институции и студентите [6]. Процесот на управување со исплатата на студентската школарина е оној што бара значителна инвестиција во време и вклучува голем број страни, вклучувајќи студенти, родители, фондации за стипендии, приватни компании за заеми. Со помош на blockchain-технологијата, можеме да ја рационализираме оваа процедура, намалувајќи ја сумата потрошена за административни трошоци и на крајот намалувајќи ја цената на партиципација за студентите.

Blockchain е дистрибутиран, децентрализиран систем за чување податоци што овозможува безбедно и ефикасно запишување трансакции. Оваа технологија е најпозната по тоа што е основа за криптовалутите, како што е биткоин (Bitcoin), но исто така се користи и во многу други области. Основните карактеристики на blockchain-технологијата вклучуваат:

- **Децентрализација:** blockchain нема централен регистар или организација што го контролира. Тоа значи дека податоците и трансакциите се зачувани на мрежата од многу компјутери, наречени „членови“ или „јазли“.
- **Блокови:** Трансакциите се групираат во блокови што потоа се поврзани и заштитени со криптографски алгоритми. Секој блок содржи информации за трансакции и референца кон претходниот блок.
- **Јавен регистар:** Секој член на мрежата има пристап до целосниот историски запис на трансакции, познат како јавен регистар. Ова овозможува преглед на сите трансакции што се случиле во мрежата.
- **Криптографска безбедност:** Секој блок е заштитен со криптографски методи, како што е хаш функција, што го прави тешко за измена на податоците во блоковите.
- **Паметни договори:** blockchain може да имплементира и да извршува „паметни договори“, што се автоматизирани, програмабилни договори што се активираат кога се исполнуваат одредени услови.

Во меѓувреме, blockchain-технологијата е веќе имплементирана за отворени модели на учење, како што се часовите за плаќање, во зависност од тоа што користат паметни договори и прифаќаат криптовалути како плаќање [7, 8]. Blockchain има потенцијал да го револуционизира начинот на кој ВОУ управуваат со нивните курсеви со безбедно складирање дигитални наставни програми и предмети [9]. Во минатото,

институциите користеа хард-дискови за оваа намена, но овие уреди може да бидат оштетени или злоупотребени. Користењето паметни договори и blockchain, исто така, може да им олесни на професорите да ја следат работата на нивните студенти [10]. Тоа е затоа што паметните договори може автоматски да ја проверат секоја задача и да ја дадат следната задача на студентот додека не се заврши целата програма. Истата технологија за паметни договори може да ја користат и професорите за да ги евалуираат студентите, и да се зачуват оценките на безбеден начин.

Друг начин на кој blockchain-технологијата може да го подобри квалитетот на учењето на далечина е рационализирање на процесот на акредитација, што го прави поотворен за контрола и олеснување на полесниот пристап за оние со потребните дозволи. Оваа технологија може да се искористи за издавање непроменливи сертификати за дигитални дипломи и подобрување на тековните ограничувања на постојните системи за проверка на сертификати [11, 12]. И покрај ваквите достигнувања, сепак, користењето паметни договори за blockchain за да се спречи фалсификување сертификати за дипломи останува ограничено.

Користејќи blockchain-технологија, би можела да се создаде дигитална верзија на сертификатот што е имуна на фалсификување, манипулација и отфрлање. Дополнително, системот треба да стане потранспарентен, истовремено гарантирајќи ја приватноста и удобноста на сите страни вклучени во екосистемот. Blockchain-технологијата има различни употреби и можности за примена во различни области. Еве неколку примери на начини како се користи blockchain:

- **Криптовалути и дигитални плаќања:** blockchain е најпознат поради користењето во криптовалутите како биткоин и етериум. Ова овозможува безбедни и директни трансакции меѓу корисниците без потреба од посредници како банки.
- **Набавка и логистика:** blockchain може да се користи за следење на ланецот на набавка, што го олеснува следењето и проверката на производите. Ова може да помогне во намалување на измамите и унапредување на ефикасноста во логистиката.
- **Здравствено снабдување и управување со здравствени податоци:** blockchain може да се користи за безбедно чување и пренос на здравствени податоци, како и за следење на лекови и медицинска опрема во ланецот на снабдување.
- **Управување со идентитет:** blockchain технологијата може да помогне во развој на сигурни системи за управување со идентитет, каде корисниците имаат контрола врз своите лични податоци.
- **Управување со интелектуална сопственост:** Blockchain може да се користи за потврдување на автентичноста и сопственоста на интелектуалната сопственост, вклучувајќи авторски права и патенти.

- **Гласање и избори:** blockchain може да обезбеди сигурно и доверливо гласање, што може да помогне во спречување изборни измами и олеснување на процесот на гласање.
- **Финансиски услуги и паметни договори:** blockchain може да се користи за обработка на финансиски трансакции и извршување паметни договори, што се програмабилни договори што автоматски се активираат кога се исполнуваат одредени услови.
- **Енергетика и управување со ресурси:** Blockchain може да се користи за исто: следење и управување со енергетските ресурси.

Она што повеќе нè интересира, а е дел од докторското истражување, е имплементацијата на blockchain во образованието, особено во ВОУ, при што ќе се обидеме детално да ја опишеме имплементацијата, предизвиците и сите карактеристики што се поврзани со blockchain во ВОУ. Blockchain-технологијата има потенцијал да го промени и да го иновира образованието во различни аспекти. Еве неколку начини на кои blockchain може да се користи во образованието:

- **Проверка на дипломи и академски документи:** blockchain може да се искористи за обезбедување безбедна и пренослива проверка на дипломи и академски записи. Секоја трансакција (додавање нови податоци) во blockchain е неизбришлива и заштитена со криптографски алгоритми, што ги прави доверливи и лесни за проверка.
- **Децентрализирани онлајн курсеви и материјали:** Образовни материјали, курсеви и ресурси можат да се ажурираат и да се архивираат на blockchain, обезбедувајќи така еден јавен и достапен извор за образование. Истовремено, blockchain може да придонесе во контролата на авторството и целосноста на образовните содржини.
- **Управување со идентитет и безбедност:** blockchain може да помогне во развивање безбедни системи за управување со идентитет на студентите и образовните работници. Ова може да биде корисно во ситуации кога е потребно проверка на идентитетот за пристап до образовни ресурси или за извршување трансакции.
- **Поддршка за стипендии и финансиска транспарентност:** blockchain може да обезбеди транспарентност и прецизност во врска со стипендии и финансиска помош за студентите. Секоја трансакција, како што се стипендиите, може да биде евидентирани на blockchain, овозможувајќи преглед на сите финансиски трансакции.
- **Евалуација и оценување:** Blockchain може да обезбеди безбеден и целосен начин за евалуација и оценување на студентите. Резултатите од тестовите и оцените можат да се внесуваат во blockchain, обезбедувајќи историски запис што може да биде прегледан од страна на студентите и на професорите.

- **Поддршка за истражување и развој:** Blockchain може да биде корисен за пренос и заштита на истражувачки податоци и резултати. Информациите за истражувачките проекти и публикации може да се зачуваат на blockchain, обезбедувајќи јавен и лесен пристап до нив.

Употребата на blockchain во ВОУ има големо значење и нуди различни потенцијални примени. Неколку клучни аспекти што ја нагласуваат важноста и потенцијалната употреба на blockchain ВОУ се:

- **Проверка на документи и академска евиденција:** blockchain може да игра клучна улога во подобрувањето на проверката на академските акредитиви и во одржувањето безбедна академска евиденција. Ова е особено важно за борба против прашања поврзани со лажни дипломи и други документи. Академските записи, вклучувајќи дипломи, записници и сертификати, можат безбедно да се складираат на blockchain. Ова обезбедува извор отпорен на манипулации и лесно проверлив за работодавците, другите образовни институции и поединците да ги потврдат академските достигнувања.
- **Децентрализирано управување со идентитетот:** blockchain нуди децентрализиран пристап за управување со идентитетот, обезбедувајќи подобрена безбедност и давајќи им на поединците поголема контрола врз нивните лични информации. Студентите и професорите можат безбедно да управуваат со нивниот идентитет на blockchain, овозможувајќи им да го контролираат пристапот до нивните лични податоци за различни образовни и административни цели.
- **Безбедни и транспарентни трансакции:** Сигурната и транспарентна природа на blockchain може да ги подобри финансиските трансакции во ВОУ, намалувајќи го ризикот од измама и обезбедувајќи транспарентност во финансиските процеси. Плаќањата за школарина, исплатите на стипендиите и другите финансиски трансакции може да се спроведат безбедно на blockchain, обезбедувајќи транспарентен и ревизорски финансиски систем.
- **Непроменливи материјали за учење:** blockchain може да помогне во одржувањето на интегритетот на образовните содржини со тоа што ќе се осигури дека материјалите за учење остануваат непроменети и автентични со текот на времето. Чувањето на образовни содржини, како што се учебници, истражувачки трудови и други материјали, преку blockchain се обезбедува зачувување на автентичноста на содржината, намалувајќи го ризикот од плагијат и неовластени измени.
- **Паметни договори за административни процеси:** Паметните договори, кодот кој самоизвршува со однапред дефинирани правила, може да ги автоматизира административните процеси, да ја намали документацијата и да ја подобри ефикасноста. Административните задачи како што се запишување, регистрација

на курсеви и барања за дипломирање може да се автоматизираат со помош на паметни договори, рационализирање на процесите и намалување на потенцијалот за грешки.

- **Истражувачка соработка и интелектуална сопственост:** blockchain може да ја олесни сигурната соработка меѓу истражувачите и да обезбеди правилно припишување и заштита на интелектуалната сопственост. Истражувачките податоци, соработките и правата на интелектуална сопственост може да се снимаат на blockchain, обезбедувајќи транспарентна и безбедна платформа за истражувачите и институциите.
- **Децентрализирани платформи за учење:** blockchain може да поддржи децентрализирани платформи за учење, намалувајќи ја зависноста од централните власти и зголемувајќи ја пристапноста. Градењето децентрализирани системи за управување со учењето на blockchain може да обезбеди безбеден и транспарентен пристап до образовните ресурси и ингеренциите, особено во региони со ограничена инфраструктура.
- **Ефикасно меѓуинституционално споделување податоци:** blockchain може да олесни безбедно и ефикасно споделување податоци помеѓу различни ВОУ. Споделените blockchain-мрежи или меѓусебно поврзани blockchain-мрежи, овозможуват беспрекорна и сигурна размена на информации, поттикнувајќи ја соработката помеѓу институциите и подобрување на севкупниот образовен екосистем.

1.1. Мотивација за изработка на докторската дисертација

Факт е дека blockchain-технологијата го достигна врвот на технолошкиот развој, а во меѓувреме сѐуште не гледаме примена во областа на образованието. Почнувајќи од овој факт, бевме мотивирани да ги истражуваме причините зошто blockchain не се применува во ВОУ и во други области каде што е потребно управување со големи податоци, безбедност, заштита на приватноста и многу други карактеристики поврзани со оваа технологија. Квалитетот во образованието е најважното нешто што можеме да го создадеме за новите генерации. Знаењето што ги добицаат студентите во ВОУ, утре ќе треба да ги спроведат во пракса, особено кога станува збор за професите што имаат врска со човечкиот живот, како што се: медицина, воздухопловство, технички науки, природни науки и многу други. Имплементацијата на blockchain-технологијата во високообразовните системи би спречила секаква можна злоупотреба, но пред сѐ би придонела за развој на квалитетот и зголемување на свеста кај студентите и професорите да бидат повнимателни во образовниот процес, бидејќи сѐ ќе се следи преку blockchain-системот.

Затоа, не треба да има толеранција при оценувањето и добивањето на дипломите во ВОУ. Blockchain нуди безбедност, транспарентност на услугите, автоматско извршување на многу услуги и пред сè следење на секоја услуга што се одвива во blockchain-системот. Blockchain-системот инсталиран во ВОУ би овозможил автоматско оценување на студентите, без никаква интервенција од професори или администратори, би го следел присуството на студентите, би овозможил онлајн-плаќање и пред сè автоматско генерирање дипломи и нивна проверка во транспарентна форма во секое време.

1.2. Предмет на истражување и хипотеза

Предмет на истражувањето е дизајн на blockchain-систем што ќе може да се примени во ВОУ, за генерирање и проверка на дипломи, но и за управување со целиот образовен процес во овие институции. Иако има одреден број образовни blockchain платформи, што се создадени за проверка на дипломите, за нив нема детали за имплементација и нема резултати дека тие покажале успех подолго време. Постои празнина во литературата во оваа насока, каде што ако истражувачот се обиде да создаде blockchain-платформа дури и за помали цели за да се имплементира во ВОУ, нема детали за практична имплементација на кој било систем од иста природа.

Blockchain-технологијата може да се користи за различни цели во образованието. Може да се користи за следење на академските достигнувања, вклучително и онлајн-курсеви, сертификати за обука или специфични курсеви што може да се складираат во blockchain-систем. Blockchain-системите може да се користат и за водење евиденција на сите дипломирани студенти, така што кога институциите треба да најдат специјалисти во различни области, преку системот може многу лесно да го направат тоа. Blockchain може да се користи и за креирање системи за научни истражувачи, за класификација на научните истражувања според одредени теми. Примената на blockchain-технологијата во ВОУ е особено важна за услугите што се чувствителни и што може да се злоупотребат. Затоа blockchain може да се користи за да се спречи злоупотреба на различни сертификати, дипломи и да овозможи нивна брза и сигурна проверка.

Повеќето студентски датотеки сè уште се чуваат во физичка форма на хартија, така што секој студент на кој му е потребна регенерација на некој документ заради различни причини, тој треба да почека подолго време за проверка и мачна работа барајќи студентски датотеки. Сепак, многу истражувачи се согласуваат со фактот дека недостига примена на blockchain-системи во ВОУ. Главната причина е што образованието не е профитабилно како индустријата, поточно не е комерцијален производ што носи финансиски придобивки, додека повеќето програмери се занимаваат со примена на blockchain во сферите каде што има големи економски придобивки, а особено со криптовалутите. И покрај иницијативите за брза дигитализација на

системите што се користат во многу ВОУ, што би овозможиле полесно управување со образовниот процес, многу услуги сè уште не се дигитализирани, и потребно е многу време додека соодветните документи не се најдат во физичка форма. Меѓу овие услуги се генерирање дипломи, проверка на диплома, проверка на други документи поврзани со студентот, како индексот, оценки добиени по одредени предмети. Ова навистина претставува голем предизвик за вработените во ВОУ-и иако постојат истражувачки обиди да се предложат решенија за стопирање на какви било злоупотреби, овој процес е многу тежок.

Главната хипотеза на истражувањето е создавање стандардизиран blockchain-систем, каде што сите високообразовни установи, јавни и приватни, ќе го користат за генерирање дипломи, што ќе овозможи безбедно обработка на податоците. Ваквиот систем што ќе го предложиме со оваа докторска дисертација, е технолошка иновација во областа на образованието, бидејќи би овозможил дигитализација на услугите во ВОУ, но би придонело и за квалитетот, брзо генерирање и проверка на различни академски документи, и пред сè сигурно и ефикасно менаџирање со образовниот процес.

Како хипотези се поставуваат:

- Едукативни blockchain-платформи што се создадени до денес, не нудат оптимални и сигурни решенија за генерирање и проверка по електронски пат на дипломи и други академски документи;
- одржувањето на услугите на blockchain-системот е тежок процес, ако ВОУ не е самоодржлива, при што за такво нешто е потребна обука и специјализација на кадарот во институцијата;
- процесот на одземање дипломи и регенерација има предизвици, бидејќи такво нешто мора добро да се анализира, затоа што дипломата не може да се генерира двапати со исти податоци користејќи иста вредност на хашот, додека безбедноста на податоците во blockchain се засновува на уникатната хаш вредност;
- може да се создаде сеопфатен blockchain-систем за управување со сите услуги во ВОУ, не само со образовниот процес.

1.3. Цели и придобивки од истражувањето

Основната цел на докторската дисертација е да се даде придонес во областа на образованието, особено во ВОУ, каде што постои поголем ризик од можни злоупотреби, бидејќи дипломата е важен документ со кој луѓето се вработуваат на различни места во приватни и јавни институции. Создавањето стандардни модели за генерирање дипломи, што би се применувале во сите ВОУ, би донело многу предности и би спречило можни злоупотреби. Сепак, за таква работа е потребна посветеност на сите ВОУ и програмери да ја согледаат можноста како подобро и поефикасно да се создадат вакви системи применливи во сите институции.

Многу процеси во сегашните централизирани системи во ВОУ не обезбедуваат целосна безбедност за генерирање документи во електронска форма. Затоа blockchain-технологијата се гледа како надеж за надминување на овие ограничувања, гарантирајќи транспарентност, непроменливост, безбедност, приватност, заштита на идентитетот и нови можности за генерирање и потврдување документи. Системот базиран на blockchain-технологијата ќе овозможи студентите, професорите и администрацијата да бидат побезбедни и ќе понуди поголемо следење на дејствата во него. Со оваа докторска дисертација ќе се придонесе, меѓу другото, во развојот на идеи, модели, архитектури, концептуални модели, па сè до детално разјаснување на процесите на генерирање и проверка на дипломите. Дисертацијата ќе даде увид во практичната имплементација на самиот систем и ќе ги претстави сите овие активности во детална форма за истражувачите во иднина да имаат водич во врска со овие важни процеси. Системот blockchain што, меѓу другото, ќе понуди дигитализација на многу процеси во ВОУ, ќе нуди целосен кредибилитет на документите генерирани од таа образовна институција.

Меѓу другото, може да се наведат и следниве цели и задачи:

- Осигурување лесна интеграција на новиот систем во постоечките образовни институции, со цел да се олесни преодот и адаптацијата на технологијата.
- Гарантирање висок степен на сигурност и приватност на податоците поврзани со студентите и нивните дипломи, преку подобрување на механизмите за шифрирање и управување со приватните клучеви.
- Имплементација на прототип што овозможува брза и едноставна проверка на дипломите со помош на blockchain-технологијата.
- Истражување и анализа на различни аспекти на blockchain-технологијата, како што се концептите, алгоритмите и примената во слични области.
- Разработка на blockchain-модел за издавање дипломи: проектирање и развивање детален модел што ќе ги вклучува основните елементи за издавање на дипломи врз blockchain.

- Испитување и оценување на сигурносните и безбедносните аспекти на системот, со цел да се минимизира ризикот од недозволен пристап и злоупотреба на податоците.
- Изведување на тестирање и валидација на разработениот прототип во реални податоци, со цел да се процени неговата ефикасност и унапредување.
- Усогласување на системот со важечките законски и регулативни стандарди поврзани со издавањето дипломи и управувањето со образовни податоци.

1.4. Структура на докторската дисертација

Првично ќе се дефинираат проблемите и ќе се опишат целите со создавање на blockchain-систем во пракса. Потоа ќе се направи анализа на актуелната литература поврзана со истиот проблем. Потребна е детална анализа на претходните решенија и анализа на недостатоците во однос на нивното спроведување. Ке се идентификуваат функционалните и нефункционалните системски барања. Потоа ќе се дизајнира концептуалниот модел и архитектура на системското работење, како и избор на соодветни технологии и алатки за имплементација на системот. Откако системот ќе биде детално дизајниран, ќе се дефинираат сите можни случаи на употреба и сценарија на системот. Потоа ќе се реализира прототипот на системот, што ќе послужи како основа за експерименти и тестирања. Откако ќе се тестира системот, перформансите на системот ќе бидат потврдени за да се подобрат негативните елементи. Многу важно во оваа насока е документирањето на секое истражување, бидејќи недостига литература, а секој опис на појавите во научното истражување пред сè ќе послужи како основа за идните истражувачи. Меѓу другото, овие елементи на структурирање на докторската дисертација може да се резимираат:

- Систематска анализа на сите истражувања поврзани со имплементацијата на blockchain-технологијата во ВОУ, а особено за процесот на генерирање и проверка на дипломи.
- Осврт на важноста на blockchain-технологијата, платформата Етериум (Ethereum), паметните договори (smart contracts) и другите алатки за реализација на blockchain-системот за ВОУ.
- Анализа на постоечките истражувачки модели, рамки, архитектури и предлог за рамка и системска архитектура за blockchain-систем за ВОУ, односно за генерирање и проверка на дипломи и други документи.
- Детален опис на процесот на генерирање и проверка на дипломи преку blockchain-системот, вклучувајќи детален графички опис.
- Опис на системските барања, презентирање на дијаграми на кориснички случаи и сценарија на кориснички случаи за blockchain-системот, како и архитектура на паметни договори што ќе се користи во blockchain-мрежата.

- Креирање прототип за генерирање и проверка на дипломи и други документи во ВОУ, базирани на архитектурата, концептот што ќе го дефинираме при дизајнирање на системот.

1.5. Очекуван научен придонес и примена на резултатите од истражувањето

Самиот факт што немаме имплементација на blockchain во областа на образованието воопшто, а особено на ВОУ, ја прави оваа докторска теза кохерентна и покорисна како од аспект на науката, така и од аспект на збогатување на литературата за идните истражувачи.

Некои од придонесите што се дел од истражувањето се:

- Новопредложениот систем ќе гарантира дека дипломата запишана во blockchain нема да може да се промени. Оваа непроменливост може да спречи модификација на податоците и да ја зајакне доверливоста на системот.
- Системот заснован на blockchain ќе обезбеди брза и сигурна проверка на различни податоци поврзани со ВОУ и ќе обезбеди интегритет на податоците, осигурувајќи дека податоците не можат да се менуваат. Ова е клучно за одржување на кредибилитетот на академскиот документ.
- Ќе се разјасни како, преку системот заснован на blockchain, поединците можат да имаат поголема контрола врз нивните академски досиеја. Тие можат да изберат да споделуваат конкретни информации и да дадат согласност за нивна употреба, што ќе ја зајакне приватноста и безбедноста на податоците.
- Ќе придонесе во аспектот на стандардизација на академските документи, каде што стандардизацијата ќе овозможи полесно генерирање документи, подобрување на интероперабилноста меѓу образовните институции и работодавачите, обезбедувајќи документите издадени од една институција да бидат лесно разбирливи и прифатени од друга ВОУ.
- Ќе се разјасне дека децентрализацијата како карактеристика на системот заснован на blockchain може да ја распредели одговорноста за водење евиденција, намалувајќи го ризикот од неуспех и зголемување на еластичноста на системот.
- Преку паметните договори, системот ќе овозможи автоматизација на многу услуги, правејќи ги поефикасни и намалувајќи ги непотребните административни трошоци.
- Преку системот заснован на blockchain, електронските дипломи може да се генерираат за многу кратко време, да се проверат за многу кратко време.

2. ЗНАЧЕЊЕ, КАРАКТЕРИСТИКИ И КЛУЧНИ ЕЛЕМЕНТИ НА BLOCKCHAIN

Blockchain-технологијата користи добро познати механизми за компјутерска наука и криптографски примитиви (криптографски хаш-функции, дигитални потписи, криптографија со асиметричен клуч) измешани со концепти за водење евиденција.

2.1. Безбедност, доверба и приватноста во blockchain-технологијата

Како и во традиционалните мрежи што се централизирани, и blockchain како децентрализирана мрежа, го има процесот на автентикација за корисниците, за полесно да се идентификуваат со тоа што ќе се осигури дека корисниците што се најавени се дел од членовите на мрежата и не е некој друг што сака да ги злоупотреби податоците на вистинскиот корисник.

Одбивање на услуги (*Denial of Services -DoS)* е еден од нападите што се користи повеќе од мрежните напаѓачи. DoS го напаѓа системот со тоа што го претвораат како нефункционален по интегритет, кредибилитет и достапност на системот.

Дигитален потпис се методи што се обидуваат да создадат идентитет на корисникот и интегритет за податоците на корисникот, врз основа на користење на асиметричен клуч.

Еден друг метод за обезбедување безбедност е *инфраструктурата за потпис без клуч* (Keyless Signature Infrastructure- KSI), што складира хаш-табели на необработени податоци и датотеки на blockchain, потврдува други копии со извршување алгоритам за хаширање, а потоа ги споредува податоците складирани во blockchain, секое манипулирање со податоците брзо ќе бидат откриени, бидејќи оригиналните хаш-табели се зачувани на милиони јазли[13].

2.2. Blockchain-алгоритми и употреба

Тие што го карактеризираат blockchain како нова иновативна технологија се неговите алгоритми, што одредуваат како ќе функционира системот. Blockchain-технологијата ги користи алгоритмите за консензус, давајќи им на сите јазли истото право да гласаат блок што треба да се потврди, оваа мрежа се нарекува P2P (peer-to-peer). Во blockchain, како да се постигне консензус меѓу недоверливите јазли е трансформација на проблемот со византиските генерали [14].

Практична византиска толеранција на грешки претставува форма на машина што генерира копии, каде што секој јазол има копија што се занимава со малициозни копии на BFT [15].

Proof of work (Доказ за работа) е алгоритам што работи во децентрализирана мрежа, како што е blockchain биткоин. Секој јазол има право да создаде нова

трансакција, а другиот јазол ќе има одговорност да го потврди блокот ако е точен и нема злонамерни податоци за да се пробие книгата.

Proof of stake (*Доказ за удел*). За да можат учесниците да ги потврдат трансакциите и да напишат нов блок на blockchain, потребно е да издвојат дел од своите средства. Тоа е начинот на кој членовите се натпреварува за нивното право. Колку е поголем влогот, толку се поголеми шансите членот да има право со консензус.

Proof of authorization –PoA (Доказ за овластување). Овој вид на консензус се заснова на функционалност каде што само неколку членови на мрежата се избрани да го потврдат блокот или можат да бидат трета страна.

Proof of Elapsed Time –PoET (Доказ за изминато време). Се заснова на времето и парите што се вложени, па затоа е потребно време за да се врати враќањето на инвестицијата.

Proof of space – PoS (Доказ за простор). Овој доказ е заинтересиран за доделените услуги што ги обезбедуваат по јазли. Процесот на селекција на јазли за валидација на блоковите се заснова на просторот што бил резервиран од јазолот за верификација, така што користи повеќе складирање на компјутерот отколку компјутерската моќ.

Ripple-консензус алгоритам Робусна анализа на главната компонента – RPCA (*Robust principal component analysis*), се применува на секои неколку секунди од сите јазли, со цел да се одржи исправноста и согласноста на мрежата.

Tendermint–е софтвер за безбедно и доследно реплицирање на апликација на многу машини. Тоа го постигнува преку византиски консензус алгоритам за толеранција на грешки (БФТ- BFT). Често се користи во развојот на blockchain како основа за градење децентрализирани апликации и blockchain-мрежи.

IoT како поврзана мрежа на нешта е поле каде што blockchain може да направи големи подобрувања во безбедноста обезбедувајќи: *безбедна комуникација* – силен критериум за автентикација на ентитет за корисниците*; безбедно складирање* – складирањето на податоците е важно да биде безбедно, бидејќи сите податоци се складираат внатре; *интегритет на јазолот* –секој јазол треба да се ажурира и да има безбедно подигање.

2.3. Карактеристики на blockchain

Овој дел ги синтетизира клучните карактеристики на blockchain од литературата. Се дискутираат и придобивките и сите можни прашања поврзани со секоја карактеристика. Дополнително, идентификувани се тековните проблеми со технологијата blockchain и истакнати се клучните истражувачки предизвици.

Децентрализацијата е можеби најважната карактеристика на blockchain. Леџерот за blockchain постои на повеќе компјутери, што често се нарекуваат јазли. Системот blockchain користи дистрибуирана системска структура за снимање, складирање, ажурирање, пренос, верификација, одржување и неколку други процеси поврзани со информациите во мрежата на blockchain [16]. Трансакциите на blockchain леџер се целосно *транспарентни* каде секој може да ги види деталите и историјата на која било трансакција. Ова ниво на транспарентност е единствено за blockchain-технологијата и обезбедува високо ниво на одговорност и интегритет на информациите, осигурувајќи дека ништо не е претерано изменето, лажно додадено или отстрането. Сите трансакции обично се засноваат на доверба што гарантира дека вклучените страни можат да зависат една од друга во исполнувањето на нивните обврски. Користејќи ја приватноста и незаменливоста на асиметричната криптографија, системот blockchain ја заштитува содржината на пораките и го потврдува идентитетот на испраќачот, обезбедувајќи *сигурни трансакции* во системот blockchain [17]. Blockchain-системите се инхерентно *безбедни* бидејќи овие системи користат асиметрична криптографија што се состои од збир на јавни клучеви видливи за секого и збир на приватни клучеви видливи само за сопственикот. *Непроменливоста* значи дека штом податоците ќе се додадат на blockchain, тие не можат да бидат изменети или манипулирани. Блоковите на податоци во структурата на blockchain имаат временска ознака и секој блок е шифриран со хаш алгоритам, што го прави внесот на податоците траен и отпорен на манипулации, освен ако не е консензус на мнозинството од јазлите на целиот систем [16], [17].

Следливоста на податоците е да се следи изворот, дестинацијата и секвенцата на различни ажурирања низ кои минуваат податоците помеѓу јазлите. Потребна за интегритет на податоците и повисоки нивоа на доверба во информациите, следливоста на податоците има и неколку други придобивки од подобро управување со податоците, усогласеност со прописите, разбирање на влијанието на промените и подобрување на квалитетот на податоците меѓу другото [18]. *Анонимноста* како карактеристика на blockchain ја поддржува приватноста, што е дефинирана како заштитена од неовластен упад или набљудување. Анонимноста се постигнува со автентичност на трансакциите без откривање на какви било лични податоци на страните вклучени во трансакцијата.

Во blockchain-систем, одлуките се носат *демократски* од сите јазли користејќи P2P пристап [19]. Алгоритмите за консензус се користат од сите децентрализирани јазли за да се дозволат специфични јазли за додавање нови блокови на постоечки blockchain, како и да се осигура дека блокот е соодветно приложен во споделената книга и неговите копии низ јазлите на blockchain се правилно синхронизирани [17,19]. *Интегритетот* на

податоците е уверување дека податоците во blockchain остануваат точни и конзистентни во текот на целиот негов циклус [20]. Оваа карактеристика е постигната поради децентрализираните и практично непроменливите споделени книги низ мрежата blockchain, што значи дека откако ќе се договори блок на податоци да се додаде во blockchain, трансакцискиот запис на тој блок не може да се уредува или да се менува. Blockchain технологијата е со отворен код и корисниците можат да развиваат апликации преку заеднички интерфејс за *програмирање* на апликации.

Blockchain е неефикасен и излишен по дизајн за да обезбеди високи нивоа на непроменливост и *толеранција* на грешки, важни карактеристики на blockchain [21]. Паметните договори на blockchain можат *автоматски* да вршат генерирање трансакции, донесување одлуки и складирање податоци [19]. Сите јазли во системот можат автоматски да вршат трансакции и да ги потврдат податоците користејќи специфични протоколи за консензус [22].

2.4. Вовед во blockchain-системите за генерирање и проверка на дипломи

Распоредувањето на децентрализирани софтверски апликации за ВОУ има потенцијал да воспостави децентрализирана мрежа меѓу различните одделенија во ВОУ. Оваа мрежа би го олеснила управувањето, проверката и генерирањето податоци на начин штое автономен, транспарентен и безбеден. Ова е овозможено поради својствените својства што ги нудат современите системи базирани на blockchain [23]. Концептот за имплементација на blockchain-технологијата во ВОУ се дискутира веќе некое време, со првични предлози што потекнуваат од Европската комисија [24]. Целта наовие предлози еда се подобри квалитетот на образованието. Сепак, до денес, недостасува сеопфатен blockchain-систем што може ефективно да го мери напредокот на студентите и да ги потврди академските акредитиви, како што се дипломите.

И покрај протоколите и криптографските безбедносни механизми за заштита на приватноста, интегритетот и пристапот до податоците во реално време, сè уште има многу ограничувања и предизвици во однос на складирањето податоци и безбедната комуникација клиент – сервер. Целта е да се надминат овие проблеми со изградба на децентрализирани архитектури за системи базирани на blockchain што функционираат, особено за одржување на податоците безбедни и достапни [25]. Безбедноста и доверливоста на blockchain-технологијата се гледа во начинот на кој таа функционира преку јазлите. Секој јазол во blockchain-мрежата ги задржува податоците од претходниот јазол, заедно со целата историја на трансакции на мрежата на која ѝ припаѓа. Затоа, автентикацијата на сопственоста, историјата и извршувањето на трансакциите се врши автоматски и невозможно е да се сменат податоците во таква структура бидејќи секој јазол содржи копија од целата книга.

Процесот на дигитална трансформација и конверзија на централизирани апликативни системи во децентрализирани системи претставуваат значителни предизвици, особено во контекст на ВОУ. Ова се должи на сложената природа на приватните и чувствителни податоци вклучени во овие институции. Таквиот процес не е само адаптација на современи технологии, туку е и процес кога мора да се пренесат сите тековни податоци, да се модифицираат сите сегашни системи, да се приспособат сите бази на податоци до промената на архитектурите и создавањето на нови модели на работа и управување со системи во ВОУ. Инкорпорирањето на вештачката интелигенција во овие области ги претставува најновите достигнувања во имплементацијата на blockchain-системи, особено во контекст на ВОУ [26].

Сметаме дека примената на blockchain-технологијата за создавање дигитални системи за генерирање и проверка на документи е иднината што треба да се применува во ВОУ и други институции од иста природа[27].

Употребата на blockchain-технологијата има капацитет фундаментално да го трансформира образовниот систем преку обезбедување нови и економски ефикасни методи, истовремено поттикнувајќи промени во динамиката на соработката помеѓу професорите и студентите.

Во денешно време, централизираните системи што се користат во ВОУ се софистицирани и имаат механизми со висока безбедност, што нудат безбеден пренос на податоци и шифрирање во реално време.

Пред да започнеме со систематска анализа на целата литература и практични имплементации што имаат врска со blockchain-технологијата за генерирање и верификација на академски документи во ВОУ, ќе дадеме краток опис на можните имплементации и синергии помеѓу вештачката интелигенција и blockchain-технологијата во процесот на генерирање и верификација на дипломи.

3. ПОДОБРУВАЊЕ НА АКАДЕМСКИТЕ АКРЕДИТИВИ: СИНЕРГИЈА НА BLOCKCHAIN И ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА

Употребата на blockchain и ВИ во академските акредитивни системи обезбедува робусно и ефикасно решение за генерирање и автентикација на дипломи. Blockchain гарантира безбедно и непроменливо зачувување на академските податоци, додека ВИ подобрува неколку аспекти на процесот на акредитирање. Имплементацијата на ВИ и blockchain во системите за генерирање и проверка на дипломи овозможува дигитализација на многу услуги на ВОУ, но пред сè спречување злоупотреба, зачувување на идентитетот, приватноста, децентрализација на услугите и нивна автоматизација. ВИ може да користи софистицирани алгоритми за препознавање шаблони и откривање аномалии за прецизно откривање на измамнички дејства, па затоа гарантира интегритет на академските сертификати снимени на blockchain. Со користење паметни договори на blockchain, алгоритмите за ВИ може да го автоматизираат и оптимизираат процесот на проверка, а со тоа да го намалат административното оптоварување поврзано со потврдување на академските квалификации.

3.1. Интеграција на blockchain и вештачка интелигенција

Децентрализираниот начин на работа P2P и многуте методи на консензус што се користат во blockchain мрежата овозможуваат широко распространето усвојување на blockchain технологијата низ бројни домени, вклучително и образованието [28]. ВИ нуди потенцијал за интелигентни уреди за справување со многуте предизвици што се појавуваат во одредени ситуации. ВИ се справува со задачата за решавање на спонтано појавуваните проблеми преку рационална интеракција со поединци, предупредувајќи ги за различни форми на недолично однесување и обезбедувајќи помош и одговори на проблемите што ги доживуваат во нивните секојдневни животи. Дистрибуирана вештачка интелигенција е нова технологија што ја интегрира вештачката интелигенција со blockchain-инфраструктури. Неговата цел е да развие интелигентни уреди способни за автономно извршување дејства, истовремено обезбедувајќи безбедност, транспарентност и искористување на карактеристиките на blockchain-технологијата. Интеграцијата на blockchain и ВИ може да направи револуција во снимањето и автентичноста на академските достигнувања преку подобрување на безбедноста, пристапноста и процедурите за проверка [29].

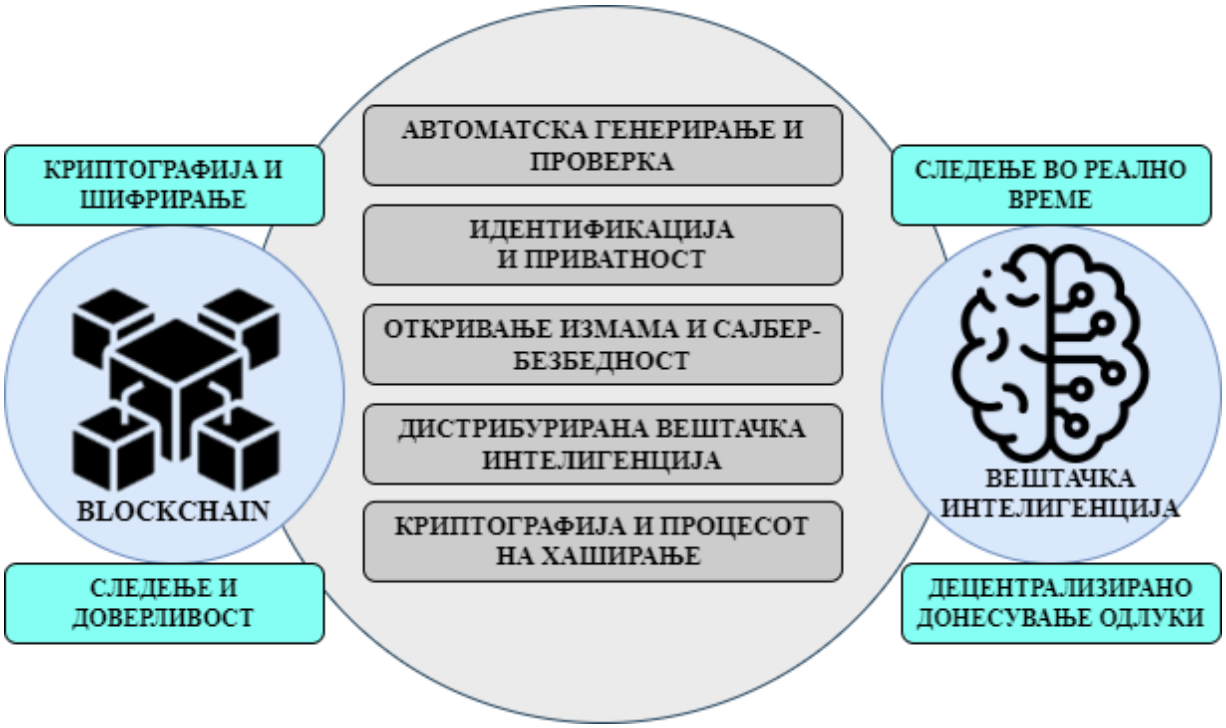
Употребата на ВИ во blockchain-системи за генерирање и проверка на академски документи може да олесни многу процеси, овозможувајќи автоматски да се генерираат дипломи, паметните договори да се извршуваат автоматски врз основа на предефинирани модели, проверката да се изврши без интервенција на трето лице, или компанија за проверка. Интеграцијата на ВИ во blockchain-системите може да придонесе пред сè за автоматско генерирање и проверка на академски документи, идентификација преку најефикасните интелигентни методи и зачувување на приватноста на податоците користејќи софистицирани методи. Многу техники за ВИ, вклучително и машинско учење, можат да влијаат на спречување злоупотреби и да обезбедат безбеден канал за правење трансакции. ВИ и blockchain може да ги комбинираат своите модели за да создадат хибридна архитектура во смисла на шифрирање и дешифрирање на податоците, особено консензус алгоритми и генерирање уникатни хаш-вредности. Преку машинското учење, blockchain-системите може да ги тестираат и да ги оценуваат студентите во различни области врз основа на моделите претходно дефинирани од самата ВОУ. Ваквите процени од паметните уреди имаат позитивен ефект врз студентите, бидејќи нудат логички прашања засновани на претходно знаење, што ги предизвикува студентите кон подлабоко знаење [30].

Алгоритмите за обработка на природни јазици (Natural Language Processing—NLP) имаат способност да ги анализираат и да ги разберат пишаните информации вклучени во дипломите. Оваа способност овозможува непречена интеграција со blockchain-системи и го олеснува ефикасното пребарување и пронаоѓање податоци [31]. Различни интелигентни уреди може да обработуваат природни јазици, да класифицираат текстови, да одговараат во интелигентна форма на повремени прашања, до повеќејазична обработка, анализа и обработка на човечките емоции. Паметните уреди успеваат да детектираат лице, човечки прсти, па дури и различни преводи и обработка на глас на различни јазици [32].

Слика 3.1 претставува една од главните карактеристики на синергијата помеѓу blockchain и ВИ во ВОУ, особено за генерирање и проверка на академски документи. Blockchain-технологијата се разликува од другите технологии во генерирањето на уникатни хаш вредности за секој процес, што се реализира преку механизми за консензус и криптографски алгоритми, што овозможуваат шифрирање и дешифрирање на податоците при нивното пренесување во blockchain-складирањето [31]. Сепак, за време на обработката на трансакциите, blockchain се карактеризира со децентрализација на услугите, безбедна и доверливост, програмабилност, следливост, заштита на приватноста на податоците и колективно одржување на сите јазли вклучени во blockchain-мрежата [32]. Од друга страна, ВИ во ВОУ се карактеризира со следење во реално време на сите процеси, особено откривање аномалии, обезбедува сигурност на системот и услугите што ги нуди, сè до приспособувањето на системот на евентуални промени. Несомнено, карактеристика на ВИ е и носење одлуки на колективна основа,

преку примање информации од сите инсталирани интелигентни агенти, со цел да се најдат оптимални решенија за различни проблеми со кои се соочува системот [33].

Синергијата на blockchain и ВИ влијае на многу процеси во ВОУ, вклучително и автоматско генерирање и проверка на академски документи, особено дипломи; заштита на приватноста и интелигентни методи за идентификација на корисникот во системот; откривање можни злоупотреби или предупредување за разни сајбер-напади; употреба на криптографски модели и механизми за консензус што содржат меѓусебно поврзување на blockchain и ВИ; приспособливост на системот, децентрализација и соработка на ВИ и blockchain при донесување системски одлуки за настани што се случуваат спонтано во системот.



Слика 3.1. Интеграција помеѓу blockchain и вештачката интелигенција

3.2. Поврзана литература

Интеграцијата на ВИ во blockchain-системите може да се случи за време на почетната развојна фаза, па дури и по развојот, со вклучување карактеристики на ВИ за подобрување на употребливоста за различни корисници. Ким и сор. [34], користеше ВИ во методот на консензус и предложи употреба на регионална конволутивна невронска мрежа за проверка на академските квалификации.

Користејќи ја техниката на повеќеслојна вештачка невронска мрежа, преку која се обиде да ги спореди вистинските дипломи и фалсификуваните дипломи, системот научи да ги дефинира и да ги спречи фалсификуваните дипломи и обидите за злоупотреба. Авторите посветија особено внимание на проверката на дипломите, користејќи невронска мрежа за проверка на интелигентен агент (Intelligent agent), како посредник помеѓу повеќеслојна вештачка невронска мрежа и складирањето облак, за да ги класифицираат податоците во структурирани и неструктурирани. Сепак, употребата на R-CNN и повеќеслојни ANN-техники има свои предности и недостатоци. Предностите се во однос на автоматизирање на проверката на дипломите, и интеграција на blockchain во складирањето на податоците што обезбедува непроменливост. Недостатоците се во однос на ресурсите за извршување на трансакциите, каде што, меѓу другото, се бараат повеќе ресурси што може да доведат до забавување на извршувањето на трансакциите, приспособливост и барања за складирање како резултат на употребата на посложени модели, прашања за приватност, интеграција и правни прашања што имаат врска со имплементацијата на интелигентни агенти.

Така, поволно е да се користат хибридни платформи во blockchain-системи за создавање и автентикација на дипломи. Тоа е затоа што сите компромитирани податоци се складираат во мрежата на blockchain, додека референтните податоци надвор од мрежата се користат за одржување рамнотежа помеѓу безбедноста, приспособливоста и брзината на обработка на трансакциите. Друго решение што користи конзорциум или хибридната платформа Хиперлеџер (Hyperledger) и аналитички модел е предложено со користење особено на вештачки невронски мрежи (ВНМ) од Шајк и сор [35]. Дистрибуираниот јазик за општа намена се користи за програмирање, СХА-256 (SHA-256) алгоритам за шифрирање податоци и интерпланетарен датотечен систем за складирање податоци. Blockchain влијае на ВИ според Жанг и сор. [36], во процесот на транспарентност и веродостојност на податоците, гарантира за рамнотежата на извршување на услугите, заштита на приватноста, дистрибуција на обработка на податоци во повеќе уреди и децентрализација. ВИ директно влијае на безбедноста на blockchain, без разлика дали се работи за паметен договор или спречување злоупотреба, но и во зголемување на ефикасноста на услугите што ги обезбедуваат blockchain-системите.

Симулацијата на употреба на квантно пресметување во различните процеси при реализација на трансакциите е, исто така, од големо значење за blockchain-системите, дури и во ВОУ. Квантното машинско учење (Quantum Machine Learning- QML) се обидува да вклучи квантни алгоритми во процесите на blockchain-системите, со цел да ја зголеми брзината и ефикасноста во обработката на податоците. Употребата на квантно пресметување не значи намалување на човечката улога во системот, туку значи користење на човечката интелигенција за користење интелигентни моќи во blockchain-системите за побрза обработка на податоците. Најголемите закани за blockchain-системите се од квантните компјутери, што имаат голема моќ за обработка на податоци,

затоа симулацијата на квантното пресметување може да се користи и за создавање криптографски алгоритми отпорни на квантно за различни процеси за проверка на податоци, вклучително и дипломи [37]. Сепак, досега сè уште нема докажано истражувачка студија каде што QML-технологијата се користи во контекст на автоматско генерирање и проверка на дипломи.

Друг обид за истражување во оваа насока беше направен со користење на DevOps. Преку методологијата DevOps беа предложени техники за автоматизација на процесите поврзани со тестирање, конфигурација, интеграција и извршување на процесите во системот [38]. Една од основните техники на оваа методологија е *Инфраструктура како код* (Infrastructure as Code -IaC), која има тенденција да го автоматизира тестирањето, конфигурацијата и распоредувањето на изворниот код на системот. Овој процес се постигнува со повторна употреба и повторливост на изворните кодови, со што се намалуваат трошоците и времето на сите инволвирани страни. Инаку, процесот на конфигурација и развој на системот до нивно одржување, односно надградби на различни верзии е познат како Dev(Sec)Ops, кој всушност вклучува комплициран процес со вклученост на многу експерти, програмери и истражувачи од различни области.

Вградени компјутери, различни сензори, интелигентни уреди, интелигентни роботи, интелигентни софтботови и логички системи што го помагаат образовниот процес и за студентите и за академскиот кадар, се некои имплементации на ВИ во образованието [33]. Една од имплементациите во денешно време од страна на студентите и академскиот кадар во различни области, е Чет џи-пи-ти (ChatGPT) и други слични системи како Гугл бард (Google Bard), Четсоник (Chatsonic), Џеспер Чет (Jasper Chat), Опенај Плејграунд (Openai Playground), Кактус Аи (Caktus Ai), Пепертајп (Peppertype), Нива Aj (Neeva Ai) [39]. Урал и сор. [40], јасно го објаснува фактот дека ВИ може да помогне во автоматизацијата на паметните договори, во процесот на проверка и автентикација, во процесот на реализација, безбедност и приватност на трансакциите, во механизмите за консензус како и многу други процеси. Сепак, сè уште останува предизвикот за примена на ВИ во процесот на криптографски функции, хаш-функции, транспарентност и отворен пристап до услуги, приспособливост и интероперабилност со различни паметни уреди.

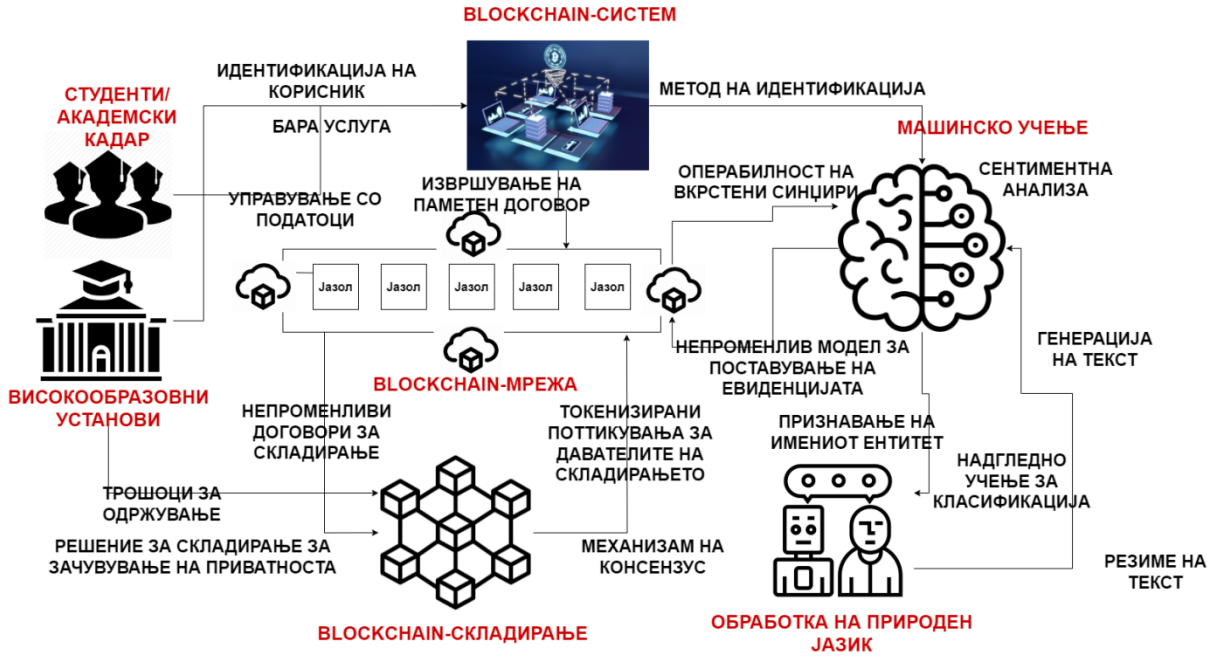
3.3. Придобивки од споредување на blockchain и ВИ

И покрај фактот што постојат голем број blockchain-решенија што се создадени со цел да се примени blockchain-технологијата за создавање blockchain-системи за генерирање и проверка на академски документи [41], сепак постои празнина во нивната практична реализација и долгорочна имплементација [42].

Една од интелигентните машини заснована на длабоко учење што покажала успех во препознавање и обработка на емоции, нивно претворање во текст и одговарање во интелигентна форма е Трансформер (Transformer), што има јасно дефинирана архитектура и донесе иновации во обработка на природен јазик (НЛП- NLP), моделирање, обработка и разбирање јазици [43]. Перцепцијата на природниот говор од страна на интелигентни машини станува уште потешка поради големиот број јазици што ги зборуваат различни народи, различните знаци што ги користат, различната синтакса, па дури и морфолошките текови на зборови и интерпункциски знаци [44]. Според Донг и сор. [45], процесот на обработка на природниот јазик од страна на интелигентни машини мора да помине низ неколку фази во текот на описот на архитектурата на НЛП (NLP), вклучувајќи: сегментација на зборови, морфолошка класификација, граматичка анализа, идентификација на ентитети, емоционална анализа и семантичка класификација.

Процесот на проверка вклучува извршување инверзни операции, почнувајќи со расклопување на податоците складирани во blockchain-складирањето во организирани елементи, со цел да се потврди интегритетот на податоците, дигиталните потписи, приватниот клуч и на крајот да се потврди автентичноста на податоците [46]. Анализата на чувствата може да придонесе за процесот на создавање и потврдување академски дипломи во систем заснован на blockchain-преку процена на погледот и довербата на јавноста во системот. Може да помогне во откривањето на какви било негативни ставови или стравувања за оригиналноста и доверливоста на дипломите засновани на технологијата на blockchain [47]. Од друга страна, прагматичната анализа се користи за тестирање на разликите на различни јазици, технички грешки или нецелосна документација на дипломите. Исто така, се проверува и дали се завршени сите субјекти, за во иднина да се проверуват дипломите, врз основа на стандардите дефинирани од самата ВОУ [48].

Моделите за машинско учење може да помогнат во производството на приспособени акредитиви со собирање релевантни информации од студентските записи, податоци за завршување на курсевите и мерки за изведба [49]. Алгоритмите за машинско учење може да ги анализираат податоците од blockchain за да ја потврдат автентичноста на акредитивот со процена на неговиот интегритет и конзистентност. Алгоритмите за машинско учење може да се користат за биометриски техники, како што е препознавање на лицето, за да се поврзе идентитетот на студентот со нивните ингеренции снимени на blockchain [50]. Машинско учење може да им помогне на институциите да ги разберат основните причини за валидноста или невалидноста на одредена сертификација во текот на процесот на проверка [51].



Слика 3.2. Интероперабилност помеѓу ВИ и системи базирани на blockchain

Во однос на децентрализацијата и приватноста на податоците многу значајна е употребата на методите за Федеративно учење (Federated learning –FL) и Доказ за учење (Proof of learning- PoL) [52]. FL се применува особено за одвојување на обработени и необработени податоци, што овозможува суровите податоци да не се складираат преку локални сервери, што влијае на приватноста на податоците [53]. На Слика 3.2. се обидовме да ја претставиме интероперабилноста помеѓу главните актери што се дел од комуникацијата на системот ВИ-blockchain, истовремено опишувајќи некои од најважните процеси во врската помеѓу актерите.

ВИ интегрирана со blockchain-системи може да го подобри процесот на идентификација со вклучување на препознавање говор заедно со отпечаток од прст и детекција на лице со помош на техники за Машинско учење (Machine learning- ML)[54]. Ова овозможува откривање на промените и можност за приспособување на околината за имплементација. Машинско учење обезбедува препораки врз основа на неговото постоечко знаење за избегнување и известување за проблеми во изворниот код [55].

3.4. Предизвици, импликации и препораки

Вистинската интеграција на ВИ и blockchain во ВОУ напредува со скромно темпо поради многуте пречки со кои се среќаваат овие технологии при ефективно справување со огромни и разновидни сетови на податоци. Шематски приказ на идентификуваните предизвици е претставен на Слика 3.3.

Од практичните имплементации на ВИ во ВОУ може да се истакне инкорпорирањето на различни chat-ботови и други интелигентни техники во образовниот процес, што е обележан со бројни предизвици. Најважниот предизвик е развојот на интелигентни роботи способни да го имитираат човечкото однесување, а со тоа да овозможат создавање вештачки човек [56].

Од друга страна, blockchain наидува на вистинска тешкотија на практична имплементација во дигитализацијата на дипломите и другите академски документи, поради непроменливоста на податоците при нивното складирање во блокови на blockchain-мрежата и складирање blockchain. И покрај постојаните напори на неколку академици и имплементацијата на неколку пилот-проекти за процена на изводливоста за изработка и потврдување на дипломите на ВОУ, постојат многу предизвици [57].

Слика 3.3. Предизвици за интегрирање на вештачката интелигенција и blockchain во академските акредитиви

Значајните предизвици во blockchain-програмирањето за ВОУ вклучуваат недостаток на истражување, сложен процес на пренесување дипломи од традиционални методи во blockchain-системи, гарантирање непроменливост на податоците во случај на грешки, отсуство на практични решенија, модели за повеќекратна употреба и архитектури и ограничената способност на blockchain-платформите за поддршка на дигитализацијата на дипломите [42].

Blockchain, меѓу другото, влијае на управувањето со компјутерската моќ, управувањето со податоците и оптимизацијата на моделите што ги користи ВИ [58]. Сепак, останува предизвик да се обезбеди усогласеност со постојните регулативи и стандарди што ја регулираат заштитата на податоците или академското водење евиденција и управувањето со финансиските импликации поврзани со распоредувањето и одржувањето на врвната компјутерска инфраструктура и blockchain-мрежите во академските институции. Решавањето на овие предизвици бара заеднички напори од академијата, индустриските чинители и регулаторните тела за да развијат иновативни решенија и да воспостават најдобри практики за искористување на ВИ и blockchain-технологијата во генерирањето академски дипломи.

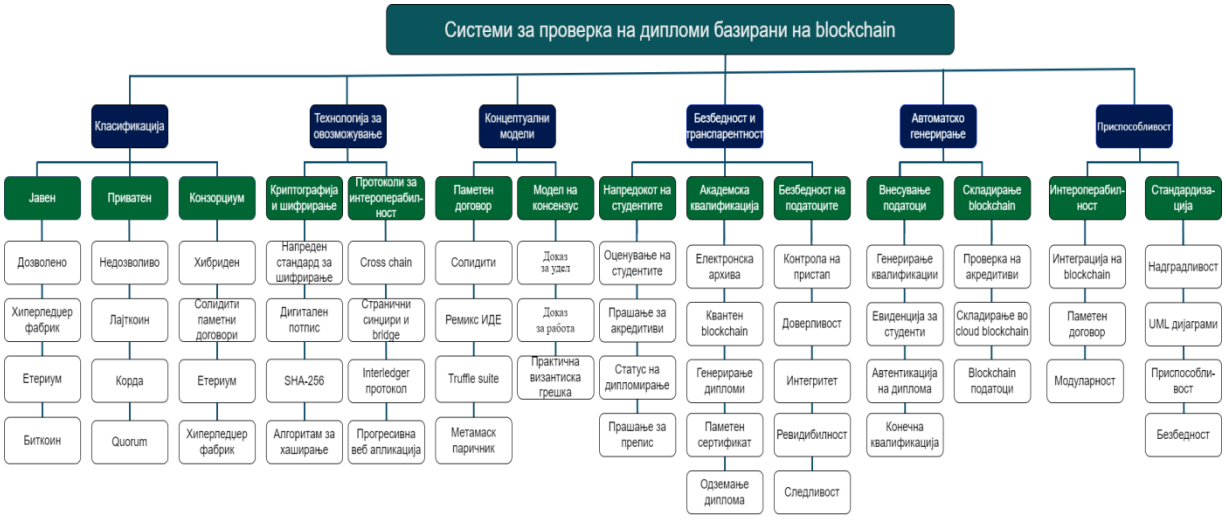
Може да се појават и правни и етички прашања во врска со валидацијата на академските документи, а недостатокот на вистински практични модели што овозможуваат безбедно, ефикасно и доверливо потврдување е прашање што треба да се реши. Потврдувањето на академските акредитиви понекогаш подразбира управување со чувствителни лични информации, како што се записници или сертификати за студенти. Неопходно е да се придржуваме до прописите за заштита на податоците, како што се ГДПР (GDPR) или ХИПАА (HIPAA), со цел да се зачува приватноста на луѓето. Кога се интегрирани во blockchain-системи, интелигентните машини може да имаат влијание врз точноста на податоците за време на креирањето или потврдувањето на дипломите. Тоа е затоа што овие машини може да се соочат со предизвици во разбирањето на податоците поради варијациите во дијалектите и процесот на означување на податоците во дипломите. Затоа е од суштинско значење да се разгледаат овие правни и етички размислувања со цел да се зачува кредибилитетот, доверливоста и интегритетот на академските институции и документите што тие ги потврдуваат.

Конвергенцијата на blockchain и ВИ ветува трансформација на образованието, справување со предизвиците, поттикнување на поддржувачка и побезбедна средина за учење и подобрување на управувањето со образованието. Оваа синергија не само што ја подобрува ефикасноста на генерирањето и верификацијата на дипломите, туку и се справува со предизвиците во екосистемот на blockchain и ВИ [59].

Како заклучок, надминувањето на предизвиците нагласени во оваа секција е императив за реализација на целосниот потенцијал за интегрирање на ВИ и blockchain во рационализирање на автоматизираното генерирање и процесите за автентикација на академските дипломи, а со тоа ќе се зајакне ефикасноста, безбедноста и кредибилитетот на академските системи за акредитирање во ВОУ.

4. СИСТЕМАТСКИ ПРЕГЛЕД НА ЛИТЕРАТУРА ЗА СИСТЕМИ БАЗИРАНИ НА BLOCKCHAIN ЗА ПРОВЕРКА НА АКАДЕМСКИ ДОКУМЕНТИ

Еден од придобивките на докторската тема е систематскиот преглед на литература на сите blockchain-решенија, што имаат врска со генерирање и проверка на дипломи во високообразовните установи. Тоа е една од првите систематски анализи од ваков вид што се занимаваат со иста тема. Литературата поврзана со нашата тема ја анализиравме користејќи ја рамката за систематски преглед на литература ПРИСМА (PRISMA) и метаанализа на претпочитани ставки за известување. Методот на ПРИСМА дава препораки за систематски прегледи што го одразуваат напредокот во идентификувањето, изборот, оценувањето и синтетизирањето на студиите [37]. Дополнително, оваа СПЛ претставува длабинска и обемна анализа на темата за дипломи базирани на blockchain, што е базирана на шест генерирани теми, како што е прикажано на Слика 4.1: тип на blockchain (класификација), автоматско генерирање дипломи, безбедност и транспарентност, приспособливост, концептуални модели и технологии за овозможување, теми што се генерирани по детална анализа на литературата.



Слика 4.1.Таксономија со главните теми и поттеми

4.1. Историјат и поврзана работа

Blockchain-технологијата беше воведена во важен економски момент кога светот се соочуваше со големи економски кризи, банкроти на некои светски познати банки, а луѓето беа во паника и почнаа да ја губат довербата во банките и се чувствуваа несигурни за спроведување различни трансакции. Не случајно, повеќе луѓе го знаат создавањето на blockchain-технологијата како биткоин, бидејќи овој период, или првата

фаза од развојот на blockchain-технологијата, беше фаза на криптовалути, особено на биткоинот како криптовалута, што ќе има поголем развој и поголем интерес од луѓето. До денес, биткоин отостанува една од криптовалутите со највисоки цени [60]. Поради специјалното управување со податоци во форма на синџир и безбедноста што ја нуди, blockchain е една од технологиите што неодамна означи револуција во многу сфери на животот, пришто наоѓа широк спектар на примена во: здравството, владата, индустријата, земјоделството, хотелите и авиокомпаниите [61]. Blockchain-технологијата нуди дистрибуирана архитектура во која повеќе компјутери можат да се поврзат во исто време и да пристапат до информациите што им се потребни. Така, имаме премин од централизиран начин на управување со податоци кон децентрализиран, транспарентен, но од друга страна, многу побезбеден начин на управување со податоците [62]. И покрај децентрализираниот начин на работа, она што ја прави blockchain-технологијата посебна е генерирањето на хаш-вредноста и складирањето на овие хаш-вредности во блоковите на blockchain-мрежата. Секој блок во blockchain-мрежата, меѓу другото, ја складира не само сопствената вредност на хашот, туку и вредноста на хашот на претходниот блок, така што секоја евентуална промена на податоците ќе ја промени вредноста на хашот на блокот и ќе биде откриена многу лесно [63]. Покрај дистрибуираната архитектура, непроменливоста поради хаш-вредностите и безбедноста што ја нуди, blockchain-технологијата се карактеризира и со транспарентност, демократија, конзистентност и интегритет. Во blockchain-мрежата, секој се чувствува слободно да се приклучи на дадена платформа и да започне да генерира трансакции [64]. Кога станува збор за придобивките од blockchain во образованието, употребата на blockchain-технологијата има потенцијал да ги подобри образовните резултати, да ги поедностави административните процедури и да ја зголеми одговорноста и транспарентноста. За разлика од другите сектори како индустријата или здравството, каде што blockchain наоѓа добра и сеопфатна примена, во ВОУ, адаптацијата на blockchain-технологијата за управување со податоци се смета за голем предизвик. Меѓутоа, во некои услуги засновани на ВОУ, blockchain покажува добри резултати, како, на пример, за време на начинот на плаќање и договорите за работа [65]. Транспарентноста е една од важните карактеристики на blockchain-технологијата. Кога услугите се транспарентни, има помали шанси да бидат злоупотребени, бидејќи можноста за нивна проверка е полесна [66].

Примената на blockchain-технологијата во ВОУ е, исто така, важна за процесот на е-учење. Оваа технологија им овозможува на образовните институции да имаат поголема соработка, овозможувајќи им на студентите да разменат знаења меѓу себе и да постигнат професионално знаење за областите што ги завршуват. Ова би се постигнало благодарение на успешната имплементација на blockchain во ВОУ, бидејќи успешната имплементација на паметните договори како важен дел од безбедноста на овој систем би го отворила патот за електронско учење бидејќи истиот систем би бил модифициран за генерирање електронски сертификати или дури и електронски дипломи за студенти

што завршуваат учење на далечина [67]. Употребата на blockchain-технологијата во ВОУ може да се категоризира, меѓу другото, во неколку точки:

- управување со различните сертификати што им се даваат на студентите, било за стекнатото знаење или за потребите на студентите;
- за оценување на способностите на студентите во различни области,
- обезбедува безбедна, транспарентна средина за развој на учењето,
- брзо, онлајн-плаќање на различни студентски услуги,
- акумулација на поени од општите евалуации во даден предмет и генерирање кредити и финална оценка,
- заштита од неовластен пристап и идентификација на пристап до одредени услуги (точно се знае кој и каква надлежност има во системот),
- развојот на електронското учење преку создавање различни виртуелни средини, онлајн генерирање сертификати за завршување на курсевите и можност за онлајн-плаќање преку валути утврдени од соодветните институции [68].

Секоја ВОУ деновиве има софтвер за управување со податоци, управување со часови, испити, дневни извештаи и оценување на студентите. Сепак, во моментов недостасува целосна дигитализација на услугите, бидејќи повеќе услуги во овие институции сè уште се обезбедуваат во физичка форма преку потпишани документи. Оттука, постојат можности за разни злоупотреби во овие институции, за кои е потребно време и труд до нивна проверка. Но, со целосна дигитализација на сите услуги, дури и со користење на современи софистицирани технологии, како што е blockchain-технологијата, ваквите услуги, освен што се побезбедни, полесно се потврдуваат дали сè уште има обиди за манипулација. Многу е важно во една земја, зошто не и пошироко низ континентот, да се генерират меѓународни дипломи што се признати во сите земји, дигитализирани и коишто многу брзо може да се проверат дали се оригинални. Секоја диплома што ја генерира ВОУ треба да биде дигитална, да биде специфицирана да работи на различни платформи, во различни системи, да овозможи ажурирање на системот без да влијае на складираните податоци. Системот треба да овозможи дипломите и другите академски документи да бидат дигитално потпишани од институцијата, што ќе важи неопределено време и дефинитивно ќе се најде механизам за дигитален потпис и од страна на примателот на дипломата, односно академските документи, што ќе биде нејзин единствен идентификатор [69]. Инаку, во [69] се дадени детали за управувањето со дипломите во Бразил, каде што Министерството за образование има поставена шема за сите институции како да управуваат со дипломите, што треба да биде присутна во сите држави за да се спречат разни злоупотреби. Употребата на blockchain во бизнисот е очигледна и од голема важност. Денес, многу големи компании што ги знаеме како: Алибаба, ИБМ, Мастеркард, Модекс (AliBaba, IBM, MasterCard, Modex) користат blockchain-технологија во своите бизниси, па дури и

помагаат да се користи оваа технологија во други сфери. Примената на blockchain во високообразовните институции има многу предности меѓу кои може да се издвојат:

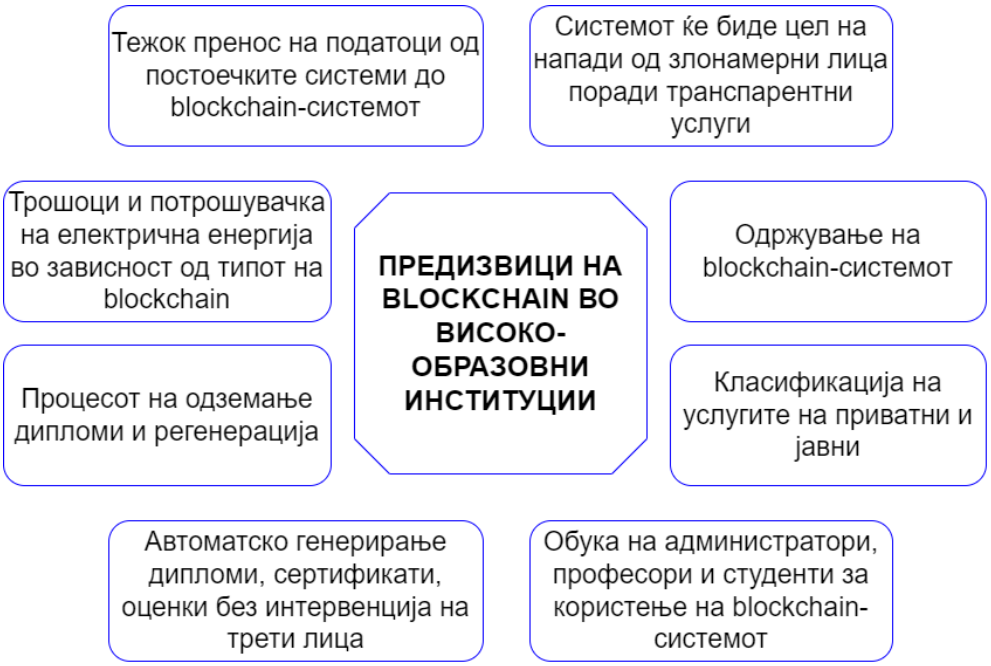
- брз пристап до автентичноста на дипломите, бидејќи луѓето имаат пристап кога сакаат до системот што треба да биде јавен;
- дипломите остануваат непроменети, бидејќи секоја промена во blockchain-технологијата предупредува за такво дејство;
- заштеда на време и непотребни трошоци за проверка на дипломите;
- во blockchain апликациите многу лесно се одвојува кои услуги се јавни, а кои приватни, што не би влијаело на приватноста на образовните институции [70].

Blockchain се користи и во апликации што се користат за комуникација или со други зборови за разговор, односно за размена на пораки помеѓу две или повеќе луѓе, како што се: Даст, Телеграм, Е-чет (Dust, Telegram, E-Chat). Но, има и апликации што сè уште не ја вклучиле blockchain-технологијата од свои причини, како што се тимовите на: Мајкрософт, Скајп за бизнис, Ватцап за бизнис (Microsoft, Skype for business, WhatsApp for business) [71]. Тоа значи дека blockchain може да се примени и во ВОУ за комуникација меѓу професорите, студентите и администрацијата. Значајно е кога се генерираат дипломи преку blockchain-системи е процесот на нивно одземање во случај тоа да е потребно. Овој процес сам по себе претставува предизвик.

4.2. Безбедност, транспарентност и предизвици на blockchain во ВОУ

Кога зборуваме за безбедноста на blockchain-технологијата, покрај дистрибуираната мрежа што ја користи оваа технологија, она што ја прави посебна е процесот на хаш-вредност што се генерира за секој процес што се извршува во blockchain-мрежата. Вредноста на хашот е единствена и за секоја промена се генерира друга хаш-вредност, па дури и ако некој се обиде да ги фалсификува податоците што се генерираат, без разлика дали се работи за дипломата на студентот, ќе се генерира друга хаш-вредност што не може да биде иста како оригиналниот. Хаш-вредностите се зачувуваат и во блоковите на blockchain-мрежата, а во секој блок, покрај вредноста на хашот на тековниот процес, се складира и вредноста на хашот на претходниот блок, што значи дека дури и ако вредноста на хашот се променува во блок, нема да биде иста хаш вредност на соседниот блок, што значи дека некој се обидел да ги фалсификува податоците [72]. Секогаш имало обиди за фалсификување документи, особено во овој аспект на дипломите како важни документи за вработување на луѓето. Процесот на нивната проверка е многу тежок, бидејќи повеќето од нив сè уште се генерират во физичка форма, барајќи ги досиејата на студентите, проверка на кредитите, професорите итн. Многу е полесно ако некоја ВОУ има дигитализирани услуги. Во дигитална форма, повеќе од овие процеси се изведуваат за кратко време. Сепак, во поголемиот дел од ВОУ, иако повеќето од нивните услуги се дигитализирани, особено

приватните институции, повторно недостига користење на blockchain во услугите што ги нудат. Транспарентноста е една од појавите што спречува можни злоупотреби. Услугите што се транспарентни, онлајн, достапни во секое време, многу лесно може да се потврди дали се точни или неточни. Blockchain е една од технологиите што нуди транспарентни услуги, иако зависи од типот на blockchain апликацијата, бидејќи приватните услуги што се категоризираат како приватен blockchain, не можат да бидат достапни за сите луѓе. Но, категоризацијата на услугите се врши во зависност од политиките на ВОУ, но и особено од прашањата за приватност на студентите. Услугите што се категоризираат како јавни, се достапни во секое време во blockchain-системот [73]. Интеграцијата на blockchain во постоечките системи преку ВОУ има многу предизвици, некои се поврзани со полето на примена од една страна, но од друга страна, исти се општите предизвици на blockchain-технологијата при примена во различни области. На Слика 4.2. презентираме некои предизвици што се поврзани со примената на blockchain во ВОУ. Меѓу многуте предизвици можеме да ги класифицираме генерирањето, проверката и одземањето на дипломите од blockchain-системот, обуката на академскиот кадар, професорите и студентите за користење на blockchain-системот, трошоците и енергијата што се користат, одржувањето на системот, класификација на услугите и вметнување на генерирани дипломи претходно, во blockchain-системот [74].



Слика 4.2. Предизвиците за имплементација на blockchain-системот во ВОУ

Во прегледот направен на [75], споменати се некои општи предизвици што се исто така поврзани со предизвиците на имплементацијата на blockchain во ВОУ. Меѓу многуте предизвици, важно е да се спомнат и трошоците на имплементацијата на blockchain, што е многу повисока во споредба со имплементацијата на централизиран

систем. Брзината на извршување на услугите во blockchain-системот зависи од оптоварувањето на услугата, а во некои случаи е дури и побавно од централизиран систем. Безбедноста е исто така предизвик на blockchain. Иако нуди поголема безбедност од сите други постоечки платформи, сепак, нападите на blockchain-платформите не престануват. Значи и тие се мета на злонамерни луѓе. Дистрибуцијата на податоците треба да биде со одобрение на соодветните институции. Затоа треба внимателно да се разграничи кои податоци ќе се третираат како јавни, а кои како приватни. Blockchain, исто така, влијае на многу меѓународни соработки и ги намалува трошоците за размена на студентите бидејќи постојат заеднички платформи каде што тие можат да разменуваат знаење. Како пример за blockchain-имплементација во ВОУ е и процесот на гејмификација (gamification), односно приспособувањена карактеристиките на игри како мисија, цел, стратешки точки во образовните процеси. Пример за рамка што го користела овој процес и го приспособила на реалните информациски системи е Октализис (Octalysis) [76]. Меѓу другите предизвици во однос на имплементацијата на blockchain е недостатокот на знаење за оваа технологија [74]. Академскиот кадар, студентите треба да бидат поподготвени за примената и употребата на оваа технологија. Да се одржат обуки и семинари во оваа насока, бидејќи иднината на општеството е поврзана со примената на оваа технологија. Многу важна карактеристика што ја овозможува примената на blockchain е зголемувањето на ефикасноста во образовните институции. Оваа е поврзана со дистрибуција на многу едукативни материјали, нудејќи им на студентите да имаат интероперабилност меѓу себе и многу полесен пристап до различни материјали. Во [77], се појаснува дека истражувањата за практична примена на blockchain во ВОУ се направени најмногу за управување со сертификати, процена на знаењето на студентите, трансфер на кредити, управување со податоци и регулирање дозволи за различен пристап во системот. Исто така,се појаснува дека најбројните проблеми со кои се соочува blockchain во ВОУ се речиси исти како претходните истражувања како што се: доверливост, трошоците, проверка на податоци, зачувување на идентитетот, непроменливост итн. Предизвици на blockchain се, исто така, погледот на универзитетот, што се создава во зависност од довербата што студентите ја создаваат кон услугите што ги нуди таа институција. Културата што мора да се создаде меѓу студентите и академскиот кадар во однос на транспарентноста на податоците од оваа технологија е исто така предизвик, бидејќи студентите и вработените не треба да се грижат за идентитетот на податоците бидејќи секој податок е хаширан [78]. Табела 1 ги прикажува предизвиците за користење blockchain во ВОУ каде, меѓу другото, предизвиците се поделени на технички, организациски и еколошки предизвици. Ова се најголем дел од предизвиците што спречуваат blockchain целосно да се применува во високообразовните институции во моментов.

Табела 1. Класификација на предизвиците за примена на blockchain во ВОУ

Технолошки предизвици	Организациски предизвици	Предизвиците на средината
безбедност и приватност на податоците	недостаток на експерти за обука на студенти за blockchain	реципиент -центричен екосистем
поништување на податоци, недостаток на знаење за blockchain	недостаток на поддршка за blockchain услуги во секое време	правни прашања и немање регулатива за општа работа со blockchain
непроменливост на податоците, ефикасност, квалитет на податоците	недостаток на обуки, семинари, работилници, конференции поврзани со blockchain во образованието	недостаток на обуки, семинари, работилници, конференции поврзани со blockchain во образованието
комплексноста на интегрирањето на податоците од тековните бази на податоци во базите на blockchain	трошоци и финансиски бариери за одржување	загриженост за долговечноста на оваа технологија
интероперабилност помеѓу студенти од различни универзитети		

Меѓу практичните предизвици на blockchain-системите за ВОУ се:

- Недостаток на знаење за обука на академскиот кадар, на литература за имплементација на blockchain-систем и недостаток на програмери што се занимаваат со практична имплементација на таков систем [79].
- Одржување и утврдување дозволи во системот, што значи поделба на обврските во системот, бидејќи за секоја услуга е добро да се знае овластеното лице.
- Тешкотии во текот на управувањето и генерирањето различни транскрипти, високи трошоци ако системот го одржуваат приватни компании [80].
- Начинот на генерирање дипломи во електронска форма, дигиталниот потпис што ќе го користат студентите, колку такво нешто ќе биде прифатливо за студентите, бидејќи како што знаеме дигиталниот потпис си има трошоци, а ако студентот го загуби дигиталниот потпис, дали има други методи со кои ќе може да го направи барањето за генерирање диплома [81].

- Елиминирањето на физичките документи поради користењето на blockchain-системот има свои предизвици. На пример, ако на студентот му треба повеќе пати генерирање диплома, процес што во моментов го правиме преку нотаризација, како истата диплома ќе се генерира преку системот. Дали ќе имаат ист или различен број на идентификација?[82]
- Хостирањето на содржината на blockchain-системот во централизирани средини е тежок процес, бидејќи самиот blockchain има децентрализирана природа [83].
- Немање поддршка за одредени услуги што ќе работат во насока надавање предлози ако студентите имаат проблеми, што е резултат на недостатокот на програмери што се занимаваат со овој проблем, но и таквите услуги имаат повисоки трошоци од сегашните услуги за поддршка [84].
- Многу е тешко, или невозможно, автоматски да се изврши паметниот договор во мрежата Етериум, бидејќи за секое извршување на трансакцијата, плаќањето мора да се врши преку одредени криптовалути [85].
- За имплементација на blockchain-систем, и покрај високите трошоци за создавање и одржување, потребна е многу повеќе работа за имплементација, бидејќи blockchain-системот има повеќе делови за меѓусебно поврзување, за разлика од windows или веб-апликациите[86].

4.3. Поврзани истражувања во врска со примена на blockchain во ВОУ

Примената на blockchain-системи во ВОУ, особено за генерирање, проверка, и одземање дипломи, е предизвик сам по себе. Во таа насока, различни истражувачи истражувале предизвици, тешкотии и различни рамки за тоа како да се постигне тој процес [77-79,87]. Сепак, сè уште нема конкретен резултат за тоа како да се дојде до целосно функционално решение со единствена цел да се спречат можни злоупотреби на академските документи. Исто така, недостига литература за систематски преглед и документирање на примената на blockchain-системи за ВОУ, специјално за генерирање, проверка и отповикување дипломи. Предизвикувачки фактор за blockchain-системот за генерирање и проверка на податоци е и ревизија на податоци и приватноста. Една од алтернативите во таа насока е создавањето рамка за управување со дистрибуирани податоци во мрежата за паметни податоци, која пред сè ќе овозможи детални контрола на пристап до податоци, управување со податоци при одржување следливост. Извршувањето на паметните договори дури и надвор од синџирот, со единствена цел побрзо извршување и зголемување на перформансите и на кредибилитетот на услугите, може да се постигне со создавање механизми, така што складирањето на податоците да се прави во blockchain-облак со помош на алгоритми за шифрирање, додека

пресметувањето на податоците ќе се изврши во доверливо средина, како што е Intel SGX [79].

Во Табела 2, прикажуваме резиме за карактеристиките на минатите истражувања. Важно е да се напомене дека ниту едно од овие истражувања не е систематско, што е главното прашање што го обработува истражувањето. Карактеристиките на blockchain-апликациите во доменот на образованието и споредбата со слични истражувања се вклучени во [78]. Сепак, авторите не го истражуваат прашањето за интеграција, проверка и одземање дипломи преку blockchain-системот, што ние го истражуваме. Покрај тоа, Кумутаво [78], проценува дека многу малку внимание се посветува на транспарентноста и безбедноста и нивните импликации за генерирање и проверка на дипломи. Газали во [77] ги разгледа безбедносните аспекти на blockchain и воведе blockchain-рамка за проверка на дипломи, меѓутоа, не се дадени детали и мотивации за тоа како системот може практично да се имплементира и кои алатки се потребни за имплементација. На крај, Ренато во [88], ги разгледа blockchain-решенијата применети во образовната средина. Постојат две главни ограничувања во тој преглед. Прво, не постои рамка за категоризирање на трудовите за тоа како blockchain-системот може да генерира и да потврди дипломи. Второ, обемот на работата е општ, а авторите не следат некој посебен протокол во процесот на рецензија. Друг неодамнешен преглед беше спроведен за да се испитаат пристапите за проверка на дигитални сертификати базирани на blockchain [80]. Беа разгледани разликите помеѓу различните апликации, механизмите за нивна имплементација и соодветните предизвици. Сепак, главното ограничување на оваа работа е методолошкиот пристап; имено, авторите не применуваат никаква типологија на прегледи на литература, ниту следат ригорозен протокол за преглед, како што е наведено од Кциао и Вотсон (Xiao и Watson) [81]. Овие разлики обезбедуваат образложение и основа за систематски преглед на blockchain-системите за проверка на диплома. Главната карактеристика што може да се види во овие други дела е тоа што недостасува правилно структурирање на прегледот.

Табела 2. Резиме на минати поврзани прегледи

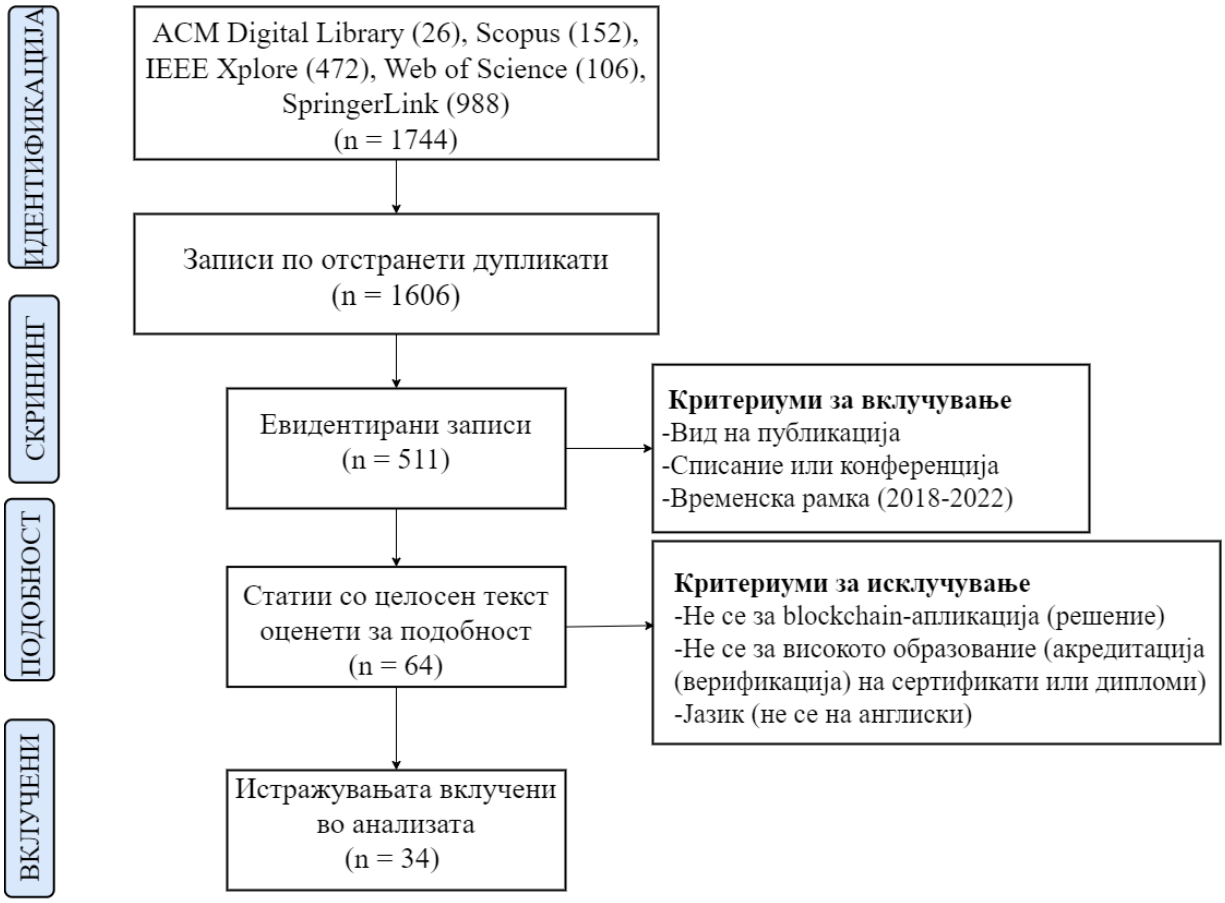
Трудови	Карактеристики
[87]	Карактеристики на некои blockchain-апликации за образованието, споредба со некои слични истражувања и краток опис на технички прашања.
[77]	Безбедносни прашања на blockchain, предлог-рамка за имплементација на Hyperledger Fabric во создавањето на blockchain-систем за проверка на дипломи.
[78]	Вовед во blockchain, прави споредба на некои образовни апликации и нивните предизвици во однос на примената на blockchain во образованието

[88]	За барањето за пребарување „диплома и blockchain“, трудовите се претставени како табела, каде за секој е даден придонесот на тој труд за оваа тема. Потоа се опишани некои blockchain-иницијативи во образованието.
[80]	Во оваа студија е претставен преглед на голем број системи за проверка на дигитални сертификати базирани на blockchain. Трудовите се споредуваат во однос на нивните цели, како и потенцијалните проблеми со процесот во иднина.
[82]	Опишани се карактеристиките на blockchain, видови на blockchain. Објаснета е анализа на сродни дела и некои образовни модели. Опишани се и предизвици за адаптација на blockchain во образованието.

4.4. Дизајн на истражувањето

Следени се процедурите наведени од Моер (Moher[83]) за да го завршиме овој СПЛ. Пронаоѓањето на најефикасните методи преку анализа на податоци е главната цел на СПЛ. Овој метод поставува фокусирани, тесни прашања и се придржува до строг збир на правила. Квалитетот на студиите е испитан и сите предрасуди предизвикани од рецензентот се бараат и систематски се отстрануваат. Дополнително, мора да се смисли протокол за истражување [84]. Нашата стратегија за пребарување користеше ПРИСМА пристап во четири чекори за да се осигуриме дека сите применливи студии се идентификувани и оценети. Слика 4.3. го прикажува целокупниот процес на пребарување. Првиот чекор на ПРИСМА е да се создаде протокол за истражување со решавање истражувачко прашање, дефинирање на збир на термини за пребарување и идентификување на библиографските бази на податоци за пребарување. Во втората фаза се применети критериумите за вклучување, а во третата се применети критериумите за исклучување. Процесот беше завршен со собирање и испитување на податоците. Истражувачките прашања (Research Questions- RQ) што ќе ја поттикнат оваа студија се:

- RQ 1: Кои се можностите на blockchain-технологијата за спречување на фалсификување академски документи и сертификати во ВОУ?
- RQ 2: Кои платформи, рамки и практични решенија од реалниот свет се развиени за да се надмине фалсификувањето на академските документи во ВОУ?
- RQ 3: Кои се моменталните случувања и потенцијалните предизвици на автоматското генерирање дипломи?



Слика 4.3. ПРИСМА-методологија за пребарување

4.4.1. Стратегија на пребарување и собирање податоци

Првата фаза вклучува развој на протокол за истражување, одредување на истражувачко прашање и клучни зборови и идентификување на библиографски бази на податоци, како што е наведено во [83]. За нашите цели за пребарување, ги користевме следните онлајн-бази на податоци и истражувачки мотори: АЦМ дигитална библиотека (ACM Digital Library -DL), ИЕЕЕ Експлор (IEEE Xplore), Спрингер (Springer), Скопус (Scopus) и Веб оф сајанс (Web of Science). Употребените термини за барање се прикажани во Табела 3. При креирањето на барањето за пребарување, секоја група клучни зборови се спојува со помош на операторот И (AND), додека самите групи се споени со помош на операторот ИЛИ (OR).

Табела 3. Низа за пребарување (прашања)

(„BLOCKCHAIN“)
И
(„АКАДЕМИЈА“ ИЛИ „ВИСОКООБРАЗОВНА УСТАНОВА“ ИЛИ „УНИВЕРЗИТЕТ“)
И
(„ВЕРИФИКАЦИЈА“ ИЛИ „АКРЕДИТАЦИЈА“)
И
(„ДИПЛОМА“ ИЛИ „СЕРТИФИКАТ“)
И
(„ИЗМАМА“)

Во процесот на стратегија за пребарување, втората фаза се нарекува фаза на проверка и вклучува примена на критериуми за вклучување. Во овој момент, трудовите што беа релевантни беа избрани врз основа на следните критериуми: (а) публикацијата мора да биде труд претставен на конференција или објавен во списание што применува рецензија; (б) трудовите мора да се објавени помеѓу 2018 и 2022 година; и (в) трудовите мора да бидат напишани на англиски јазик. Оваа одлука се заснова на наодите и заднината на претходните трудови. Трудови објавени пред 2018 година не беа соодветни за да одговорат на одредени истражувачките прашања. Затоа, избравме добро избалансирано времетраење на годината на објавување за овој СПЛ со цел да имаме веродостојни податоци со кои ќе одговориме на целите на овој преглед. Како што е прикажано во Табела 4., по примената на горенаведените критериуми, вкупно 511 трудови пронајдени во различни складишта беа прифатени како релевантни студии со цел понатамошно истражување и проверка, од вкупно 1606 трудови.

Табела 4. Трудови пронајдени во различни академски складишта

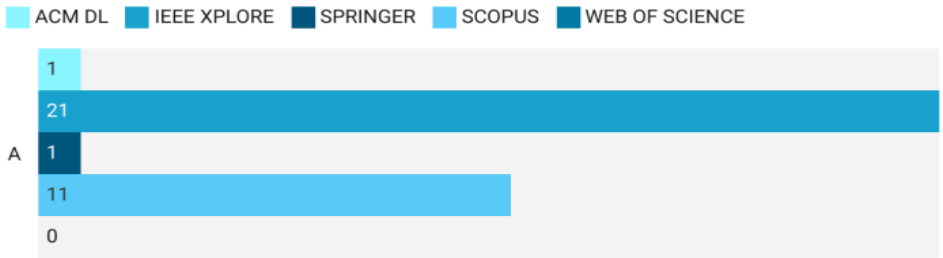
Година	**АЦМ ДЛ (ACM DL)**	**ИЕЕЕ Експлор (IEEE Xplore)**	**Скопус**	**Веб оф сајанс (Web of science)**	**Спрингер**	**Вкупно**
2018	3	33	4	2	5	47
2019	2	36	20	7	4	69
2020	8	32	26	17	12	95
2021	4	39	44	34	17	138
2022	9	30	56	39	28	162
Вкупно	26	170	150	99	66	511

Важно е да се напомене дека не вклучивме за анализа ниту еден труд на кој недостасуваше целосен текст или беа напишани на јазик различен од англискиот. Таквите трудови беа исклучени од разгледување.

4.4.2. Избор на релевантни студии

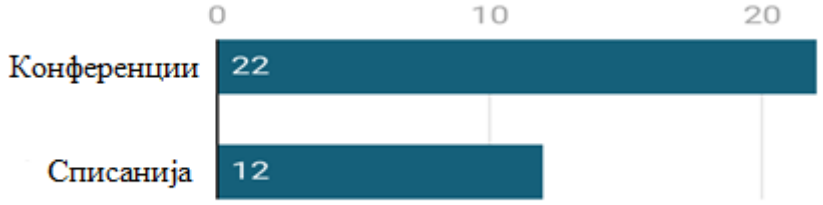
Во третата фаза од примената на критериумите за исклучување, беа елиминирани трудовите што не истражувале користење на blockchain-технологија во ВОУ или не беа за проверка на дипломи. Во овој момент, сите наслови, апстракти и клучни зборови беа анализирани со цел да се утврди кои трудови се квалификуваат за следната фаза. Утврдено е дека во анализата треба да продолжат да бидат вклучени вкупно 64 трудови. Дополнително, по внимателно читање и набљудување на сличните трудови, беше откриено дека на триесет од шеесет и четири труда им недостига целосен текст или се трудови со наративен преглед, без да се обезбедат богати информации за процесот на проверка на диплома базиран на blockchain. Поради ова, тие трудови беа дисквалификувани, со што вкупниот број на релевантни трудови беше заокружен на 34.

На Слика 4.4. го прикажуваме вкупниот број избрани трудови идентификувани во последната фаза. Од сликата, јасно се гледа дека најмногу научни трудови има од IEEE Xplore, со 21 труд, а потоа следи Scopus со 11 трудови.



Слика 4.4. Дистрибуција на истражувачки трудови во академски складишта

Слика 4.5. ја прикажува распределбата на меѓу 34 трудови; 22 беа конференциски трудови додека 12 припаѓаа на списанија.



Слика 4.5. Број на собрани трудови од конференции и списанија во 2018-2022 година

Детално резиме на релевантните трудови, нивниот опис и корелација со истражувачките прашања е дадено во Табела 5.

Табела 5. Резиме на идентификуваните трудови и нивната корелација со RQs

Истражувања	Цели	Поврзаност со RQ
[89], [11], [74]	платформи за генерирање, проверка и одземање дипломи	RQ1,RQ2,RQ3
[90]	проверка на академски документи	RQ2
[91]	следење на напредокот на студентите	RQ1
[92], [93]	автоматско управување со студентските датотеки	RQ2, RQ3
[94], [95]	пилот-проекти за генерирање и проверка на дипломи	RQ1, RQ2
[96]	преглед на проверка на дипломи, дизајн на систем	RQ1, RQ2
[97]	модел за упис на студенти	RQ1, RQ2, RQ3
[74], [98]	следење во реално време, генерирање и проверка на дипломи	RQ1, RQ2
[99]	модел за процесот на одржување испити и проверка на дипломи	RQ1, RQ2
[100], [101], [102]	модели за проверка базирани на платформата Етериум	RQ1, RQ2, RQ3
[103], [104]	модели за верификација на платформата Етериум	RQ1, RQ2
[105]	национална blockchain-платформа за проверка на дипломи	RQ1, RQ2
[106]	Merkle tree модел за проверка на дипломи	RQ1, RQ2
[107]	модел базиран на крипто-управување	RQ1, RQ2
[108]	дизајнирање на blockchain-систем преку УМЛ-дијаграми	RQ1, RQ2
[48]	приватен blockchain-систем за проверка на диплома	RQ1, RQ2
[109], [110]	blockchain-систем базиран на платформата Хиперлеџер фабрик	RQ1, RQ2
[111]	генерирање паметни сертификати	RQ1, RQ2
[112]	Церберус, систем за проверка дипломи преку паметни договори	RQ1, RQ2
[113]	blockchain-систем заснован на квантна криптографија	RQ1, RQ2
[114], [115], [116]	blockchain-систем базиран на ИПФС	RQ1, RQ2, RQ3
[117]	тестирање на блок-системот користејќи ја архитектурата РИСК-В (RISC-V)	RQ2, RQ3
[118]	проверка на дипломи врз основа на повеќе потписи	RQ1, RQ2

4.4.3. Ограничувањата за имплементирање blockchain во ВОУ

Секоја истражувачка работа вклучува голем број ограничувања. Треба да се земат предвид неколку фактори при оценувањето на овој СПЛ, бидејќи тие може да влијаат на валидноста на наодите. Овие фактори вклучуваат:

- За студијата беа избрани само трудови напишани на англиски јазик. Откривме поврзани трудови на други јазици додека ги пребарувавме базите на податоци за истражување; овие трудови не се вклучени.
- Вклучените релевантни трудови во студијата се написи извлечени од шесте бази на податоци за дигитални истражувања претставени на Слика 4.4. Затоа, можеби сме пропуштиле трудови што биле индексирани во други дигитални библиотеки.
- За оваа студија беа избрани само трудови од научни списанија и конференции. Не беа вклучени научни студии што не беа рецензирани. Ова вклучува кратки написи, извештаи за искуства и студии за асимилација, кои обично прикажуваат работа во тек или прелиминарни студии за кои се смета дека имаат мала важност за областа.
- Не вклучивме трудови објавени пред 2018 година, бидејќи нашето пребарување не даде доволно релевантни студии што беа во контекст на нашата студија и што можеа да ни дадат доволно информации за да одговориме на прашањата од истражувањето, да ги оцениме доказите критички и да извлечеме соодветни заклучоци. Во оваа студија беа избрани само дела објавени помеѓу 1 јануари 2018 и 25 ноември 2022 година. Можеби имало конференциски трудови презентирани пред 25 ноември 2022 година, што не биле објавени до крајниот датум на студијата, па затоа не биле вклучени во прегледот на литературата.

4.5. Тематска анализа

Пристапот за СПЛ мора да биде добро опишан за да може прегледите на литературата да бидат доверливи и независно да се репродуцираат [119]. Овој процес подразбира и квалитативна анализа и проценка на релевантните трудови. За спроведување на квалитативната анализа на трудовите, користена е тематска анализа за групирање и синтетизирање на аналитички теми. Тематската анализа е добро приспособена за методично анализирање на широк опсег на квалитативни информации со цел да се подобри точноста и чувствителноста во разбирањето и толкувањето на податоците. Во тематската анализа се користат повеќекратни повторувања на внимателно читање и кодирање за да се најдат и да се организираат доминантни, повторливи или неочекувани теми. Постојат шест фази на овој процес: запознавање со податоците, креирање почетни кодови, барање теми, прегледување теми, дефинирање теми и именување на темите, како што е опишано во [120]. Во нашиот конкретен

пример, сеопфатниот процес даде вкупно шест теми, од кои секоја е разгледана подлабоко во следните делови. 34-те трудови беа организирани во групи, а заедничките трудови беа пребарувани и категоризирани во теми. Табелата 6. ги прикажува идентификуваните теми и нивната поврзаност со релевантните трудови.

Табела 6. Теми и нивната поврзаност со релевантните трудови

Теми	Студии
Тип на blockchain (класификација)	[85-86],[95-96],[99-100],[102-104],[106], [108-11], [112-113], [116]
Автоматско генерирање дипломи	[11],[85-86],[92,94,96],[99-102],[104],[108],[114],[117]
Безбедност и транспарентност	[74],[85,86,90],[92],[94],[96],[99-104],[106-109],[111],[114-115],[117-118]
Приспособливост (Adaptability)	[93],[96],[99],[103],[114-115]
Потребни технологии	[85],[90-91],[93],[96-97],[100],[102],[48],[110],[114-116]
Концептуални модели и рамки	[11],[74],[85-86],[93-96],[98-99],[101],[103-113], [115-117]

По идентификување на листата на релевантни студии и теми, следниот чекор е да се објаснат и да се анализираат темите за да може да се одговори на прашањата од истражувањето.

4.5.1. Тип на blockchain (класификација)

Примената на blockchain во високообразовните системи има многу предизвици, а меѓу нив е и класифицирањето на услугите штосистемот ги нуди како јавни или приватни. Оваа класификација е добро да се земе предвид во раните фази на создавање модели и рамки бидејќи самиот blockchain е исто така поделен на приватен, јавен и конзорциум [95]. Разликата помеѓу овие типови blockchain е во транспарентноста на услугите што ги нудат. Во јавниот blockchain, сите услуги се јавни, транспарентни и без да се бара одобрение; сепак, извршувањето на барањето е побавно и троши повеќе енергија, за разлика од приватниот blockchain, каде што услугите се извршуваат побрзо [113]. Конзорциумскиот blockchain е инаку познат како хибриден начин на работа, каде што некои услуги се јавни, а некои се приватни, во зависност од природата на системот што се создава и политиките на соодветната институција [78].

Од прегледаните трудови, очигледно е дека blockchain-технологијата не може да се примени во сите области на образованието бидејќи образованието не е индустрија, а студентите не се криптовалути што можат да се извршат [121]. Оттука, постои недостиг на интерес кај истражувачите во оваа насока, бидејќи најголемиот дел од истражувањето е ориентиран само на криптовалутите и економските придобивки што ги носи оваа технологија [48]. Изборот на јавен пред приватен blockchain зависи од типот на услуги за кои ќе се имплементира blockchain-системот во одредена институција [64]. Меѓутоа, ако системот е посеопфатен и започнува од периодот на регистрација на студентите до завршување на студиите, односно од процесот на запишување до генерирање на дипломата, повеќе од потребно е да се користи конзорциумскиот blockchain, т.е. два вида blockchain, јавен и приватен [97]. Јавните служби на ВОУ може да ги класифицираат оние документи што универзитетот му ги издава на општеството (на пример, дипломи, уверенија и уверенија за положени испити), така што секој може во секое време да ја провери нивната валидност и точноста на податоците во тие документи [64]. Приватните услуги во blockchain системот може да се категоризираат како сите услуги во рамките на ВОУ, каде што професорите, студентите и администрацијата ќе имаат пристап до евиденција на трансакции поврзани со студентската датотека (овој систем би бил поотпорен на безбедносни прекршувања отколку традиционалните системи базирани на бази на податоци) [71]. При класифицирање на услугите како приватни или јавни, мора да се внимава да се заштити приватноста на податоците, а политиките на релевантната институција мора ригорозно да се почитуваат.

4.5.2. Автоматско генерирање дипломи

Автоматското генерирање дипломи и многу други документи во ВОУ би избегнало евентуална злоупотреба што може да се случи [100]. Сепак, колку е можен таков процес и како може да се постигне, останува еден од предизвиците. За да се постигне овој процес, blockchain мора прво да се инсталира во текот на првите фази од регистрацијата на студентите, а целиот процес треба да се спроведе онлајн и преку blockchain-системот, вклучувајќи плаќања, евалуација од професори, испити и заработени кредити [97]. Автоматско генерирање на диплома е можно само кога студентот ги завршил сите испити и уплати, и има поднесено онлајн барање за генерирање диплома. Во меѓувреме, системот ги испитува обврските на студентот, вклучувајќи ги плаќањата и испитите, без да бара од студентот да преземе какви било активности. Ова би спречило кој било друг корисник да пристапи до системот за време на генерирањето на академски документи, но дипломата би се генерирала автоматски и без интервенција за краток временски период, за разлика од традиционалните методи каде овој процес е подолг [100]. Таквиот процес што може да се генерира автоматски би

го олеснил процесот на проверка на дипломите, а безбедноста на податоците би се зголемила бидејќи тие би можеле да се генерираат без интервенција на трета страна.

Автоматското генерирање дипломи, нивна проверка и нивна регенерација (поради можни проблеми што може да се појават или технички грешки) е транспарентен процес, лесно достапен и пред сè процес што би следел каква било интервенција во системот [107]. Автоматското генерирање дипломи преку blockchain-системот го елиминира и процесот на нотаризација на документите, бидејќи во многу земји таков процес е сè уште активен, додека со автоматското генерирање дипломи, секоја документ ќе биде дигитално потпишан и може само да се генерира и да се издаде од соодветната институција [86].

Автоматското генерирање диплома или дури и сертификати е можно преку паметните договори, бидејќи паметниот договор се извршува само откако ќе се исполнат предусловите, односно само откако ќе се проверат податоците, тогаш дипломата може да се генерира или да се проверува [111]. Таквиот процес несомнено бара многу работа, претставува предизвик и, пред сè, обезбедува безбедно пренесување на сите прелиминарни дипломи во blockchain-системот, што мора да се спроведе правилно и без грешки.

4.5.3. Безбедност и транспарентност

Безбедноста на податоците има многу важна улога во секој систем што се занимава со управување со податоци, бидејќи секое дешифрирање на податоците може да доведе до големи катастрофи, прекршување на авторитетот и приватноста, па дури и злоупотреба на личните податоци. Така, при дизајнирање blockchain-систем за ВОУ, многу е важно улогите, правата за пристап и дозволите да се одвоени [116]. Администрацијата на дипломите во ВОУ е услуга што може лесно да се управува со blockchain, бидејќи дипломите може да се гледаат како трансакции со база на податоци, што може полесно да се управува во дистрибуираната мрежа на blockchain[122]. Она што ја прави blockchain-технологијата посебна и посигурна е хаш-кодирањето, што е многу важен процес бидејќи го идентификува секој процес [101]. Секоја промена во процесот го менува хаш-кодот. Карактеристика на хаш-кодот е тоа што инверзниот процес не може да се генерира; ако некој процес е придружен со одредена вредност на хашот преку генератор на хаш, не можеме да се вратиме на почетната точка, што го отежнува, на пример, процесот на одземање дипломи кога се прават технички грешки [99].

Друг феномен што ја прави blockchain-технологијата и нејзините услуги безбедни е начинот на кој тие функционираат во децентрализирана форма [48]. Ова значи дека нема контрола од одредени поединци, но целата безбедност зависи од самиот систем, алгоритмите што се користат, архитектурата на системот, рамката и безбедносните слоеви што се користат во системот [108].

Многу е важно да се нагласи вклучувањето на квантната криптографија и квантните компјутери во blockchain-системите. Од најновото истражување направено во оваа насока, се чини дека квантните компјутери имаат исклучително голема моќ за управување со blockchain-системи и, во исто време, за заштита од можни напади од злонамерни поединци [113]. Создавањето паметни договори и програмите што се користат за нивно извршување се од големо значење за безбедноста на blockchain-системите [115]. Безбедноста и транспарентноста се секогаш два процеса што се тесно поврзани еден со друг.

Секој процес штое транспарентен бара и поголема безбедност, бидејќи е цел на разни напади. Сепак, безбедноста и транспарентноста зависат од типот на blockchain. Blockchain-системот за ВОУ мора да обезбеди транспарентни, секогаш достапни услуги што на студентите им обезбедуваат различни услуги во секое време, без разлика дали се за генерирање дипломи, проверка или регенерација поради потенцијални технички грешки.

4.5.4. Приспособливост

Често, поради економски и временски причини, се претпочита да се користат претходно креирани софтверски платформи, што можат да се приспособат и повторно да се користат во други апликации од иста природа [122]. Повторната употреба на постоечките платформи или дури и архитектурите на платформата е можна доколку платформите се со отворен код или јавен blockchain [123]. Дури и некои воспоставени образовни платформи нудат можност за повторна употреба на нивните архитектури без промена на политиките за дистрибуција на трансакциите, прифаќајќи ги постојните политики на поврзаната платформа [113]. Во тој контекст, националната платформа што би била имплементирана од сите ВОУ, исто така, би можела да го подобри процесот. Во таков случај, би било уште полесно особено за проверка на дипломите, бидејќи е многу лесно да се провери дали дипломата што ја презентира соодветното лице ѝ припаѓа на таа институција или не, преку онлајн blockchain-системот што нуди услуги непречено [86]. Сепак, многу е важно да се посвети големо внимание на безбедноста и методот за автентикација при адаптацијата на образовните платформи [95].

Како што е наведено од Хсу (Hsu) [48], постои тенденција да се претпочита генерирање дипломи преку blockchain-системи. Меѓутоа, во случај на приспособување на постоечка архитектура, најважниот предизвик се врти околу автентикацијата на студентите. За поголема безбедност при генерирањето дипломи, неопходно е, покрај потребните дигитални потписи, да се користат и други механизми за безбедност што помагаат за попрецизна проверка. Меѓу нив е употребата на криптографски шеми за време на создавањето на архитектурата на blockchain-системот, како и употребата на механизми за идентификација како што се препознавање на лицето или идентификација на отпечатоци од прст [124].

Архитектурата што се користи при креирањето на blockchain-систем е основа за функционалноста на системот и, пред сè, неговата безбедност [113]. Сепак, од клучно значење е да се анализираат добрите и лошите страни на постоечките јавно достапни системи, и врз основа на тие параметри, можеби е препорачливо да се создаде нов blockchain-систем за ВОУ. На овој начин ќе се создаде посигурен систем, заедно со сите потребни механизми што ги обезбедуваат сите услуги на системот, како што се генерирање дипломи, нивна проверка, па дури и нивно поништување.

4.5.5. Потребни технологии

За да може blockchain-технологијата да функционира правилно, таа мора да има помошни алатки за работа, бази на податоци каде се чуваат податоците, поврзаните техники за извршување на транскриптите и оперативната мрежа, меѓу другото [115]. За време на создавањето на blockchain-систем, неопходно е да се има програмски јазик што е посветен на креирање паметни договори. Паметните договори всушност ги претставуваат услугите што корисниците ги создаваат во тој систем [85].

Постојат различни програмски јазици што овозможуваат такво нешто, но Солидити (Solidity) е најадекватниот програмски јазик за креирање паметни договори [125]. За тестирање паметни договори, бидејќи секое извршување во blockchain-мрежата има свој трошок, се користат комплементарни апликации за компилација и извршување што, исто така, може да се најдат на интернет [126]. Тие немаат реални трошоци, но всушност се извршуваат со пресметување на цената на трансакцијата во гасот етериум[127]. За создавање виртуелна blockchain-инфраструктура, апликациите, исто така, се користат во зависност од користената платформа, така што ако Етериум се користи како платформа, се претпочита виртуелната машина Етериум (Ethereum Virtual Machine- EVM) [100]. Причината зошто ЕВМ (EVM) се користи повеќе е тоа што им овозможува на програмерите и на истражувачите да ги извршуваат програмите на начинот на кој тие претпочитаат без да мора да вклучуваат однапред дефинирани методи и команди [93]. За креирањето и дизајнирањето на системот е повеќе од потребно да се користат интерфејси што се полесни за луѓето што не се приспособени на користење на компјутер. Поради оваа причина, се користат веб-ориентирани апликации, вклучувајќи ХТМЛ, ЦСС, и Јаваскрипт (HTML, CSS и JavaScript) [115]. Во зависност од природата на системот, различни бази на податоци или дистрибуирани системи за складирање датотеки, како што е ИПФС, се користат за складирање на податоци во blockchain.

Системите засновани на blockchain за ВОУ се системи што бараат безбедност на податоците, безбеден пренос, брз пристап до податоци и економичност. Врз основа на анализа на овие фактори, мора однапред да се развие архитектура за функционирање на blockchain-системот и сите помошни алатки потребни за оптимално работење.

4.5.6. Концептуални модели и рамки

Една од најпредизвикувачките задачи за време на создавањето на кој било систем, вклучувајќи го и blockchain-системот, е создавањето и дефинирањето на моделот и рамката, како суштинска компонента на blockchain-технологијата [104]. Рамката всушност ја игра улогата на конвертирање на паметниот договор во разбирлив јазик што треба да го изврши машината, соодветно, со други алатки што овозможуваат тестирање, контрола и проверка на паметниот договор [129]. Една од рамките што се користат во создавањето на blockchain-системи е рамката Трафл (Truffle), што всушност претставува можност да се олесни работата на програмерите и практичарите и нуди повеќе можности за создавање на blockchain-системот [88]. Друга рамка што се користи во blockchain-системот е рамката Лиск (Lisk), која не користи книги, туку свои приватни токени. За веб-апликации во blockchain-системи, потребна е рамката РеактЈс (ReactJs), која само бара употреба на Ноде.јс (Node.js) и всушност претставува Јаваскрипт (JavaScript) на страната на серверот [48].

За ВОУ да се префрлат од традиционалните системи за управување со податоци на blockchain-системот, прво треба да се воспостави blockchain-рамка [104]. Оваа рамка мора да се заснова на добро истражени и тестирани архитектури и механизми [117]. Една од рамките што се користи кога се работи со конзорциум blockchain-системите е рамката Хиперлеџер фабрик (Hyperledger Fabric) [77], што претставува рамка со претходно дефинирани услови, така што само учесниците што претходно добиле дозвола можат да се приклучат на blockchain-мрежата и да набљудуваат или да извршат одредени трансакции. Предноста на користењето на оваа рамка е нејзината транспарентна природа, слободниот пристап до мрежите, претходна автентикација на сите учесници во мрежата и одредено временско ограничување за секоја трансакција што ќе се изврши [124]. Концептуалниот модел и рамката се многу важни, затоа што ако системот е добро дизајниран со сите детали, вклучувајќи ја и архитектурата на функционирањето на системот, делот за имплементација е полесна работа и се врши многу побрзо [129].

За време на создавањето на blockchain-систем, може да се создаде нова рамка од самиот почеток, или постоечките рамки може да се модифицираат со користење на веќе создадени испробани и вистинити образовни платформи. И двата пристапа се предмет на пречки и ова е најтешката фаза од процесот на развој на blockchain-системот за ВОУ. Проверката, генерирањето и одземањето на дипломите се процеси што ја вклучуваат приватноста на студентот; затоа, од најголема важност е, при изградбата на рамката, да се направи разлика кои активности треба да се третираат како јавни, а кои како приватни.

4.6. Наоди од систематскиот преглед на литературата

Во следните параграфи, се елаборирани наодите од истражувачките прашања што беа клучни за овој СПЛ.

RQ1: **Кои се можностите на blockchain-технологијата за спречување на фалсификување дипломи и сертификати во ВОУ?**

Истражувањата покажуваат дека има злоупотреби во ВОУ и покрај напорите тие да се спречат. И денес имаме различни случаи на злоупотреба и фалсификување документи, особено дипломи, важен документ за лицата што бараат вработување во јавни и приватни институции. Blockchain-технологијата несомнено би помогнала во овој контекст; генерирањето и проверката на дипломите би се вршеле токму преку системот, а би се спречиле можностите за фалсификување документи. Мултинационалните компании, како што се ИБМ (IBM) и Алибаба (Alibaba), меѓу другите, даваат се од себе за да ја промовираат blockchain-технологијата во други земји во светот, додека азиските земји, како Јапонија и Јужна Кореја, се водечки земји кога станува збор за примената на оваа технологија. Исто така, вреди да се напомене дека меѓу европските земји, Естонија се обидува да ја дигитализира секоја услуга и да ја претвори земјата во дигитална држава каде секоја услуга се базира на blockchain [11].

Кога зборуваме за фалсификати во ВОУ, покрај фалсификувањето на дипломите како важен документ, имаме и случаи кога дипломите се генерирани од непостоечка институција. Во такви случаи, може да се направат фалсификати во рамките на дипломата со менување на податоците внатре, или фалсификати се прават за време на процесот на заверка кога студентот студира во странство, па дури и може да се направат фалсификати од трети лица или вработени во администрацијата со намерно менување на студентските досиеја. Blockchain-технологијата нуди можност за проверка на ингеренциите без потреба од посредник или трето лице бидејќи сите податоци од почетокот на студиите до дипломирањето ќе се складираат во blockchain и ќе се набљудуваат сите можни промени [86].

Предноста на користењето blockchain-технологија во ВОУ е транспарентноста и онлајн пристапот до јавните податоци. Легитимноста не е загрозена и нема потреба да се грижиме за интегритетот на податоците бидејќи blockchain се грижи за непроменливоста на податоците. Без оглед на сомнежите што ги имаме за записите за дипломи, тие можат лесно да се проверат во blockchain-системот [104]. Кога се користи blockchain-систем, пожелно е да се користат квантни и суперквантни компјутери бидејќи тие се поотпорни на сајбер-напади во дистрибуирана blockchain-мрежа [113]. Blockchain-системот за ВОУ не само што би ги спречил лажните дипломи туку и би ги спречил лажните институции и примателот на дипломата, што можеби е лажен човек. Ова може да се направи со употреба на механизми за биометриска идентификација и

Хиперлеџер фабрик (Hyperledger Fabric), преку кои се контролира пристапот до податоците [124].

За да се спречи каква било злоупотреба и да се има докази за тоа, се препорачува инсталирање на blockchain-систем во ВОУ, од процесот на упис до доделување на дипломата. На овој начин студентите континуирано ќе бидат следени за секое оценување, ќе има докази за присуство на часовите и навремена исплата и на тој начин лесно може да се провери секој сомнеж [94].

RQ2: **Кои платформи, рамки и практични решенија од реалниот свет се развиени за да се надмине фалсификувањето на дипломите и на сертификатите во ВОУ?**

Литературата покажува дека повеќе истражувачи и програмери се фокусирани на криптовалутите и придобивките што тие ги носат [100]. Така, тие не се особено заинтересирани да ги направат апликациите за blockchain оперативни и приспособени за ВОУ. Кога станува збор за создавање blockchain-апликација за ВОУ, вреди да се спомене дека е тешко да се приспособи апликацијата за сите модули на системот или да се создадат паметни договори што ќе одговорат на сите потребни услуги за таков систем.

Што се однесува до алатките потребни за креирање blockchain-систем, најпрво потребно е апликацијата преку која ќе комуницира со blockchain-мрежата, потоа базата на податоци или датотечен систем што ќе служи за складирање и дистрибуција на податоците во мрежата, веб-технологии што ќе се користат за дизајнирање и стандарди што овозможуваат креирање и дистрибуција на апликации од работната површина до облакот [115]. Речиси сите пилот-проекти што се создадени мора да ги користеле овие програми за да стигнат до практично решение, иако очигледно различни истражувачи можат да користат различни апликации што имаат за цел да ги постигнат истите задачи. На пример, во пилот-проектот изведен од Бадлани и сор. [116], платформата Етериум се користи за комуникација на blockchain-мрежата, Ганаш (Ganache) за тестирање на паметни договори, Солидити (Solidity) за програмирање на паметни договори, Трафл (Truffle) за домаќин на паметни договори на Ганаш (Ganache) и паричникот Метамаск (Metamask) се користи за спроведување трансакции. Се користи рамката Џанго РЕСТ (Django REST Framework) за бекенд (backend), а за фронтенд (frontend) се користат ХТМЛ, ЦСС и Јаваскрипт (HTML, CSS и JavaScript).

Кога станува збор за платформите што се користат за имплементација на blockchain-мрежата, најотворени платформи во однос на пристапот до мрежата, каде што секој може да прави трансакции, се етериум и биткоин, додека Хиперлеџер (Hyperledger) е платформа со ограничени дозволи, каде што можат да бидат само

претходно дефинираните копачи (miners), дел од мрежата за извршување трансакции [77].

Во литературата има предложени многу модели, рамки, дизајни, архитектури, па дури и практични решенија за генерирање и проверка на дипломи. Многу од нив беа само пилот-проекти што се имплементирани само преку модели, кои претставуваат само архитектури без никаква практична имплементација, но има и од оние што нашле примена и се практично тестирани. Оние платформи што се развиени и предложени од истражувачката заедница се претставени во Табела 7. Главната карактеристика на овие платформи е тоа што тие најчесто се имплементирани на платформата Етериум, а услугите се извршуваат во форма на паметни договори.

Табела 7. Резиме на Blockchain образовните платформи за проверка на дипломи

Труд	Наслов	Решение (стандардно)	Јавно/приватно Blockchain	Извршување услуги
[11]	CVSS	Систем	Етериум	Паметен договор
	OPENBADGES	Дигитална значка (badge)	Етериум	Паметен договор
[69]	G-CLOUD BRIEFCASE	Електронска архива	Етериум	Вештачка интелигенција
[79]	BCDIPLOMA	Платформа за акредитиви	Етериум	Паметен договор
[80]	EDUCTX	Кредитна платформа	Етериум	Доказ за удел (PoS)
	DISCIPLINA	Платформа (доказ за удел)	Етериум	Доказ за удел (PoS)
[87]	OPENCERTS	Платформа	Етериум	Паметен договор
	BLOCKCERTS	Стандард	Хиперлеџер фабрик	Доказ за работа (POW)
	BTCERTS	Отворен извор	Биткоин	Криптографска техника
	BLOCK.CO	Платформа	Биткоин	Доказ за работа (POW), Proof-of-reputation
[90]	CERBERUS	Платформа	Етериум	On-chain Паметен договор
[92]	BCERT	Систем	Етериум	Паметен договор
[94]	EDUCRYPTO	Едукација за криптовалути	Етериум	Паметен договор

RQ3: **Кои се моменталните случувања и потенцијалните предизвици на автоматското генерирање дипломи?**

Со имплементацијата на blockchain-системот во ВОУ, постои можност и за автоматско генерирање и проверка на многу услуги, вклучително и дипломи. До денес не постои постоечка јавна платформа за ВОУ што овозможува автоматско генерирање на дипломи без посредници, иако во оваа насока има предлози и мислења од различни истражувачи. Со примената на blockchain-системот во ВОУ може да се спречат злоупотреби во однос на генерирањето и проверката на дипломите. Сепак, секој автоматски процес подразбира отстранување на посредникот за да се постигне резултатот. Автоматското генерирање би овозможило да се надминат сите грижи за можни злоупотреби бидејќи најголемиот дел од работата би се работела без интервенција на администраторите на соодветната институција [94].

Многу важен процес за време на автоматското генерирање на дипломи и нивна проверка од blockchain-системот е несомнено процесот на регистрација на студентите во ВОУ. Бидејќи blockchain-системот се применува на почетокот на студиите на студентот, вклучително и апликацијата, регистрацијата во конкретниот курс, плаќањата на семестарот, доказите на студентите и евалуациите од професорите, и на овој начин автоматското генерирање на дипломата е многу полесно. Тоа е затоа што самиот систем ќе ги генерира податоците во зависност од влезните податоци дадени од студентот, администраторот или самиот професор во конкретниот случај [97]. Автоматското генерирање е предизвик и бара многу работа и посветеност при дизајнирањето на механизмите, бидејќи за секоја можна грешка во дадените податоци, дипломата мора да се одземе, а одземањето на дипломата е процес сам по себе полн со други поврзани предизвици.

За разлика од конвенционалните апликации што корисниците ги инсталираат, без разлика дали се на одреден оперативен систем или на веб, blockchain-системите за секое извршување паметни договори имаат одредени трошоци. Колку повеќе извршување ќе се изврши, толку повеќе ќе се зголеми цената на blockchain-мрежата на која се извршуваат овие услуги. Исто така, цената и платформата каде што се извршуваат услугите играат важна улога во времето на извршување на тие услуги [100].

Мирчеа и сор.[114] предложија модел што има способност автоматски да открива лажни институции користејќи вештачка интелигенција преку автоматско сортирање на податоци. Мустафа и сор [101], сметаат дека во blockchain-системите за генерирање и проверка на дипломи, некои процеси може да се вршат автоматски, почнувајќи од електронска проверка, автентикација, проверка на приватноста. На тој начин, улогата на трети страни станува непотребна во текот на овие процеси.

Автоматизацијата на процесите, колку што е важна за blockchain-системите, исто така е тешко да се примени и е поврзана со многу предизвици поврзани со

процесот на генерирање и проверка на дипломи. Самите паметни договори се извршуваат автоматски откако ќе се исполнат предусловите меѓу двете страни, но тоа е предизвик бидејќи тие се непроменливи, а предизвикот се потпира на создавање стандарден паметен договор за генерирање и проверка на дипломи, како и можноста за нивно ажурирање.

Одржувањето на системот, исто така, претставува предизвик за автоматизација на процесите во blockchain-системите за генерирање и проверка на дипломи. Факт е дека одржувањето на blockchain-системите е потежок од она на централизираните системи. Затоа се предвидува дека со употреба на вештачка интелигенција може да се постигне автоматско следење на системот и предупредувања за какви било сомнителни проблеми, како и способноста на системот да учи, развива и поправа недостатоци од претходните активности.

4.7. Дискусии и импликации

4.7.1. Идентификувани празнини

Технолошката иновација зад blockchain им овозможува на образовните институции да соработуваат поефективно, што пак им овозможува на студентите да го споделат своето знаење еден со друг и да го унапредат своето ниво на експертиза во предметите што ќе ги научат [73]. Развојот на нови системи или интегрирањето на blockchain-технологијата во веќе постоечките системи во образовните институции претставува една од многуте предизвици, од кои некои се специфични за полето на примена. Во нашиот СПЛ, откривме дека има потреба да се работи повеќе на системи засновани на blockchain за проверка на дипломи во многу насоки. Списокот претставен во Табела 8 ги сумира некои од најитните проблеми, каде што секој предизвик е мапиран на нашите истражувачки прашања.

Табела 8. Идентификувани празнини поврзани со прашањата за истражување

Идентификувани празнини	Research Question
Комплексен процес на пренос на дипломи	RQ1
Барање за одржување	RQ1
Несоодветни безбедносни механизми	RQ1
Потреба од помошни алатки	RQ2
Посредници	RQ3
Ограничени рамки/модели	RQ3

1. **Комплексен процес на пренос на дипломи.** Еден од предизвиците е процесот на пренесување на дипломите генерирани од ВОУ од основањето до имплементацијата на blockchain-системот. Овој процес е доста тежок и бара максимална посветеност од администрацијата на институцијата за податоците да се проверат точно, и да не се прават грешки при нивното вметнување во системот [86].
2. **Барање за одржување.** Повеќето од пристапите идентификувани во студиите истражени во овој СПЛ ја заобиколуваат потребата за одржување. Одржувањето на системот е од примарно значење, бидејќи институцијата нема опрема, соодветен персонал за одржување. Затоа мора да ангажира надворешна компанија за одржување, и во овој аспект, зависи од тоа колкава ќе биде цената на таквата услуга [73].
3. **Несоодветни безбедносни механизми.** Подобрената безбедност за време на генерирањето дипломи бара употреба на дополнителни безбедносни механизми, како што се дигитални потписи, што помагаат за попрецизна проверка. Тие вклучуваат инкорпорирање на биометриски идентификатори како лицето на корисникот или отпечатоци од прсти во дизајнот на архитектурата на blockchain [125] и употребата на криптографски шеми за време на фазата на дизајнирање.
4. **Потреба од помошни алатки.** За имплементација на blockchain-систем потребни се повеќе помошни алатки, т.е. повеќе алатки за поддршка кои овозможуваат практична имплементација на тој систем. Во централизирани системи програмски јазик, база на податоци и безбедносни механизми што се користат за пренос на податоци се доволни [115].
5. **Посредниците.** Процесот на автоматско генерирање дипломи е тешко да се постигне без посредници, но не и невозможен [86]. Бидејќи најголемиот дел од работата би се извршила без интервенција на администраторите на институцијата, автоматското генерирање би овозможило да се елиминираат сите грижи во врска со потенцијалните злоупотреби, дури и во blockchain-системот [94]. Сепак, овој предизвик сè уште не беше целосно адресиран или решен во рецензираните трудови.
6. **Ограничени рамки и модели.** Не најдовме литература, рамка или модел што точно покажува како целиот процес на генерирање, проверка и одземање дипломи во ВОУ може автоматски да се генерира на практичен начин. Процесот на автоматско отповикување е тежок или невозможен, а проверката е единствениот процес што може да се изврши без интервенција на трето лице [11,116].

4.7.2. Препораки и идни насоки за истражување

Во овој дел обрнуваме внимание на неколку истражувачки насоки што истражувачите во областа можат да ги следат додека го разгледуваат развојот на системи за проверка на дипломи базирани на blockchain.

Прво, од перспектива на *приспособливост и интероперабилност*, процесот на имплементација на blockchain-системи во ВОУ треба да оди во фази, каде прво треба да се имплементираат услугите кои се полесно приспособливи, до генерирање и проверка на дипломи. Многу е важно да се анализира и да се види можноста за пренос на податоци од постојните бази на податоци во blockchain-базите на податоци, соодветно, да се анализираат најчесто користените blockchain-облак платформи и да се истражи можноста за конверзија на податоци во безбедна форма. Меѓутоа, со цел да се постигнат највисоки перформанси и приспособливост во спроведувањето на трансакциите во blockchain-системот, треба да се направи комбинација на складирање надвор од синџирот и во синџир, како и меѓусебно поврзување на blockchain-мрежите вклучени во системот [130]. За да се олеснат трансакциите без користење интерфејси од трета страна, секоја мрежа има единствен пристап кон интероперабилноста на blockchain. Така, технологијата со вкрстени синџири има огромно ветување за овозможување на интероперабилност на blockchain, што може да реши различни проблеми и да елиминира многубројни ограничувања на blockchain и други мрежи. Тоа е исто така клучно бидејќи ја подобрува ефикасноста на синџирот, ја намалува сегментацијата и им олеснува на корисниците да комуницираат со различни blockchain.

Второ, од *перспектива на сигурност, приватност и верификација*, проверката на дипломите со blockchain-систем би ја олеснила долгата и напорна работа на администраторите во ВОУ. Пред сè, тоа би спречило можни злоупотреби, бидејќи би било можно многу лесно и за кратко време да се потврди дека дипломата ѝ припаѓа на назначената институција. Сепак, генерирањето и одземањето дипломи останува предизвик, бидејќи безбедноста на blockchain се заснова на единствена хаш-вредност. Секое одземање на дипломата значи промени во хаш вредноста, што го доведува во прашање идентитетот на студентот. Треба да се направат повеќе истражувања за blockchain базите на податоци и можностите за нивна имплементација во сегашните системи, со единствена цел да се осигури дека податоците првично се пренесуваат безбедно. Одржливо решение би ги разгледало прописите за приватност и заштита на податоците (како општата регулатива за заштита на податоците). Вреди да се повтори дека непроменливоста на податоците на blockchain може да го отежне придржувањето до одредени прописи, како што е „правото да се биде заборавен“. За решавање на овој предизвик, треба да се земат предвид социјалните и организациските фактори, да комуницираат со веќе постоечките технолошки решенија и да го решат проблемот со архивирање на претходно издадени сертификати и податоци.

Трето, од *перспектива на доверба и одржливост*, потребни се повеќе емпириски истражувања за да се обезбеди доверливост на оваа технологија. Луѓето стекнаа доверба

бидејќи секоја услуга е транспарентна, безбедна и непроменлива. Сепак, како би се измерил или потврдил кредибилитетот на организациите што издаваат академски документи овозможени со blockchain? По анализата на прегледаната литература, докажавме дека користењето на blockchain овозможува дополнителни опции и придобивки, како што се новите модели на онлајн-учење. Постојат групни дискусии, презентации и истражувачки задачи што се дел од овие часови и модели за онлајн-учење. На пример, Универзитетот во Никозија користи дистрибуирана леџер-технологија (DLT) за да ги потврди ингеренциите за MOOK. Со цел да понуди доверливи услуги за складирање и управување со податоци, Sony Global Education одлучи да имплементира blockchain-технологија. Кога станува збор за онлајн образованието, Технолошкиот институт во Масачусетс МИТ (MIT) исто така разви дигитална значка базирана на blockchain. ДЛТ (DLT) се користи за прв пат за следење на дипломите и другите академски записи во училиштето Холбертон. Овде, дистрибуираните книги користат студентски ИД за секој запис [122].

И покрај овие употреби, сè уште постои јаз во довербата и знаењето на пазарот во врска со потенцијалот на blockchain-технологијата во образованието, особено во контекст на проверка на дипломите. Дистрибуираните книги на blockchain даваат големо ветување за рационализирање и централизирање на управувањето во академската сфера. Сепак, целосно недостасуваат решенија, а неговата вистинска употреба е делумно ограничена на проверка на идентитети и дипломи, а во некои случаи, плаќање за школарина и давање добротворни донации.

Утврдено е дека техничките и филозофските ограничувања на blockchain се примарните причини за неговото бавно прифаќање во образовниот сектор. Во моментов не постои работен пример на глобален образовен blockchain што работи на истиот масовен размер како и криптовалутите (во милиони). Едноставно кажано, не постои убедлива причина да се спроведе неговото докажување на работа. Така, идните истражувачки напори може дополнително да ги истражат причините зад споменатите ограничувања за усвојување на blockchain.

Конкретно, усогласувањето на вистинската примена на blockchain во образованието со автентичната филозофија на одржлив развој на образованието заслужува дополнително истражувачко внимание. Високото образование е високо регулирана активност, што претставува уште еден, многу важен предизвик за вистинска имплементација на blockchain-системи. Секоја реална имплементација на овој систем мора да биде целосно усогласена со позитивната законска рамка во земјата/регионот, којашто може да вклучува закони, подзаконски акти, статути на ВОУ, внатрешни правилници, одлуки итн. Дополнително, системот треба да овозможи флексибилност за да биде способен да ги имплементираа честите промени што се случуваат во законската регулатива, што само по себе е посебен предизвик.

5. КОНЦЕПТУАЛЕН МОДЕЛ НА BLOCKCHAIN-СИСТЕМ ЗА АВТОМАТСКО ГЕНЕРИРАЊЕ АКАДЕМСКИ ДИПЛОМИ: СЛУЧАИ ЗА УПОТРЕБА И СЦЕНАРИЈА

Преглед на карактеристиките својствени на системите базирани на blockchain, вклучувајќи, но не ограничувајќи се на безбедност, заштита на идентитетот, транспарентност на услугите, класификација и ефективно и безбедно генерирање и верификација на академски документи е даден во [131].

Иако се воведени неколку образовни решенија засновани на blockchain во ВОУ, вклучително и оние за проверка на диплома [71], постои недостиг од емпириски истражувања за нивната употреба и ефикасност. Додека некои решенија и платформи беа подложени на ограничено тестирање, во моментов нема докази за поддршка на нивното широко усвојување или за оценување на нивните резултати.

Во овој дел на докторскиот труд имаме за цел да го решиме ова прашање со опишување на системските барања и презентирање на дијаграми на кориснички случаи на прототип-систем базиран на blockchain што имаме за цел да го развиеме. Исто така, главната цел на овој систем ќе биде автоматско генерирање и проверка на академските дипломи.

5.1. Значењето на паметните договори

Паметните договори играат важна улога во подобрувањето на безбедноста и ефикасноста на трансакциите преку олеснување на нивното извршување на структуриран и координиран начин [132]. Примарната предност на паметниот договор е во неговата способност да го изврши кодот на детерминистички начин, обезбедувајќи јасност и прецизност, по исполнување на одредени критериуми. Вклучувањето посредник во толкувањето или преговарањето на исходот е непотребно, со што се елиминира потребата од потпирање на доверливи посредници. Паметните договори претставуваат програмски делови што се извршуваат на blockchain-платформа што овозможуваат, меѓу другото, извршување, проверка и контрола на трансакциите што се генерираат преку програмските јазици. Нудат непроменливост, сигурност и транспарентност на услугите што се извршуваат, што многу зависи од рамката и платформата каде што ќе бидат распоредени, бидејќи паметните договори имаат одредени трошоци, што директно влијае на брзината на нивното извршување, перформанси и безбедност [133]. Извршувањето на паметниот договор се врши автоматски, откако ќе се исполнат предусловите поставени од двете страни што ја вршат трансакцијата. Секој паметен договор претставува дигитален објект во blockchain-системот. Следствено, постои скептицизам околу способноста на паметните договори да постигнат оптимални перформанси, со оглед на нивното ограничено прифаќање и компатибилност со други платформи. Паметните договори може да се

користат во ВОУ, особено во областа на дигиталните сертификати. Овие договори го олеснуваат складирањето, проверката и валидацијата на сертификатите, а со тоа ги рационализираат поврзаните процеси.

Употребата на паметните договори во процесот на генерирање и проверка на академски акредитиви е неизбежна. Би било поефикасно и побрзо доколку се создадат и стандардизирани паметни договори [134], обезбедувајќи генерирање на дипломи во стандардна форма, што исто така би ја олеснило нивната проверка. Сепак, процесот на адаптирање и стандардизирање на паметните договори поставува значителен предизвик, што најмногу произлегуваат од инхерентните ограничувања што ги поседуваат [133].

5.2. Тестирање и распоредување паметни договори

Процесот на распоредување и извршување на паметниот договор е многу важен процес што овозможува паметниот договор да се изврши во blockchain-мрежата, откако ќе ги исполни предусловите, соодветно, управува со ресурсите и нуди различни услуги за кои се посветени [135]. Една од главните карактеристики што го разликува паметниот договор е неговата непроменливост. Затоа, добро е, пред да биде распоредено, да се тестира, да се потврди за точноста и потоа да се изврши. Тоа е затоа што ако има грешки, тогаш единствената можност е да го избришете, да ги поправите грешките и потоа повторно да го распоредите, феномен што би одзело двојно повеќе време. За да се надминат грешките, повеќекратните повторувања, бришењето и прераспоредувањето на паметниот договор, се користи процесот на нивна проверка, овој процес се спроведува во транспарентна, отворена форма, а во исто време ја зајакнува безбедноста на паметниот договор, бидејќи нуди отворена инфраструктура на blockchain-мрежа. За проверка на паметниот договор, постојат формални јазици што го овозможуваат процесот на проверката, кои во текот на целото време се трудат да креираат техники и алатки со единствена цел паметниот договор да биде посигурен. Еден од методите за тестирање паметни договори е и тестирањето на мутации (mutation testing), кое има за цел да го промени изворниот код со секвенци на код создадени од развивачите на софтвер, со цел да се види реакцијата на програмата со некои мали промени во изворниот код. Ако по промените изворната програма се промени од излезот на тестот, тогаш се избира тој тест-случај [136]. Меѓу другото, во [136] се споменуваат и некои алатки или техники што се претставени од различни автори што се користат за тестирање на паметни договори: ОИЕНТЕ (OYENTE) што користи симболи за анализа на паметни договори, Зевс (Zeus), користи формални методи за анализа на паметни договори и тестирање, Вандал (Vandal) кој се користи за анализа на безбедноста на паметниот договор со цел да се пронајдат грешки во него, КонтактФузер (ContractFuzzer) исто така има врска со тестирање за безбедност на паметни договори. ГасСејвер (GasSaver) [137], алатка за оптимизирање на паметни договори што се

извршуваат во Солидити, покажа дека речиси половина од паметните договори што се поинтерактивни имаат барем еден или повеќе проблеми со оптимизација.

Нивната претходна оптимизација ќе помогне да се намалат трошоците за распоредување. Оптимизацијата на паметниот договор, според ГасСејвер (GasSaver) може да се постигне на неколку начини:

- декларација на непроменливи типови на варијабли, наместо константи за сите оние варијабли кои при извршувањето не ни требаат нивна вредност, туку откако ќе се изврши, соодветната вредност што е посветена на таа варијабла се зачувува како непроменлива варијабла;
- намалување на непотребните оператори во изразите што се користат во паметниот договор или за нивно поедноставување;
- комбинација на исти циклуси во паметниот договор, односно делови од кодот што се циклуси и имаат речиси иста природа на извршување, добро е да се вклучат во циклус, со што се оптимизира кодот, што ја подразбира логиката на самиот паметен договор, но и време и други трошоци;
- со подредување на податоците во паметниот договор според логиката на нивното работење и според потребата, затоа не треба да се пријавуват типови на податоци што не се неопходни, бидејќи ги зголемуваат трошоците;
- декларирањето константи за вредности што нема да бидат променливи за време на извршувањето е многу важно, бидејќи исто така го намалува времето и трошоците[138].

Смартбаг (SmartBug) е уште една рамка што овозможува тестирање паметни договори, кои главно се засноваат на *python3* и други алатки што лесно се интегрираат во паметниот договор и овозможуваат тој да се тестира и да се пронајдат пропусти или грешки во однос на секвенците на кодови. Меѓу другото, покрај тестирањето, Смартбаг (SmartBug) има за цел да покаже дека повторната употреба на различни алатки во паметниот договор е лесна и интеграбилна. Откако паметните договори се добро тестирани, пред да се извршат, добро е да се распоредат во апликации што овозможуваат такво нешто, дури и ако е бесплатен и со отворен код. Сите трансакции извршени во blockchain-мрежата Етериум се транспарентни, достапни за сите корисници и многу лесно истото може да се потврди во Етерскен, што всушност претставува блок-истражувач посветен на платформата Етериум. Меѓу другото, цената на етерот, пазарната капа, вкупниот број на трансакции се постојано дадени во Етерскен, а за секоја трансакција се дадени детали за имплементацијата, адресата, вредноста на хашот, времето и другите елементи прикажани на слика 5.1.

Block Height:	17075861
Status:	Finalized
Timestamp:	17 mins ago (Apr-18-2023 08:15:47 PM +UTC)
Proposed On:	Block proposed on slot 6252077, epoch 195377
Transactions:	166 transactions and 99 contract internal transactions in this block
Withdrawals:	16 withdrawals in this block
Fee Recipient:	beaverbuild in 12 secs
Block Reward:	1.422408012923460434 ETH (0 + 3.086454278828721464 - 1.66404626590526103)
Total Difficulty:	58,750,003,716,598,352,816,469
Size:	81,820 bytes
Gas Used:	15,935,790(53.12%) +6% Gas Target
Gas Limit:	30,000,000
Base Fee Per Gas:	0.000000104421949957 ETH (104.421949957 Gwei)
Burnt Fees:	1.66404626590526103 ETH
Extra Data:	beaverbuild.org (Hex:0x626561766572627569 6c642e6f7267)
Hash:	0xa4f123818de9ec8d01e75779276ed3faaf08eb5c9584e49b24d07303fb154e2d
Parent Hash:	0xee0af62bbac5f094f7da35258f57cf433f50ba3e9780feb5c8c0739b37a5a880
StateRoot:	0x00e1df93a7b2101b0324f9f66e67158e10d4a0296b0dc1dbceadd1c97e8741d1
WithdrawalsRoot:	0x066723f716155d2e4ddb099a5989e6995ce7895c3871c8864af7726f2fca7940
Nonce:	0x0000000000000000

Слика 5.1. Етерскен — пример за успешна трансакција

Она што го прави blockchain корисна технологија е, меѓу другото, транспарентноста за секоја трансакција што се извршува. Податоците што треба да бидат јавни се јавни за сите корисници, додека очигледно паметните договори што се извршуваат се заштитени од blockchain-мрежата и не се достапни за никого.

5.3. Предизвиците за усвојување blockchain во ВОУ

Употребата на blockchain-технологија во системите на ВОУ има неколку придобивки во однос на дистрибуирана мрежа, транспарентен пристап до информации и активности со одредени дозволи [133]. Од безбедносни причини, вредноста на хашот се чува во blockchain, додека другите документи со податоци во ИПФС (IPFS) [139]. Имплементацијата на blockchain-систем за генерирање дипломи, проверка и нивно одземање претставува предизвик во однос на неговата практична примена. Еден таков предизвик е значителната потрошувачка на електрична енергија, што произлегува од

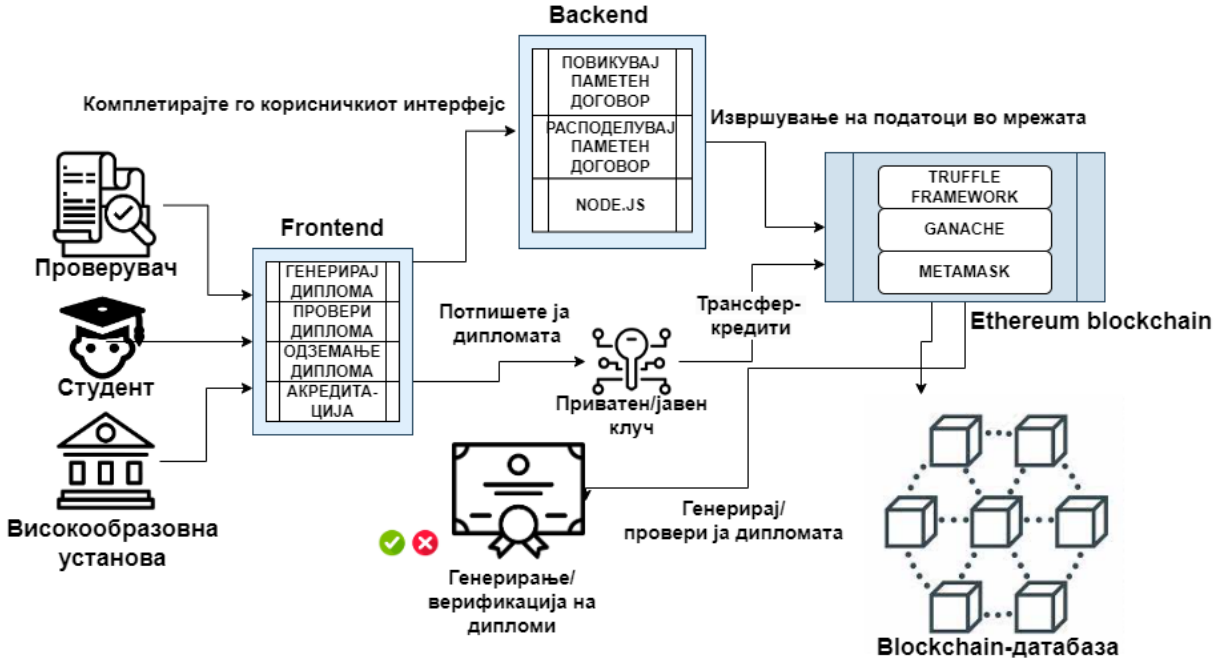
користењето моќна хардверска опрема. Дополнително, се појавуваат грижи во врска со приватноста, особено кога процесот на проверка е доверен на приватни субјекти. Понатаму, перформансите на системот се ограничени и неговата приспособливост зависи од нивото на направени инвестиции, бидејќи цената е директно пропорционална со перформансите на системот. И на крај, недостатокот на мотивација кај програмерите и истражувачите претставува дополнителна пречка за успешното усвојување на оваа технологија. Табелата 9 дава сеопфатен преглед на ограничувањата, придружен со соодветни објаснувања и решенија добиени од тековните научни истражувања [133-142].

Табела 9. Ограничувања и решение за blockchain-системи за ВОУ

Ограничувања	**Опис**	**Решение**
Безбедност	може да понуди уште поголема безбедност, користејќи посовремени механизми	подобрувања во консензусните алгоритми, адресирање на ограничувањата на тековните алгоритми [134]
Управување со големи податоци	се покажа дека е ограничен за пренос на големи количини податоци	едно од решенијата е хибридна архитектура, комбинирање на blockchain со други технологии, како што е складирање на blockchain-облак или дистрибуирани бази на податоци [140]
Стандардизација	недостига стандардна платформа за академски акредитиви, секој универзитет има свој шаблон	креирање стандардни паметни договори за генерирање дипломи и нивна проверка [133]
Пренос надвор од синџирот	обработката на податоците надвор од синџирот, ја покажа потешкотијата подоцна во преносот на податоците	создавање безбедна инфраструктура надвор од синџирот или користење доверлива трета страна [141]
Приспособливост и повторна употреба	адаптацијата на blockchain-платформите е тешка, повторната употреба на архитектури и модели е тешка	креирање на паметни договори со можност за ажурирање, како и нивно документирање [142]
Недостаток на знаење	има недостаток на програмери, недостаток на обука за оваа технологија	да се организираат обуки, да се мотивираат студентите да се занимаваат со оваа проблематика, да ја документираат секоја акција [143]
Идентитетот на	повеќето решенија не користат	промовирање на концептот на

студентот	соодветен метод за идентификување на студентите	самосуверен идентитет (SSI), каде што студентите имаат целосна контрола врз нивните методи за дигитална идентификација [135]
Потрошувачка на енергија	во последно време се прават напори за нови механизми за поголема заштеда на електричната енергија	можност за користење зелени енергетски ресурси во рударскиот процес [136]
Одржување	одржувањето е многу поскапо од централизираните системи	употребата на вештачка интелигенција за автоматско следење и предупредувања за каква било интервенција, исто така системот да научи да прави подобрувања и поправки на грешки [137]

Употребата на blockchain-технологија за издавање дипломи се смета за проактивен пристап за ублажување на ризикот од фалсификување акредитиви во ВОУ.



Слика 5.2. Поедноставена архитектура на предложениот blockchain-систем

Постојат неколку пристапи за имплементација за распоредување на таков систем во практични поставувања, зависни од фактори како што се платформата, типот на

blockchain, користените апликации и базите на податоци. Сепак, императив е секој blockchain-систем да вклучува суштински компоненти што обезбедуваат целосна функционалност на системот. Со Слика 5.2. презентираме друга поедноставена архитектура што ги претставува главните компоненти во друга перспектива, како продолжение на архитектурата претставена во [48].

5.4. Определување на барањата

Барањата претставуваат клучна фаза во развојот на системот бидејќи тие служат како основа за целиот процес на развој, обезбедувајќи дека системот ги задоволува потребите на засегнатите страни. Постојат два вида барања, т.е. функционални и нефункционални. Додека функционалните барања испитуваат какво однесување треба да понуди системот, нефункционалните барања одредуваат специфично својство или ограничување на системот. По темелно истражување на релевантната литература во врска со системите базирани на blockchain [48], ги идентификувавме двата типа на барања за нашиот прототип, како што е опишано подолу.

Функционалните барања на системот вклучуваат:

- *Управување со корисници.* Ова вклучува поделба на улогите на студент, професор, проверувач, издавач, подадминистратор, раководство со институција, администратор.
- *Управување со часови.* Тука вклучуваме создавање училница, вклучување на студентите во училницата, дистрибуција на материјали, евалуација на студентите.
- *Управување со испитите за студенти.* Студентите во соработка со професорите се договараат за начинот на одржување на испитите. Системот нуди можност за одржување онлајн, нудејќи безбедност и приватност за двете страни.
- *Чување податоци во базата на податоци подолго време.* Во таков систем за ВОУ, потребно е покрај реализацијата на трансакциите и привременото складирање на податоците, било во складирање на датотеки или други методи, и нивно складирање подолго време во blockchain-база на податоци.
- *Генерирање дипломи, сертификати и други документи поврзани со студентите и академскиот кадар.* Системот треба да генерира диплома, сертификат или кој било друг документ, врз основа на претходно вметнати податоци.
- *Заверка на дипломи, уверенија и други документи на студентите и академскиот кадар.* Системот треба да ги проверува барањата обработени од компанијата за проверка, а кои се однесуваат на студенти, како што се проверка на дипломи, сертификати или други документи.

- *Споделување дозволи, можност за дигитален потпис.* За да се поделат дозволите во системот, секое лице одговорно за својата работа да има можност за дигитален потпис, како што е академскиот кадар што работи во канцеларијата за дипломи. За време на генерирањето или проверката на дипломите, има можност да се потпише дигитално, пред да се обработи до раководството на институцијата.
- *Можност за регенерирање дипломи, уверенија и други документи.* И покрај фактот дека blockchain е непроменлив, неопходно е да се понуди можност за одземање дипломи и документи од различни причини и нивна регенерација.
- *Извршување на паметниот договор врз основа на параметрите дадени во системот.* Откако ќе се дадат параметрите и податоците потребни како влезови во системот, тој ќе го изврши паметниот договор и автоматски ќе започне генерирање различни барања.
- *Управување со плаќања и научно истражување на студентот.* Сите плаќања мора да се вршат во blockchain-мрежата преку трансакции и научни истражувања и сите работилници, конференции мора да се управуваат во профили на студенти.

Од друга страна, нефункционалните барања на системот се:

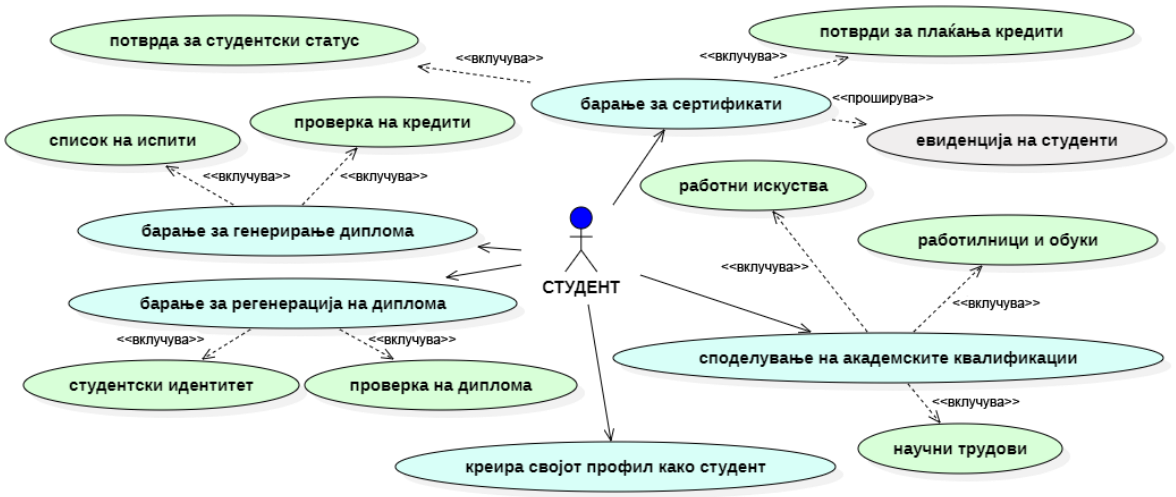
- *Достапност и безбедност.* Системот треба да обезбеди континуирана достапност, осигурувајќи дека студентите и другите засегнати страни имаат неограничен пристап до него, истовремено обезбедувајќи безбедност и транспарентност. Безбедносните мерки мора да бидат од висок степен поради очекуваната фреквенција на напади врз системот, што се припишува на чувствителната природа на информациите со кои тој ќе ракува.
- *Брзина и перформанси.* За време на извршувањето на паметниот договор, што значи дека системот мора да генерира барања што е можно побрзо.
- *Компатибилност.* Системот мора да биде компатибилен со паметни уреди, вклучително и преносливи компјутери.
- *Следливост и непроменливост на услугите.* Системот мора да ги следи постапките на сите. Што значи дека системот треба да ги има точно информациите, која трансакција ја извршил кој од актерите во системот.
- *Употребливост.* Системот треба да поседува кориснички интерфејс и универзално прифатен дизајн, што обезбедува компатибилност со многу групи корисници, без оглед на возраста или техничката експертиза. Дополнително, треба да обезбеди интуитивна функционалност и сеопфатна помош за справување со сите потенцијални несигурности.
- *Стандардно генерирање документи.* Ова би значело дека сите документи генерирани од системот се засновани на стандарди и прифатливи од сите институции кои се дел од blockchain-системот.

- *Брзо и безбедно.* Со оглед на сложеноста, големиот број трансакции што може да ги изврши, системот мора да биде способен да обработува големи количини на трансакции и да складира големи количини на податоци, земајќи го предвид складирањето на податоците за долго време, односно во blockchain-базата на податоци [143].

5.5. Случаи за употреба и сценарија

Главните актери на прототипот на blockchain-системот се: студентите, академскиот кадар, компанијата за проверка, издавач на сите услуги што може да бидат ВОУ или приватна компанија и администратор на blockchain-мрежата. Згора на тоа, системот е исто така незаменлив дел од него, што е одговорен не само за потребите на ВОУ, туку и за целата платформа што вклучува и други релевантни институции.

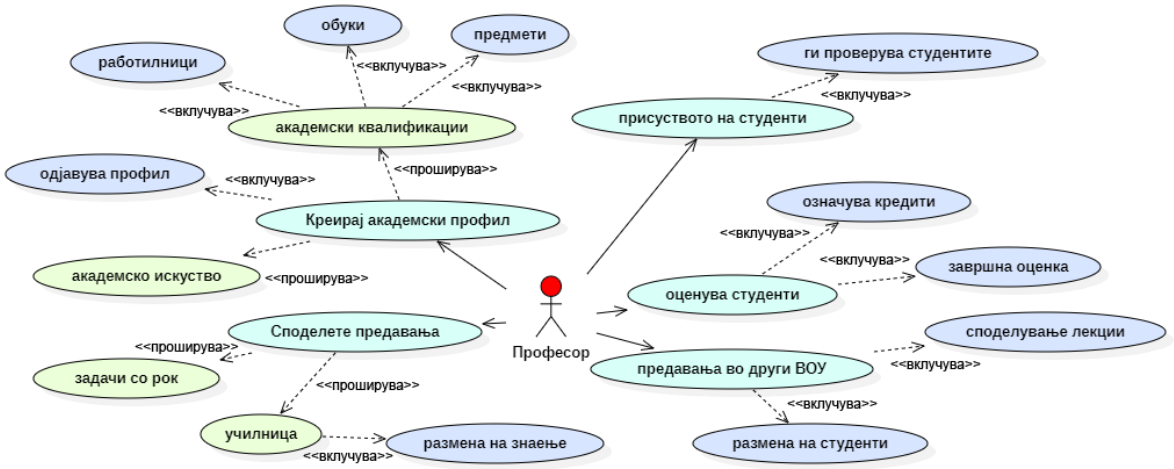
Слика 5.3. го претставува дијаграмот на кориснички случаи за студентите прикажувајќи ги можностите и активностите што студентот може да ги реализира во таков систем. Секој студент има можност: да го креира својот профил како студент, врз основа на официјалната е-пошта на ВОУ; да го ажурира својот профил со неговата биографија, претходни искуства, вештини. Исто така, студентот може на профилот да ги додаде своите работилници и конференции на кои присуствувал, да поднесува барања за генерирање или регенерирање дипломи, пријавување испити итн. Студентите исто така можат електронски да потпишат документи што ги бара ВОУ, да аплицираат за размена на други ВОУ и да контактираат со професорите од другите институции.



Слика 5.3. Дијаграм на кориснички случаи за студентот

Слика 5.4. го претставува дијаграмот на кориснички случаи за професорот, опишувајќи ги задачите и можностите што ги има во blockchain-системот. Овде, секој

професор во ВОУ има можност да го креира својот профил во системот, врз основа на неговата официјална е-пошта. Покрај тоа, професорите се договараат за распоредот на наставата, испитите и консултациите, вклучувајќи го и видот на наставата. Професорите, исто така, ќе бидат одговорни за оценување на студентите и потпишување различни документи со дигитален потпис, како и проверка на евалуацијата на студентите и другите документи генерирани во електронска форма. Други улоги за професорите се илустрирани на сликата.

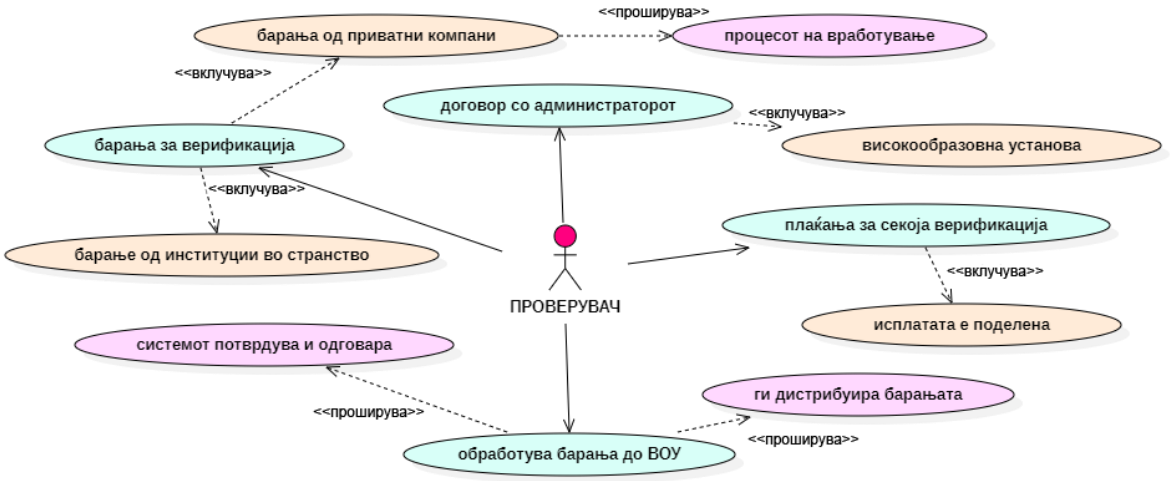


Слика 5.4. Дијаграм на кориснички случаи за професорите

Слика 5.5. го прикажува дијаграмот на кориснички случаи за издавачот на диплома, додека Слика 5.6. го прикажува дијаграмот на кориснички случаи за проверувачот на диплома. За процесот на проверка на диплома, првично, администраторот треба да генерира сметка врз основа на прелиминарните договори помеѓу ВОУ и компанијата за проверки. Потоа, администраторот ги прифаќа сите барања за проверка од различни институции. Ваквите барања прво ги проверува и самиот систем и се уверува дека не се злонамерни лица, а секое такво барање би го наплатувала самата институција. Назначениот оддел ќе ги обработи барањата до раководството на ВОУ и други одговорни лица за да провери дали се работи за проверка на дипломи, научна работа, апликант итн. Проверувачот е одговорен за проверка на документите и за да се осигури дека нема грешки во текот на овој процес. Административниот персонал на ВОУ е одговорен да се погрижи при обработката на барањата тие да бидат упатени до назначените лица. Тие, исто така, ги проверуваат исплатите на студентите, евиденцијата, испитите и кредитите, а исто така ја играат улогата на издавачот во координација со раководството на ВОУ. Секое одговорно лице од административниот персонал по барањето го потпишува дигитално и го проследува до раководството на ВОУ за понатамошна обработка. Истото барање му се враќа на подносителот, со однапред легитимирање на неговиот идентитет, заедно со исплатите за

генерирање документи, што има свој трошок. Повеќето од услугите во blockchain-системот се автоматски и се засноваат на паметни договори. Академскиот кадар треба само да провери бидејќи тие се генерираат автоматски. Проверката може да вклучува различни документи што се иницирани како барање од проверувачот, т.е. да се генерираат дипломи врз основа на барањата на студентите, вклучувајќи различни сертификати, заработени кредити итн.

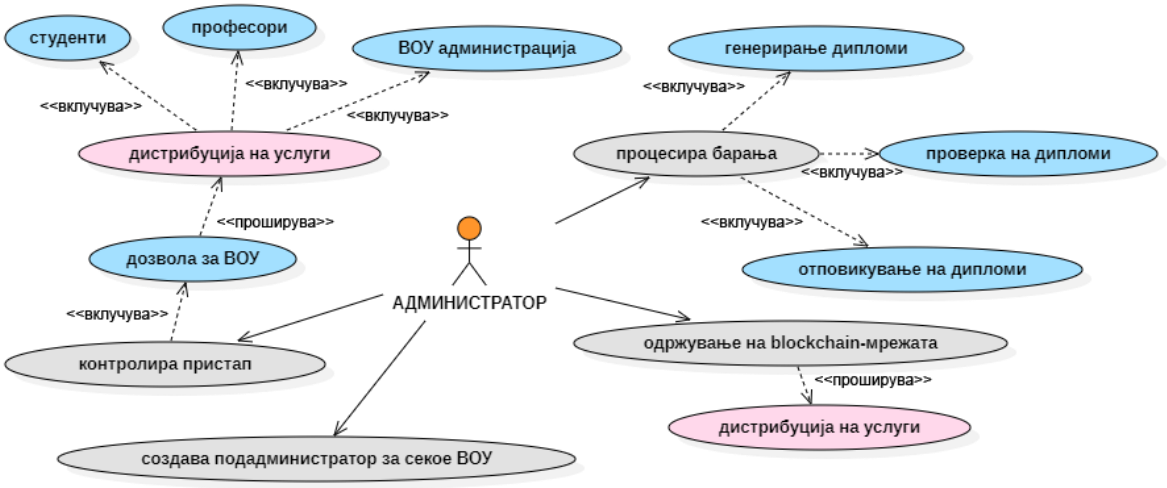
Слика 5.5. Дијаграм на кориснички случаи за издавачот



Слика 5.6. Дијаграм на кориснички случаи за проверувачот

Слика 5.7. го илустрира дијаграмот на кориснички случаи за системски администратор, кој вообичаено е приватна компанија. Системскиот администратор е одговорен за целокупното одржување на blockchain-мрежата и за проверка на трансакциите извршени од ВОУ. Таквите трансакции вклучуваат додавање, ажурирање

и бришење јазли во мрежата, како и управување со јазлите. Системскиот администратор, исто така, има право да креира дозволи за подадминистраторите за секое високо образование, да ги фактурира месечните трошоци на ВОУ и да нуди поддршка за сите услуги во секое време.



Слика 5.7. Дијаграм на кориснички случаи за администраторот

Овој дел дава концизен преглед на основните атрибути на blockchain-технологијата и паметните договори во однос на ВОУ и предлага пристап за развој на прототип на blockchain-систем за автоматско генерирање дипломи. Ги наведовме функционалните и нефункционалните барања за предвидениот прототип на blockchain-систем што е наменет за развој. Дополнително, беа креирани дијаграми на кориснички случаи за да ги претстават примарните актери вклучени во процесот на креирање и проверка на дипломи на blockchain-системот. Покрај употребата на дијаграми на кориснички случаи, обезбедивме и детален приказ на сценаријата на случаи на употреба за секој актер. Овој пристап го олеснува беспрекорното напредување на процесот на дизајнирање за целосно интегрираниот систем, со вклучување на УМЛ (UML) дијаграми.

Со ова се исполнети сите услови за да се започне со дизајнирање на системот базиран на blockchain, креирање детална архитектура на системот до архитектура на паметните договори што ќе бидат кодирани.

6. ДИАР (DIAR): СИСТЕМ ЗАСНОВАН НА BLOCKCHAIN ЗА ГЕНЕРИРАЊЕ И ПРОВЕРКА НА АКАДЕМСКИ ДИПЛОМИ

Првично, системот што ќе го дизајнираме, а што ќе биде blockchain-систем за генерирање и верификација на дипломи, го насловивме како ДИАР (DIAR) систем. Во однос на тоа што подразбираме под системот ДИАР (DIAR) и зошто го насловивме вака, ги даваме следните појаснувања. **D** – Централниот документ што го претставува завршувањето на образовната програма на студентот. Blockchain-технологијата може да се користи за безбедно издавање и потврдување дигитални дипломи. **I** – Обезбедувањето на интегритетот на евиденцијата на дипломите е клучно. Непроменливоста на blockchainгарантира дека откако ќе се евидентира дипломата, таа не може да се менува без консензус. **A** – Механизмите за автентикација базирани на blockchain можат да ја потврдат автентичноста на дипломите. Ова ги спречува лажните тврдења и ја зајакнува довербата. **R** – blockchain одржува евиденција за дипломи што не дозволуваат манипулации, вклучувајќи детали како датум на дипломирање, насока и институција. До овие записи може безбедно да се пристапи.

Предложениот blockchain-систем е темелно објаснет, прво со презентација на концептуалниот модел, проследено со детална архитектура на процесите што системот би ги извршил, со посебен акцент на генерирањето и автентикацијата на академските акредитиви. Дополнително, дадена е анализа за значењето на паметните договори во програмирањето на blockchain-системи. Ова вклучува детално објаснување на главната архитектура на паметни договори што се користи во предложениот blockchain-систем. Овој дел има за цел да го истражи развојот на предложениот blockchain-систем и неговата практична имплементација за цели на тестирање користејќи специфични сценарија и податоци.

6.1. Поврзана литература

Пред да се продолжи со фазата на дизајнирање на концептуалниот модел и деталната архитектура на овие процеси, во овој дел се обезбедуваат основни информации и е напревен преглед на литература што се однесува на придружните проблеми во доменот на blockchain и високото образование. Иако се развиени различни прототипови за генерирање и проверка на академските акредитиви, како што е сумирано во Табела 8, во моментов не постои истражување што ја демонстрира нивната успешна имплементација и позитивните резултати. Ова истражување има за цел да ги истакне разликите помеѓу различните blockchain-решенија. Дополнително ќе ги наведеме разликите помеѓу нашиот пристап и постоечките, објаснувајќи го фактот дека предложената архитектура и нејзината детална структура имаат потенцијал практично да се имплементираат во блиска иднина. Во споредба со ЦЕРТбчеин (CERTbchain),

систем што визуелно ја претставува проверката на академските акредитиви додека практично не се имплементира, системот ДИАР (DIAR) е прецизно дизајниран, со сеопфатна архитектура и концептуален модел. Имено, тој дава детален приказ на генерирањето и проверка на дипломите, што се клучни во ВОУ. Системот ДИАР (DIAR) е компатибилен со платформата Етериум и нуди повеќе од само паметен договор. Обезбедува сеопфатно решение што оди подалеку од потврдување на уникатната вредност на хашот [144]. Покрај ова, системот ќе користи ИПФС (IPFS), како складирање на датотеки, во првата фаза од имплементацијата за тестирање валидација и перформанси, за разлика од ЦЕРТбчеин (CERTbchain), кој не користеше никаква база на податоци, туку само Метамаск за потврдување на завршувањето на трансакцијата за проверка, и менаџер на услуги како интерфејс помеѓу корисникот и blockchain-мрежата.

Докчеин (Docschain) е уште едно blockchain-решение [145], за надминување на некои ограничувања на платформата Блоксертс (Blockcerts) [146], воведувајќи препознавање на знаци со оптичка употреба и овие податоци се складираат заедно со сите други податоци за студентите. Меѓу другото, Докчеин (Docschain) нуди решенија за трите ограничувања на Блоксертс (Blockcerts). Да се поправи протокот на генерирање документи, каде што во Блоксертс (Blockcerts) протокот се менува и истиот не се покажа како успешен за генерирање дипломи. Докчеин (Docschain) нуди решенија за надминување на проблемот со издавање поединечни дипломи, односно една по една, како и нуди решенија за надминување на проблемот со студентите што дипломирале и како да се внесат во системот. Системот ДИАР, за разлика од Докчеин што нуди само проверка, нуди генерирање и проверка на дипломи. ДИАР се заснова на најсофистицираните методи за идентификација, најбезбедните механизми за заштита на приватноста и пред сè нуди обработка и проверка во реално време на повеќе дипломи во паралелна форма.

Курми (Curmi) [147]-, презентираше истражување за придобивките од користењето на blockchain, некои методологии за развој на систем за проверка на документи, без да даде детали за имплементацијата, предлагајќи каков било концептуален модел или дури и архитектура на кој било систем. Тоа е опис во кратки точки, но корисен при започнување на фазата на дизајнирање на blockchain-систем за генерирање и проверка на дипломи. За разлика од СПЛ, каде дискутиравме имплементацијата на blockchain за генерирање и проверка на дипломи во ВОУ [48], Раимундо и соработниците [148], спроведоа систематски библиометриски преглед на литература во врска со апликациите на blockchain во областа на образованието. Нема ништо конкретно во однос на примената на blockchain во ВОУ во однос на генерирање и проверка на дипломи, а уште помалку каков било модел или предлог-архитектура, или какво било теоретско решение за овој проблем.

6.1.1. Blockchain-решение за ВОУ

До денес се создадени се значителен број blockchain-решенија поврзани со ВОУ, каде што некои од нив се добро документирани преку моделирање, детални архитектури, па дури и реални имплементации преку интерфејси; сепак, во моментов има недостиг од современи истражувања што ја демонстрираат употребата и ефективноста на истите практики на ВОУ [48]. Меѓу другото, има голем број предизвици што ја прават blockchain-технологијата ограничена во ВОУ, но пред се, blockchain-програмирањето зависи од паметните договори, додека паметните договори имаат свои предизвици, што во овој случај го прават blockchain-системот зависен и ограничен во многу аспекти. Табела 10 претставува сеопфатен преглед на различни blockchain-решенија што се однесуваат на генерирање и проверка на академски акредитиви. Табелата ги прикажува платформите на кои се создадени овие решенија, како тие моментално се користат, методите за складирање што се користеле, колку се скалабилни врз основа на резултатите од тестирањето во реалниот свет, нивната документирана структура и кодови и како се паметните договори искористени. Дополнително, Табелата ја проценува стабилноста на овие решенија со испитување на нивното моментално постоење и статус на одржување до денес.

Важно е да се напомене дека сè уште нема развој на blockchain-бази на податоци што ќе соработуваат со децентрализирани blockchain-системи, иако има напори во насока на создавање децентрализирани бази на податоци. Сепак, постојат ограничувања во однос на пристапот до податоци и управувањето со големите податоци [149]. Решенијата за blockchain поврзани со управувањето со податоци често користат или складирање датотеки или централизирани бази на податоци. Меѓутоа, во некои случаи, базите на blockchain може да се користат и за цели на тестирање. Ова ограничување служи како еден од факторите штого попречуваат континуираниот раст на blockchain-програмирањето паралелно со унапредувањето на blockchain-технологијата во областа на управувањето со податоци [150]. Неодамна, програмерите успеаја да создадат хибридна рамка за функционирање на blockchain-системи, користејќи централизирани бази на податоци, но поврзувајќи ја со механизмите на blockchain-мрежата за шифрирање на податоците, алудирајќи на овој начин на функционирање на blockchain-систем. Како и да е, проблемот лежи во работењето на складирањето надвор од синџирот и на синџирот, бидејќи примарна грижа во овој поглед е преносот во реално време и манипулацијата со податоци користејќи blockchain-складирање во синџир [151].

Имплементацијата на децентрализирани системи во ВОУ се карактеризира и со автоматско генерирање дипломи, класификација на јавни, приватни и хибридни услуги, повторна употреба и адаптација на податоци во различни платформи, безбедност и транспарентност, помошни алатки што помагаат во извршувањето на паметните договори во blockchain-мрежата, како и архитектури и концептуални модели на децентрализирани системи. Спроведувањето на процесите во автоматска форма без интервенција на трето лице е овозможено со паметниот договор, што го извршува кодот

само откако ќе се исполнат предусловите. Сите услуги во blockchain се транспарентни, што значи дека во blockchain-системот студентите, професорите и целата администрација можат да пристапат во секое време за да ги добијат потребните информации. Безбедноста на податоците се обезбедува преку безбедносни механизми за автентикација, заштита на идентитетот на податоците, а за разлика од централизираните системи, безбедноста е загарантирана во blockchain-системите. Повторната употреба на податоците во blockchain-системот зависи од можната повторна употреба на паметниот договор, што всушност го претставува процесот на стандардизација на паметниот договор, додека приспособувањето на системот и неговите карактеристики на различни платформи е несомнено предизвик и зависи од одржувачите на системот како ќе можат да ги приспособат услугите на најновите платформи [146]. Blockchain-системот не може да функционира независно, без да има помошни технологии што нудат реализација на услуги. Несомнено, нивната употреба е во директна пропорција со трошоците и потрошувачката на енергија. Повеќе за предизвиците и ограничувањата на blockchain во управувањето со податоци, а особено за ВОУ, опишуваме во претстојниот дел.

Табела 10. Резиме на најсовремени карактеристики на blockchain-решенија

Тр-уд	**Име**	**Практ .имп.**	**Block. платф.**	**Складирање**	**Прис по-собли вост**	**Документа -ција и водичи**	**Ста-бил-ност**
[25]	CVSS	Да	Етериум	Централизирана база на податоци	Не	Не	Не
[25]	OPEN-BADGES	Да	Етериум	Централизирана база на податоци	Не	Не	Не
[26]	EDU-CRYPTO	Да	Етериум	Меѓупланетарен датотечен систем	Не	Да	Не
[27]	EDUCTX	Да	Етериум	blockchain-база на податоци	Да	Да	Да
[28]	OPEN-CERTS	Да	Етериум	Јавна книга	Да	Да	Да
	BLOCK-CERTS	Да	Хиперлеџ ер фабрик	Споделени книги	Да	Не	Да
	BT-CERTS	Да	Етериум	Локална база на податоци	Не	Не	Не
	BLOCK.CO	Да	Етериум	Незаменливи	Не	Не	Да

				токени			
[29]	CER-BERUS	Не	Етериум	Локална база на податоци	Не	Да	Не
[30]	VerDe	Не	Етериум	Децентрализира на база на податоци	Не	Да	Не
[12]	CERT-bchain	Да	Етериум	Управник за услуги	Не	Не	Не
[13]	DOCS-CHAIN	Не	Хиперлеџ ер фабрик	Леџер на Docschain	Да	Не	Да
[14]	Плат-форма за проверка на сертифи-кати базирана на blockchain	Не	JCOH (JSON)	Складирање надвор од синџирот	Не	Не	Не

Системот ДИАР е во фаза на имплементација на прототип што вклучува тестирање на валидноста, мерење на ефикасноста и перформансите во реално време. Платформата Етериум нуди многу алатки што овозможуваат, меѓу другото, програмирање, извршување и тестирање на паметните договори без дополнителни трошоци, до нивна вистинска имплементација. Другата причина зошто ги сметаме Етериум и ИПФС е фактот што Етериум го поддржува процесот на токенизација, нудејќи стандардни токени, заменливи и незаменливи токени, додека дипломите се класифицирани како незаменливи токени [84]. Складирањето датотеки во blockchain се претпочита и кога станува збор за прототипови, бидејќи сè уште нема децентрализирана база на податоци што во пракса покажала добри резултати во однос на управувањето со променливи податоци. ИПФС (IPFS), исто така, овозможува складирање податоци врз основа на нивната единствена вредност, генерирана преку сметката на Етериум, додека складирањето на податоците врз основа на генерираната хаш-вредност го олеснува нивното потврдување. Меѓу другото, платформата Етериум е отворена платформа за секој штосака да се приклучи на blockchain-мрежата, додека другите платформи, како што е Хиперлеџер фабрик (Hyperledger Fabric) имаат ограничувања и потребни се претходни предупредувања за пристап до мрежата [48].

6.1.2. Предизвици на blockchain во ВОУ

Во контекст на ВОУ, се обезбедуваат разновидни услуги, што резултира со забележителна хетерогеност на понудите. Овие услуги опфаќаат финансиски услуги, управување со податоци, обработка во реално време, транспарентност, заштита на идентитетот и зачувување на приватноста. Присуството на овие различни карактеристики дополнително го отежнува воспоставувањето сеопфатен систем што би го олеснил управувањето и обработката во реално време на значителната количина на податоци генерирани во овие институции. Во blockchain-системите, олеснувањето на извршувањето на услугата би било значително зголемено преку воспоставување стандардизирани протоколи. Секоја услуга ќе се придржува до специфични стандарди, а со тоа ќе го рационализира извршувањето на соодветните паметни договори.

Цената на услугите и нивното долгорочно одржување во blockchain-системите има значајна важност. Во однос на генерирањето дипломи, трошоците се релативно ниски во споредба со физичкото производство. Ова се должи на употребата на методи за дигитално генерирање, при што дипломите се креираат во дигитален формат и се потпишуваат со дигитален потпис, често претставен како пдф-датотека. Затоа, процесот на проверка на дипломите повлекува повикување на паметен договор, при што поврзаните трошоци се зависни од трошоците за извршување на паметниот договор и одбраната платформа за распоредување.

Во однос на имплементацијата и адаптацијата на blockchain-системот на постоечките платформи, обуката на академскиот кадар, студентите и сите други актери во користењето на системот е многу поскапа отколку во централизираните системи. Во исто време, трошокот директно зависи од големината на blockchain-мрежата, количината на податоци што ќе се складираат во базата на blockchain и нивната обработка во реално време. Односно, колку повеќе дипломи се обработуваат, толку повеќе се зголемува реалната цена на системот, а во исто време и нивното одржување [151]. Спротивно на тоа, имплементациите на Blockchain-системи во реалниот свет низ различни домени покажаа намалување на годишните трошоци за одржување на системот. Ова се должи на елиминацијата на посредниците, особено во финансиските апликации како компаниите за трансфер на пари, што во голема мера имаат корист од усвојувањето на blockchain-системи [86]. Приспособливоста и ограничувањето на компјутерската опрема за обработка на трансакции е една од причините што може да доведе до високи трошоци во blockchain-системите [150]. Пред сè, трошоците за имплементација на blockchain-системот во ВОУ зависат од многу фактори, како што се избраната платформа, blockchain-базата на податоци, безбедносните механизми, интеграцијата во постоечките системи и обуката потребна за користење на системот [151]. Со оглед на фактот дека го избравме Етериум како платформа, секоја трансакција што се врши се пресметува со етериум гас (Ethereum Gas), а за секоја трансакција нужно мора да имаме максимална граница за гас. За време на практичната имплементација, ќе разгледаме и обезбедување на деталите за имплементација на трошок за трансакциски

гас, вроден трошок за гас, трошок за извршување гас, трошок за распоредување гас, цена за проширување на меморијата [86].

Стабилноста на системот првенствено зависи од практиките за одржување имплементирани во оперативната платформа на системот. Стабилноста на blockchain-системот очигледно зависи од повеќе фактори, меѓу кои ги споменуваме трошоците за одржување и обработка на трансакциите во реално време, избраната платформа, базата на податоци, механизмите за консензус, приспособливост, интероперабилност, безбедност, паметен договор [152]. Анализата на сите безбедносни пропусти и алатките за анализа за паметните договори на Етериум е многу важна за системот да биде стабилен. Со оглед на фактот дека во предложената архитектура користиме пософистицирани механизми за безбедност, заштита и идентификација на приватноста, а истовремено користиме шеми и механизми за економичност, што е една од главните причини системот да биде долгорочен и стабилен, ние сметааме дека системот ДИАР ќе биде одржлив, стабилен и ќе ги нуди сите механизми за брза, безбедна и транспарентна обработка на сите услуги што ќе ги нуди.

Паметните договори мора да се креираат во стандардизирана форма за генерирање, проверка и одземање дипломи. Таквото нешто би овозможило полесна имплементација, зголемена ефикасност, побрза обработка на податоците и ублажување на потенцијалните грешки во фазата на распоредување [153]. Обработката во реално време и комуникацијата на податоци помеѓу blockchain-јазлите е, исто така, многу важна. За побрза обработка на податоците постојат различни техники и механизми, но обработката на помали волумени е една од опциите што практично покажа резултати [128]. Зачувувањето на идентитетот и заштитата на приватноста на податоците е предизвик сам по себе, каде што се користат различни техники за ВИ. Меѓу другите, можеме да ги издвоиме техниките за самоидентификација, што обезбедуваат идентификација без интервенција на трети лица [154]. Приспособувањето и употребата на помошни алатки се важни за стабилноста на системот. Исто така, повторната употреба на различни структури, архитектури, концептуални модели, рамки би ги намалиле дополнителните трошоци и времето за имплементација на blockchain-систем за ВОУ [155]. Употребата на дистрибуирани бази на податоци и повеќе јазли во нив е еден од најдобрите методи за управување со големи податоци, проблем што е во секоја сфера од животот, вклучително и ВОУ. Преносот на податоци во складирање надвор од синџирот, соодветно на складирање на blockchain-облак е можен со користење паметни агенти, облак-компјутери и други методи на ВИ [153]. Одржувањето подолго време, потрошувачката на електрична енергија и складирањето на електронските дипломи во blockchain складирање на неодредено време е предизвик. Затоа, едно од најдобрите решенија во оваа насока е да се дефинираат законски прописи за складирање податоци во овие системи [156]. Во Табела 11 ги прикажуваме функционалните и нефункционалните барања, како и практичните предизвици поврзани со спроведувањето на системот ДИАР.

Табела 11. Функционални и нефункционални барања, практични предизвици на системот ДИАР

Функционални барања	**Практични предизвици**	**Нефункционални барања**
Управување со улогите на корисниците во системот	Пренос на податоци од постоечки системи до складирање на blockchain	Системот треба да обезбеди сигурност и да биде достапен во секое време
Создавање виртуелни простори, управување со часови, евалуација на студентите	Тешкотии во користењето на blockchain-системот, недостаток на тренери и програмери	Обработка на податоци и перформанси
Чување и пренос на податоци надвор од синџирот, утврдување на законски прописи	Централизирана база на податоци со карактеристики на blockchain, децентрализирана база на податоци или децентрализирано складирање на датотеки	Компатибилност со сите паметни уреди
Генерирање и проверка на академски документи, вклучително и дипломи	Многу алатки за развој на системот, скапи и паметни договори не може да се ажурираат откако ќе бидат распоредени	Следливост и непроменливост на услугите
Споделување дозволи, дигитален потпис, методи за идентификација	Дигиталниот потпис, методите на самосуверен идентитет, регенерацијата на документите се скапи за корисниците, особено за студентите	Кориснички интерфејс, поддршка во секое време
Blockchain-платформа, состави и распореди паметен договор, валидација, извршување и дебагирање паметен договор	Ограничување на програмските јазици за создавање паметни договори, blockchain платформи, приспособливи децентрализирани бази на податоци, управување со податоци и нивно ажурирање	Повторна употреба и генерирање стандардни паметни договори
Управување со плаќање, трошоци за одржување	Методите на извршување на трансакции со криптовалути генерирани од самата високообразовна институција, со дефинирани законски прописи	Брзо и безбедно извршување различни трансакции

Овие барања во детална форма, вклучувајќи дијаграми на корснички случаи, сценарија на корснички случаи за главните актери вклучени во системот, исто така може да се најдат во [143].

6.2. Предложен blockchain-систем за генерирање и проверка на академски дипломи

Едно од ограничувањата поврзани со употребата на blockchain-технологијата во ВОУ се однесува на недостигот на научни истражувања, литература, прирачници и темелни описи во кои се детализира практичната имплементација на blockchain-решенијата. Според сеопфатниот СПЛ што се однесува на генерирањето и проверката на дипломите, конкретно фокусирајќи се на периодот од 2018 до 2022 година, евидентно е дека само ограничен број студии дале темелно објаснување за овој процес. Очигледно, бројот на трудови поврзани со примената на blockchain за ВОУ е многу поголем [48], сепак, во нашата анализа сакавме да бидеме што е можно поблиску до практичните решенија на blockchain-системите за ВОУ, со посебен акцент на генерирање и проверка на дипломи.

Оваа секција воведува blockchain-систем што става значителен акцент на процесите на генерирање, проверка и отповикување, што се специфични за регенерација на академските акредитиви, со посебен фокус на дипломите како клучни документи во рамките на ВОУ. Во овој дел даваме детален преглед на blockchain-систем за ВОУ, прво опишувајќи го концептуалниот модел, софистицираната архитектура, што се состои од повеќе слоеви на обработка на трансакциите, па сè до систематската архитектура на процесот на генерирање и проверка на дипломите и архитектурата на паметни договори што е во процес на програмирање. Од нашата анализа, произлегува дека повеќе од истражувачките студии имаат практични резултати од нивните прототипови без да се наведат детали за имплементацијата на архитектурата што ја имаат имплементирано или имаат само површен дизајн на архитектурата без никаква детална анализа на практичната имплементација. Најблиските истражувања, што наликуваат на природата на нашиот систем, според нашите сознанија, се Церберус (Cerberus) [111] и Верде (Verde) [84], што во детална форма го имплементирале целиот систем што го предлагаат. За разлика од овие два система, системот ДИАР нуди јасно дефиниран концептуален модел, опишувајќи го во јасна форма односот помеѓу главните актери што ќе го користат системот, како и детална архитектура од седум слоеви на обработка на податоци, нудејќи стабилност, безбедност и заштита на идентитетот. Системот е јасно опишан, со детален опис на процесот на генерирање и проверка на дипломите и му дава важност на процесот на токенизација на дипломите, што е полесен за обработка на дипломите и складирање во blockchain-складирање.

Значењето на приоритетот на дипломите е вкоренето во дигитализацијата на бројни процеси во современите централизирани системи што ги користат ВОУ. И покрај електронското генерирање различни документи, дипломите, што се клучни акредитиви, сè уште не се генерирани во електронски формат. Ова првенствено се должи на неможноста на централизираните системи да обезбедат безбедност и приватност потребни за генерирање и проверка на таквите документи. Отсуството на механизми за безбедност и следливост во овие системи дополнително го влошува

потенцијалот за злоупотреба од страна на корисниците вклучени во процесите на генерирање и проверка.

Утврден факт е дека по завршувањето на студиите, студентите продолжуваат да поднесуваат барање за диплома, процес што во последно време одзема повеќе време. Ова доцнење најмногу се припишува на темелната проверка на академската евиденција на студентот. Сепак, овој продолжен период на проверка предизвикува загриженост за потенцијални случаи на измамни активности. Поточно, постои можност податоците вклучени во дипломите да бидат изменети за време на процесот на генерирање, со што се олеснуваат различните форми на злоупотреба. Тарик и сор. [111], појасни четири типа на можна злоупотреба во ВОУ во однос на академските акредитиви, вклучувајќи ги и дипломите. Првиот е поврзан со фалсификување на дипломата, вклучувајќи детали за диплома, ознаки, кредити, потписи, печати, итн. менување на досиејата на студентите од почеток за да не се остават траги. Третиот тип на злоупотреба е поврзан со генерирањето фиктивни дипломи, каде што институциите не постојат или не се ВОУ но генерираат дипломи со лажни печати и потписи. И четвртиот вид злоупотреба има врска со поширока мрежа на фалсификување, кога на ВОУ и се дава дозвола за акредитација за различни курсеви без да има академски кадар и да не ги исполнува потребните услови за работа на таа институција.

Системот на blockchain тука може да придонесе со самиот факт што податоците вметнати во складиштето на blockchain не можат да се променат, но дури и да се, тие го предупредуваат системот. Непроменливоста на податоците е тесно поврзана со природата на blockchain, каде што покрај генерализираната книга, каде што се чуваат записи за сите блокови и секое дејство на мрежата, секој блок, исто така, води евиденција за оваа книга, како и за активностите на соседните блокови. Промената на податоците е речиси невозможна. За вториот тип на злоупотреба, blockchain придонесува со карактеристиката на следливост, каде што секој во системот е одговорен за дејствата што ги извршува, како и во зависност од привилегиите што ги има. Не секој може да пристапи до приватните податоци, освен оние што се одговорни. За секоја евентуална промена во системот, blockchain го предупредува раководството на ВОУ. Што се однесува до третиот и четвртиот тип на разни злоупотреби, тоа што дипломите се дигитализирани, може лесно да се потврди преку овој транспарентен систем за сите корисници. Во овој контекст, создавањето на национална платформа би помогнало во процесот на селекција на ВОУ. Во таков случај би било уште полесно, особено за проверка на дипломите, бидејќи многу лесно може да се провери дали дипломата што ја презентира соодветното лице припаѓа на таа ВОУ или не, преку онлајн blockchain-системот што нуди услуги непречено, а секоја ВОУ ќе биде сертифицирана од соодветните државни институции [48].

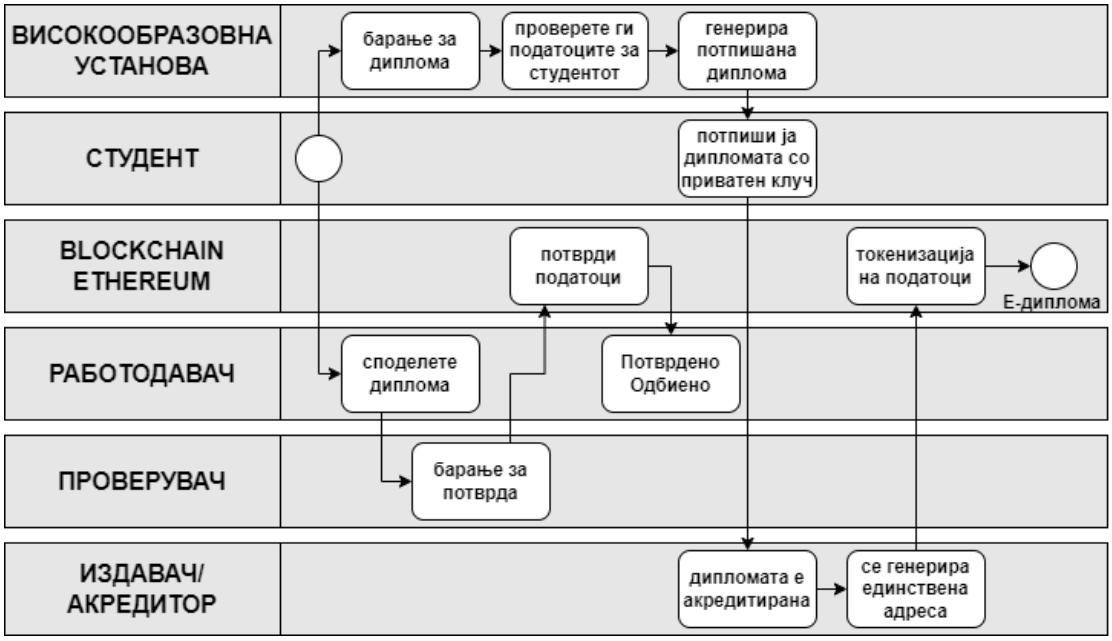
Слика 6.1. Концептуален модел на предложениот blockchain-систем

Имплементацијата на blockchain-технологијата во ВОУ има потенцијал да ги подобри различните процеси, како што се регистрацијата на студентите, следењето на семестарот и трансакциите за плаќање. Со користење на blockchain-системот, овие задачи може да се автоматизираат, обезбедувајќи поголема ефикасност и безбедност. Дополнително blockchain-системот може да генерира оценки врз основа на проценките на професорите, заменувајќи ја потребата за рачно оценување. Генерално, усвојувањето на blockchain-технологијата во образовните услови нуди значителни предности во однос на ефикасноста и спречувањето злоупотреба. Сепак, спроведувањето на таквата постапка бара значителен напор и посветеност. Следствено, има случаји каде што постоечките системи во ВОУ вклучуваат генерирање и проверка на дипломи или алтернативно да воспостават посебен систем за исполнување на оваа цел.

Концептуалниот модел на предложениот систем базиран на blockchain е претставен на Слика 6.1, што ги вклучува главните ентитети и актери, како и нивните улоги. Како што може да се види, по завршувањето на сите академски барања, ВОУ му издава на студентот дигитална диплома. Оваа диплома е дигитално потпишана од институцијата и бара од студентот да генерира свој дигитален потпис. Пред оваа активност, студентот мора да ја потврди точноста на релевантните податоци. Последователно, дипломата е акредитирана од одржувачот на системот, што може да биде или самата ВОУ или приватна компанија со која ВОУ склучила договор. Потоа, процесот на акредитација ја претвора дипломата во непроменлив токен, што се складира во blockchain-мрежата и на крајот во blockchain складирање за долгорочно зачувување. Употребата на приватниот клуч, без разлика дали е дигитален потпис или

кој било друг вид идентификација на студентите, е единствениот метод со кој тие во иднина ја идентификуваат сопственоста на дипломата, но и нејзината непроменливост. Со цел да се олесни процесот на проверка, се препорачува секоја генерирана диплома да биде опремена со QR-код што содржи релевантни информации. Оттука, кога работодавачот бара да потврди автентичност на диплома преку акредитиран проверувач, можно е навремено да се потврди неговата валидност со користење на blockchain-системот и испитување на QR-кодот. Овој процес вклучува и потврдување дали се направени какви било модификации на адресата на blockchain-мрежата, со што се обезбедува автентичноста на дипломата. Одземањето на дипломата се врши на барање на ВОУ, од различни причини, но и студентот е информиран, а таа потоа се регенерира со друга адреса во blockchain-мрежата.

Употребата на интелигентни агенти е клучна за подобрување на ефикасноста на нашиот систем преку ублажување на злоупотребите, издавање предупредувања и забрзување на процедурите. Овие интелигентни агенти стекнуваат информации преку човечки интеракции и имаат способност да го користат тоа знаење во сценарија за решавање проблеми што се протегаат надвор од нивното претходно постоечко знаење [155]. Употребата на интелигентни чет-ботови е една можна употреба во предложениот систем. Овие чет-ботови служат како средство за студентите, раководството и сите корисници на системот да добијат поедноставена помош при навигацијата низ системот. Друга имплементација е создавањето на различни виртуелни простори и виртуелни симулации што им овозможуваат на студентите да размислуваат за различни реални случаи, да развијат интелигенција при решавање проблеми или со други зборови преку правење на учењето попривлечно преку конкретни примери во виртуелни простори [56]. Понатаму, употребата на ВИ може да се имплементира во процесите на идентификација и автентикација на корисникот. Ова го претставува потенцијалот за корисниците да избираат од низа методи за идентификација, како што се препознавање на лицето, скенирање на отпечатоци од прст или други техники за самоидентификување [157]. Заштитата од разни сајбер-напади што можат да се случат на blockchain-системот и навремено предупредување, преку интелигентни агенти, е исто така добра можност за примена на интелигенција во blockchain-системот [158]. Слика 6.2 служи како продолжение на Слика 6.1, илустрирајќи го секвенцијалното претставување на процесите со соодветните процеси што се одвиваат во секој актер на blockchain-системот.



Слика 6.2. Графикон на тек на издавање и потврда на диплома

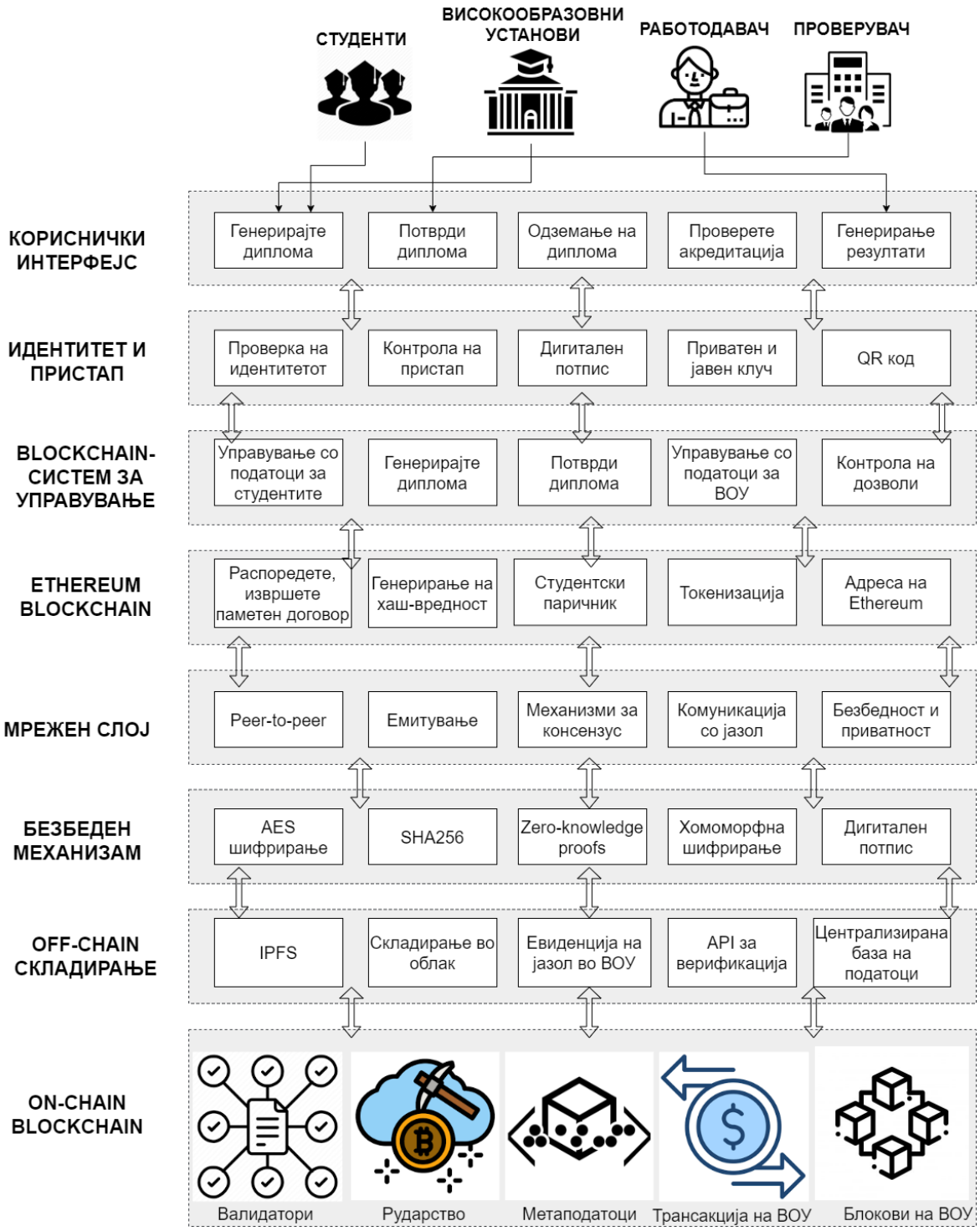
6.2.1. Системска архитектура на blockchain-систем

Изборот на издавачот и акредиторот на дипломите има значајна важност. Субјектот може да биде или самата ВОУ или лиценцирано трговско претпријатие што има формален договор со ВОУ. Слика 6.3. ги илустрира нивоата на архитектурата на blockchain-систем специјално дизајниран за ВОУ. Системот на blockchain ги опфаќа главните актери, имено ВОУ, студентите, работодавците и проверувачите. Во тој контекст, ВОУ ја презема двојната функција на генератор на сертификати и акредитор бидејќи таа е одговорна за издавање и потврдување на дипломите.

Потоа го имаме слојот на корисничкиот интерфејс, што служи како визуелна компонента на системот, што ја олеснува комуникацијата помеѓу примарните актери и системот. Аспектот на идентитетот и пристапот се однесуваат на употребата на техники што ги користат актерите за идентификација, имено самосуверени или методи на децентрализиран идентитет. Компонентата за управување на blockchain-системот ја опфаќа фазата во која се автентицираат ингеренциите на актерите, проследено со последователна обработка на податоците врз основа на конкретното барање. Компонентата на blockchain-етериум се однесува на разновидноста на развојни алатки вклучени во мрежата Етериум. Овие алатки олеснуваат различни функционалности, како што се распоредување паметни договори, создавање карактеристични етериум-адреси, хаш-вредности и токенизација, меѓу другото. Мрежниот слој се однесува на распоредот на јазлите внатре во blockchain-мрежата, вклучувајќи ги врсниците, комуникациските протоколи и механизмите за консензус.

Пред да се пренесат податоците во складиштето, од суштинско значење е податоците да бидат подложени на шифрирање и успешно да ги поминат воспоставените безбедносни протоколи. Во однос на складирањето податоци, често се користи хибриден систем за управување со податоци, вклучувајќи интерпланетарен датотечен систем ИПФС (IPFS), складирање облак и централизирани бази на податоци. Предложениот систем ќе го користи ИПФС (IPFS) во врска со централизирана база на податоци. На крајот, го истакнавме и делот од blockchain на синџирот што се однесува на извршувањето трансакции во контекст на ВОУ, вклучувајќи ги процесите на рударство, валидаторите и блоковите на ВОУ.

Безбедносниот аспект и механизмите што ќе се користат за заштита на податоците се многу важни, бидејќи тие механизми мора да обезбедат заштита на приватноста на податоците на студентите и на другите корисници во системот. Несомнено, во системот мора да имаме класификација на податоци, како за студентите, така и за другите актери во него [143], затоа предвидуваме користење јавен, приватен и конзорциумски blockchain во системот, во зависност од природата на податоците [48]. Од различните методи што се користат за заштита на приватноста [150], ние, меѓу другото, предлагаме комбинација на zero-knowledge proof, AEC (AES), CXA256 (SHA256), хомоморфно шифрирање и *signature ring*, во зависност од природата на понудените услуги, што се претставени во безбедностиот слој во рамките на архитектурата на системот ДИАР. Zk-Snark е специфичен метод за докажување на нула знаење (knowledge zero), со гаранции дека не се споделуваат информации помеѓу примачот и испраќачот; идентитетот, приватноста и автентикацијата се зачувани соодветно, и дека само оние информации што треба да бидат јавни се споделуваат, и покрај долгиот процес на верификација, идентификација на корисниците или дури и за време на генерирањето на различни академски документи [159]. Поради нивната отвореност, blockchain-системите се ранливи на различни закани. Сепак, моделите на blockchain-сметки и системите за издавање сертификати обезбедуваат поголем предизвик, бидејќи бара внимателна класификација на услугите во соодветни категории на blockchain врз основа на нивните карактеристики. Комбинацијата на безбедносни механизми, со соодветните повеќе специфицирани техники, помага да се создаде посигурна шема за зачувување на идентитетот, приватноста и обезбедување сигурна комуникација помеѓу главните актери на системот, секогаш имајќи ја предвид blockchain-платформата и помошната опрема што се користи за извршување трансакции [160].

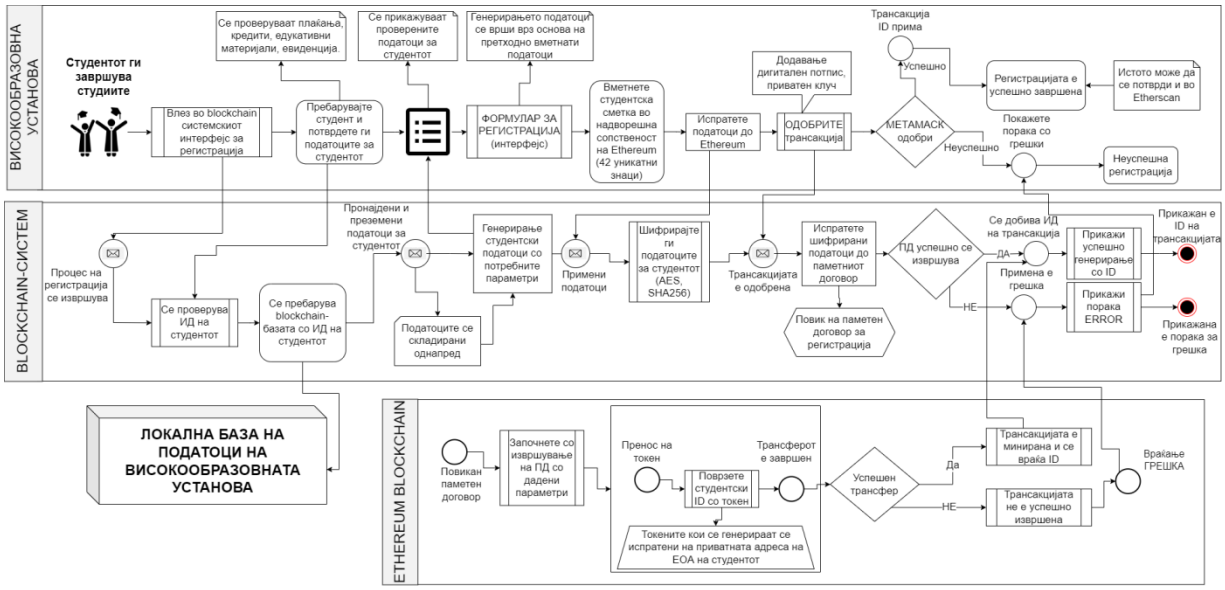


Слика 6.3. Архитектура на blockchain-систем

6.2.2. Процес на издавање диплома

Развиена е модифицирана архитектура базирана на платформата за blockchain Верде (Verde) [84] и темелната анализа каде што авторите го презентираа моделот на системот на процесите во рамките на blockchain-системот, специјално за процесот на генерирање и проверка на дипломи. Целосната процедура за изработка на дипломи или други академски сертификати е прикажана на Слика 6.4. Првата активност на студентот е да поднесе формално барање за издавање диплома. Последователно, системот го започнува процесот на составување на евиденцијата на студентите по завршувањето на нивните студии. Ова подразбира собирање информации во врска со исплатите на студентот, заработените кредити и сите други релевантни факти поврзани со нивното академско патување. Откако податоците ќе поминат низ верификација внатре во blockchain-системот, тие потоа се внесуваат во надворешната сметка на платформата Етериум пред да бидат испратени за понатамошна обработка во рамките на blockchain-системот. Начинот на креирање или вметнување податоци во сметка во надворешна сопственост на blockchain мрежата на Етериум се однесува на:

- генерирање приватен клуч, што обично е хексадецимален број поврзан со адресата на Етериум и мора да се чува во тајност бидејќи пристапот е направен преку овој број;
- изведување на соодветниот јавен клуч од приватниот клуч;
- пресметка на адресата на Етериум откако ќе биде изведена од соодветниот јавен клуч;
- со складирање на адресата на Етериум и приватниот клуч во безбедна форма, приватниот клуч не смее да се споделува додека адресата на Етериум може да биде јавна бидејќи всушност ја идентификува сметката на студентот;
- користејќи ја сметката Етериум, по проверката, може да се извршат трансакции или дури и да се пристапи до паметни договори во blockchain-мрежата [161] .



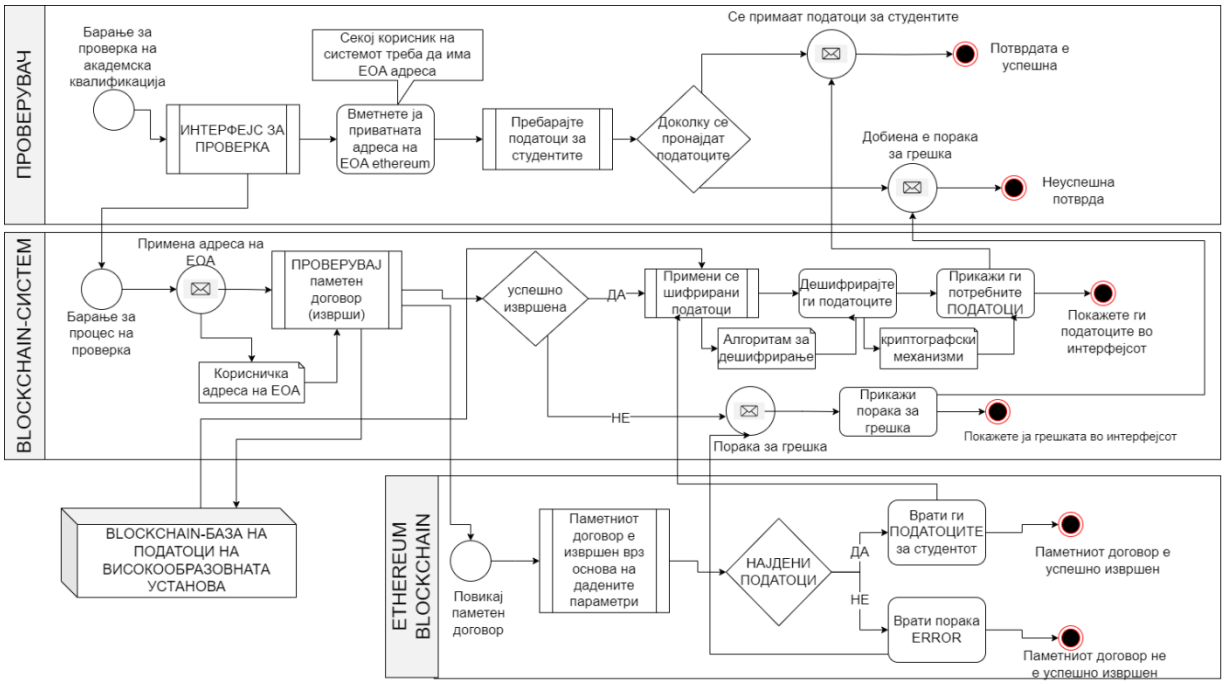
Слика 6.4. Детален процес на издавање диплома

Само откако трансакцијата ќе се потврди дека сè е во ред, тогаш ингеренциите на студентот се шифрираат преку криптографски механизми со помош на алгоритми како AEC (AES) или CXA256 (SHA256). Откако податоците ќе се шифрираат, тогаш паметниот договор се повикува да ги сними податоците во складиштето на blockchain, а потоа се повикува друг паметен договор за генерирање на податоците на студентот. Употребата на токени претставува гаранција за складирање на заработените кредити на студентот и генерирање ИД за време на складирањето во blockchain. По повикувањето на паметниот договор одговорен за генерирање дипломи, процесот на извршување започнува, имајќи ги предвид дадените параметри. Клучен чекор во овој процес вклучува споредба на токенот со идентификацијата на студентот. Ако токенот се совпаѓа со ИД на студентот, дипломата се генерира за соодветниот студент. Успешноста на целата постапка зависи од проверката на идентификацијата на студентот преку употреба на токенот што беше произведен претходно.

Процесот на генерирање токени и нивно испраќање на адресата на надворешната сопственост на сметката (EOA) во blockchain на Етериум е сложено поврзан со извршувањето паметен договор. Ова вклучува развој, извршување, генерирање, пренос и на крајот, испорака на токени до приватната адреса на EOA поврзана со студентот. Вреди да се спомене дека освен извршувањето на паметниот договор, има дополнителни трошоци поврзани со обработката и генерирањето на токените додека не се префрлат на адресата на студентот. Овие трошоци служат како надомест за рударите вклучени во обработката на трансакцијата, без оглед на нејзиниот исход.

6.2.3. Процес на верификација на дипломата

Процесот на проверка е спротивен на генерацијата. Проверувачот, откако ќе се најави на неговата надворешна сметка на Етериум, го бара студентот преку интерфејсите во системот. Пребарувањето се врши со одредени критериуми, по што следи иницирање на паметниот договор за проверка. Последователните процедури вклучуваат валидација на податоците на студентот, дешифрирање на податоците и на крајот прикажување на резултатите до проверувачот, доколку се успешни. Целиот овој процес очигледно има свој трошок, кој верификаторот мора да го плати преку сметката на ЕОА. Слика 6.5. го илустрира процесот на проверка на диплома, прикажувајќи ги вклучените субјекти, имено верификаторот, blockchain-системот и платформата Етериум. Дијаграмот дава преглед на последователните чекори вклучени во процесот на проверка.



Слика 6.5. Детален процес на проверка на диплома

6.2.4. Архитектура на паметни договори

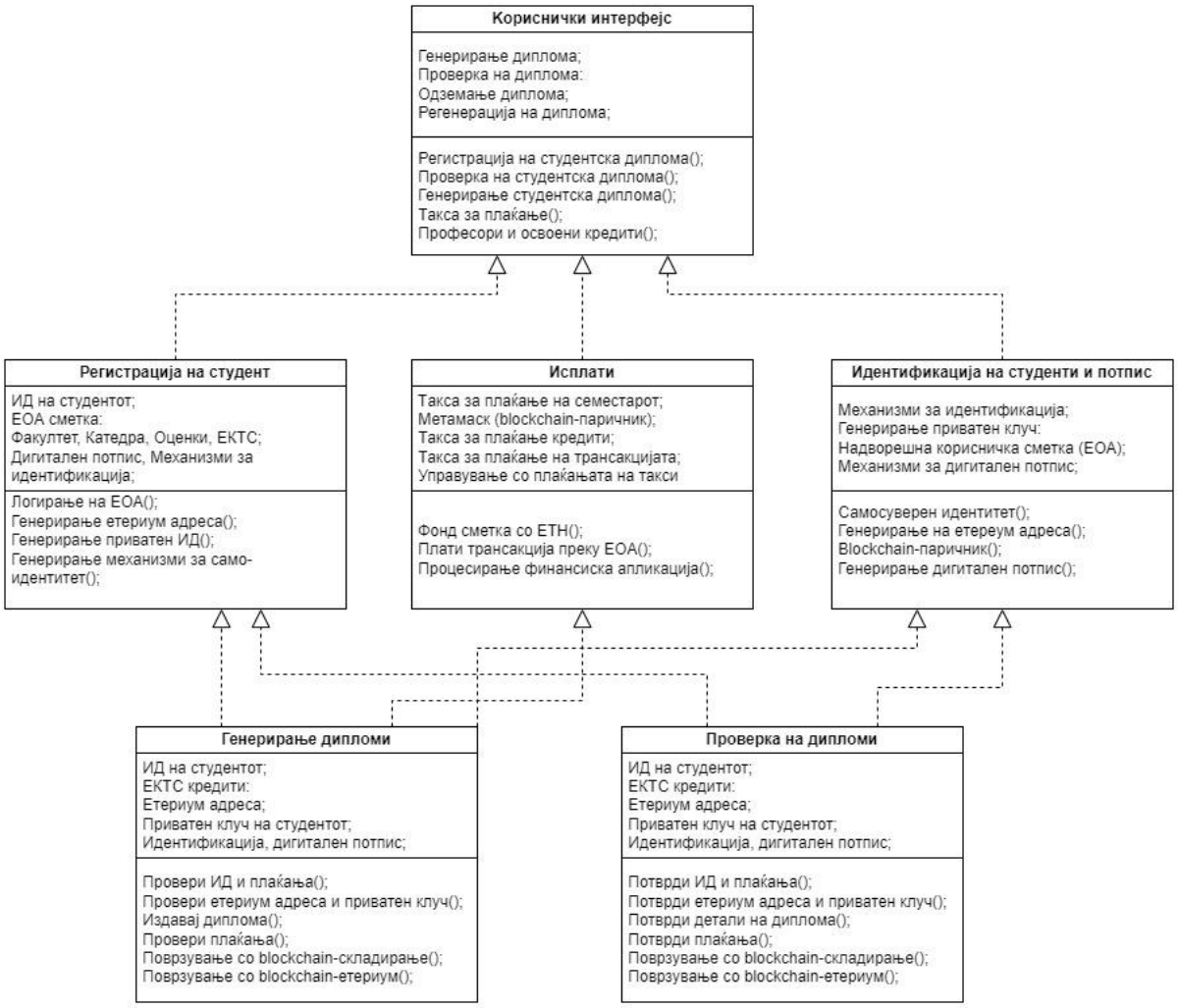
Децентрализираните апликации (Decentralized applications — Dapps), функционираат со користење на виртуелната машина етериум (EVM), што претставува виртуелна машина. Овие апликации работат со извршување паметни договори, што се интегрални компоненти на програмскиот код Солидити. Паметните договори ја олеснуваат интеракцијата помеѓу blockchain-системите и основната blockchain-мрежа [141]. Кога паметниот договор се става на blockchain-мрежа, неговата непроменливост осигурува дека договорот останува непроменлив, дури и со самиот договор. Во случај паметниот договор да наиде на грешки во текот на неговото извршување, од суштинско значење е да се раскине договорот бидејќи нема способност да претрпи модификации во текот на оваа фаза.

Паметните договори се појавија како практично решение во областа на финансиите, олеснувајќи го извршувањето на трансакциите без потреба да се потпираме на традиционални финансиски посредници како што се банките [162]. Овие услуги понекогаш се нарекуваат децентрализирани финансии (Decentralized finance — DeFI) услуги. Дигиталниот идентитет е област каде што може да се користат паметни договори. Оваа технологија им овозможува на корисниците и на студентите да воспостават свои автономни системи за идентификација. Употребата на паметни договори се гледа и во администрацијата на децентрализирани системи, при што нивната автоматизирана функционалност овозможува извршување на однапред одредени услуги без потреба од надворешно вклучување [163]. Покрај тоа, технологијата за паметни договори сè повеќе се користи во областа на медицината, особено во областите на управување со податоци за пациентите, меѓуклиничко поврзување, управување со историјата на пациентот и фармацевтски апликации. Исто така, паметните договори сè повеќе се користат во развојот на разменливи и незаменливи токени, служејќи како практични примери за сценарија од реалниот свет.

Во тек се напори за развој на автоматизирани механизми способни да ги заштитат паметните договори од различни напади [164]. Дополнително, овие механизми имаат за цел автоматски да ги отстранат проблемите со паметните договори во случаи кога се појавуваат грешки без да бараат какви било модификации на внатрешната структура на паметниот договор. Истовремено, важно е паметниот договор да се заштити од различни надворешни закани во текот на целиот негов процес на извршување. Сепак, употребата на blockchain-технологијата, особено паметните договори, останува ограничена во неколку домени, вклучително и ВОУ. Постојат неколку фактори што придонесуваат за ова, вклучувајќи го и ограниченото усвојување на Солидити како програмски јазик за паметни договори. Прво, Солидити е релативно нов јазик и затоа има одредени ограничувања. Второ, значителен број програмери имаат мал интерес за развој на Солидити и паметни договори поради воочениот недостаток на профитабилност во споредба со другите активности поврзани со криптовалути. И на крај, непроменливоста на паметните договори поставува предизвици во различни

домени, бидејќи сите грешки идентификувани за време на извршувањето не можат да се поправат, туку напротив бараат уништување на договорот и целосно рестартирање на процесот. Во таков процес, трошокот е значителен [133]. Надминувањето на овие недостатоци може да се види во стандардизацијата на паметниот договор. Сепак, концептот на стандардизација опфаќа повеќе од само развој на стандарден паметен договор за одредени активности. Исто така, вклучува воспоставување стандардни услови за паметни договори, вклучувајќи барања, карактеристики и нивна употреба во различни контексти. Само темелно истражување на платформата и нејзината намена може да доведе до стандардизација на паметните договори.

Предложената архитектура на паметните договори што се користат во blockchain-системот за генерирање и проверка на дипломи е прикажана на Слика 6.6. Заедно со другите елементи, имаме дополнителни шест значајни паметни договори. *Кориснички интерфејс* (*User Interface)* служи како канал преку кој сите корисници се поврзани со blockchain-системот. *Регистрација на студентот* (*Student Registration)* опфаќа сеопфатно собирање на релевантни податоци потребни за издавање дипломи. Сите финансиски трансакции внатре во blockchain-системот, вклучувајќи го издавањето и проверката на дипломите, како и другите трансакции, ќе бидат олеснети исклучиво со паметниот договор *Исплати* (*Payment).* Концептот *Идентификација и дигитален потпис* (*Identification and Digital Signature)* е паметен договор што се фокусира на употребата на механизмите за идентификација од страна на корисниците во системот. Исто така, ја нагласува употребата на приватни клучеви или приватни дигитални потписи за потпишување електронски документи. Паметниот договор *Генерирање диплома* (*Generate Diploma)* е дизајниран да го олесни создавањето на дипломи, додека паметниот договор *Проверка на диплома* (*Verify Diploma)* служи за валидација на дипломите што ги стекнале студентите по завршувањето на нивните академски програми.



Слика 6.6. Архитектура на паметни договори

6.3. Дискусија за предложениот систем

Во овој дел се разгледуваат својствата на системот ДИАР, вклучувајќи ги неговите предности и ограничувања во однос на најсовремените други алтернативи. Има недостиг на сеопфатни научни студии што ги нагласуваат сложеноста на процесот, архитектурата, концептуалниот модел и програмските компоненти што се користат во практичната имплементација на паметните договори. Вреди да се одбележи дека во овој конкретен контекст, платформите Церберус (Cerberus) [111] и Верде (Verde) [84] беа користени како извори на мотивација во нашата работа. Овие платформи се детално опишани и обезбедуваат допирливи изгледи за практична примена. Предложениот

систем се карактеризира со неговата повеќеслојна мрежна архитектура, при што секое ниво инкорпорира различни техники за обработка на податоци. Овој дизајн ја подобрува безбедноста на шифрирањето на податоците, дешифрирањето и преносот во складирање надвор од синџирот за подолги периоди. Темелно се разгледани неопходните чекори за вметнување податоци во blockchain-складирање, вклучувајќи ги правните и софтверските протоколи. Дополнително, внимателно се испитани придружните средини потребни за успешно извршување на паметниот договор. Преостанатата задача вклучува кодирање на паметните договори и утврдување на нивната компатибилност со blockchain системот за складирање на податоците што ќе се тестираат. Табела 12 ги прикажува атрибутите на blockchain-системите, заедно со нивните соодветни објаснувања. Понатаму, обезбедена е систематска архитектура на нашиот систем, што ги означува слоевите што ја вклучуваат секоја карактеристика.

Табела 12. Опис на карактеристиките на системите базирани на blockchain вклучувајќи го и ДИАР-системот

Карактеристики	**Опис**	**Предложен blockchain-систем**
Контрола и авторитет	Децентрализирана власт, нема посредници, податоците се контролирани од мрежните јазли	Слој за идентитет и пристап
Транспарентност	Сите трансакции се транспарентни, постојат механизми што ја штитат злоупотребата	Ethereum blockchain, on-chain blockchain
Доверба и сигурност	Безбедноста се дистрибуира до секој јазол, постои ризик од напад на индивидуален јазол, довербата на луѓето е поголема	Слој на безбедносни механизми, blockchain во синџир
Трошоци и одржување	Одржување по повисоки трошоци за подолг временски период	Слој на апликација и кориснички интерфејс
Приспособливост	Поскалабилна, паралелна обработка во јазли	Мрежен слој
Грешки и напади	Дури и ако некој мрежен јазол е нападнат, системот работи нормално	Мрежен слој, слој на безбедносни механизми
Ефикасност и брзо извршување	Не се многу ефикасни поради механизмите за консензус	Етериум blockchain, on-chain blockchain
Донесување одлуки	Тоа зависи од одлуките на сите јазли што се дел од мрежата	Управување со blockchain систем, Етериум blockchain, безбедносни механизми, blockchain на синџир

Непроменливост	Податоците се непроменливи и не можат да се менуваат за време на процесот на извршување	Слој на податоци, системско управување, blockchain во синџир, складирање надвор од синџирот
Следливост	Секој јазол има дистрибуирана книга, покрај историјата на дневникот, ја зачувува и историјата на другите јазли	Складирање надвор од синџирот, слој на консензус, слој на податоци, управување со blockchain-систем

Со овој дел имавме за цел да ја објасниме систематската рамка на blockchain-системот. Ова подразбира разграничување на основните нивоа што го сочинуваат blockchain-системот, заедно со релевантните делови што може да се интегрираат во секој слој. Blockchain-системот ќе обезбеди зголемена безбедност и приватност на податоците со елиминирање на посредниците за време на преносот на податоци и спречување на неовластен пристап до базата на податоци. За разлика од централизираните системи, каде што администраторот има привилегиран пристап до сите услуги, blockchain-системот ќе обезбеди повисоко ниво на безбедност и валидација. Системот на blockchain за шифрирање податоци ќе го користи алгоритмот АЕС (AES) со комбинација на СХА256 (SHA256), иако другите алтернативи предвидени во архитектурата не се исклучени. Безбедноста на системот зависи и од механизмите за консензус, валидацијата и проверката на трансакциите, безбедноста на паметните договори и нивното безбедно извршување, приватноста, ревизијата и следењето. Процесот на валидација има значајна важност во обезбедувањето на безбедноста на секој даден процес. Оттука, концептот на валидација ќе опфати неколку аспекти, како што се валидација на мрежниот блок, валидација на трансакцијата, валидација на токени и валидација на паметни договори. Покрај тоа, механизмот за консензус, исто така, игра посебна улога во валидацијата, што всушност го претставува договорот што јазлите го постигнуваат меѓу себе за тоа како ќе соработуваат меѓу себе [165]. Инаку, валидаторите се дел од on-chain blockchain, бидејќи тие се присутни во секој процес што се спроведува во рамките на blockchain-мрежата.

Во однос на следливоста и идентитетот, blockchain-системот нуди можност секоја услуга што се извршува да му биде позната на авторот на услугата; дури се прават обиди да се прекине извршувањето на паметниот договор или да се предупреди системот при неовластен пристап. Blockchain-технологијата нуди механизми за создавање методи за генерирање на самиот идентитет без потреба од интервенција од трета страна, но самиот корисник го избира методот на идентификација, што го складира во складиштето на blockchain. Blockchain-системите во ВОУ имаат потенцијал да го поддржат интегритетот преку непроменливоста и децентрализација.

Имплементацијата на blockchain-технологијата обезбедува паметните договори да останат непроменливи, а со тоа да се поттикне стандардизацијата на овие договори. Децентрализацијата е, исто така, многу важна за безбедноста на податоците бидејќи дозволува независни процеси и го ограничува пристапот до складирање на blockchain [141].

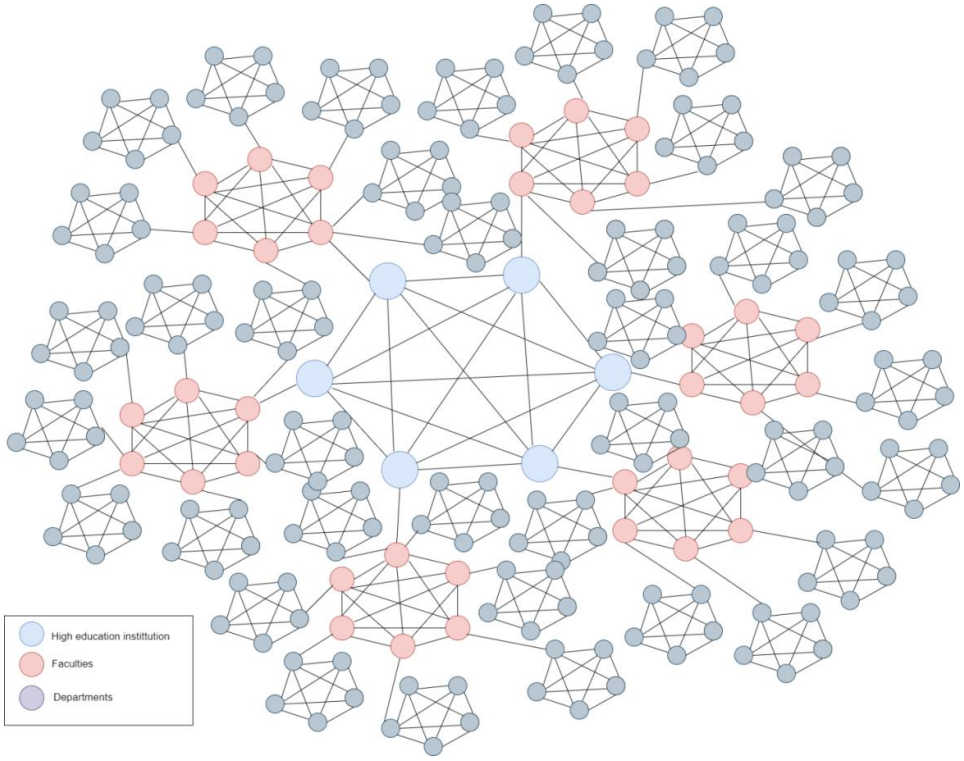
Идејата што се поставува нуди многу придобивки во врска со безбедноста, механизмите за консензус и употребата на функции во синџирот, што се клучни за подобрување на оперативната ефикасност на системот. Една придобивка од нашиот предлог е можноста студентите да го приспособат својот начин на идентификација во системот за потпишување документи, особено дипломи, покрај можноста за користење дигитален потпис. Ова вклучува употреба на интелигентни агенти. Системот Верде (Verde) ја инкорпорира токенизацијата како клучна процедура во рамките на неговите механизми за консензус и безбедносен слој. Слично на тоа, системот Церберус (Cerberus) има заеднички карактеристики во однос на неговиот дизајн и концептуален модел.

Иако blockchain-системот за ВОУ би бил иновација, нудејќи услуги што до денес не се применуваат во дигитална форма, тој сепак има ограничувања, вклучувајќи го и предложениот систем. Еден од предизвиците одговара на релативно побавната брзина на трансакцијата во blockchain-мрежите во споредба со постоечките системи што користат високоефикасни механизми за обработка на податоци. Времето потребно за генерирање резултати во blockchain-мрежите е значително подолго, бидејќи зависи од специфичната платформа и дополнителната опрема што се користи. Ова првенствено се должи на инхерентната природа што одзема многу време на обработката на податоците во самата мрежа. Одржувањето е уште еден предизвик, бидејќи ќе го одржува истиот администратор на централизираниот систем, или ќе треба да го одржува специјализирана приватна компанија, при што месечните трошоци може да го надминат дури и централизираниот систем.

По целосното дизајнирање концептуален модел, систематската архитектура на процесот на генерирање и верификација на дипломите, и дизајнот на архитектурата на паметните договори, исполнети се условите за создавање прототип со кој конкретно ќе го тестираме процесот на генерирање и верификација на дипломата, бидејќи создавањето сеопфатна платформа во високообразовна институција бара многу трошоци и подолга тимска работа. Затоа преку прототипот ќе се обидеме да го објасниме она што го кажавме за blockchain-системите, за во иднина да го прошириме уште повеќе, до вистинска имплементација во ВОУ.

7. ИМПЛЕМЕНТАЦИЈА НА ПРОТОТИП ЗА ГЕНЕРИРАЊЕ И ПРОВЕРКА НА ДИПЛОМИ

Почнувајќи од фактот дека повеќе од креираните системи што ги користеле различни истражувачи користеле централизирани бази на податоци, тргнавме од овој факт за да создадеме најпрво прототип базиран на програмските јазици Пајтон, Ноде.јс и МонгоДБ (Python, Node.js и MongoDB), само за да ја покажеме разликата и да ги опишеме предностите и недостатоците помеѓу двата системи, централизираниот и децентрализираниот, што всушност теоретски ги опишавме и во горните поглавја. Создавањето blockchain-систем за генерирање и проверка на дипломи може да се имплементира во рамките на оддел на ВОУ, може да се имплементира во целата ВОУ со поврзување на сите катедри во blockchain-мрежа, но може да се имплементира и низ целата земја, креирајќи поширока мрежа на сите јавни и приватни ВОУ што би олесниле многу работи помеѓу студентите, професорите и академскиот кадар. Сликата 7.1. покажува како би изгледала blockchain-мрежа со повеќе ВОУ поврзани еден со друг, со соодветните факултети и катедри.



Слика 7.1. Blockchain-мрежа на blockchain-системот за повеќе ВОУ

7.1. Создавање системски прототип за генерирање и проверка на дипломи на централизиран начин

Пред да започнеме со описот на централизираниот прототип, накратко ќе ја елаборираме важноста на Пајтон, МонгоДБ и Ноде.јс (Python, MongoDB и Node.js), со кои создадовме едноставен прототип со кој генерираме и проверуваме академски дипломи.

Ноде.јс (Node.js) е опкружување за извршување на Јаваскрипт (JavaScript) од страна на серверот што им овозможува на програмерите да градат скалабилни и мрежни апликации со високи перформанси. Користи event-driven, неблокирачки И/О (I/O) модел, што го прави лесен и ефикасен, совршен за апликации во реално време со интензивни податоци. Ноде.јс (Node.js) може да се користи во неколку улоги на системите. Node.js служи како основа за развој на задниот дел на системот. Обезбедува *runtime* средина за извршување на код од страна на серверот напишан во Јаваскрипт (JavaScript). Ноде.јс (Node.js) може да креира HTTP сервери кои се справуваат со дојдовни HTTP барања од клиенти. Овие барања може да вклучуваат активности како што се запишување студент, генерирање диплома или проверка на информации за студентот. Со Ноде.јс (Node.js), можете да дефинирате рути и среден софтвер за справување со различни типови барања. На пример, ПОСТ (POST) бара запишување студенти и ГЕТ (GET) барања за проверка на информациите за студентите. Ноде.јс (Node.js) може да се поврзе со бази на податоци како што е МонгоДБ (MongoDB) за складирање и преземање податоци за студенти, информации за дипломи и записи за проверка. Користи асинхрони операции, овозможувајќи истовремено да се извршуваат повеќе барања за базата на податоци без да се блокира серверот. Заднинската логика на системот, како што е генерирање дипломи засновани на информации за студентите, проверка на студентските ингеренции и управување со автентикација на корисникот, се имплементира со помош на функциите Јаваскрипт (JavaScript) што се извршуваат на Ноде.јс (Node.js). Најчесто се користи за изградба на РЕСТФул АПИ (RESTful API) (интерфејси за програмирање на апликации) што овозможуваат комуникација помеѓу предниот дел и задниот дел на системот. API ги дефинираат крајните точки и форматите на податоци за размена на информации помеѓу различни компоненти на системот. За системот за генерирање и проверка на студентски дипломи, задниот дел на Ноде.јс (Node.js) ги изложува крајните точки за дејства како што се запишување студенти, генерирање дипломи и проверка на студентски акредитиви. Ноде.јс (Node.js) е добро приспособен за апликации за комуникација во реално време, благодарение на архитектурата управувана од настани и поддршката за Вебсокетс (WebSockets). Иако комуникацијата во реално време можеби не е примарен услов за генерирање дипломи и систем за проверка, може да биде од корист за функции како што се инстант известувања или ажурирања во врска со статусот на барањата за дипломи. Ноде.јс (Node.js) беспрекорно се интегрира со предните технологии како Реакт, Ангјулар или

Bjy.jc (React, Angular или Vue.js). Ова овозможува унифициран stack за развој, каде што компонентите на предниот и на задниот дел се напишани во Јаваскрипт (JavaScript), со што се олеснува повторната употреба на кодот, одржливоста и продуктивноста на развивачите на системите [166].

Пајтон (Python) е програмски јазик на високо ниво, со отворен код, објектно-ориентиран, и употребан за општа намена. Главните предности од користењето на Python што го прават толку моќен и распространет програмски јазик се:

- има интуитивна синтакса што наликува на природен англиски јазик и затоа е лесен за учење, особено за луѓе што влегуваат во светот на програмирањето;
- поради синтаксата погодна за луѓето, лесно е да се пишува, чита и дебагира;
- обезбедува обемна стандардна библиотека и широк избор на добро документирани и сеопфатни дополнителни библиотеки и модули;
- бесплатен е и за поединци и за бизниси;
- благодарение на огромната заедница за поддршка, Пајтон (Python) постојано се развива, се подобрува и се проширува;
- може да се интегрира во кој било проект и да се користи за решавање напредни проблеми;
- бидејќи е јазик за општа намена, тој има различни примени во многу сфери [167].

Пајтон (Python) може да се користи за автоматизирање на генерирањето на студентски дипломи врз основа на претходно дефинирани шаблони и информации за студентите. Библиотеки како Рипортлаб (ReportLab) или Пипдф2 (PyPDF2) им овозможуваат на развивачите да креираат програмски, пдф-документи, што овозможува генерирање на приспособени дипломи со динамична содржина како имиња на студентите, датуми и академски постигнувања. Python игра клучна улога во имплементирањето на механизми за верификација за осигурување на автентичноста на студентските дипломи и академските кредити. Ова може да вклучува криптографски техники како дигитални потписи или функции за хаш за обезбедување на документите за диплома и спречување на манипулација. Библиотеки пајтон како криптографи (cryptography) или хашлиб (hashlib) можат да се искористат за имплементација на овие безбедносни мерки. Екосистемот на библиотеки на Пајтон (Python), како што се пандас (pandas), матплотлиб (matplotlib) и сеаборн (seaborn) може да се искористи за анализа на податоци и известување. Ова овозможува на заинтересираните страни да добијат идеи за трендовите на запишување на студентите, стапките на издавање на дипломи и успешноста на верификацијата, што овозможува донесување одлуки базирани на податоци [168].

МонгоДБ (MongoDB) е документ-ориентирана, НоСКЛ-база (NoSQL) на податоци што обезбедува флексибилно зачувување и манипулација на податоци. Наместо традиционалните табеларни структури, МонгоДБ (MongoDB) зачувува податоци во ЈСОН (JSON) подобни документи, што ги прави посебно погодни за

апликации со динамичка структура на податоци или апликации што се развиваат во променливиот околен свет на веб и мобилните апликации. МонгоДБ може да биде искористен за зачувување на информации за студентите, како што се нивните имиња, броеви на дипломи, датуми на дипломирање и други детали. Поради тоа што МонгоДБ е флексибилен, документите може да се обогатат со различни полиња во зависност од потребите на апликацијата. МонгоДБ може да биде искористен за зачувување записи за верификација на дипломите. Овие записи може да вклучуваат информации како што се датумот на верификација, резултатот од верификацијата и дополнителни детали за студентот и дипломата. МонгоДБ нуди голема флексибилност и скалабилност, што го прави погоден за апликации се развиваат и растат во време. Со МонгоДБ, може лесно да се додаваат нови атрибути во документите или да се променуваат моделите на податоци во согласност со новите потреби на апликацијата [169].

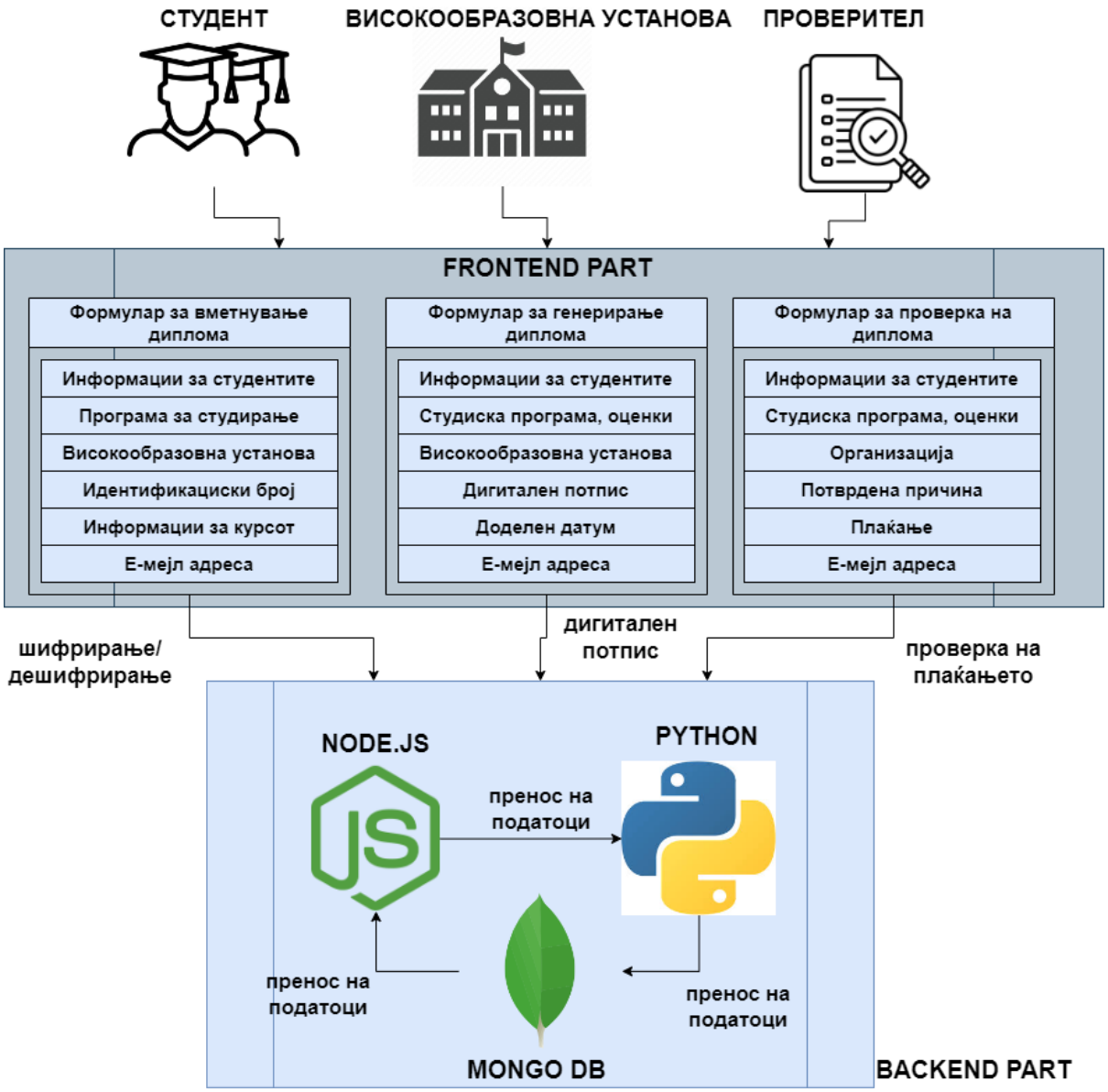
Внесувањето на податоците во базата, што е неопходно за генерирање и проверка на податоците од диплома, ќе се врши преку програмскиот јазик Пајтон. Најпрво се прави врска со главниот драјвер на Пајтон (pymongo), што ни овозможува да ги увеземе класите што ќе ги користиме во системот и истовремено го поврзува програмскиот јазик со базата на податоци МонгоДБ. Врзувањето се прави со назначување на локалниот хост што ќе се користи на соодветниот сервер, базата на податоци и соодветната табела или колекцијата на податоци. Потоа податоците се вметнуваат врз основа на релевантните функции што овозможуваат вметнување во зависност од колекциите што ги создадовме. За време на секое вметнување на податоци, истото го поврзуваме со уникатен ИД на секој запис што е вметнат во базата на податоци.

Многу е важно да се нагласи дека МонгоДБ е многу различен од традиционалните централизирани бази на податоци. МонгоДБ е НоСКЛ база на податоци, што користи документ-ориентиран модел за складирање на податоци (а не табеларен модел). МонгоДБ нема строга шема и дозволува флексибилност во дизајнот на податоците, додека традиционалните дата-бази имат строга шема што треба претходно да се дизајнира и имплементира. Со други зборови МонгоДБ е многу подобра за системи каде што има потреба од флексибилност и скалабилност на податоците. Откако податоците ќе се вметнат во базата на податоци, тие може да се генерираат преку Пајтон или Ноде.јс., генерирајќи дипломи за секој студент, или во форма на извештаи, во пдф или дури и во форма користејќи директно дигитален потпис на самиот ВОУ. Генерирањето очигледно се прави во зависност од шаблонот што го користи самиот ВОУ, дизајнирајќи го со сите потребни елементи што треба да бидат јавни.

Додека проверката на дипломите што се веќе вметнати може да ја врши верификаторот, па дури и самата универзитетска администрација, во дизајнираниот систем, каде што едноставно врз основа на бројот на дипломата, па дури и ИД-бројот што треба да ја има самата диплома, може да се бара дали таа диплома е валидна или не.

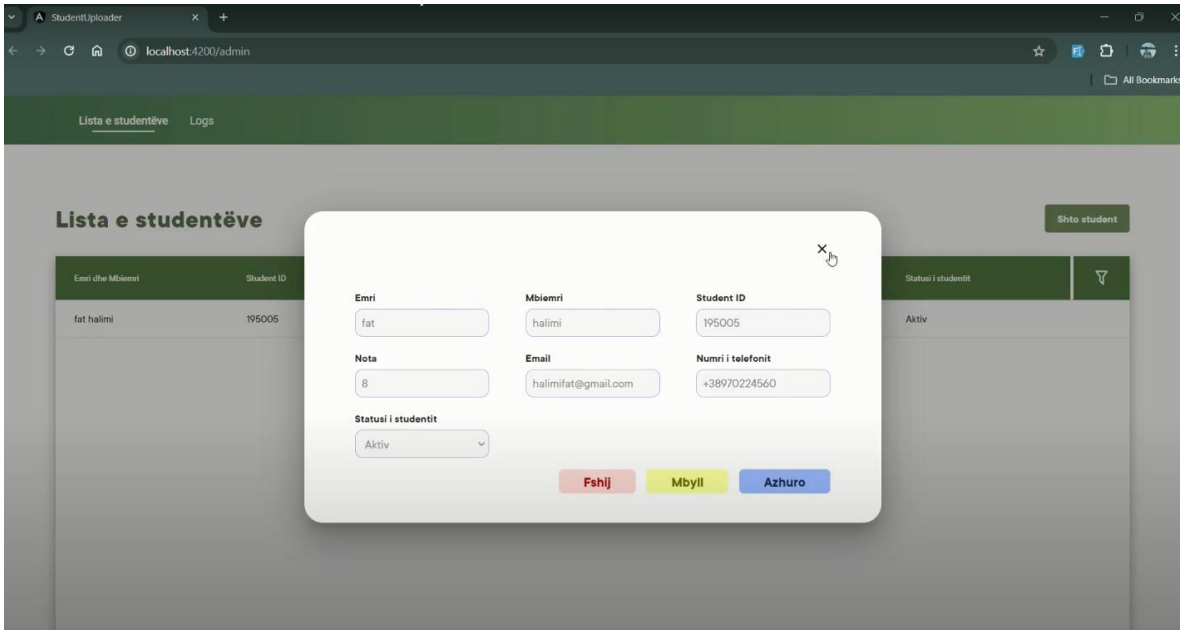
Преку програмата можеме да ја направиме секоја промена во базата преку системот, да го информираме раководството и другите лица одговорни за дипломите. Известувањето може да се изврши или преку известување преку е-пошта, или дури и самото известување на сметката на одговорните лица. Овој метод се обидува да го зачува интегритетот на податоците на студентите.

Меѓутоа, ако промените се случат директно во базата на податоци, каде што нема пристап освен за администраторите и луѓето што го одржуваат системот, тогаш таквата промена нема да се забележи, што ја прави сомнителна употребата на централизираните системи. Промената може да се открие, но потребни се детални проверки од ИТ експерти, што бара дополнително време, труд и трошоци. Затоа, употребата на централизирани системи, и покрај предностите во генерирањето, проверката, можноста за ажурирање на податоците што биле погрешни, има недостатоци во зачувувањето на идентитетот, приватноста и транспарентноста на услугите, што ја прави сомнителна за употреба во средини каде што имаме приватни информации. Иако при генерирањето и верификацијата на дипломите може да се користат и криптографски алгоритми за шифрирање и дешифрирање на податоците, повторно тоа не ја спречува можноста за модификација на податоците директно од базата, што несомнено би можело да го направи ИТ експерт. Затоа, не случајно, до денес немаме никаков случај на генерирање и проверка на дипломи во дигитална форма, во ниту еден веб систем на било кој ВОУ која се користи за генерирање и проверка на дипломи. Сите ВОУ користат дигитални системи за управување со дипломи, што ги користи само академскиот кадар, за да се олесни работата при генерирање, печатење и барање информации што им се потребни. Слика 7.2. дава поедноставен приказ на работата на централизираниот систем, опишувајќи го предниот дел, што всушност го претставува системот дизајниран за корисници, како што се студенти, академски кадар и проверувачи. Заднинскиот дел е всушност Пајтон, Ноде.јс и МонгоДБ кои имаат интеракција меѓу себе во зависност од фактот дека е потребно вметнување, генерирање или проверка на дипломите на студентите.



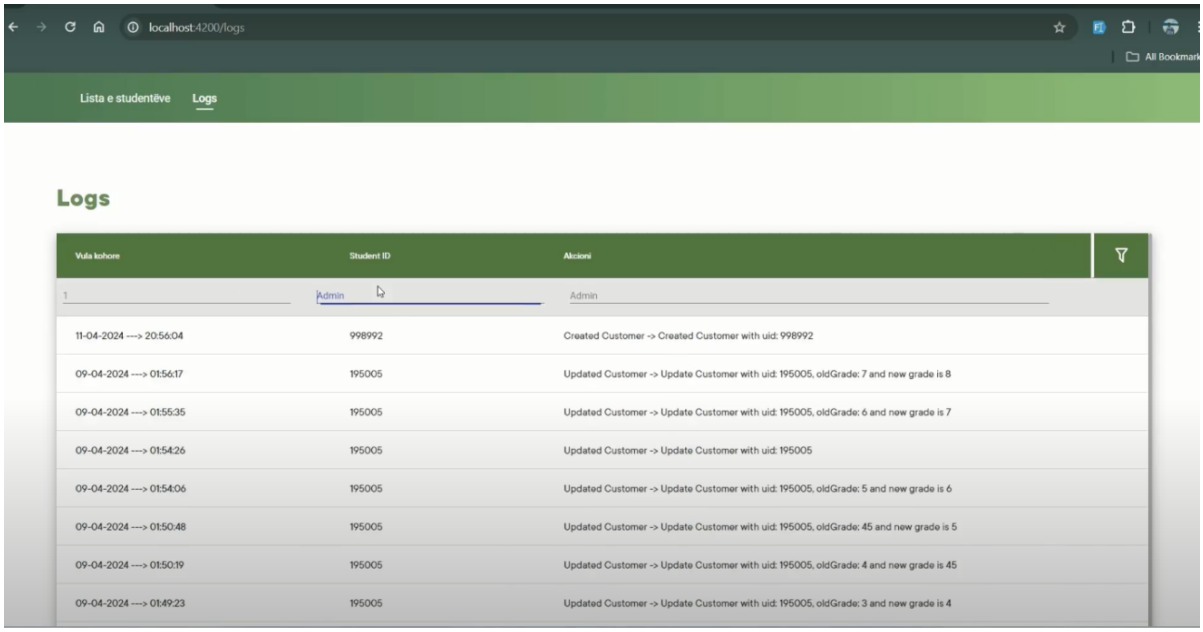
Слика 7.2. Поедноставен приказ на работата на централизираниот систем

Прототипот што е креиран за генерирање и проверка на дипломи, на централизиран начин, е создаден во наједноставна форма за да се разјасни разликата и во исто време можностите на централизиран систем. Со помош на Ноде.јс (Node.js) се врши вметнување, бришење и ажурирање на податоците во системот. Слика 7.3. го претставува системскиот интерфејс што го прикажува овој дел.



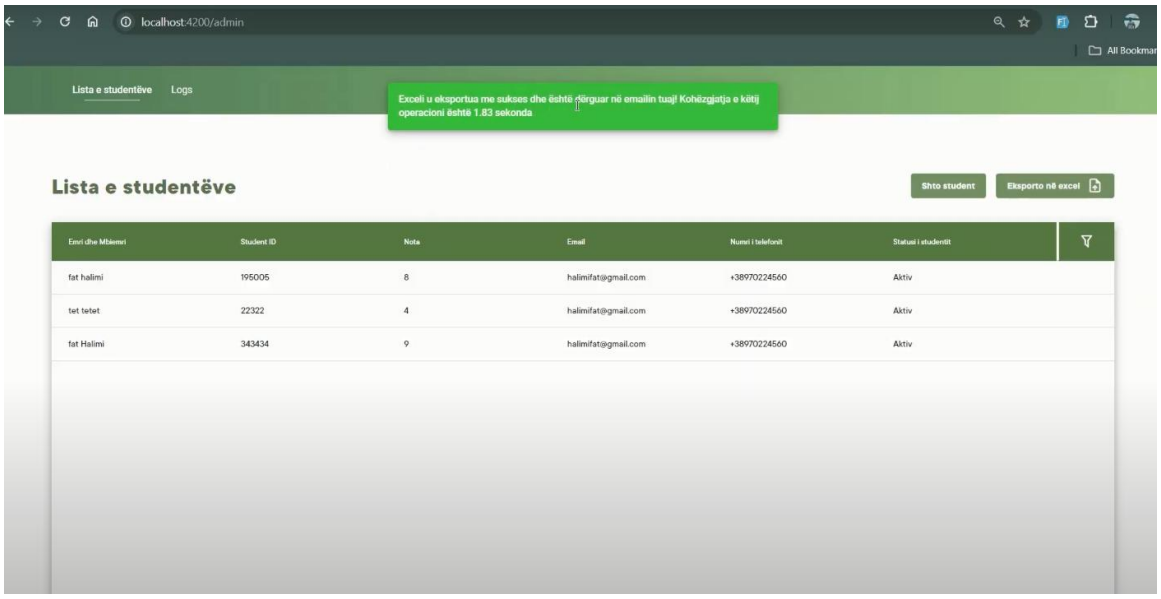
Слика 7.3. Вметнување, ажурирање и бришење податоци преку системот

Секоја промена во системот, без разлика дали е бришење, ажурирање или дури и вметнување, се зачувува во дневникот на администраторите, како што е прикажано на слика 7.4. Исто така, секоја промена, во зависност од тоа каде е направена промената во оценката или на кој студент, истовремено ги известува администраторот, студентот и соодветниот професор по електронска пошта за направената промена.



Слика 7.4. Дневникот на администраторите

Со користење на Пајтон (Python), се прави генерирањето на дипломи, било во ПДФ или други можни апликации (пр. Ексел), бидејќи МонгоДБ е полуструктурирана база на податоци, а во Ексел податоците излегуваат во поструктурирана форма. Исто така, и за генерирањето на дипломите, системот ги известува студентот и менаџментот на ВОУ, не само во дневникот на системот, но и во нивните е-пошти што се потврдени. На Слика 7.5. претставен е интерфејсот за генерирање дипломи преку копчето шифрирано во Пајтон.



Слика 7.5. Генерирање на дипломи во ПДФ или Ексел

Додека Пајтон, Ноде.јс и МонгоДБ (Python, Node.js и MongoDB) се популарни технологии, секоја од нив има свој сет на недостатоци кога се користи во систем за генерирање и проверка на дипломи. Што се однесува до недостатоците на Пајтон, меѓу најважните се:

- Пајтон (Python) е интерпретиран јазик, што може да го направи сситемотпобавен во споредба со компајлираните јазици како C++ или Јава (Java). Ова може да биде загрижувачко ако системот треба да се справи со голем обем на барања или сложени пресметки.
- Python's Global Interpreter Lock (GIL) може да ги ограничи перформансите на апликациите со повеќе *threads*, што потенцијално ќе влијае на истовременоста и приспособливоста.
- Управувањето со зависноста на Пајтон понекогаш може да биде предизвик, особено кога се работи со конфликтни зависности или проблеми со компатибилноста на верзии.

- Динамичното пишување и флексибилноста на Пајтон може да го направи повеќе склон кон одредени видови безбедносни пропусти доколку не се користи внимателно.

Што се однесува до недостатоците на Ноде.јс (Node.js), меѓу најважните се:

- Иако Ноде.јс (Node.js) е многу ефикасен за ракување со операции поврзани со влез/излез, тој не е толку погоден за задачи интензивни на процесорот поради неговата природа со една *thread*. Ова може да биде ограничување ако системот на диплома вклучува тешки пресметковни задачи.
- Иако Ноде.јс (Node.js) е познат по своите перформанси во задачи поврзани со И/О (I/O), тој можеби не е најдобриот избор за операции врзани за процесорот поради неговата неблокирачка природа управувана од настани.
- Управувањето со зависности со нпм (npm — менаџер на пакети Ноде.јс) може да доведе до проблеми со ширење на зависноста, конфликти на верзии и безбедносни пропусти ако не се управува правилно.

Што се однесува до недостатоците на МонгоДБ, меѓу најважните се:

- МонгоДБ е НоСКЛ база на податоци, што значи дека нема цврста структура на шема на традиционалните релациски бази на податоци. Иако оваа флексибилност може да биде поволна, таа исто така бара внимателен дизајн за да се обезбеди конзистентност и интегритет на податоците, особено во системот на диплома каде што точноста на податоците е од клучно значење.
- Неподдржувањето на МонгоДБ за трансакции и приклучоци може да биде неповолна положба во сценарија каде што се потребни сложени манипулации со податоци или атомски операции.
- Додека МонгоДБ може хоризонтално да се скалира со додавање повеќе јазли во кластерот, управувањето и скалирањето на дистрибуираната МонгоДБ околина може да биде сложено во споредба со традиционалните релациски бази на податоци.
- МонгоДБ жртвува некои својства (атомичност, конзистентност, изолација, издржливост) во корист на перформансите и приспособливоста, што можеби не е идеално за апликации каде строгата конзистентност на податоците е најважна, како, на пример, во системот за верификација на дипломи.

Сумирано, додека Пајтон, Ноде.јс и МонгоДБ (Python, Node.js и MongoDB) нудат многу предности и се широко користени во различни апликации, тие исто така имаат свои ограничувања и размислувања што треба да се земат предвид при дизајнирање и имплементација на систем за генерирање и потврдување дипломи.

7.2. Имплементација на blockchain-прототип за генерирање и проверка на дипломи

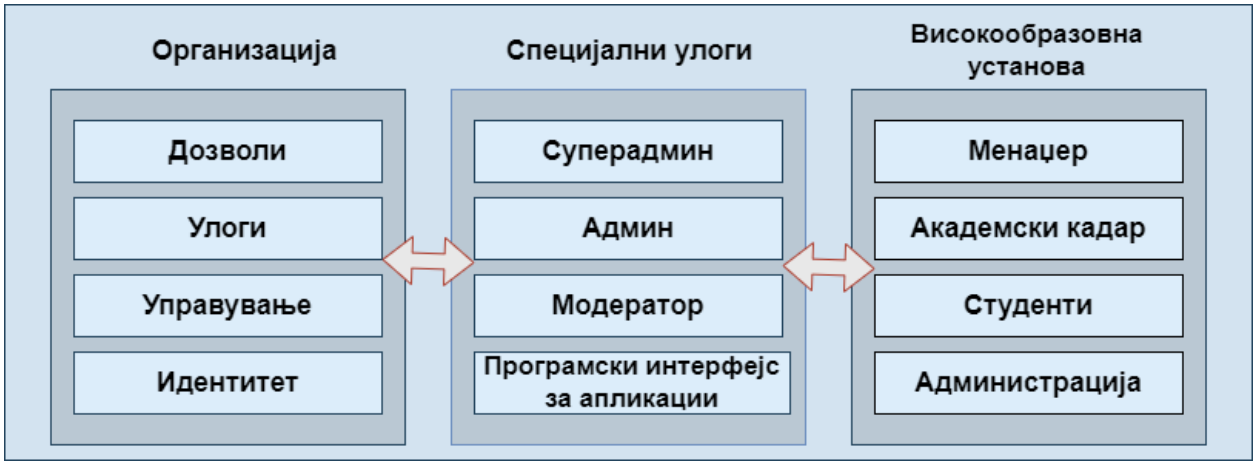
Централизираните системи може да бидат побрзи во извршувањето на програмата, можат да бидат полесни за користење, со помала опрема за извршување, но безбедноста, приватноста и транспарентноста на услугите не се на вистинското ниво, особено кога станува збор за генерирање и проверка на дипломи, како важни документи. Од таа причина, единствена можност за обезбедување безбедност, целосна дигитализација на услугите за генерирање и проверка на дипломи и други документи во ВОУ се само blockchain-системи и blockchain-бази на податоци што нудат децентрализиран начин на функционирање и нивно дешифрирање чини многу пари и стотици години време, што всушност ја претставува нивната неможност за дешифрирање.

Прототипот што е креиран е во blockchain, иако е посветен на еден факултет, па дури и на катедра, може да се прошири во иднина, за да се создаде поширока blockchain-мрежа меѓу сите приватни и јавни ВОУ во земјата. Преку прототипот, се прикажани некои уникатни карактеристики што ги има blockchain-системот и коишто се разликуваат од централизираните системи, а тоа се децентрализиран дигитален идентитет, запознај го твојот корисник (Know Your Customer- KYC) за повеќекратна употреба, децентрализирано управување со доверба, доказ за идентитет.

Првично, за да го користи blockchain-системот, корисникот мора да го создаде својот единствен идентитет, преку методи на самосуверен идентитет, овозможувајќи му на корисникот децентрализиран, независен метод за создавање идентитет. Системот им дава на корисниците целосна контрола врз нивните лични податоци. Корисниците може безбедно да управуваат со нивните податоци за идентитетот, вклучувајќи ги личните податоци, ингеренциите и проверките, на blockchain. Овој децентрализиран пристап ја елиминира потребата од централни авторитети за идентитетот, осигурувајќи дека корисниците се единствените сопственици на нивниот дигитален идентитет.

Што се однесува до организацијата на системот и дефинираните улоги во системот, има вкупно 4, меѓу кои: суперадмин, админ, модератор и интерфејс за програмирање апликации (API). Суперадмин (Superadmin) е највисокото ниво на системска организација, што дури може да ја избрише целата системска организација, да додаде или да постави одредени дозволи за корисникот на системот. Потоа, админот има право да ги ажурира деталите за организацијата веќе создадени од суперадминот, да ги ажурира улогите на членовите на организацијата. Во една ВОУ таква улога може да има самото раководство на ВОУ. Модераторот има право да повика членови или дури да брише членови на организацијата создадена од суперадминот.

А последното ниво на организација е можноста за поврзување на оваа организација со системот (API). Односно, овде учествуваат студенти, професори, академски кадар, со кои можат да креираат, читаат, бришат податоци за нивната лична сметка. Слика 7.6. дава опис на главните улоги на системот, организацијата на системот и главните актери во ВОУ.



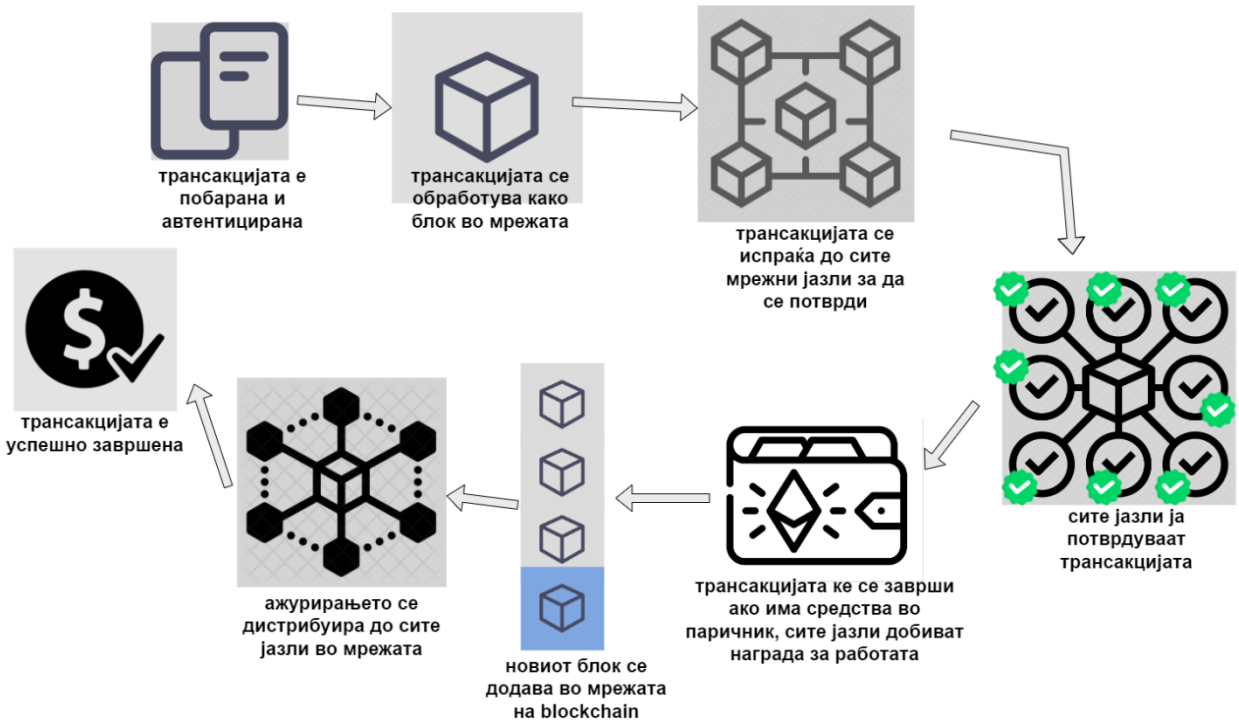
Слика 7.6. Организација на улоги на blockchain-системот

Мошне важно при креирањето на сметката е верификацијата на адресата на е-пошта и вашата сметка мора да биде потврдена преку процесот Запознај го твојот корисник (Know Your Customer -KYC), што е збир на процедури и протоколи што ги користат бизнисите и финансиските институции за да го потврдат идентитетот на нивните клиенти. Процесот на КИК (KYC) вклучува собирање лични информации и документи од клиентите за да се обезбеди усогласеност со регулаторните барања и да се ублажат ризиците поврзани со измама, перење пари, финансирање тероризам и други незаконски активности. Процесот обично ги вклучува следните чекори:

- **Поставување документи:** корисниците ги поставуваат своите лични документи на платформата базирана на blockchain. Овие документи може да вклучуваат лични документи (како пасоши, возачки дозволи или национални лични карти), доказ за адреса (како сметки за комунални услуги или изводи од банка) и сите други потребни документи.
- **Хаширање на документи:** поставените документи се хашираат, создавајќи единствен дигитален отпечаток од прст за секој документ. Хаширањето вклучува користење на алгоритам за претворање на содржината на документот во низа знаци со фиксна должина. Овој хаш е уникатен за документот и не може да се направи обратно за да се открие оригиналниот документ.

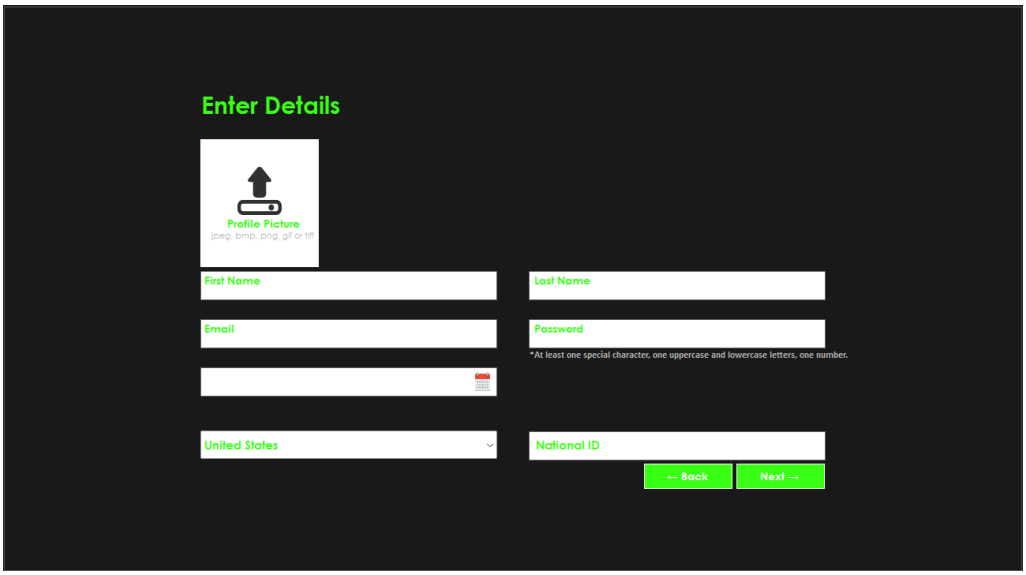
- **Децентрализирано складирање:** документите се чуваат на децентрализиран начин, обично користејќи шифрирани решенија за складирање или дистрибуирани датотечни системи. Ова осигурува дека корисниците имаат контрола врз сопствените податоци и дека ниту еден ентитет нема пристап до сите документи.
- **Шифрирање и приватност:** за заштита на приватноста на корисниците, чувствителните информации во документите може да се шифрираат пред складирањето. Корисниците ја задржуваат контролата врз клучевите за шифрирање, осигурувајќи дека само овластени страни можат да пристапат до нивните информации.
- **Дозволен пристап:** Корисниците им даваат дозвола на овластените страни, како што се банките или финансиските институции, да пристапат до нивните проверени документи. Правата за пристап се управуваат со помош на паметни договори или криптографски клучеви, со што се обезбедува дека само одобрените ентитети може да ги гледаат документите.
- **Верификација и валидација:** Овластените страни можат да ја потврдат автентичноста на документите со споредување на хашовите на документите зачувани на blockchain со вистинските документи обезбедени од корисникот. Ова им овозможува да потврдат дека документите не се манипулирани и дека се оригинални.
- **Проверки на усогласеност:** системот КИК (KYC) базиран на blockchain може да вклучи проверки на усогласеност за да се осигури дека процесот на верификација ги исполнува регулаторните барања, како што се законите за спречување на перење пари АМЛ (AML) и за борба против финансирање тероризам ЦТФ (CTF). Ова може да вклучува проверка на корисниците во однос на списоците за следење на санкционирани поединци или субјекти.
- **Корисничка контрола и согласност:** корисниците ја одржуваат контролата врз сопствените податоци и можат да ја отповикаат дозволата за пристап во секое време. Тие имаат целосна видливост до која страните пристапиле до нивните документи и можат да ја следат употребата за да обезбедат усогласеност со прописите за приватност [170].

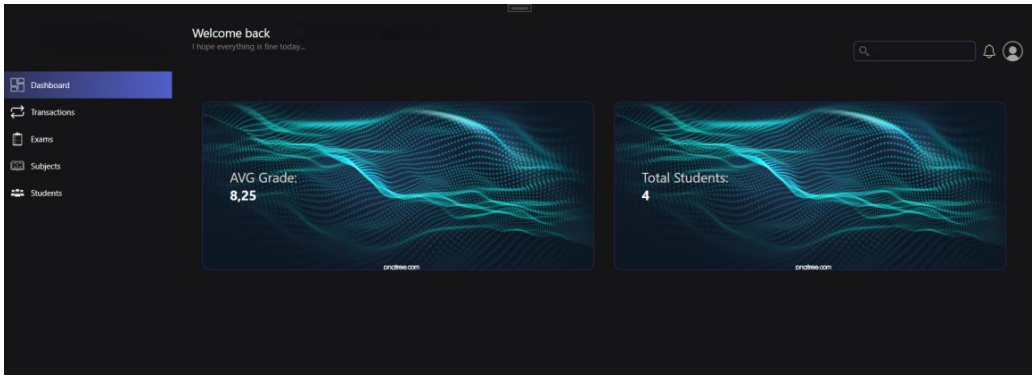
Кога имаме blockchain-мрежа, со повеќе јазли во мрежата, како што е случајот со blockchain-системот за генерирање и проверка на дипломи, што значи повеќе корисници во blockchain-мрежата, мора да има поврзан договор за клуч од сите јазли за да се валидираат трансакциите и да ги синхронизирате сите копии на податоци во дистрибуираната книга. Дистрибуираните книги се отпорни на злонамерно однесување од страна на мал сет јазли, давајќи им високо пристапна и децентрализирана дигитална инфраструктура. Сепак, дистрибуирана леџер технологија има неколку негативни страни во врска со приспособливоста и приватноста. Blockchain се подмножество на ДЛТ и веројатно се најшироко користени [171]. Главната карактеристика на blockchain е тоа што трансакциите се здружуваат во блокови и секој блок од податоци ја носи вредноста на хашот од претходниот блок. На Сликата 7.7. е прикажан процесот на blockchain, односно обработка на трансакција, што во нашиот систем е генерирање на дипломата, или нејзина верификација.



Слика 7.7. Процесот на blockchain за реализација на трансакција (диплома)

Секој корисник на системот мора прво да креира сметка, а потоа да се најави. Слика 7.8. го прикажува интерфејсот за време на регистрацијата на корисникот и по најавувањето во системот.



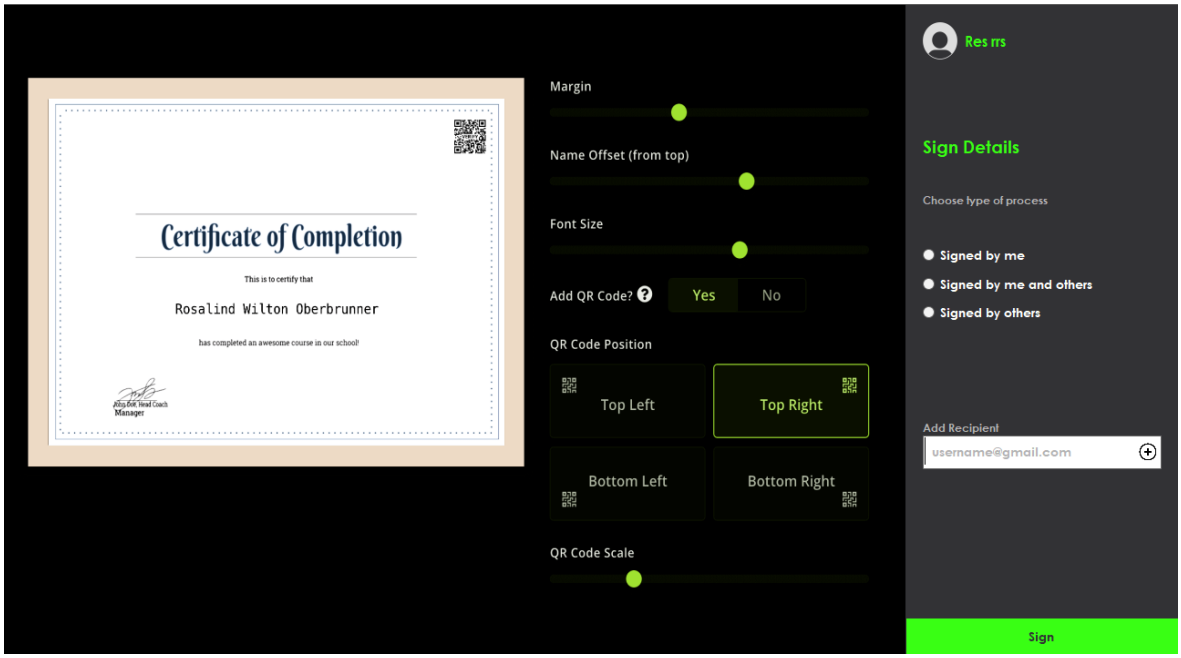


Слика 7.8. Интерфејс на регистрирање и логирање на blockchain-системот

7.3. Вметнување податоци во blockchain системот и генерирање дипломи

Вметнувањето податоци во blockchain системот е тежок процес, бидејќи секој податок мора да биде добро контролиран и само откако ќе заврши процесот на распоредување на паметни договори не може да се ажурираат, бидејќи самите паметни договори се карактеризираат со непроменливост како карактеристика и на blockchain технологијата. Вметнувањето на податоците во системот blockchain ќе биде направено преку платформата Етериум (Ethereum), користејќи го програмскиот јазик Солидити (Solidity), за распоредување на паметните договори. Системот првично ќе има пристап до студентот и раководството, во овој случај лица што припаѓаат на ВОУ, коишто за време на вметнување дипломи во базата на blockchain, ги имаат нивните соодветни улоги што мора дигитално да ја потпишат истата диплома пред да се зачува во базата на податоци. Самиот ВОУ, како админ во системот, има право да определи системски модератори, што ќе имаат право да додаваат, да гледаат и да обработуваат податоци до други актери, во овој случај дипломите до студенти.

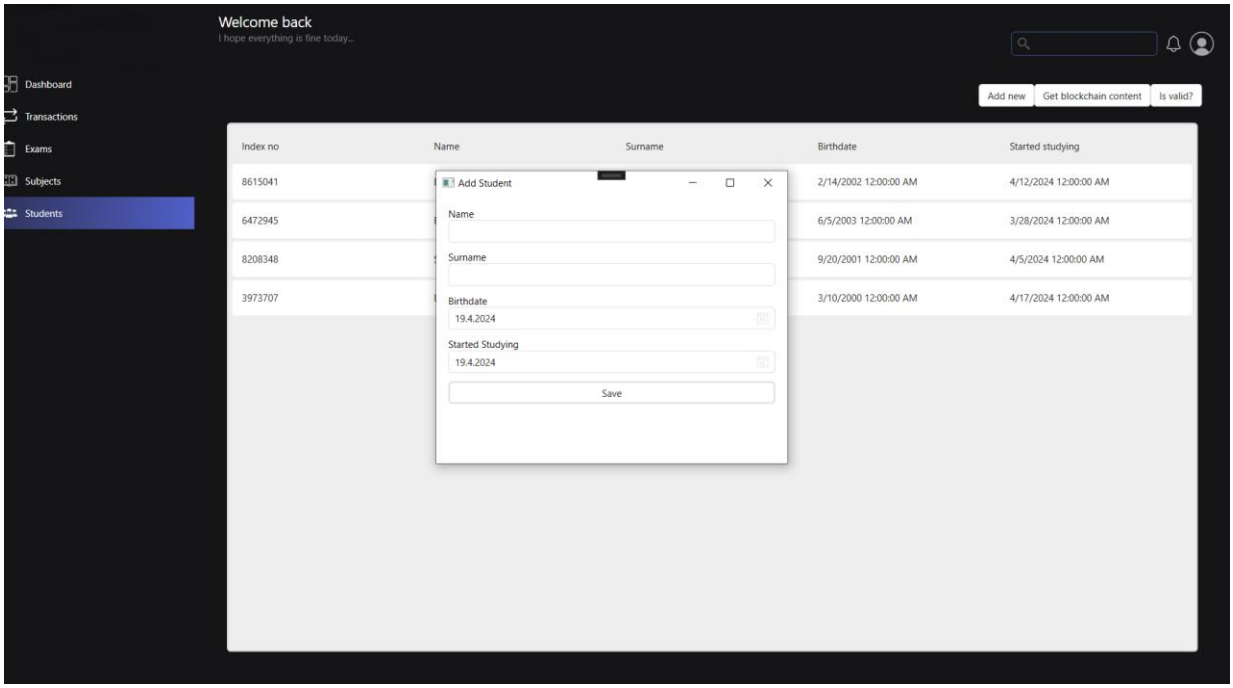
Идејата за функционирање на системот е при вметнувањето на дипломите, со соодветните податоци, откако тие ќе бидат потпишани во дигитална форма од раководството на ВОУ, таа да му се појави на студентот во системот на неговата сметка. Потоа студентот уште еднаш ја проверува дипломата за да нема можни грешки во неговите оценки и откако ќе ја потпише во дигитална форма, со отпечаток или потпис со помош на специјални алатки, како да се потпишува на физичка хартија, по потпишувањето, ќе има опција да кликне на копчето за поднесување. Откако ќе се кликне копчето за поднесување, истото ни се испраќа уште еднаш во мејл за потврда, а откако ќе биде потврдено од студентот, и потпишано од менаџментот, тогаш документот започнува со процесот на шифрирање уште еднаш пред да биде распореден и испратен до blockchain-базата на податоци со единствена хаш-вредност, што гарантира непроменливост, транспарентност и онлајн можност за самоидентификација и дигитален потпис. Слика 7.9. го прикажува интерфејсот на потписот на дипломата што треба да се складира подоцна во форма на токен во базата на податоци на blockchain.



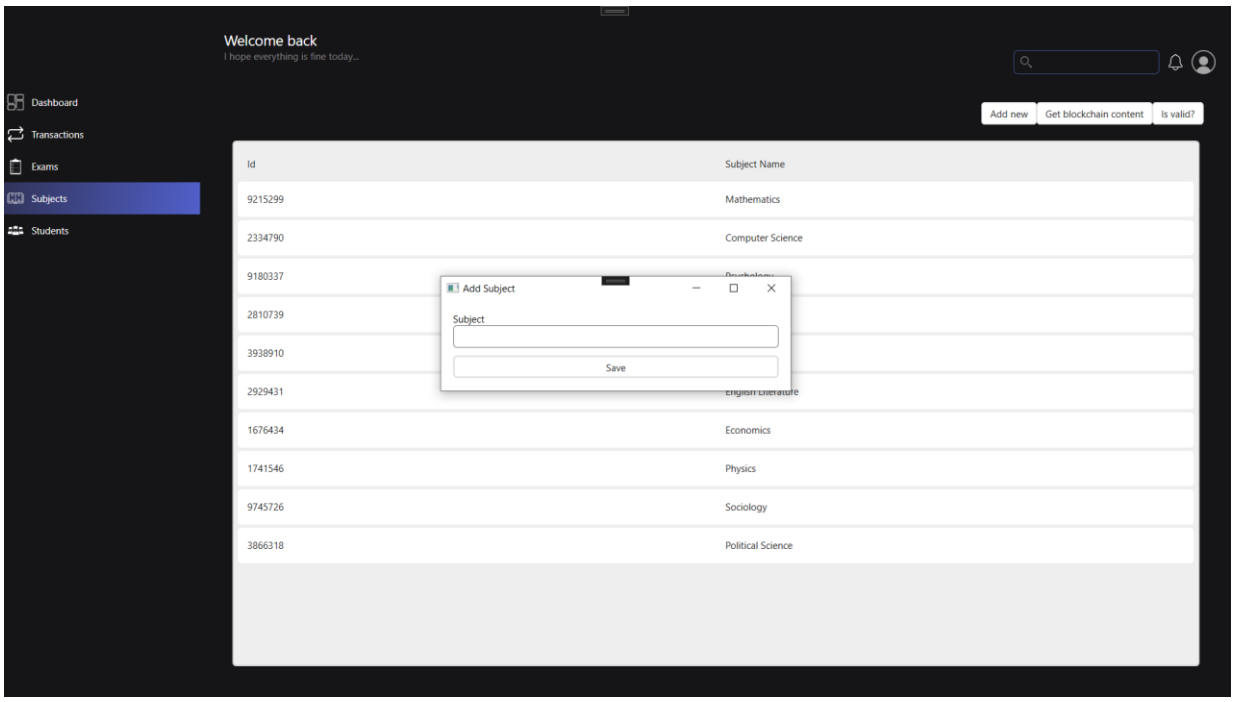
Слика 7.9. Пример за потпишување на дипломата при вметнување

Секоја идна промена во дипломата, што е сочувана во базата на blockchain, без разлика дали е од менаџментот на ВОУ или од кој било друг актер, се генерира друга хаш-вредност, и веднаш системот ги известува сите страни што се вклучени преку дневникот на активности, но и во е-пошта, и истиот документ нема да ја има хаш-вредноста што ја имаше на почетокот, бидејќи за секоја промена ќе се генерира друга хаш-вредност, различна од почетната. Со ова се докажува дали дипломата е сменета или не, што многу

лесно ни овозможува во иднина да провериме дали дипломата е оригинална или не, преку хаш-вредноста што била почетна при нејзиното вметнување. Слика 7.10. го прикажува интерфејсот за управување на студенти, додека Слика 7.11. го прикажува интерфејсот за управување на предмети.



Слика 7.10. Интерфејс за управување со студенти



Слика 7.11. Интерфејс за управување со предметите

Во следните точки од 1 до 5, ја опишавме практичната процедура за вметнување податоци во blockchain-базата на податоци, чекор по чекор во форма на псевдокод, за да им биде појасно на читателите.

1. Поврзете се со blockchain-јазол (мрежа, адреса)

```
ДОБИЈ Web3.js ID од мрежата ethereum {
Доколку (мрежниот ID е точен) Поврзете се на eth.net, мрежниот ID;
Else (catch грешка) Прикажи порака за грешка при поврзување();}
```

2. Вчитај бинарен интерфејс за апликација (Application Binary Interface- ABI) на паметниот договор и адресата на паметниот договор што е deploy

```
ДОБИЈ адреса, инстанца;
Доколку е точно { поставете вредности;
Поставете хаш вредности;
Добијте адреса на Account, испратете хаш на трансакцијата;
Доколку е вистина, {се праќа потврда за трансакција;
друго грешка при поставување вредност;}
друго (грешка при фаќање) Прикажи порака за грешка();}
```

3. Иницијализирајте ја инстанцата на паметниот договор

```
Потребна е инстанца web3.js;
Дефинирајте ја адресата на јазолот;
Дефинирајте ABI на паметниот договор;
Распоредете паметен договор (покажи адреса);
Креирајте нова инстанца за паметен договор (ABI инстанца, адреса);
Ако е точно, поставете ги податоците на паметен договор
Друго грешка при поставување на податоци;
```

4. Web.js фајл со паметниот договор за вметнување податоци

```
Добијте вредности на податоци од веб-форма;
Конвертирај ги внесените податоци;
ОБИДЕТЕ СЕ {
Подгответе трансакција;
Проценете ги трошоците за гас за трансакцијата;
Потпишете и испратете трансакција;
Почекајте го приемот на трансакцијата;
Дефинирајте ги податоците што треба да се шифрираат;
Шифрирајте ги податоците со AES алгоритам (потребна е крипто библиотека
node.js) И дефинирајте клуч за шифрирање;
```

```
Изврши паметен договор за вметнување податоци (испрати трансакција со
дадените податоци)}
ДРУГО
{ Грешка при вметнување податоци, прикажи порака за грешка();}
```

5. Солидити (Solidity)-фајл (паметен договор):

```
Паметниот договор Generation (){
дефинирај конструктор();
дефинирај структура Generation (студент_инфо, орг_инфо, предмет_ инфо,
оценување, година)
мапирање на јавни сертификати;
функција генерирај_диплома ( string ИД, string студент_инфо, string орг_инфо,
string предмет_инфо, string оценување, uint256 година)
барај (сертификати[id]) ==постои, „Диплома со дадена идентификација постои“
емитирај генерирана_сертификата(ИД);
функцијата ЗемиПодатоци();}
```

Во продолжение се објаснети сите методи што се користат во датотеката Солидити (Solidity):

- **дефинирај конструктор()** – дефинирањето на конструкторите е направено поради нивната потреба во текот на процесот на распоредување; Тие се користат за иницијализирање на променливите што се потребни пред договорот да стане оперативен;
- **дефинирај структура Generation()** – дефиницијата за структури е слична на онаа на другите програмски јазици, за да се организираат податоци, да се намалат трошоците и да се децентрализираат податоците;
- **мапирање јавни сертификати** – мапирањето се користи за пребарување или потврдување на податоците што веќе ги имаме во складирањето на blockchain, што имаат идентификациска вредност, или хаш-вредност или идентификација генерирана при вметнување;
- **функција генерирај_диплома()** – се користи за генерирање диплома, врз основа на податоците што ги даваме и нив ќе ги мапираме на дефинираните сертификати, но ако истите не постојат, напротив, трансакцијата нема да се изврши;
- **функција ЗемиПодатоци()** – овозможува примање податоци веќе вметнати во IPFS, или друга blockchain-база на податоци и нивно извлекување во предниот дел или веб-формата на корисникот.

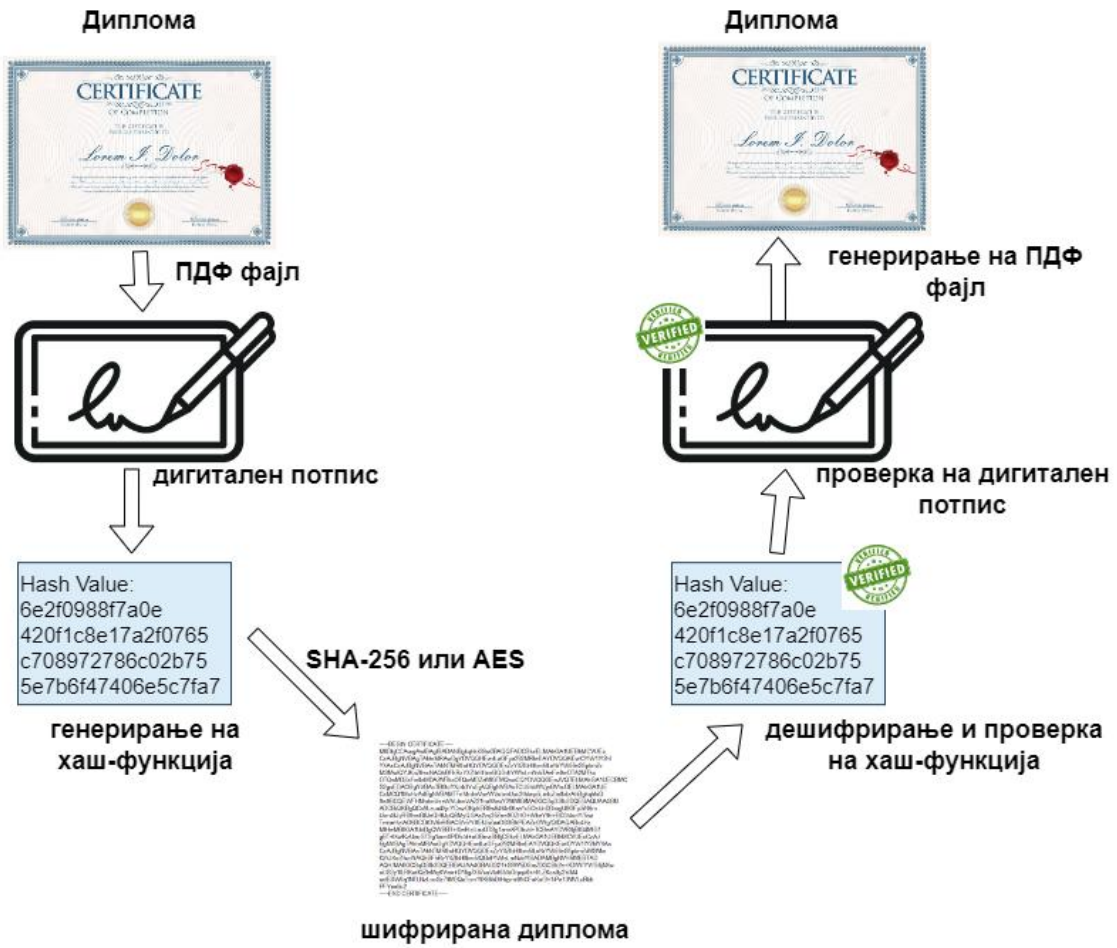
Генерирањето на единствената хаш вредност на документот, откако дигитално е потпишана од главните актери, се врши преку паметниот договор во Солидити (Solidity), каде како пример ги имаме следните кодни секвенци, сепак, генерирањето на единствена хаш-вредност може да се направи и во Пајтон, во централизираниот систем. Во Солидити, имаме пример:

```
contract PDFHash {
function generateHash(bytes memory _pdfData) public pure returns (bytes32) {
bytes32 hashValue = keccak256(_pdfData);
return hashValue;
}
}
```

Во Пајтон, како пример ги имаме следните кодни секвенци:

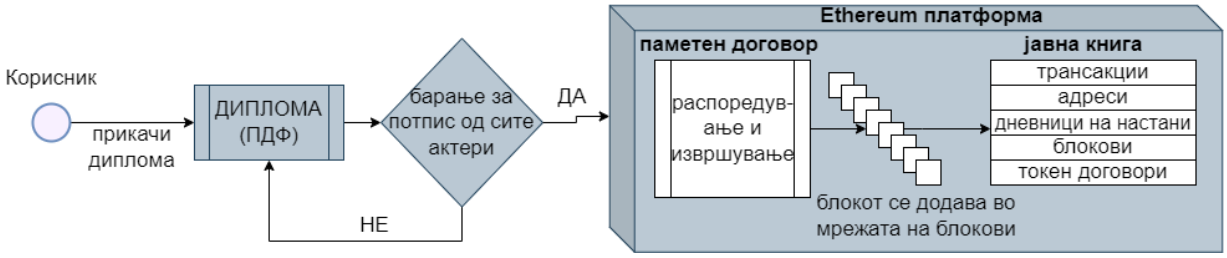
```
import hashlib
def calculate_hash(pdf_content):
hash_value = hashlib.sha256(pdf_content.encode()).hexdigest()
return hash_value
pdf_content = "Hello, this is a PDF document."
hash_value = calculate_hash(pdf_content)
print("Hash Value:", hash_value)
```

На Слика 7.12. на едноставен начин е објаснет процесот на шифрирање и дешифрирање на дипломите.



Слика 7.12. Опис на процесот на шифрирање и дешифрирање на дипломата

На Сликата 7.13, претставивме блок дијаграм, вклучувајќи ја и платформата Етериум, за да го прикажеме процесот на вметнување податоци.



Слика 7.13. Блок-дијаграм за процесот на генерирање диплома

7.4. Проверка на дипломи преку blockchain-системот

Проверката на дипломите е полесен процес, ако нивното вметнување се врши правилно, без грешки. Во системот, суперадминот има право да додава или да отстранува изведувачи, да проверува дипломи, што очигледно мора да биде во договор со раководството на ВОУ. При верификацијата на дипломите точките од 1 до 3 (од вметнување и генерирање на дипломата) се речиси исти. Во продолжение ќе го претставиме само псевдокодот во Веб3.јс (Web3.js) и Солидити што го прикажуваат процесот на верификација на диплома.

1. Веб.јс (Web.js) фајл со паметниот договор за проверка на податоци

```
дефинирање на IPFS_Api клуч;
дефинирање на приватен клуч;
дефинирање на ABI паметен договор;
најавете се во системот (мрежата ethereum) {
ако е точно прикажи userAddres, повторно вчитај ги корисничките податоци();
else show Порака за грешка за неоткривање на Метамаск паричник();
проверете ги податоците со хаш-вредности();
читање/запишување податоци во нашиот договор (проверете Метамаск
паричник());
асинхронизирана функција за проверка на хаш (){
ако вредноста на хашот е точна , печатете информации за потврда (резултат,
точно);
друго печатење информации за верификација (резултат, неточно);
функција провери_URL ();
функцијата информации за проверка на печатење (резултат, е проверена);
асинхронизирана функција добијте_Ethereum_биланс();
асинхронизирана функција испрати_датотека_на_IPFS();
асинхронизирана функција испрати_хаш ();
асинхронизирана функција избриши_хаш ();
функцијата генерирај_QR_код();
функција печатење_трансакција (податоци);
}}
```

2. Солидити (Solidity) фајл:

```
Паметен договор за проверка (){
дефинирај конструктор();
мапирање хаш();
мапирање приватни извозници();
```

```
проверка на Сопственик (), валидна_адреса (), овластен_извозник();
Додади хаш-вредности ();
функција додади_извозници ();
функција смени_извозник ();
функција најди_хаш_на_документи ();
функција избриши_хаш ();
функцијата добиј_податоци ();
}
```

Во продолжение ќе ги разјасниме сите функции кои се дел од Солидити договорот:

- **мапирање хаш();** – можеме да ставиме хаш-вредности на податоците и да ги користиме истите вредности како клучевите во процесот на мапирање, за дополнителна безбедност;
- **мапирање на приватни извозници();** – ја користиме оваа функција за складирање на адресите на генераторите на дипломи, додека приватниот клуч е хашот на податоците за дипломите, додека вредноста е адресата на извозникот;
- **проверка на Сопственик (), валидна_адреса (), овластен_извозник();** – оваа функција се користи за да се провери дали дадената адреса му припаѓа на основачот на договорот или не, дали истата адреса е валидна или не, и потврдувајќи дали адресата е овластен извозник, можете да додадете соодветни функции на модификатор на вашиот договор;
- **додадете хаш-вредности ();** – оваа функција се користи ако сакате да додадете функционалност за складирање на хаш вредностите на потврдените дипломи во вашиот договор, за да вклучи мапирање за складирање на вредностите на хашот заедно со статусот на верификација;
- **додади_извозници ();** – ги додава адресите на секој генератор на дипломи;
- **функција смени_извозник ();** – се користи за промена на статусот на извозник (генератор на дипломи) во активен или неактивен, во зависност од договорите што ги имаат меѓу себе;
- **функција најди_хаш_на_документи ();** – оваа функција служи за преземање на податоците од документот како влез и генерирање на нивната соодветна хаш-вредност;
- **функција избриши_хаш ();** – ќе ја земе вредноста на хашот како влез и ќе ја избрише од мапирањето каде што ги складирате вашите проверени хашови на диплома.
- **функција добиј_податоци ();** – за враќање на податоците поврзани со одредена хаш вредност

Без да навлегуваме во деталите за имплементацијата, за да им биде појасно на читателите, презентираме секвенци на кодови, кои накратко го прикажуваат складирањето и проверката на дипломите во ИПФС (IPFS). Подолу се главните кодови со релевантни елаборации во солидити и веб3.js (Solidity и Web3.js).

Солидити код:

```
pragma solidity ^0.8.0;

contract DiplomaRegistry {
    mapping(address => string) public diplomaRecords;

    function storeDiploma(address recipient, string memory ipfsHash) public {
        require(bytes(ipfsHash).length > 0, "IPFS hash must not be empty");
        require(bytes(diplomaRecords[recipient]).length == 0, "Diploma already registered");

        diplomaRecords[recipient] = ipfsHash;
    }

    function verifyDiploma(address recipient) public view returns (string memory) {
        return diplomaRecords[recipient];
    }
}
```

Веб3.js код:

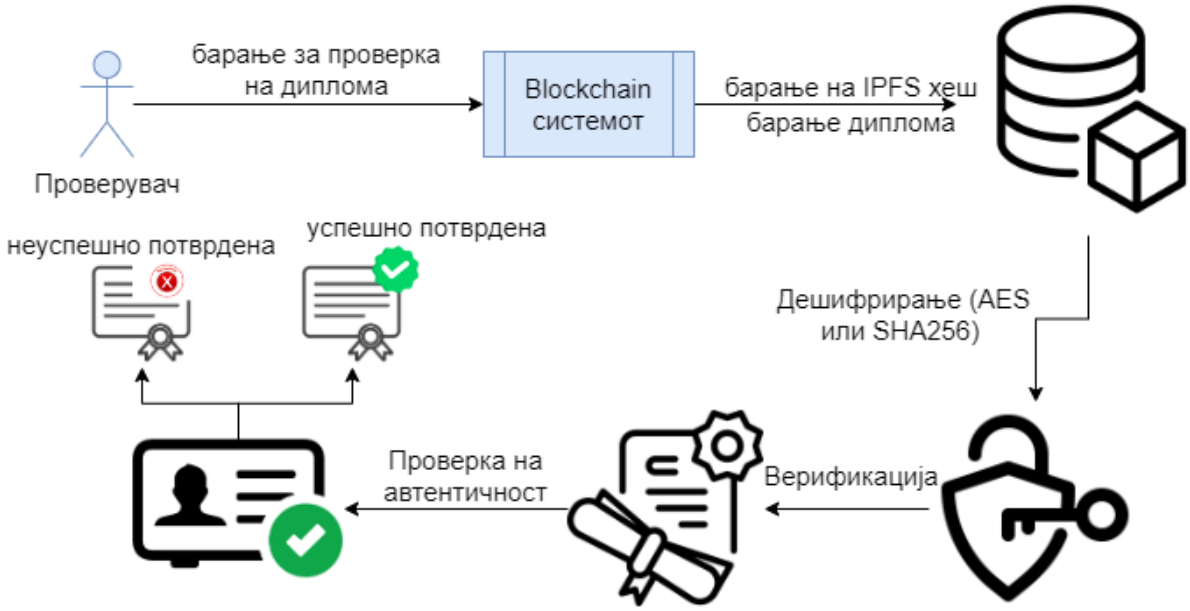
```
// Договор ABI (интерфејс)
const contractAbi = [
    // Записи на ABI овде
];

// Адреса на договорот
const contractAddress = „Адреса на договорот“;

// Инстанца на договор
const contract = new web3.eth.Contract(contractAbi, contractAddress);

// Функција за складирање диплома
async function storeDiploma(recipient, ipfsHash) {
    await contract.methods.storeDiploma(recipient, ipfsHash).send({ from: YOUR_ADDRESS
});
}
```

```
// Функција за проверка на диплома
async function verifyDiploma(recipient) {
   const ipfsHash = await contract.methods.verifyDiploma(recipient).call();
   return ipfsHash;
}

const recipient = АДРЕСА НА ПРИМАЧ;
const ipfsHash = IPFS HASH НА ДИПЛОМА;
await storeDiploma(recipient, ipfsHash);

const recipient = АДРЕСА НА ПРИМАЧ;
const verifiedHash = await verifyDiploma(recipient);
// Користи ја портата IPFS за да добиете документ за диплома користејќи verifiedHash
```

За проверка на диплома преку blokchain системот треба да следат следниве чекори :

- **Пристап до паметен договор:** проверувачот (на пример, работодавач, друга образовна институција) пристапува до распоредениот паметен договор на blockchain етериум користејќи веб3.јс. или слична библиотека.
- **Барање информации за диплома:** проверувачот го бара паметниот договор со адресата Ethereum на примачот на диплома.
- **Враќање на ИПФС хаш:** Паметниот договор го враќа хашот ИПФС поврзан со Етериум адресата на примачот, што одговара на неговата диплома.
- **Враќање диплома од ИПФС:** Користејќи го преземениот хаш ИПФС (IPFS), верификаторот ја враќа шифрираната или дигиталната диплома со обичен текст од мрежата IPFS.
- **Дешифрирање**: Ако дипломата била шифрирана, верификаторот ја дешифрира со помош на соодветниот клуч за дешифрирање. Овој чекор осигурува дека дипломата е во читлив формат.
- **Проверка**: Проверувачот ја споредува добиената диплома со информациите дадени од примачот. Ова може да вклучува потврдување на името на институцијата, името на примателот, стекнатата диплома, датумот на издавање и сите други релевантни детали.
- **Проверка на автентичност**: верификаторот може да ги вкрсти деталите на дипломата со информациите достапни од образовната институција или други доверливи извори за да се осигури нејзината автентичност.
- **Потврда:** Ако дипломата одговара на очекуваните критериуми и е потврдена како автентична, процесот на верификација е успешен. Во спротивно, може да биде потребна дополнителна истрага.

Слика 7.14 дава графички опис на овој процес.



Слика 7.14. Опис на процесот на проверка на диплома

7.5. Валидација на системот

Тестирањето и валидацијата на blockchain-системот за генерирање и потврдување дипломи вклучува неколку клучни чекори за да се обезбеди неговата сигурност, безбедност и функционалност. Прво, треба да се тестира функционалната валидација на системот. Да се потврди дали системот ги исполнува дефинираните функционални барања, пред сè да овозможи генерирање и функционална верификација на дипломи. Такво нешто овозможува прототипот што го создадовме. Прототипот што го направивме го поддржува процесот на токенизација на дипломите, како процес штопред сè ќе понуди полесна обработка на дипломите, бидејќи дипломите што ги зачувуваме во пдф се потпишани во дигитална форма од потребните страни (студентот, ректорот и деканот), и се чуваат во форма на токен во базата на податоци, што е шифриран со софистицирани алгоритми како AEC (AES) или CXA256 (SHA256) и тоа многу лесноможе да се потврди во секое време. Мораме да внимаваме при валидацијата да тестираме дали системот ја обезбедува потребната безбедност или дали ги зачувува приватноста, интегритетот и податоците. Првично, системот нуди методи за дигитална идентификација, што самиот корисник ги одредува. Дипломите се потпишуваат во дигитална форма преку самосуверен идентитет, при што студентот по потпишувањето го потврдува идентитетот, а потоа документот повторно дигитално се потпишува од самата институција и се шифрира. На овој начин, дипломата веќе има уникатни

вредности, дека ако некој нешто промени или ако се обиде да прави што сака, таквата промена е многу тешка, односно невозможна.

Првично, за да се направи промена во blockchain-мрежата, мора да се добие одобрение од сите јазли во blockchain-мрежата, бидејќи високообразовните институции, очигледно, се повеќе актери.

Второ, невозможно е да се ажурираат податоците за токен, дури и ако се зачувани како токен и ако да се зачува почетната вредност на хашот. Секоја евентуална промена ќе се генерира нова хаш-вредност што е најдобар гарант дали дипломата е оригинална или не. И, конечно, мора да се осигурите дека системот е усогласен со релевантните прописи и стандарди што ја регулираат заштитата на податоците и образовната акредитација.

Слика 7.15., каде што го претставивме кодот зад вметнувањето на податоците во базата на blockchain. Меѓу другото, гледаме дека при вметнување податоци, било да се тоа студенти, субјекти или други податоци, се создава blockchain-мрежа, каде што секој запис има единствена вредност на хашот, како и дека е поврзан со следниот запис и гледаме дека секоја додадена вредност, покрај хаширањето на уникатната вредност, има и претходни хаш на претходните податоци, како и статусот на податоците е во очекување, додека сите јазли во мрежата не ги потврдат податоците.


```
1
2   "PendingTransactions": [],
3   "Chain": [
4     {
5       "Index": 0,
6       "PreviousHash": null,
7       "Hash": "00011KFv7zgidm1rlER27QgrbBrV/PNeDJ1IJVO/LnI=",
8       "Transactions": []
9     },
10    {
11      "Index": 1,
12      "PreviousHash": "00011KFv7zgidm1rlER27QgrbBrV/PNeDJ1IJVO/LnI=",
13      "Hash": "00IqgSGRxFrR+RyrQLX7Gb8fqTytaMoq0oJuEjGZ0Hs=",
14      "Transactions": [
15        {
16          "exam_id": 7071617,
17          "exam_date": "2024-02-07T00:00:00",
18          "index_id": 8615041,
19          "student_name": "Emily  Johnson",
20          "subject_id": 9215299,
21          "subject_name": "Mathematics",
22          "grade": 7
23        }
24      ]
25    },
26    {
27      "Index": 2,
28      "PreviousHash": "00IqgSGRxFrR+RyrQLX7Gb8fqTytaMoq0oJuEjGZ0Hs=",
29      "Hash": "00GPUC25a1Y7OSyMIRSQ/vJ7ETY0Vtsgg/AsLXX3zMM=",
30      "Transactions": [
31        {
32          "exam_id": 1120035,
33          "exam_date": "2024-02-07T00:00:00",
34          "index_id": 6472945,
35          "student_name": "Ethan  Parker",
36          "subject_id": 9215299,
37          "subject_name": "Mathematics",
38          "grade": 8
39        }
40      ]
41    },
42    {
43      "Index": 3,
44      "PreviousHash": "00GPUC25a1Y7OSyMIRSQ/vJ7ETY0Vtsgg/AsLXX3zMM=",
45      "Hash": "00oG1clDl/rokOrTLmNvMbOLGBGFZTAvrNj51swMoZ4=",
46      "Transactions": [
47        {
48          "exam_id": 3434316,
```


Слика 7.15. Процесот на креирање на blockchain-мрежата од вметнување на податоците

Користејќи ги ресурсите на Етерскен (Etherscan), како апликација посветена на платформата Етериум, каде отворено ги прикажува сите трансакции во секој момент, а во исто време обезбедува одредена статистика, на Слика 7.16. се прикажани за еден месец промените што се случија во времето и големините на блоковите, вкупно креираните блокови, и новите адреси што се додадени во платформата.

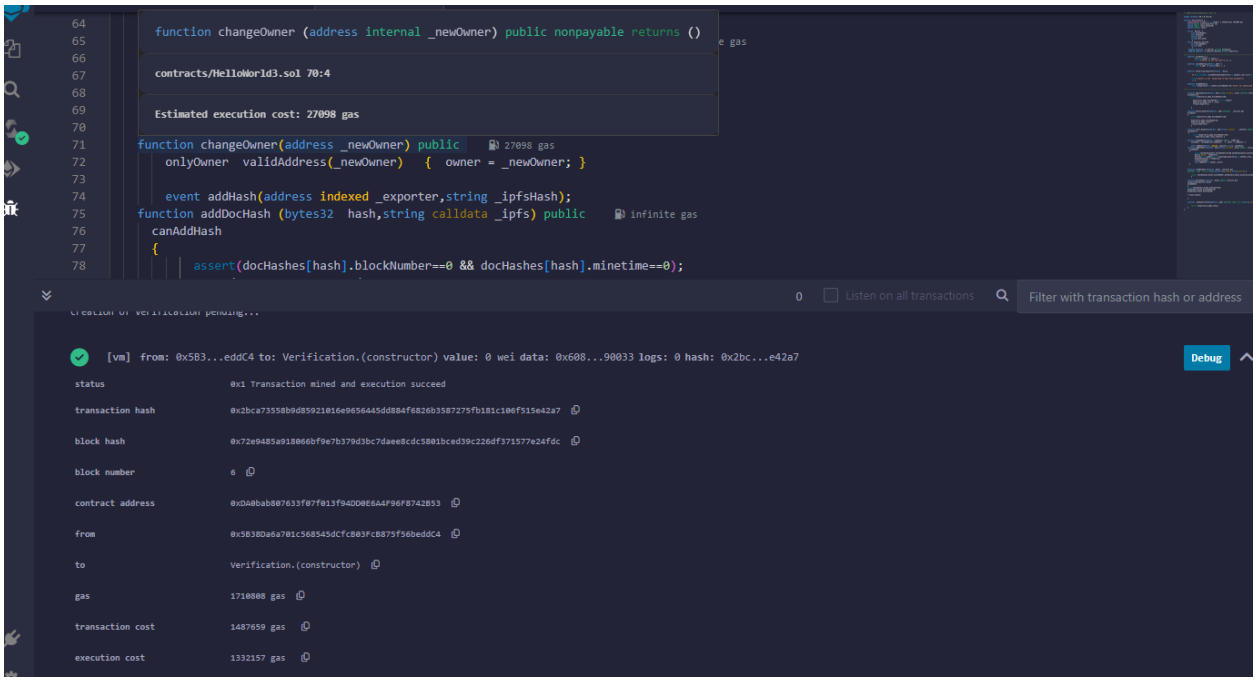
Слика 7.16. Време и големина на блокови, и нови адреси на Етериум (17 март - 17 април 2024)

Сега, благодарение на софистицираните апликации, сите паметни договори може да се извршат и да се тестираат пред да бидат распоредени на blockchain-мрежата, па дури можеме да ги знаеме точно трошоците за трошење пред да бидат распоредени. Постојат многу веб-базирани интегрирани развојни околини, специјално дизајнирани за развој на паметни договори на Етериум. Еден од најсофистицираните од нив е РемиксИДЕ (RemixIDE- што нуди пакет алатки и функции за рационализирање на процесот на пишување, тестирање, дебагирање и распоредување паметни договори на blockchain етериум. Некои клучни карактеристики на РемиксИДЕ вклучуваат:

- РемиксИДЕ обезбедува вграден уредник за пишување паметни договори солидити, програмски јазик на етериум за креирање паметни договори.
- Вклучува компајлер солидити што може да состави паметни договори напишани во солидити во бајтекод, што може да се распореди на blockchain етериум.

- Ремикс нуди алатка за дебагер што им овозможува на програмерите да чекорат низ нивните паметни договори линија по ред, да ги проверуваат променливите и да ја следат состојбата на договорот на секој чекор.
- Околина за тестирање: програмерите можат да пишуваат тестови за единиците за нивните паметни договори директно во Ремикс (Remix) и да ги извршат за да ја осигураат исправноста и издржливоста на нивниот код.
- Ремикс (Remix) го олеснува распоредувањето на паметните договори на blockchain етериум, обезбедувајќи директен интерфејс за специфицирање на параметрите за распоредување и интеракција со мрежата Етериум.
- Поддржува систем на приклучоци што им овозможува на програмерите да ја прошират функционалноста на ремикс со дополнителни алатки и функции.

На сликата подолу е прикажано извршувањето на паметниот договор за верификација, што го имаме распоредено во РемиксИДЕ, и како што можеме да видиме, покрај тоа што ни го прикажува успешното или неуспешното извршување на процесот на распоредување, во исто време, во секоја функција во рамките на датотеката, ги пресметува и трошоците за извршување на таа функција, освен крајните трошоци што се пресметуваат на крајот од извршувањето.



Слика 7.17. Успешно извршување на паметен договор во РемиксИДЕ

Паметниот договор во солидити, всушност, претставува збирка од кодови (со сите функции) и соодветните податоци, што се наоѓаат на одредена адреса во blockchain-мрежата. Дури и паметните договори, како објектно-ориентираните програмски јазици,

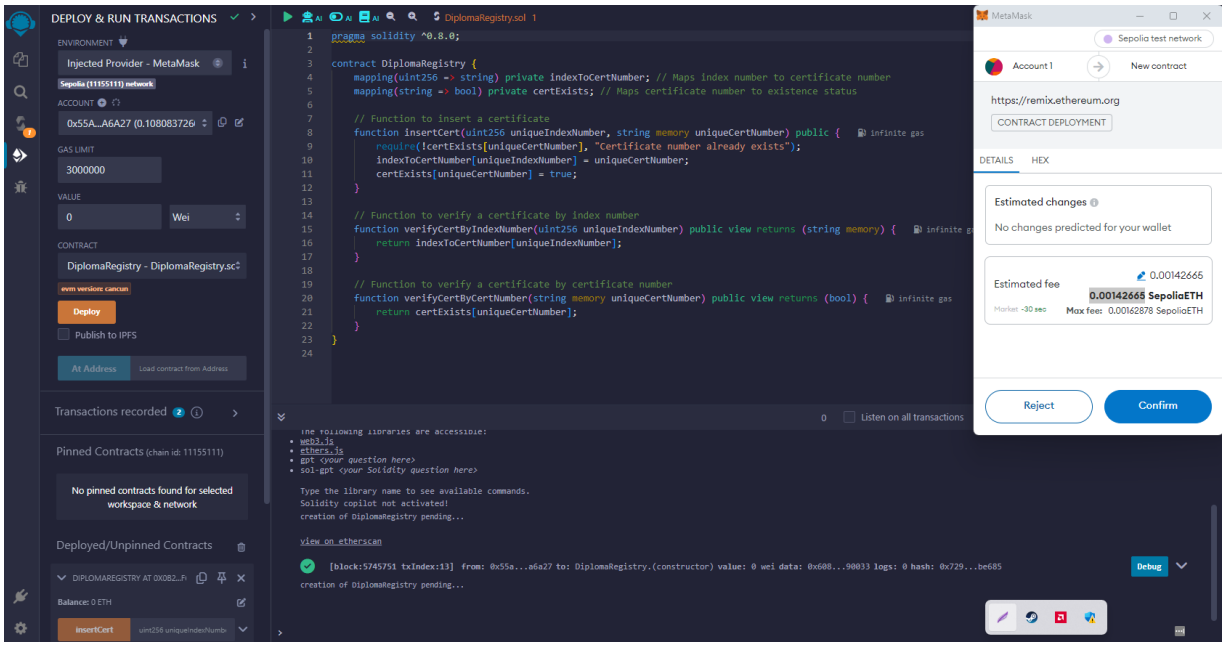
поддржуваат конструктори, специфични функции што се повикуваат само за време на нивното извршување и не можат да се извршат потоа. Имајќи ја предвид оваа сличност со објектно-ориентирани програми, тогаш можеме слободно да споредиме во однос на нивната структура, дека паметните договори личат на класи, состојби со атрибути.

Постојат неколку случаи што мора да се земат предвид при тестирањето на паметниот договор во солидити [172]:

- Тестирањето на оверфлоу (Overflow) и андерфлоу (underflow) во паметните договори е од клучно значење за да се обезбеди сигурност и исправност на логиката на договорот, особено кога се работи со аритметички операции на цели броеви. Оверфлоу се случува кога резултатот од аритметичка операција ја надминува максималната репрезентативна вредност за типот на податоци, додека underflow се случува кога резултатот е помал од минималната репрезентативна вредност.
- Тестирањето за контрола на пристап во паметните договори е од суштинско значење за да се осигури дека само овластени корисници или договори можат да вршат специфични дејства во системот.
- Тестирањето на механизмот за повик на трансакции во паметен договор вклучува проверка дали функциите правилно комуницираат со други договори или надворешни сметки.
- Тестирањето на механизмот за заштита во паметниот договор вклучува проверка дали се спроведуваат одредени услови пред да се дозволи извршување одредени функции.
- Тестирањето на операторот за самоуништување во паметен договор вклучува проверка дали договорот се однесува како што се очекува кога се повикува функцијата за самоуништување.
- Константните својства во паметниот договор во солидити обично се однесуваат на променливи што се декларирани како константни или непроменливи. Овие променливи се поставени во времето на компајлирање и не можат да се менуваат за време на извршувањето на договорот. Тестирањето на таквите својства вклучува проверка дека нивните вредности се правилно иницијализирани и остануваат непроменети.
- Тестирањето на модификаторите на функции во паметниот договор солидити вклучува проверка дали модификаторите правилно го ограничуваат или менуваат однесувањето на функциите на кои се применуваат.
- Во солидити, функцијата конструктор се дефинира без име, туку едноставно со клучниот збор конструктор. Кога тестирате паметен договор, можете да потврдите дека конструкторот правилно ги иницијализира променливите за состојбата на договорот.

Секој паметен договор пред да биде распореден, без разлика дали е во РемиксИДЕ или која било апликација што овозможува негово извршување, мора да ја имаме нашата единствена адреса поврзана со адресата на паричникот Метамаск, што пред да биде распоредена бара потврда на алатките што ги имаме во Метамаск. Само откако тоа ќе се потврди може да се изврши, но секое извршување има свој трошок.

Ако ја анализираме Сликата 7.18. од десната страна каде што го имаме Метамаск паричникот, го имаме и проценетиот надоместок за извршување на трансакцијата, што ни го покажува трошокот за извршување на тој паметен договор.



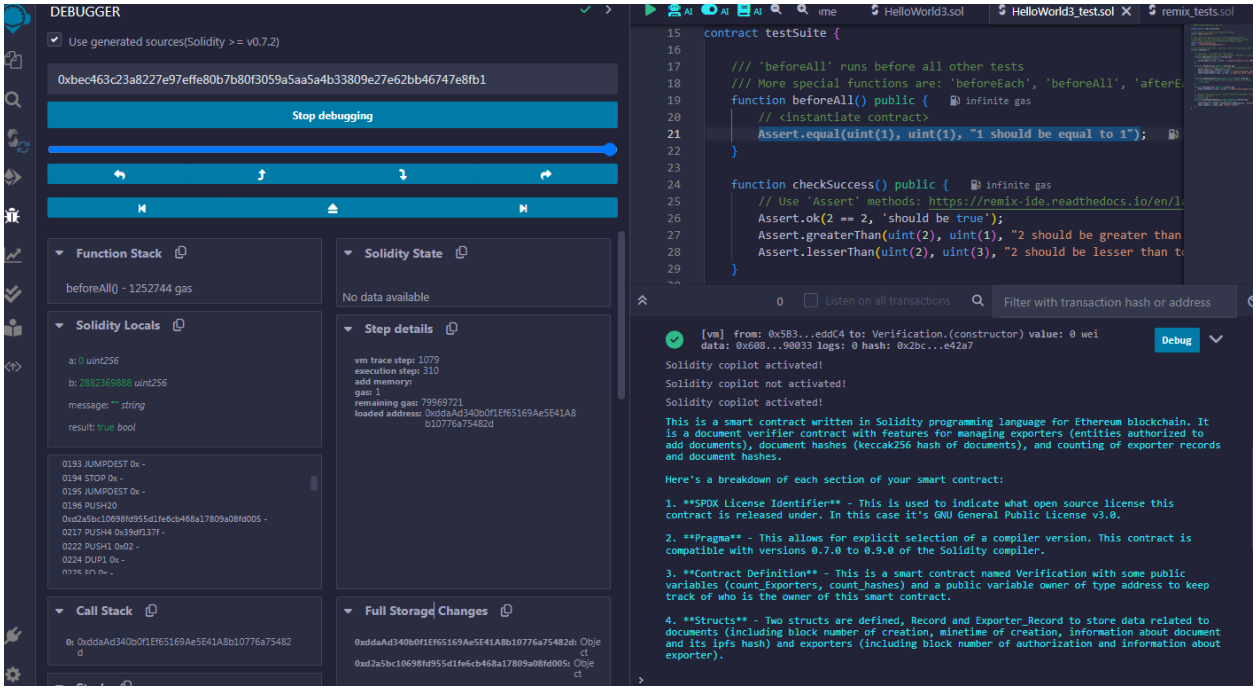
Слика 7.18. Проценет надоместок за трансакцијата, во очекување потврда од паричникот на Метамаск

Следно, ќе го дадеме псевдокодот во кратки точки што служат за мерење на метриката на паметен договор што е дебагиран во Солидити.

Паметен договор Калкулатор за метрика{
Дефинирај **променливи за складирање на метрика** {
вкупна трансакција;
вкупен пренесен етер;
просечна вредност на трансакцијата;
}
емитувај настан *трансакција* за секоја снимена трансакција;
функција **трансакција за евиденција** {
Пресметај:

```
 вкупната трансакција,
 вкупниот пренесен етер,
просечната вредност на трансакцијата,
 емитирана трансакција;
}
функција добиј вкупна трансакција {
добијте вкупен број на трансакции;
}

функција добиј ја количината на етер {
префрлете го вкупниот етер;
}
функција добиј просечна вредност на трансакцијата{
добиј просечни вредности на трансакцијата;}
}
```

Многу апликации што овозможуваат програмирање, компилација и дебагирање паметни договори, исто така, вклучуваат библиотека за тестирање паметни договори, што истовремено покажува грешки и дава дополнителни појаснувања. Повторно, ќе го земеме РемиксИДЕ како пример, бидејќи овозможува и бесплатни услуги. На сликата подолу, јасно се гледа дека тој овозможува тестирање на паметниот договор, но го вклучува и роботот со вештачка интелигенција, штоим помага на програмерите таму каде што е потребно, давајќи дополнителни објаснувања за што и да извршат. Помошта што ја нудат роботите со вештачка интелигенција е поразновидна, но меѓу најважните се генерирање код, статичка анализа и безбедност, документација и помош за код, приспособени приклучоци и др.



Слика 7.19. Процесот на тестирање паметни договори и вклучување интелигентни агенти во РемиксИДЕ (RemixIDE)

Што се однесува до креираните паметни договори, распоредени се користејќи Сеполиа тестнет (Sepolia Testnet), што се во суштина тест-мрежи што ги користат програмерите за да експериментираат со нови blockchain-технологии или апликации без да ризикуваат реални средства. Една од главните карактеристики на blockchain е транспарентноста на паметниот договор. Како што може да се види на сликата подолу, во Етерскен (Etherscan), можеме да пристапиме и до паметниот договор (изворниот код), но тој може да се тестира на лице место, како да се веб-сервиси, но само дека секој тест мора да се поврзе со метамаск-паричникот и ги потврдеме плаќањето.

Sepolia Testnet

Search by Address / Txn Hash / Block / Token

Contract Name: **DiplomaRegistry**

Optimization Enabled: **No** with **200** runs

Compiler Version **v0.8.25+commit.b61c2a91**

Other Settings: **default** evmVersion, **MIT** license

Contract Source Code (Solidity)

IDE | Outline | More Options

```
1  /**
2   *Submitted for verification at Etherscan.io on 2024-04-21
3  */
4
5  pragma solidity ^0.8.0;
6
7  contract DiplomaRegistry {
8      mapping(uint256 => string) private indexToCertNumber; // Maps index number to certificate number
9      mapping(string => bool) private certExists; // Maps certificate number to existence status
10
11     // Function to insert a certificate
12     function insertCert(uint256 uniqueIndexNumber, string memory uniqueCertNumber) public {
13         require(!certExists[uniqueCertNumber], "Certificate number already exists");
14         indexToCertNumber[uniqueIndexNumber] = uniqueCertNumber;
15         certExists[uniqueCertNumber] = true;
16     }
17
18     // Function to verify a certificate by index number
19     function verifyCertByIndexNumber(uint256 uniqueIndexNumber) public view returns (string memory) {
20         return indexToCertNumber[uniqueIndexNumber];
21     }
22
23     // Function to verify a certificate by certificate number
24     function verifyCertByCertNumber(string memory uniqueCertNumber) public view returns (bool) {
25         return certExists[uniqueCertNumber];
```

Contract ABI

Export ABI


```
[{"inputs":[{"internalType":"uint256","name":"uniqueIndexNumber","type":"uint256"},{"internalType":"string","name":"uniqueCertNumber","type":"string"}],"name":"insertCert","outputs":
[],"stateMutability":"nonpayable","type":"function"},{"inputs":[{"internalType":"string","name":"uniqueCertNumber","type":"string"}],"name":"verifyCertByCertNumber","outputs":
[{"internalType":"bool","name":"","type":"bool"}],"stateMutability":"view","type":"function"},{"inputs":
[{"internalType":"uint256","name":"uniqueIndexNumber","type":"uint256"}],"name":"verifyCertByIndexNumber","outputs":
[{"internalType":"string","name":"","type":"string"}],"stateMutability":"view","type":"function"}]
```


Слика 7.20. Транспарентноста на паметните договори во Етерскен

Слика 7.21 покажува како паметниот договор може да се тестира директно во Етерскен, како кај веб-сервисите што можеме да ги тестираме при нивното извршување, меѓутоа, овде веднаш бара потврда за извршувањето на паметниот договор во Метамаск. Што значи дека, во blockchain-мрежата Етериум, секоја услуга мора да се плати со етер.

Sepolia Testnet

Search by Address / Txn Hash / Block / Token

Transactions | Token Transfers (ERC-20) | Contract | Events

Code | Read Contract | Write Contract

Connected - Web3 [0x55A2...6A27]

1. insertCert (0x1a8f8283)

uniqueIndexNumber (uint256) +

3612111003

uniqueCertNumber (string)

400231

Write

Sepolia test network

Account 1 → 0x0b276...f...

https://sepolia.etherscan.io

0x0b276...f618e : CONTRACT INTERACTION

DETAILS | HEX

Estimated changes

No changes predicted for your wallet

Estimated fee 0.00026074

0.00026074 SepoliaETH

Market ~30 sec Max fee: 0.00029725 SepoliaETH

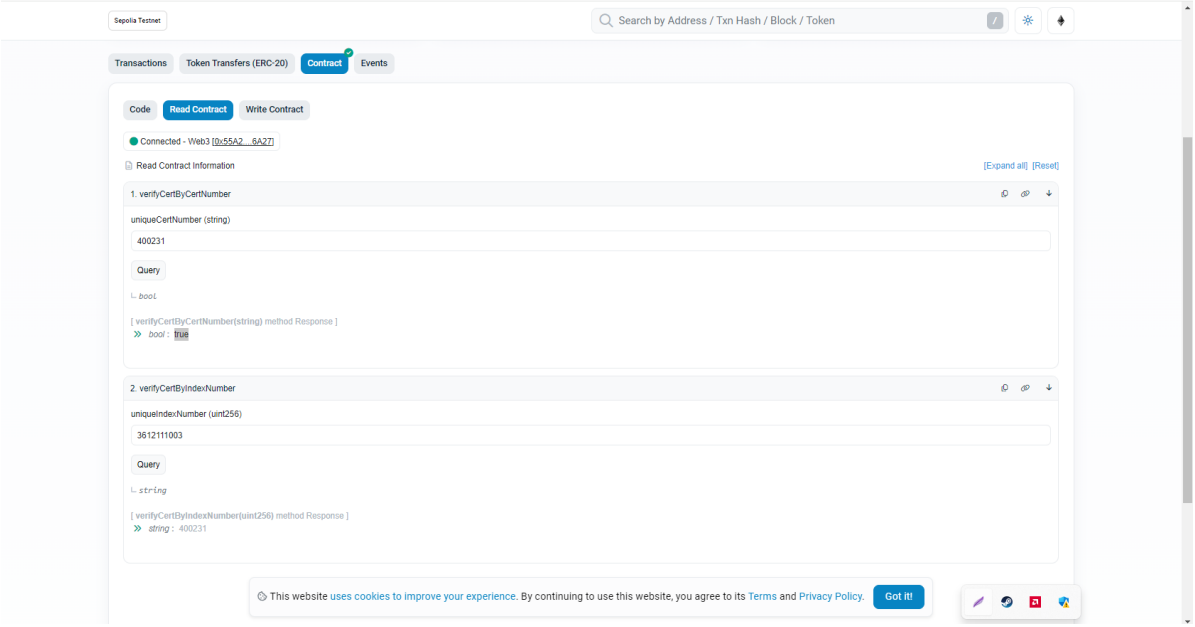
Reject | Confirm

A contract address hosts a smai

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

Слика 7.21. Тестирање на паметниот договор во Етерскен

Слика 7.22. ја прикажува успешната верификација на диплома, врз основа на бројот на единствениот индекс на студентот, дали тоа е зачувано или не во blockchain-мрежата и ни го дава единствениот број на дипломата. Потоа тестиравме дали таа диплома со единствен број постои во базата на blockchain или не, каде од сликата гледаме дека е валидна, и дека таа постои. Ова всушност претставува само кратка низа од паметниот договор за верификација, што всушност ја покажува успешната валидација на паметниот договор и дека тие се функционални.



Слика 7.22. Потврда на диплома врз основа на студентски ИД и број на диплома

7.6. Повеќекратни регресивни предвидливи анализи за проверка на диплома

Линеарната регресија е модел што може да ја предвиди работата во машинското учење. Преку овој метод се настојува да се приближи што е можно попрецизно до одредена вредност што ќе се случи во иднина. Пример за примена на овој тип на регресија е, на пример: ефикасноста на потрошувачката на автомобил врз основа на моќноста на моторот и цилиндрите што ги имаат автомобилите, тежината на автомобилот, моторните сили итн. [173]. Регресивните техники може да се користат за да се предвидат и да се анализираат перформансите на blockchain-системот за да се анализираат перформансите на системот во одредени временски интервали. Техниката на регресија може да се користи за предвидлива анализа, откривање аномалија на системот, распределба на ресурси, процена на ризик, оптимизација на перформансите на системот, анализа на пазарот итн., паметен договор и цената на трансакциите. Иако предвидувачките техники се техники што зависат од многу фактори, сепак

математичките пресметки што ги користат овие техники успеале да ги предвидат резултатите, а повеќето од нив се покажале точни, со што веродостојноста се зголемила на 95%. Меѓутоа, за овие анализи да бидат попрецизни, влезните променливи треба да бидат поблиску до реалните. Иако постојат многу техники за предвидување, може да се разликуваат три главни категории: предвидувачки, описни и модели на одлучување. Класификацијата главно има врска со влијанието на надворешните фактори во пристапот кон варијаблите земени како основа за анализата [174]. Низ работата и техниките на повеќекратна регресија ќе се обидеме да прикажеме некои статистички податоци поврзани со верификацијата на дипломите во рок од една година, во високообразовна институција. Првично, претпоставуваме дека високообразовната установа има четири (4) факултети во нејзин состав, а за секој месец генерираат одреден број барања за заверка на дипломи, што подетално се дадени во Табела 13. Пресметката на трошокот за Етериум зависи од неколку фактори, што ги зедовме како примери на податоците подолу:

Цена на гас: 50 Gwei (0,00000005 ETH)

Ограничување на гас по трансакција за верификација: 200.000 гасни единици

Надомест за распоредување на паметен договор: 0,1 ETH

Табела 13. Цена на Етериум за проверка на диплома за една година (симулирани податоци)

Месец	Просечна вредност на трансакција	Тотал трансакции	Тотал Етер	Фак. 1	Фак .2	Фак. 3	Фак. 4
1	0.010304878	328	3.38 ETH	151	55	77	45
2	0.007398374	263	2.73 ETH	142	25	75	21
3	0.0102710027	369	3.79 ETH	145	121	58	45
4	0.0102518892	397	4.07 ETH	254	115	14	14
5	0.0102123142	471	4.81 ETH	255	114	25	77
6	0.0101934236	517	5.27 ETH	254	109	65	89
7	0.0101930502	518	5.28 ETH	266	152	44	56
8	0.0101644737	608	6.18 ETH	255	177	121	55
9	0.0101683502	594	6.04 ETH	215	200	154	25
10	0.0101808318	553	5.63 ETH	159	201	148	45
11	0.0101004016	996	10.06 ETH	455	265	254	22
12	0.0101564945	639	6.49 ETH	155	222	250	12

Врз основа на податоците од Табела 13, и користење на достапниот софтвер за пресметување на повеќекратна регресија, без да се губи време во деталната обработка на сите математички равенки, следните табели се резултатите од регресијата.

Табела 14. Повеќекратни техники на регресија за проверка на дипломи (податоци од Табела 13)

Статистика за регресија	
Повеќекратни P	1
R Square	1
Adjusted R Square	1
Стандардна грешка	3.05965E-16
Набљудувања	12

	df	***SS***	***MS***	***F***	***Significance F***
Регресија	4	39.82889167	9.957222917	1.06364E+32	2.5708E-111
Остаток	7	6.55303E-31	9.36147E-32		
Вкупно	11	39.82889167			

	Коефициенти	***Стандардна грешка***	***t Stat***	***P-value***	***Lower 95%***	***Upper 95%***	***Lower 95.0%***	***Upper 95.0%***
Прекинување	0.1	3.32429E-16	3.00816E+14	1.1849E-99	0.1	0.1	0.1	0.1
Факултет 1	0.01	1.26123E-18	7.92875E+15	1.3407E-109	0.01	0.01	0.01	0.01
Факултет 2	0.01	2.43781E-18	4.10204E+15	1.3514E-107	0.01	0.01	0.01	0.01
Факултет 3	0.01	2.07142E-18	4.82759E+15	4.3218E-108	0.01	0.01	0.01	0.01
Факултет 4	0.01	4.41264E-18	2.26622E+15	8.6032E-106	0.01	0.01	0.01	0.01

Равенката што ни овозможува да ја пресметаме регресијата е $Y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + ... + \beta_p x_p + \varepsilon$, каде ε е редна променлива еднаква на нула и σ е стандардна девијација чија вредност не ја знаеме.
Исто така, не ги знаеме вредностите на променливите $\beta_0, \beta_1, \beta_2, ... \beta_p$. Сите овие (p+2) непознати променливи мора да се пресметаат, од променливите за кои имаме конкретни вредности. Податоците се состојат од n редови што ги нарекуваме случаи, што ни даваат вредности како $y_i, x_{i1}, x_{i2}, ..., x_{ip}; i = 1,2,....., n$. Проценките за коефициентите β се пресметуваат така што да се минимизира збирот на квадрати на разлики помеѓу вградените (предвидените) вредности на набљудуваните вредности во податоците.

За да обезбедиме практични податоци за времето на трансакцијата, потребни ни се конкретни информации како што се blocktimestamp за тоа кога трансакцијата е минирана и деталите за трансакцијата. Во Етериум, можете да го добиете blocktimestamp користејќи block.timestamp во рамките на паметниот договор солидити или со барање на blockchain-експлорер или АПИ (API) на јазол. Ако имате специфичен хаш на трансакцијата, можете да користите истражувач на blockchain како етерскен за да ги видите деталите за таа трансакција, вклучувајќи го и временскиот печат кога е минирана. Секвенца од кодови што може да се користи во рамките на паметниот договор во Солидити за да се прикаже времето на извршување на трансакцијата, како и времето на снимање на трансакцијата е дадена подолу:

```
pragma solidity ^0.8.0;
contract TransactionTime {
uint256 public transactionTimestamp;
function recordTransaction() external {
transactionTimestamp = block.timestamp;
}
function getTimeElapsed() external view returns (uint256) {
require(transactionTimestamp > 0, "No transaction recorded");
uint256 currentTime = block.timestamp;
return currentTime - transactionTimestamp;
}
}
```

7.7. Законски прашања во врска со спроведувањето на систем заснован на blockchain во ВОУ

Несомнено, сите закони и правни акти во нашата земја се регулираат во Собранието, со мнозинство гласови од пратениците. Дури и Законот за високо образование е регулиран со сите законски акти во парламентот, а последната верзија што ја изгласаа пратениците, а која и денеска е во сила е Законот за високо образование, изгласан на 2 мај 2018 година. со бр. 08-2973/1. Со член 97, што ги покажува надлежностите на Универзитетскиот сенат, овој закон јасно дефинира дека Сенатот има право да креира правни акти и прописи за работа со кои се дефинира доделувањето на диплома, додатокот за дипломирање и други постапки за стекнување на диплома во потребни случаи. Во член 155 од законот за високо образование во однос на дипломите, се појаснува дека секој студент што ќе ги заврши студиите, во одредена насока, мора да му биде обезбедена универзитетска диплома за студиите што ги завршил. Со дипломата студентот се прецизира за одредена област на студии, било да е тоа прв, втор или дури трет циклус на студии, каде освен со дипломата, студентот мора да му биде доделена и додатокот на диплома. Дипломата мора да биде потпишана од ректорот и деканот или директорот на одделението (одделот) и да биде со сув печат на ВОУ. Со овој закон е регулирано и прашањето за јазикот за генерирање дипломи, каде што се наведува дека таму каде што се изучува на јазик различен од македонскиот јазик, ВОУ имаат право да генерираат дипломи во стручниот јазик како и на македонски јазик на студентот. Содржината, формата на дипломата и прописите за изработка на дипломата ги уредува министерот надлежен за оваа област, односно министерот за образование. Дипломата на студентот може да му се одземе, доколку се докажат неправилности при стекнувањето на истата, звање може да се земе ако е незаконски стекната, меѓутоа овие акти и правилници се составени од самите универзитети преку нивниот сенат. Сите студенти што ќе ги завршат студиите на ВОУ мора да бидат евидентирани во книговодствената книга на соодветниот ВОУ, а за начинот, времетраењето и зачувувањето на истите одлучува министерот за образование преку соодветните законски акти и прописи. Министерството за образование преку инспекторатите има должност да ја контролира работата на ВОУ за доделување дипломи, а доколку има неправилности или дури и доделување дипломи во неправилна форма, во согласност со законите и правните акти утврдени со Министерството, можно е истите да се прогласат за неважечки, и во правна форма да поднесува до јавниот обвинител пријава за кривично гонење на одговорното лице. Некои ВОУ, иако генерирањето го прават во физичка форма, сепак имаат дигитализирани системи со кои управуваат со процесот на генерирање и верификација на дипломите, има случаи дека во текот на генерирањето, кај дипломите се прикачуваат и QR кодови, со цел тие лесно да се проверуваат во нивниот систем. Дипломите и додатокот на дипломата генерално ги содржат овие податоци: податоци за носителот на дипломата, податоци за стекнатата квалификација, податоци за степенот (циклусот) на квалификацијата, податоци за содржините и за постигнатите резултати, податоци за

користење на квалификацијата, податоци за заверка на додатокот на дипломата, податоци за системот на високото образование во Република Северна Македонија.

Примената на blockchain-системи во ВОУ претставува предизвик за сите главни актери вклучени во системот, меѓутоа, покрај предизвиците поврзани со трошоците, енергијата, одржувањето, приспособувањето на корисниците, постојат и правни предизвици што ВОУ мора да ги почитуваат при имплементирање на таков систем заснован на blockchain-технологија. Покрај законот за високо образование, секоја ВОУ има статут со кој се уредуваат сите правни акти со коишто работи. Во Северна Македонија, имплементацијата на ваков систем заснован на blockchain претставува голем предизвик, бидејќи повеќето услуги во овие институции сè уште се генерираат во физичка (хартиена) форма, а нивната дигитализација бара максимална посветеност од сите учесници (Универзитетско управување тела, академски кадар, административен персонал, студенти итн.). Меѓу другото, секоја ВОУ има свој образец за тоа како ги генерира дипломите. Нема стандардизација на дипломите, па затоа нивната верификација е многу потешка, во споредба со предложената дигитална верификација на дипломите, каде што покрај пократкото време, би било многу побезбедно, ефикасно, транспарентно и се нуди кредибилитетот на податоците. Но, пред да се направи каква било промена во таа насока, на неа мора да ѝ претходат измени на членовите во законската рамка, поточно статутот и другите релевантни правни акти засновани на статутот. Но, целосната дигитализација на дипломите, односно нивното генерирање во електронска форма, нивната верификација во електронска форма, мора да добие одобрение и од владата на земјата, односно Министерството за образование и наука, бидејќи се работи за генерирање документи кои се важни, а треба да го одржуваат државата и релевантните институции одговорни за високото образование во нашата земја. Сепак, главниот предизвик останува практичното создавање на blockchain-системот за генерирање и верификација на дипломи и академски документи. Правните аспекти, со измени на законските акти, може да се менуваат и да се дозволи електронско генерирање дипломи, иако мора да се прецизира и прашањето за дигитално складирање на податоците, односно до кога ќе се чуваат документите, во електронска форма во системот, бидејќи нивното складирање на неопределен период очигледно има високи трошоци за одржување и управување со мориските простори, кога знаеме дека за blockchain-системите одржувањето е многу поскапо од сегашните централизирани системи [175].

8. ПРИДОНЕСИ ОД ДОКТОРСКАТА ДИСЕРТАЦИЈА

Во оваа докторска тема е дефиниран нов модел на управување на јавните и приватните универзитети, каде како студија на случај се зема едно ВОУ, а потоа може да се имплементира за поширока мрежа на ВОУ. Имплементацијата на blockchain-систем би означила технолошка револуција, но пред сè би помогнала во дигитализацијата на услугите не само во ВОУ, туку и во други институции бидејќи има недостиг од дигитализација на услугите, а сепак повеќето документи се генерираат во физичка форма, бидејќи недостига еден безбеден и сигурен систем, што ќе овозможува да се чува интегритетот и приватноста на понудените услуги. Конкретно, проблематично е кога станува збор за податоци кои се врзани со приватноста на луѓето, како што се дипломите и другите приватни документи.

Темата на докторската дисертација влијае на унапредување и развој на оваа технологија во областа на образованието, за генерирање и проверка на дипломи, иако таков проблем постои насекаде во светот, а долгорочно решение за овој проблем сè уште не е најдено. Оттука очекуваме дека темата ќе влијае на пробудување на интересот на страните како алтернатива во блиска иднина да ја видат имплементацијата на blockchain во системите за управување со податоци во ВОУ. Едно е фактот што истражувачите кај нас и пошироко не се занимаваат со blockchain-програмирање, туку се занимаваат со криптовалути и економските придобивки што ги носи оваа технологија.

Со темата на докторската дисертација е направена детална анализа на имплементацијата на blockchain-технологијата за генерирање и проверка на дипломи, спроведувајќи систематски преглед на сите трудови што се поврзани со нашата тема. Во овој случај, се идентификувани празнините, причините зошто blockchain има делумна имплементација во ВОУ, генерирајќи нови теми поврзани со оваа проблематика и чекор по чекор разјаснувајќи ги во детали. Потоа истражувањето продолжува кон создавање на архитектура на blockchain-систем за имплементација во високообразовните институции. Дефинирани се сите функционални и нефункционални барања на системот, дефинирани се дијаграми за случаи на употреба и сценарија за главните актери вклучени во системот, за да се олесни процесот кон концептуално моделирање и создавање системска архитектура. Опишана е и целата потребна опрема за создавање на blockchain систем за генерирање и проверка на дипломи, со конкретни студиски случаи. Откако е направено детална споредба со сите практични решенија што постојат денес, а кои се создадени, но не наидоа на имплементација подолго време, откако се идентификувани и нивните празнини, создаден е концептуален модел на blockchain-системот, архитектурата на повеќе нивоа на blockchain-систем, систематска архитектура на процесот на генерирање и проверка на дипломи и конечно архитектурата на паметните договори и нивна меѓусебна поврзаност. Ова всушност ја претставува основата на нашата докторска тема, бидејќи успеавме да претставиме нов модел на

имплементација на blockchain-систем, со нова архитектура и јасно дефинирани паметни договори.

Темата продолжува со можностите за имплементација на вештачка интелигенција во blockchain-системот, бидејќи во денешни денови гледаме имплементација на многу интелигентни роботи, а зошто да не и во иднина вештачката интелигенција да не биде имплементирана во blockchain-системот за генерирање и проверка на дипломи, што многу би ја олеснило работата на системот. На крајот, е направен прототип на системот, каде се претставени некои од најважните делови од генерирањето и проверката на дипломите во посебно поглавје, истовремено правејќи споредби со централизиран систем. Blockchain-технологијата е факт дека има многу предности во имплементацијата, но има и недостатоци што се детално разсјаснети низ работата и токму тоа се веројатно причините поради што и во денешно време таа не се имплементира во образовните институции.

Од сите анализи, споредби и имплементација на прототипот на blockchain системот, гледаме дека, всушност, практичната имплементација на blockchain не е толку лесна како што изгледа во теорија. Практичната имплементација има многу предизвици, меѓу кои особено ќе го споменеме недостатокот на blockchain-база на податоци, што ќе може да складира големи количини на податоци. ИПФС е дистрибуиран систем за складирање и пристап до датотеки, користејќи P2P мрежа. Тоа е особено добро приспособено за сценарија каде што традиционалните централизирани сервери може да се борат да ракуваат со големи количини на податоци или каде вишокот и достапноста се клучни. Во таа смисла, тоа може да биде решение за предизвиците со големи податоци. Сепак, тој не е исклучиво приспособен за големи податоци. IPFS може да се користи за различни цели, освен за складирање на големи податоци, вклучувајќи веб-хостинг, испорака на содржина, па дури и градење децентрализирани апликации. Значи, иако ИПФС (IPFS) навистина може да се справи со големи податоци, тоа не е неговата единствена цел. Тоа е разновидна технологија со апликации во различни домени.

Втората е неможноста на системот да ги ажурира податоците, па дури и да ги зачува податоците и да ги прикажува кога сакаме. Тоа е затоа што практично податоците на крајот, пред да се складираат во форма на табели, класи, секоја од нив има единствената хаш-вредност која што се генерира во мрежата. Секоја единствена хаш-вредност е поврзана со соодветната хаш-вредност на претходно внесените податоци, со што се создава меѓусебно поврзана мрежа, која, за разлика од централизираните системи, е многу потежок за управување и пристапот до податоците е многу потежок.

Трето, во однос на безбедноста на податоците, blockchain-системите се многу побезбедни, бидејќи не е можно да се сменат податоците, а не да се потврдат со други јазли во мрежата. За разлика од централизираните системи, што може да се менуваат директно од базата на податоци и многу е тешко да се разликува таква промена. Значи, секоја промена на податоците во мрежата мора да биде потврдена од сите јазли што се

дел од мрежата и дури тогаш може да се додадат податоците, додека практично процесот на одземање дипломи е невозможен, и таа да се генерира пак со иста хаш-вредност. Одземањето на дипломите доаѓа во израз само со регенерација на дипломите, со друга единствена хаш-вредност.

Докторската дисертација е кохерентна тема, тема за која има посебен интерес од сите истражувачи ширум светот, за кои научните истражувања што се занимаваат со имплементација на blockchain-системи, се сите кохерентни и од последниве години. Преку практичната имплементација потврдивме дека системот е функционален, додека работата што ни остана е да го тестираме со конкретни случаи на студирање, земајќи вистински дипломи и во реално време да тестираме колку ќе биде генерирањето и проверката во реално време на повеќе дипломи. Ваков blockchain-систем може да се имплементира и во други области, како што се медицината, финансиите и секаде каде што има потреба од управување со големи податоци, а во исто време и обработка на податоци во реално време. Може да се имплементира низ целата земја за да се создаде blockchain-платформа, со која ќе се управуваат сите високообразовни институции, јавни и приватни, со цел да се надминат различните проблеми со злоупотреба на податоци, разни научни трудови и разни академски звања што се во корист и од страна на студенти и професори од различни ВОУ.

9. ЗАКЛУЧОК И ПОНАТАМОШНА РАБОТА

Досегашното истражување уште еднаш ја потврдува главната хипотеза, дека blockchain-системите се побезбедни, потранспарентни и всушност претставуваат технолошка револуција за ВОУ, со која покрај дигитализацијата на услугите ќе се нудат и други важни услуги, како што се генерирањето и проверката на дипломите. Ова истражување може да го спроведат повеќе ВОУ во нашата земја, создавајќи широка blockchain мрежа, каде ќе бидат поврзани сите јавни и приватни ВОУ, што би претставувало целосна дигитализација на сите понудени услуги во ВОУ.

Покрај главната, исто така се потврдуваат и посебните хипотези:

- едукативни blockchain-платформи што се создадени до денес, не нудат оптимални и сигурни решенија за генерирање и проверка на електронски начин на дипломи и други академски документи;
- одржувањето на услугите на blockchain системот е тежок процес, доколку ВОУ не е самоодржлива, при што за такво нешто е потребна обука и специјализација на кадарот во институцијата;
- процесот на одземање дипломи и регенерација има предизвици, бидејќи такво нешто мора добро да се анализира, затоа што дипломата не може да се генерира двапати со исти податоци користејќи иста вредност на хашот, додека безбедноста на податоците во blockchain се засновува на уникатната хаш вредност;
- може да се создаде сеопфатен blockchain-систем за управување со сите услуги во ВОУ, не само со образовниот процес.

Докторскиот труд се разликува од сите други истражувања досега, бидејќи му дава посебно значење на процесот на токенизација на дипломите. Тоа значи дека дипломите, откако ќе се изготват, се потпишуваат во дигитална форма од сите страни кои се неопходни, се чуваат во базата на податоци во форма на токени, кои несомнено имаат свои уникатни карактеристики, а пред сѐ гарантираат непроменливост на нивните податоци. Во повеќето blockchain-системи, самите токени обично претставуваат фиксни единици на вредност или сопственост и не се дизајнирани да се ажурираат откако ќе се создадат. Сепак, податоците поврзани со токен, како што се метаподатоци или атрибути, може да се ажурираат преку различни механизми во зависност од специфичниот протокол на blockchain и функционалностите на паметниот договор. Кога податоците поврзани со токен се ажурираат, како што се менување на метаподатоци или атрибути, вредноста на хашот што ги претставува тие податоци навистина ќе се промени. Оваа промена се случува затоа што хаш-функцијата, што ја генерира вредноста на хашот, е дизајнирана да произведе единствен излез за секоја промена во влезните податоци. На пример, ако токен претставува диплома и метаподатоците поврзани со таа диплома се ажурираат (како што е додавање дополнителен акредитив

или ажурирање на институцијата што ја издава), ажурираните метаподатоци ќе резултираат со различна вредност на хашот. Ова осигурува дека секоја страна што ја потврдува автентичноста на токенот може да открие промени на основните податоци. Сепак, важно е да се забележи дека менувањето на податоците поврзани со токен може да бара конкретни дозволи или да следи одредени правила дефинирани со протоколот за blockchain или паметниот договор што го регулира токенот. Дополнително, ажурирањето на податоците за токените може да предизвика такси за трансакциите и да бара консензус од учесниците во мрежата, во зависност од blockchain-системот што се користи.

Преку оваа докторска дисертација е направено:

1. Сеопфатен преглед и систематизација на сите blockchain-базирани системи за употреба во ВОУ во светот денес,
2. Предлог на нова архитектура на систем за генерирање и проверка на дипломи,
3. Имплементација на blockchain-прототип, со што се потврдува дефинираната архитектура, и дека системот е функционален.
4. Системска валидација, предвидувачка анализа преку математички техники, и претставување на прототипот преку интерфејси.
5. Анализа на правни прашања поврзани со имплементацијата на blockchain-системот преку ВОУ.

Како понатамошна работа останува:

1. Можноста за сеопфатна имплементација на системот ДИАР (DIAR), што бара многу тимска работа, и трошоци до вистинска практична имплементација.
2. Тестирање на системот ДИАР во реални дипломи, во која било ВОУ, за тестирање на перформансите, при паралелна обработка на неколку дипломи.
3. Можноста за имплементација на интелигентни агенти во системот ДИАР, со цел да се дозволи и заштити од разни напади и да им се олесни на сите актери користењето.
4. Можност за модифицирање на системот ДИАР и негово имплементирање во други сфери, за генерирање и верификација на документи што се важни за различни јавни и приватни институции.

Имплементацијата на ДИАР-системот, во ВОУ, ако не за која било друга цел, туку за генерирање и проверка на дипломи, би го забрзала процесот на генерирање дипломи, би го олеснила процесот на проверка на дипломите и би спречило какво било сомневање за можните злоупотреби што можат да се направат на овие важни документи. „**Дизајн на безбеден систем за генерирање и проверка на академски документи базиран на blockchain-технологија**", е кохерентна тема, каде истражувачите ширум светот му даваат големо значење на имплементацијата на таков систем, иако е полн со предизвици и тешкотии. Дизајн на новиот blockchain-систем ДИАР, неговата системска архитектура и модели дефинирани во оваа докторска тема, веруваме, ќе бидат поттик за идните истражувачи.

10. ТРУДОВИ ОБЈАВЕНИ ОД ДОКТОРСКАТА ДИСЕРТАЦИЈА

Ја сумираме докторска теза со 16 научни трудови, меѓу другото во списанија со импакт-фактор, меѓународни конференции, кои меѓу другото и индексирани во бази на податоци како ИЕЕЕ, Скопус, Спрингер, Веб оф сајанс. Списокот на научни трудови е:

1. A. Rustemi, F. Dalipi, V. Atanasovski, A. Risteski, "DIAR: a Blockchain-Based System for Generation and Verification of Academic Diplomas", Journal of Discover Applied Science, Volume 6, Article 297 (2024). https://doi.org/10.1007/s42452-024-05984-1 Springer, 2024.
2. A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," in IEEE Access, vol. 11, pp. 64679-64696, 2023, doi: 10.1109/ACCESS.2023.3289598.
3. A. Rustemi, V. Atanasovski and A. Risteski, "Design of the Blockchain System for the Generation and Verification of Diplomas," 2023 XXXII International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 2023, pp. 1-6, doi: 10.1109/ET59121.2023.10279743.
4. A. Rustemi, V. Atanasovski, A. Risteski and B. Popovski, "Analysis of Blockchain Platforms for Generation and Verification of Diplomas," 2023 12th Mediterranean Conference onEmbedded Computing (MECO), Budva, Montenegro, 2023, pp. 1-4, doi: 10.1109/MECO58584.2023.10154926.
5. A. Rustemi, V. Atanasovski, A. Risteski and P. Latkoski, "Challenges of Blockchain in Higher Education Institutions for Protection Against Diploma Forgery," 2023 International Balkan Conference on Communications and Networking (BalkanCom), İstanbul, Turkiye, 2023, pp. 1-6, doi: 10.1109/BalkanCom58402.2023.10167986.
6. A. Rustemi, V. Atanasovski and A. Risteski, "Identification During Verification Of Diplomas In The Blockchain System," 2023 30th International Conference on Systems, Signals and Image Processing (IWSSIP), Ohrid, North Macedonia, 2023, pp. 1-5, doi: 10.1109/IWSSIP58668.2023.10180241.
7. A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "Towards a Conceptual Model of a Blockchain System for Automatic Generation of Academic Diplomas: Use Cases and Scenarios," 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Plovdiv, Bulgaria, 2023, pp. 1-6, doi: 10.1109/CIEES58940.2023.10378773.
8. A. Rustemi, V. Atanasovski and A. Risteski, "Overview of Blockchain Data Storage and Privacy Protection," 2022 International Balkan Conference on Communications and Networking (BalkanCom), Sarajevo, Bosnia and Herzegovina, 2022, pp. 90-94, doi: 10.1109/BalkanCom55633.2022.9900867.
9. Avni Rustemi, Vladimir Atanasovski, Aleksandar Risteski, “Security and transparency of blockchain systems in higher education institutions”, Journal of Natural Sciences

and Mathematics of UT, Vol 8, No.15-16, ISSN(print): 2545-4072,ISSN (online):2671-3039.

10. A. Rustemi, V. Atanasovski, A. and Risteski, "Database Design in a Blockchain-Based System for Generating and Verifying Academic Credentials". Journal of Electrical Engineering and Information Technologies, pp.93-100. 2023. 210.
11. A. Rustemi, V. Atanasovski, A. Risteski, V. Angelkoska, "Legislation issues regarding the implementation of blockchain-based application in higher education institution in North Macedonia", 2nd International Scientific Conference : the Future of Science, University "Ukshin Hoti" Prizren, ISBN 978-9951-510-31-8.
12. Avni Rustemi, Vladimir Atanasovski and Aleksandar Risteski, "Framework for Using BigchainDB in Software Application", held at the Faculty of Computer Science and Engineering, Skopje, North Macedonia 5-6th May, 2022, pp.64-69, ISBN 978-608-4699-15-6.
13. Aleksandar Risteski., Avni Rustemi., "The Application of the Internet of Things in Everyday Equipment Affects to Have a More Efficient and Quality Life", ETAI 2021, online conference, 23-24 September 2021, pp.242-247, ISSN:2545-4489.
14. A. Rustemi, V. Atanasovski, A. Risteski, F. Idrizi and V. Angelkoska, "Theoretical Approach Of Implementing Blockchain And Artificial Intelligence For Diploma Verification," 2024 13th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2024, pp. 1-4, doi: 10.1109/MECO62516.2024.10577813.
15. A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "Enhancing Academic Credentials: The Synergy of Blockchain and Artificial Intelligence," 2024 7th International Balkan Conference on Communications and Networking (BalkanCom), Ljubljana, Slovenia, 2024, pp. 206-211, doi: 10.1109/BalkanCom61808.2024.10557185.
16. Avni Rustemi, Vladimir Atanasovski, Aleksandar Risteski, V. Angelkoska “Decentralized Artificial Intelligence for Diploma Verification: Regression Techniques Analyses”, Journal of Natural Sciences and Mathematics of UT, Vol 9, No.17-18, ISSN(print): 2545-4072,ISSN (online):2671-3039.

КОРИСТЕНА ЛИТЕРАТУРА

[1] G. M. Alam, ‘‘Does online technology provide sustainable HE or aggravate diploma disease? Evidence from Bangladesh—A comparison of conditions before and during COVID-19,’’ Technol. Soc., vol. 66, Aug. 2021, Art. no. 101677, doi: 10.1016/j.techsoc.2021.101677.3

[2] P. Luik, R. Suviste, M. Lepp, T. Palts, E. Tõnisson, M. Säde, and K. Papli, ‘‘What motivates enrolment in programming MOOCs?’’ Brit. J. Educ. Technol., vol. 50, no. 1, pp. 153–165, Jan. 2019, doi: 10.1111/bjet. 12600.

[3] E. Whitford and J. Novack (Forbes Staff). (Feb. 2023). How Thousands Of Nurses Got Licensed With Fake Degrees. Accessed: Mar. 1, 2023. [Online]. Available: https://www.forbes.com/sites/emmawhitford/2023/02/21/howthousands-of-nurses-got-licensed-with-fake-degrees/?sh=2edbdf8f5c6d

[4] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," Sustain. Energy Technol. Assessments, vol. 52, Aug. 2022, Art. no. 102039, doi: 10.1016/j.seta.2022.102039.

[5] T. Savelyeva and J. Park, ‘‘Blockchain technology for sustainable education,’’ Brit. J. Educ. Technol., vol. 53, no. 6, pp. 1591–1604, Nov. 2022, doi: 10.1111/bjet.13273.

[6] A. O. J. Kwok and H. Treiblmaier, "No one left behind in education: blockchain-based transformation and its potential for social inclusion," Asia Pacific Educ. Rev., vol. 23, no. 3, pp. 445–455, Sep. 2022, doi: 10.1007/s12564-021-09735-4.

[7] F. P. Oganda, N. Lutfiani, Q. Aini, U. Rahardja, and A. Faturahman, "Blockchain education smart courses of massive online open course using business model canvas,’’ in Proc. 2nd Int. Conf. Cybern. Intell. Syst. (ICORIS), Oct. 2020, pp. 1–6, doi: 10.1109/ICORIS50180.2020.9320789.

[8] E. Kahraman. (Oct. 28, 2021). Wharton Accepts Crypto Payments for Blockchain Program Tuition Fees. Accessed: Feb. 14, 2023. [Online]. Available: https://cointelegraph.com/news/wharton-accepts-crypto-payments-for-blockchain-program-tuition-fees

[9] P. Bhaskar, C. K. Tiwari, and A. Joshi, ‘‘Blockchain in education management: Present and future applications,’’ Interact. Technol. Smart Educ., vol. 18, no. 1, pp. 1–17, May 2021, doi: 10.1108/ITSE-07-2020- 0102.

[10] H. A. Alsobhi, R. A. Alakhtar, A. Ubaid, O. K. Hussain, and F. K. Hussain, ‘‘Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review,’’ Knowl.-Based Syst., vol. 265, Apr. 2023, Art. no. 110238, doi: 10.1016/j.knosys.2022.110238.

[11] D.-H. Nguyen, D.-N. Nguyen-Duc, N. Huynh-Tuong, and H.-A. Pham, ‘‘CVSS: A blockchainized certificate verifying support system,’’ in Proc. 9th Int. Symp. Inf. Commun. Technol. (SoICT), 2018, pp. 436–442, doi: 10.1145/3287921.3287968.

[12] S.-K. Kim, ‘‘Blockchain smart contract to prevent forgery of degree certificates: Artificial intelligence consensus algorithm,’’ Electronics, vol. 11, no. 14, p. 2112, Jul. 2022, doi: 10.3390/electronics11142112.

[13] Research on Information Security Technology Based on Blockchain, Liang Liu ;Budong Xu, 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China

[14] "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", Zibin Zheng, ShaoanXie, Hongning Dai, Xiangping Chen, and Huaimin Wang, 2017 IEEE 6th International Congress on Big Data

[15] “Byzantine Fault Tolerance Explained” ;by:Binance Academy ; 06.12.2018 available: https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained

[16] I.-C. Lin and T.-C. Liao, ``A survey of blockchain security issues and challenges," Int. J. Netw. Secur., vol. 19, no. 5, pp. 653659, Sep. 2017, doi: 10.6633/IJNS.201709.19(5).01.

[17] Y. Xinyi, Z. Yi, and Y. He, ``Technical characteristics and model of blockchain," in Proc. 10th APCA Int. Conf. Control Soft Comput. (CONTROLO), Jun. 2018, pp. 562-566.

[18] A. Javed. Managing Data Traceability: Impact and Benets. Accessed: May 11, 2019. [Online]. Available: http://www.xorlogics.com/2017/04/10/managing-data-traceability-impact-and-benefits/.

[19] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, ``A survey of blockchain technology applied to smart cities: Research issues and challenges," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 27942830, Feb. 2019.

[20] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, ``Integrated blockchain and edge computing systems: A survey, some research issues and challenges," IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 15081532, 2nd Quart., 2019, doi: 10.1109/COMST.2019.2894727.

[21] D. Massessi. Blockchain Consensus and Fault Tolerance in a Nutshell. Accessed: May 12, 2019. [Online]. Available: https://medium.com/ coinmonks/Blockchain-consensus-and-fault-tolerance-in-a-nutshell765de83b8d03

[22] Y. Lu, ``Blockchain: A survey on functions, applications and open issues," J. Ind. Integr. Manage., vol. 3, no. 4, Dec. 2018, Art. no. 1850015.

[23] Marchesi L, Marchesi M, Tonelli R, Lunesu MI (2022) A blockchain architecture for industrial applications. Blockchain: Research and Applications. 3(4), 100088. https://doi.org/10.1016/j.bcra.2022.100088

[24] Hadzhikoleva S, Uzunov A, Hadzhikolev E, Cheresharov S (2022) Conceptual Model of a Quality Assurance System in Higher Education. In 2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH). March, pp. 1-6. IEEE. https://doi:10.1109/INFOTEH53737.2022.9751316

[25] Härer F, Fill HG (2022) Decentralized attestation and distribution of information using blockchains and multi-protocol storage. IEEE Access. 10, 18035-18054. https://doi:10.1109/ACCESS.2022.3150356

[26] Xu M, Zou Z, Cheng Y, Hu Q, Yu D, Cheng X (2022) SPDL: A blockchain-enabled secure and privacy-preserving decentralized learning system. IEEE Transactions on Computer. 72(2), 548-558. https://doi: 10.1109/TC.2022.3169436

[27] Toapanta SMT, Durango RHDP, Díaz EZG, Trejo JAO, Gallegos LEM, Arellano MRM, Vizuete MZ, Hifóng MMB (2023) Proposal for a security model applying artificial intelligence for administrative management in a higher education institution. In 2023 International Conference on Computer, Information and Telecommunication Systems (CITS). July 2023, (pp. 1-5). IEEE. https://doi:10.1109/CITS58301.2023.10188801

[28] H. A. Alsobhi, R. A. Alakhtar, A. Ubaid, O. K. Hussain, F. K. Hussain, "Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review", Knowledge-Based Systems, Volume 265, 2023, 110238, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2022.110238 .

[29] M. R. H. Polas, A. A. Jahanshahi, A. I. Kabir, A. S. S.U. Zaman, A. R. Osman, and R. Karim, "Artificial Intelligence, Blockchain Technology, and Risk-Taking Behavior in the 4.0IR Metaverse Era: Evidence from Bangladesh-Based SMEs", Journal of Open Innovation: Technology, Market, and Complexity 8, no. 3: 168. 2022. https://doi.org/10.3390/joitmc8030168.

[30] I. Khan, A. R. Ahmad, N. Jabeur, M. N. Mahdi, "An artificial intelligence approach to monitor student performance and devise preventive measures". Smart Learn. Environ. 8, 17 (2021). https://doi.org/10.1186/s40561-021-00161-y.

[31] Y. Peng, X. Yang, and H. Zhou, “Blockchain Technology and Higher Education: Characteristics, Dilemma and Development Path”. In Proceedings of the 2020 4th International Conference on Education and E-Learning (ICEEL '20). Association for Computing Machinery, New York, 2021, NY, USA, 173–176. https://doi.org/10.1145/3439147.3439185.

[32] Sh. Liu and L. Ba, “Blockchain Technology and Its Application Prospect in Higher Education”. In Proceedings of the 13th International Conference on Education Technology and Computers (ICETC '21). Association for Computing Machinery, New York, 2022, NY, USA, 237–242. https://doi.org/10.1145/3498765.3498802

[33] L. Chen, P. Chen and Z. Lin, "Artificial Intelligence in Education: A Review," in IEEE Access, vol. 8, pp. 75264-75278, 2020, doi: 10.1109/ACCESS.2020.2988510.

[34] S.K. Kim, "Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm". Journal of Electronics 2022, 11, 2112. https://doi.org/10.3390/electronics11142112

[35] Z. A. Shaikh, A.A. Khan, L. Baitenova, G. Zambinova, N. Yegina, N. Ivolgina, A.A. Laghari, S.E. Barykin, "Blockchain Hyperledger with Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture". Journal of Applied Science, 2022, Volume 12, 2534. https://doi.org/10.3390/ app12052534.

[36] Zh. and S. Zhang, X. and L. Lei, J. and W. Yin, Y. and L. Dapeng, "Recent Advances in Blockchain and Artificial Intelligence Integration: Feasibility Analysis, Research Issues, Applications, Challenges, and Future Work". Security and Communication Networks. 2021. 1-15. 10.1155/2021/9991535.

[37] H. M.-Leong, and S.-M. Cheah, "Forging the Future: Strategic Approaches to Quantum AI Integration for Industry Transformation", 2024, AI journal, Volume 5, no. 1: 290-323. https://doi.org/10.3390/ai5010015

[38] M. Cankar, N. Petrović, J. P. Costa, A. Černivec, J. Antić, T. Martinčič, and D. Štepec, "Security in DevSecOps: Applying Tools and Machine Learning to Verification and Monitoring Steps". In the Companion of the 2023 ACM/SPEC International Conference on Performance Engineering (ICPE ’23 Companion), April 15–19, 2023, Coimbra, Portugal. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3578245.3584943.

[39] A. Koubaa, W. Boulila, L. Ghouti, A. Alzahem and S. Latif, "Exploring ChatGPT Capabilities and Limitations: A Survey," in IEEE Access, vol. 11, pp. 118698-118721, 2023, doi: 10.1109/ACCESS.2023.3326474.

[40] O. Ural and K. Yoshigoe, "Survey on Blockchain-Enhanced Machine Learning," in IEEE Access, vol. 11, pp. 145331-145362, 2023, doi: 10.1109/ACCESS.2023.3344669.

[41] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin and X. Li, "A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications," in IEEE Communications Surveys & Tutorials, vol. 25, no. 4, pp. 2494-2528, Fourthquarter 2023, doi: 10.1109/COMST.2023.3315374.

[42] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," in IEEE Access, vol. 11, pp. 64679-64696, 2023, doi: 10.1109/ACCESS.2023.3289598.

[43] R. G. Luis, T. Watt, K. O. Babaagba, Ch. Chrysolaus, A. Homay, R. Rangarajan, and X. Liu, “Emotion Recognition on Social Media Using Natural Language Processing (NLP) Techniques”. In 2023 The 6th International Conference on Information Science and Systems (ICISS 2023), August 11–13, 2023, Edinburgh, United Kingdom. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3625156.3625173.

[44] P. Lahoti, N. Mittal, and G. Singh, "A Survey on NLP Resources, Tools, and Techniques for Marathi Language Processing". ACM Trans. Asian Low-Resour. Lang. Inf. Process. 22, 2, Article 47 (December 2022), 34 pages. https://doi.org/10.1145/3548457.

[45] J. Dong, "Natural Language Processing PreTraining Language Model for Computer Intelligent Recognition Technology". ACM Trans. Asian Low-Resour. Lang. Inf. Process.(June 2023). https://doi.org/10.1145/3605210.

[46] Y. Yuan, J. Zhang, W. Xu, Zh. Li, “Identity-based public data integrity verification scheme in cloud storage system via blockchain”. The Journal of Supercomputing 78, 8509–8530 (2022). https://doi.org/10.1007/s11227-021-04193-6

[47] A. Rustemi, V. Atanasovski, A. Risteski and B. Popovski, "Analysis of Blockchain Platforms for Generation and Verification of Diplomas," 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2023, pp. 1-4, doi: 10.1109/MECO58584.2023.10154926.

[48] C.-S. Hsu, S.-F. Tu, and P.-C. Chiu, ‘‘Design of an E-diploma system based on consortium blockchain and facial recognition,’’ Educ. Inf. Technol., vol. 27, no. 4, pp. 5495–5519, May 2022, doi: 10.1007/s10639-02110840-5.

[49] M. Khan, T. Naz, “Smart Contracts Based on Blockchain for Decentralized Learning Management System”. SN Computer Science, 2, 260 (2021). https://doi.org/10.1007/s42979-021-00661-1.

[50] L. K. Ramasamy, F. Khan, “Blockchain-Based Certification System: Ensuring Trust in Educational Credentials”. In: Blockchain for Global Education, 2024, Springer, Cham. https://doi.org/10.1007/978-3-031-52123-2_7.

[51] V. Hassija, V. Chamola, A. Mahapatra et al. “Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence”. Cognitive Computation, 16, 45–74 (2024). https://doi.org/10.1007/s12559-023-10179-8.

[52] L. Cui, C. Zhu, R. Hare, et al. MetaEdu: a new framework for future education. Discover Artificial Intelligence Volume 3, 10 (2023). https://doi.org/10.1007/s44163-023-00053-9

[53] Z. Han, Y. Tu and C. Huang, "A Framework for Constructing a Technology -Enhanced Education Metaverse: Learner Engagement With Human–Machine Collaboration," in IEEE Transactions on Learning Technologies, vol. 16, no. 6, pp. 1179-1189, Dec. 2023, doi: 10.1109/TLT.2023.3257511.

[54] Farley et al “OCR - Optical Character Recognition”, online, 2023, Url (https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/overview-ocr), Accessed: 01.02.2024.

[55] Z. Shahbazi and Y. -C. Byun, "Blockchain-Based Event Detection and Trust Verification Using Natural Language Processing and Machine Learning," in IEEE Access, vol. 10, pp. 5790-5800, 2022, doi: 10.1109/ACCESS.2021.3139586.

[56] Chaka C (2023) Fourth industrial revolution—a review of applications, prospects, and challenges for artificial intelligence, robotics and blockchain in higher education. Research and Practice in Technology Enhanced Learning. 18, 002-002. https://doi.org/10.58459/rptel.2023.18002

[57] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, ``Making smart contracts smarter," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2016, pp. 254-269.

[58] X. Wang, X. Ren, C. Qiu, Z. Xiong, H. Yao and V. C. M. Leung, "Integrating Edge Intelligence and Blockchain: What, Why, and How," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2193-2229, Fourthquarter 2022, doi: 10.1109/COMST.2022.3189962.

[59] R. Salama, F. Al-Turjman, ―Blockchain Technology, Artificial Intelligence, and Big Data in Education‖. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, 2023, vol 1115. Springer, Cham.https://doi.org/10.1007/978-3-031-42924-8_16.

[60] D. Moher, ‘‘Preferred reporting items for systematic reviews and metaanalyses: The PRISMA statement,’’ Ann. Internal Med., vol. 151, no. 4, p. 264, Aug. 2009, doi: 10.7326/0003-4819-151-4-20090818000135.

[61] H. Gaikwad, N. D’Souza, R. Gupta, and A. K. Tripathy, ‘‘A blockchainbased verification system for academic certificates,’’ in Proc. Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN), Puducherry, India, Jul. 2021, pp. 1–6, doi: 10.1109/ICSCAN53069.2021.9526377.

[62] N. Chowdhury, Inside Blockchain, Bitcoin, and Cryptocurrencies. Boca Raton, FL, USA: Auerbach Publications, 2019.

[63] N. Kumar, K. Upreti, R. D. Raut, and D. Mohan, ‘‘Blockchain adoption for data integrity in higher education E-learning,’’ in Proc. Int. Conf. Data Analytics Bus. Ind. (ICDABI), Oct. 2021, pp. 1–6, doi: 10.1109/ICDABI53623.2021.9655928.

[64] U. Rahardja, M. A. Ngad, S. Millah, E. P. Harahap, and Q. Aini, ‘‘Blockchain application in educational certificates and verification compliant with general data protection regulations,’’ in Proc. 10th Int. Conf. Cyber IT Service Manage. (CITSM), Sep. 2022, pp. 1–7, doi:10.1109/CITSM56380.2022.9935909.

[65] N. Ahmad, R. P. George, R. Jahan, and S. Hussain, ‘‘Integrated IoT and block chain for secured access and managing education data,’’ in Proc. 3rd Int. Conf. Intell. Comput. Instrum. Control Technol. (ICICICT), Aug. 2022, pp. 1201–1204, doi: 10.1109/ICICICT54557.2022.9917643.

[66] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, ‘‘Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions,’’ IEEE Commun. Surveys Tuts., vol. 24, no. 1, pp. 160–209, 1st Quart., 2022, doi: 10.1109/COMST.2021.3131711.

[67] O. S. Saleh, O. Ghazali, and N. Bashah Idris, ‘‘A new decentralized certification verification privacy control protocol,’’ in Proc. 3rd Int. Cyber Resilience Conf. (CRC), Langkawi Island, Malaysia, Jan. 2021, pp. 1–6, doi: 10.1109/CRC50527.2021.9392485.

[68] Y. Peng, X. Yang, and H. Zhou, ‘‘Blockchain technology and higher education: Characteristics, dilemma and development path,’’ in Proc. 4th Int. Conf. Educ. E-Learning, Nov. 2020, pp. 173–176, doi: 10.1145/3439147.3439185.

[69] Q. Tang, ‘‘Towards using blockchain technology to prevent diploma fraud,’’ IEEE Access, vol. 9, pp. 168678–168688, 2021, doi: 10.1109/ACCESS.2021.3137901.

[70] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, ‘‘A survey on metaverse: Fundamentals, security, and privacy,’’ IEEE Commun. Surveys Tuts., vol. 25, no. 1, pp. 319–352, 1st Quart., 2023, doi: 10.1109/COMST.2022.3202047.

[71] N. Kumar, K. Upreti, R. D. Raut, and D. Mohan, ‘‘Blockchain adoption for data integrity in higher education E-Learning,’’ in Proc. Int. Conf. Data Analytics Bus. Ind. (ICDABI), Sakheer, Bahrain, Oct. 2021, pp. 1–6, doi: 10.1109/ICDABI53623.2021.9655928.

[72] S. Agrawal and A. K. Mishra, ‘‘Deploying blockchain in education: Security, challenges, and solutions,’’ in Proc. 5th Int. Conf. Inf. Syst. Comput. Netw. (ISCON), Mathura, India, Oct. 2021, pp. 1–5, doi: 10.1109/ISCON52037.2021.9702501.

[73] F. A. Sunny, P. Hajek, M. Munk, M. Z. Abedin, Md. S. Satu, Md. I. A. Efat, and Md. J. Islam, ‘‘A systematic review of blockchain applications,’’ IEEE Access, vol. 10, pp. 59155–59177, 2022, doi: 10.1109/ACCESS.2022.3179690.

[74] A. Averin, D. Snegireva, and A. Ladejshchikov, ‘‘Model of a monitoring system for academic performance and the issuance of diplomas using blockchain technology,’’ in Proc. Int. Conf. Quality Manage., Transp. Inf. Secur., Inf. Technol. (ITQMIS), Yaroslavl, Russia, Sep. 2020, pp. 88–91, doi: 10.1109/ITQMIS51053.2020.9322966.

[75] Y. Wang, H. Peng, Z. Su, T. H. Luan, A. Benslimane, and Y. Wu, ‘‘A platform-free proof of federated learning consensus mechanism for sustainable blockchains,’’ IEEE J. Sel. Areas Commun., vol. 40, no. 12, pp. 3305–3324, Dec. 2022, doi: 10.1109/JSAC.2022.3213347.

[76] Y. Wang, Z. Su, J. Li, N. Zhang, K. Zhang, K. R. Choo, and Y. Liu, ‘‘Blockchain-based secure and cooperative private charging pile sharing services for vehicular networks,’’ IEEE Trans. Veh. Technol., vol. 71, no. 2, pp. 1857–1874, Feb. 2022, doi: 10.1109/TVT.2021.3131744.

[77] S. O. Ghazali, O. Rana, and M. Ehsan, ‘‘Blockchain based framework for educational certificates verification,’’ J. Crit. Rev., vol. 7, pp. 79–84, Mar. 2020, doi: 10.31838/jcr.07.03.13.

[78] K. K and S. Jayalakshmi, ‘‘The impact of the blockchain on academic certificate verification system-review,’’ EAI Endorsed Trans. Energy Web, Jul. 2018, Art. no. 169426, doi: 10.4108/eai.29-4-2021.169426.

[79] Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, and Z. Zhou, ‘‘SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain,’’ IEEE Trans. Ind. Informat., vol. 17, no. 11, pp. 7688–7699, Nov. 2021, doi: 10.1109/TII.2020.3040171.

[80] S. Pathak, V. Gupta, N. Malsa, A. Ghosh, and R. N. Shaw, ‘‘Blockchainbased academic certificate verification system—A review,’’ in Advanced Computing and Intelligent Technologies (Lecture Notes in Electrical Engineering), vol. 914, R. N. Shaw, S. Das, V. Piuri, and M. Bianchini, Eds. Singapore: Springer, 2022, doi: 10.1007/978-981-19-2980-9_42.

[81] Y. Xiao and M. Watson, ‘‘Guidance on conducting a systematic literature review,’’ J. Planning Educ. Res., vol. 39, no. 1, pp. 93–112, Mar. 2019.

[82] S. Sharma and R. S. Batth, ‘‘Blockchain technology for higher education sytem: A mirror review,’’ in Proc. Int. Conf. Intell. Eng. Manage. (ICIEM), London, U.K., Jun. 2020, pp. 348–353, doi: 10.1109/ICIEM48762.2020.9160274.

[83] M. Staples and M. Niazi, ‘‘Experiences using systematic review guidelines,’’ J. Syst. Softw., vol. 80, no. 9, pp. 1425–1437, Sep. 2007, doi: 10.1016/j.jss.2006.09.046.

[84] N. Nousias, G. Tsakalidis, G. Michoulis, S. Petridou, and K. Vergidis, ‘‘A process-aware approach for blockchain-based verification of academic qualifications,’’ Simul. Model. Pract. Theory, vol. 121, Dec. 2022, Art. no. 102642, doi: 10.1016/j.simpat.2022.102642.

[85] O. Ghazali and O. S. Saleh, ‘‘A graduation certificate verification model via utilization of the blockchain technology,’’ J. Telecommun., Electron. Comput. Eng., vol. 10, nos. 2–3, pp. 29–34, Sep. 2018.

[86] O. Salau and S. A. Adeshina, ‘‘Secure document verification system using blockchain,’’ in Proc. 1st Int. Conf. Multidisciplinary Eng. Appl. Sci. (ICMEAS), Abuja, Nigeria, Jul. 2021, pp. 1–7, doi: 10.1109/ICMEAS52683.2021.9739812.

[87] C. Renato and M. A.-Y. Oliveira, ‘‘Blockchain and higher education diplomas,’’ Eur. J. Invest. Health, Psychol. Educ., vol. 11, no. 1, pp. 154–167, 2021, doi: 10.3390/ejihpe11010013.

[88] K. Kumutha and S. Jeyalaksshmi, ‘‘Blockchain technology and academic certificate authenticity-review,’’ in Proc. ICOECA, Bangalore, Jun. 2021, pp. 1–13.

[89] A. O. J. Kwok and H. Treiblmaier, ‘‘No one left behind in education: blockchain-based transformation and its potential for social inclusion,’’ Asia Pacific Educ. Rev., vol. 23, no. 3, pp. 445–455, Sep. 2022, doi: 10.1007/s12564-021-09735-4.

[90] A. Serek, A. Bazarkulova, A. Chazhabayev, and A. Akhmetov, ‘‘Analysis of supervisors and students in the context of diploma defense,’’ in Proc. 16th Int. Conf. Electron. Comput. Comput. (ICECCO), Kaskelen, Kazakhstan, Nov. 2021, pp. 1–4, doi: 10.1109/ICECCO53203.2021.9663776.

[91] M. C. Stana, N. Goga, C. V. Marian, R. Popa, C. Vulpe, and C. Taslitchi, ‘‘G-cloud briefcase–electronic archive for academic certificates and general certificates of education documents using public private hyperspace for E-government library services based on NOSQL databases,’’ in Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom), Bucharest, Romania, May 2021, pp. 1–5, doi: 10.1109/BlackSeaCom52164.2021.9527826.

[92] J. C. Cheng, N. Y. Lee, C. Chi, and Y. H. Chen, ‘‘Blockchain and smart contract for digital certificate,’’ in Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI), Chiba, Japan, Apr. 2018, pp. 1046–1051, doi: 10.1109/ICASI.2018.8394455.

[93] F. M. Enescu, N. Bizon, and V. M. Ionescu, ‘‘Blockchain technology protects diplomas against fraud,’’ in Proc. 13th Int. Conf. Electron., Comput. Artif. Intell. (ECAI), Pitesti, Romania, Jul. 2021, pp. 1–6, doi: 10.1109/ECAI52376.2021.9515107.

[94] K. Nikolskaia, D. Snegireva, and A. Minbaleev, ‘‘Development of the application for diploma authenticity using the blockchain technology,’’ in Proc. Int. Conf. Quality Manage., Transp. Inf. Secur., Inf. Technologies (ITQMIS), Sochi, Russia, Sep. 2019, pp. 558–563, doi: 10.1109/ITQMIS.2019.8928423.

[95] A. Cernian, E. Vlasceanu, B. Tiganoaia, and A. Iftemi, ‘‘Deploying blockchain technology for storing digital diplomas,’’ in Proc. 23rd Int. Conf. Control Syst. Comput. Sci. (CSCS), Bucharest, Romania, May 2021, pp. 322–327, doi: 10.1109/CSCS52396.2021.00059.

[96] Meyliana, Surjandy, E. Fernando, C. Cassandra, H. A. Eka Widjaja, Y. U. Chandra, and H. Prabowo, ‘‘A blockchain technology-based for university Student enrollment process,’’ in Proc. 6th Int. Conf. Comput. Eng. Design (ICCED), Sukabumi, Indonesia, Oct. 2020, pp. 1–4, doi: 10.1109/ICCED51276.2020.9415856.

[97] T. de Souza-Daw and R. Ross, ‘‘Fraud in higher education: A system for detection and prevention,’’ J. Eng., Design Technol., vol. 21, no. 3, pp. 637–654, May 2023, doi: 10.1108/JEDT-12-2020-0504.

[98] T. Nurhaeni, I. Handayani, F. Budiarty, D. Apriani, and P. A. Sunarya, ‘‘Adoption of upcoming blockchain revolution in higher education: Its potential in validating certificates,’’ in Proc. 5th Int. Conf. Informat. Comput. (ICIC), Gorontalo, Indonesia, Nov. 2020, pp. 1–5, doi: 10.1109/ICIC50835.2020.9288605.

[99] D. Čeke and S. Kunosić, ‘‘Smart Contracts as a diploma anti-forgery system in higher education—A pilot project,’’ in Proc. 43rd Int. Conv. Inf., Commun. Electron. Technol. (MIPRO), Opatija, Croatia, 2020, pp. 1662–1667, doi:10.23919/MIPRO48935.2020.9245391.

[100] M. A. Ali and W. S. Bhaya, ‘‘Higher education’s certificates model based on blockchain technology,’’ J. Phys., Conf. Ser. vol. 1879, Dec. 2021, Art. no. 022091, doi:10.1088/1742-6596/1879/2/022091.

[101] M. Bahrami, A. Movahedian, and A. Deldari, ‘‘A comprehensive blockchain-based solution for academic certificates management using smart contracts,’’ in Proc. 10th Int. Conf. Comput. Knowl. Eng. (ICCKE), Mashhad, Iran, Oct. 2020, pp. 573–578, doi: 10.1109/ICCKE50421.2020.9303656.

[102] F. R. Vidal, F. Gouveia, and C. Soares, ‘‘Revocation mechanisms for academic certificates stored on a blockchain,’’ in Proc. 15th Iberian Conf. Inf. Syst. Technol. (CISTI), Seville, Spain, Jun. 2020, pp. 1–6, doi: 10.23919/CISTI49556.2020.9141088.

[103] Sh. Alam, H. Abdullah, R. Abdulhaq, A. Hayawi, ‘‘A blockchain-based framework for secure educational credentials,’’ Turkish J. Comput. Math. Educ., vol. 12, pp. 5157–5167, Apr. 2021.

[104] I. A. Brusakova and N. B. Tselobanov, ‘‘Features of processes management of verification of digital diplomas by means of blockchain technologies,’’ in Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus), St. Petersburg, Moscow, Russia, Jan. 2020, pp. 1634–1636, doi: 10.1109/EIConRus49466.2020.9039195.

[105] A. M. San, N. Chotikakamthorn, and C. Sathitwiriyawong, ‘‘Blockchainbased learning credential verification system with recipient privacy control,’’ in Proc. IEEE Int. Conf. Eng., Technol. Educ. (TALE), Yogyakarta, Indonesia, Dec. 2019, pp. 1–5, doi: 10.1109/TALE48000.2019.9225878.

[106] R. Taufiq, A. Trisetyarso, Meyliana, R. Kosala, B. Ranti, S. Supangkat, and E. Abdurachman, ‘‘Robust crypto-governance graduate document storage and fraud avoidance certificate in Indonesian private university,’’ in Proc. Int. Conf. Inf. Manage. Technol. (ICIMTech), Jakarta/Bali, Indonesia, vol. 1, Aug. 2019, pp. 339–344, doi: 10.1109/ICIMTech.2019.8843784.

[107] A. W. Reza, K. Islam, S. Muntaha, and O. B. A. Rahman, ‘‘Education certification and verified documents sharing system by blockchain,’’ Int. J. Intell. Eng. Syst., vol. 15, pp. 682–691, Nov. 2022, doi: 10.22266/ijies2022.1231.60.

[108] A. Wicaksana and J. Ch Wira, ‘‘Security analysis of private blockchain implementation for digital diploma,’’ Int. J. Innov. Comput., Inf. Control, vol. 18, no. 5, pp. 1–15, Oct. 2022.

[109] K. B. Dubey and M. Goyal, ‘‘Smart certificate using blockchain,’’ J. Comput. Sci., vol. 18, no. 9, pp. 877–884, Sep. 2022, doi: 10.3844/jcssp.2022.877.884.

[110] A. Tariq, H. B. Haq, and S. T. Ali, ‘‘Cerberus: A blockchain-based accreditation and degree verification system,’’ IEEE Trans. Computat. Social Syst., early access, Sep. 2, 2022, doi: 10.1109/TCSS.2022.3188453.

[111] M. K. Shrivas, S. Kachhwaha, A. Bhansali, and S. Vir Singh, ‘‘Quantumresistant university credentials verification system on blockchain,’’ in Proc. IEEE Nigeria 4th Int. Conf. Disruptive Technol. Sustain. Develop. (NIGERCON), Lagos, Nigeria, Apr. 2022, pp. 1–6, doi: 10.1109/NIGERCON54645.2022.9803153.

[112] E. Leka, E. Kordha, and K. Hamzallari, ‘‘Towards an IPFS-blockchain based authentication/management system of academic certification in western Balkans,’’ in Proc. 45th Jubilee Int. Conv. Inf., Commun. Electron. Technol. (MIPRO), Opatija, Croatia, 2022, pp. 1448–1453, doi: 10.23919/MIPRO55190.2022.9803625.

[113] E. Leka and B. Selimi, ‘‘Development and evaluation of blockchain based secure application for verification and validation of academic certificates,’’ Ann. Emerg. Technol. Comput., vol. 5, no. 2, pp. 22–36, Apr. 2021.

[114] S. Badlani, T. Aditya, S. Maniar, and K. Devadkar, ‘‘EduCrypto: Transforming education using blockchain,’’ in Proc. 6th Int. Conf. Intell. Comput. Control Syst. (ICICCS), Madurai, India, May 2022, pp. 829–836, doi: 10.1109/ICICCS53718.2022.9788237.

[115] B. Mahesh Goud, D. Lilaramani, and M. Swain, ‘‘Generation and authentication of digital certificates using ethereum based decentralized mechanism for mitigating data fraud on RISC-V,’’ in Proc. Int. Conf. Comput. Perform. Eval. (ComPE), Shillong, India, Dec. 2021, pp. 905–909, doi: 10.1109/ComPE53109.2021.9752130.

[116] A. H. Lone and R. Naaz, ‘‘Forgery protection of academic certificates through integrity preservation at scale using ethereum smart contract,’’ Scalable Comput., Pract. Exper., vol. 21, no. 4, pp. 673–688, Dec. 2020, doi: 10.12694/scpe.v21i4.1806.

[117] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, ‘‘How to conduct a systematic literature review: A quick guide for computer science research,’’ MethodsX, vol. 9, 2022, Art. no. 101895, doi: 10.1016/j.mex.2022.101895.

[118] R. E. Boyatzis, Transforming Qualitative Information: Thematic Analysis and Code Development. Newcastle upon Tyne, U.K.: SAGE, 1998.

[119] V. Braun and V. Clarke, ‘‘Using thematic analysis in psychology,’’ Qualitative Res. Psychol., vol. 3, no. 2, pp. 77–101, Jan. 2006.

[120] A. Rangasamy, V. Nagaraj, and K. Nandhakumar, ‘‘Software reuse management for better efficiency and turnaround time,’’ in Proc. IEEE Technol. Eng. Manage. Conf. Eur. (TEMSCON-EUR), Dubrovnik, Croatia, May 2021, pp. 1–4, doi: 10.1109/TEMSCON-EUR52034.2021.9488643.

[121] Inayatulloh, ‘‘Blockchain technology model to protect higher education E-certificates with open source system,’’ in Proc. 3rd Int. Conf. Cybern. Intell. Syst. (ICORIS), Makasar, Indonesia, Oct. 2021, pp. 1–4, doi: 10.1109/ICORIS52787.2021.9649606.

[122] G. Ramakrishnan, M. Rehan, and G. Sujatha, ‘‘Solidity vulnerability scanner,’’ in Proc. Int. Conf. Data Sci., Agents Artif. Intell. (ICDSAAI), Chennai, India, vol. 1, Dec. 2022, pp. 1–5, doi: 10.1109/ICDSAAI55433.2022.10028877.

[123] J. F. Ferreira, P. Cruz, T. Durieux, and R. Abreu, ‘‘SmartBugs: A framework to analyze solidity smart contracts,’’ in Proc. 35th IEEE/ACM Int. Conf. Automated Softw.

[124] P. Gugnani, W. W. Godfrey, and D. Sadhya, ‘‘Ethereum based smart contract for event management system,’’ in Proc.IEEE 6th Conf. Inf. Commun. Technol. (CICT), Gwalior, India, Nov. 2022, pp. 1–5, doi: 10.1109/CICT56698.2022.9997939.

[125] K. Saini, A. Roy, P. R. Chelliah, and T. Patel, ‘‘Blockchain 2.O: A smart contract,’’ in Proc. Int. Conf. Comput. Perform. Eval. (ComPE), Shillong, India, Dec. 2021, pp. 524–528, doi: 10.1109/ComPE53109.2021.9752021.

[126] S. Lin, Z. Li, S. Zhao, H. Zhao, Y. Li, and S. Wang, ‘‘Design and implementation of blockchain-based college education integrity system,’’ in Proc. IEEE 5th Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE), Dalian, China, Sep. 2022, pp. 276–281, doi: 10.1109/ICISCAE55891.2022.9927601.

[127] A. Aderibole, A. Aljarwan, M. H. Ur Rehman, H. H. Zeineldin, T. Mezher, K. Salah, E. Damiani, and D. Svetinovic, ‘‘Blockchain technology for smart grids: Decentralized NIST conceptual model,’’ IEEE Access, vol. 8, pp. 43177–43190, 2020, doi: 10.1109/ACCESS.2020.2977149.

[128] M. Jurgelaitis, L. ceponiene, and R. Butkiene, ‘‘Solidity code generation from UML state machines in model-driven smart contract development,’’ IEEE Access, vol. 10, pp. 33465–33481, 2022, doi: 10.1109/ACCESS.2022.3162227.

[129] E. Leka and B. Selimi, ‘‘BCERT—A decentralized academic certificate system distribution using blockchain technology,’’ Int. J. Inf. Technol. Secur., vol. 12, no. 4, pp. 103–118, 2020.

[130] V. Gatteschi, F. Lamberti, and C. Demartini, ‘‘Blockchain technology use cases,’’ Advanced Applications of Blockchain Technology. Studies in Big Data, vol. 60, S. Kim and G. Deka, Eds. Singapore: Springer, 2020, doi: 10.1007/978-981-13-8775-3_4.

[131] M. Smits and J. Hulstijn, " Blockchain Applications and Institutional Trust". In Front. Blockchain 3:5.,2020, doi: 10.3389/fbloc.2020.00005

[132] L. Zhao, T. Wen, H. Wang and W. Pang, "Research on smart contract evaluation method for open source blockchain," 2023 3rd International Symposium on Computer Technology and Information Science (ISCTIS), Chengdu, China, 2023, pp. 475-479, doi: 10.1109/ISCTIS58954.2023.10213088

[133] V. Capocasale and G. Perboli, "Standardizing Smart Contracts," in IEEE Access, vol. 10, pp. 91203-91212, 2022, doi: 10.1109/ACCESS.2022.3202550.

[134] J. Liang, X. Liu, X. Wu and R. Chen, "Improvement and Application of Blockchain Consensus Algorithm for Distributed Power Energy System," 2023 IEEE 8th International Conference on Big Data Analytics (ICBDA), Harbin, China, 2023, pp. 77-82, doi: 10.1109/ICBDA57405.2023.10104765.

[135] M. Popa, S. M. Stoklossa and S. Mazumdar, "ChainDiscipline - Towards A Blockchain-IoT-Based Self-Sovereign Identity Management Framework," in IEEE Transactions on Services Computing, doi: 10.1109/TSC.2023.3279871.

[136] X. Ge et al., "Blockchain and Green Certificates Based Market Structure and Transaction Mechanism of Direct Power-Purchase for Industrial Users," in IEEE Transactions on Industry Applications, vol. 59, no. 3, pp. 2892-2903, May-June 2023, doi: 10.1109/TIA.2023.3246966.

[137] A. Rustemi, V. Atanasovski and A. Risteski, "Design of the Blockchain System for the Generation and Verification of Diplomas," 2023 XXXII International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 2023, pp. 1-6, doi: 10.1109/ET59121.2023.10279743.

[138] M. Song, J. Han, H. Eom and Y. Son, "IPFSz: An Efficient Data Compression Scheme in InterPlanetary File System," in IEEE Access, vol. 10, pp. 122601-122611, 2022, doi: 10.1109/ACCESS.2022.3223107.

[139] T. Kumari, R. Kumar and R. K. Dwivedi, "Designing Blockchain Based Consensus Mechanism for Smart Healthcare IoT," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 878-884, doi: 10.1109/IITCEE57236.2023.10090882.

[140] Y. Wang, Z. Su, Q. Xu, R. Li, T. H. Luan and P. Wang, "A Secure and Intelligent Data Sharing Scheme for UAV-Assisted Disaster Rescue," in IEEE/ACM Transactions on Networking, doi: 10.1109/TNET.2022.3226458

[141] S. Ji, D. Kim and H. Im, "Evaluating Countermeasures for Verifying the Integrity of Ethereum Smart Contract Applications," in IEEE Access, vol. 9, pp. 90029-90042, 2021, doi: 10.1109/ACCESS.2021.3091317.

[142] S. H. Abbas, S. Sanyal, P. Nagpal, J. Panduro-Ramirez, R. Singh and S. Pundir, "An Investigation on a Blockchain Technology in Smart Certification Model for Higher Education," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 1277-1281.

[143] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "Towards a Conceptual Model of a Blockchain System for Automatic Generation of Academic Diplomas: Use Cases and Scenarios," 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Plovdiv, Bulgaria, 2023, pp. 1-6, doi: 10.1109/CIEES58940.2023.10378773.

[144] Malsa N, Vyas V, Gautam J, Ghosh A, Shaw RN (2021) CERTbchain: A Step by Step Approach Towards Building A Blockchain based Distributed Application for Certificate Verification System. In 2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA), Arad, Romania, 2021, pp. 800-806, doi: 10.1109/ICCCA52192.2021.9666311.

[145] Rasool S, Saleem A, Iqbal M, Dagiuklas T, Mumtaz S, Qayyum ZU (2020) Docschain: Blockchain-Based IoT Solution for Verification of Degree Documents. In IEEE Transactions on Computational Social Systems, vol. 7, no. 3, pp. 827-837, June 2020, doi: 10.1109/TCSS.2020.2973710.

[146] Liu B, Xiao L, Long J, Tang M, Hosam O (2020) Secure digital certificate-based data access control scheme in blockchain. IEEE Access. 8, 91751-91760. https://doi.org/10.1109/ACCESS.2020.2993921

[147] Curmi A, Inguanez F (2019) BlockChain Based Certificate Verification Platform. In: Abramowicz, W., Paschke, A. (eds) Business Information Systems Workshops. BIS 2018. Lecture Notes in Business Information Processing, vol 339. Springer, Cham. https://doi.org/10.1007/978-3-030-04849-5_18

[148] Raimundo R, Rosário A (2021) Blockchain System in Higher Education. European Journal of Investigation in Health, Psychology and Education. 2021; 11(1):276-293. https://doi.org/10.3390/ejihpe11010021

[149] Zainab A, Ghrayeb A, Syed D, Abu-Rub H, Refaat SS, Bouhali O (2021) Big data management in smart grids: Technologies and challenges. IEEE Access. 9, 73046-73059. https://doi.org/10.1109/ACCESS.2021.3080433

[150] Rustemi A, Atanasovski V, Risteski A (2022) Overview of Blockchain Data Storage and Privacy Protection. In 2022 International Balkan Conference on Communications and Networking (BalkanCom). August, (pp. 90-94). IEEE. https://doi.org/10.1109/BalkanCom55633.2022.9900867

[151] Zhou E, Hong Z, Xiao Y, Zhao D, Pei Q, Guo S, Akerkar R (2022) MSTDB: A Hybrid Storage-Empowered Scalable Semantic Blockchain Database. IEEE Transactions on Knowledge and Data Engineering. https://doi.org/10.1109/TKDE.2022.3220522

[152] Pawar MK, Patil P, Sharma M, Chalageri M (2021) Secure and Scalable Decentralized Supply Chain Management Using Ethereum and IPFS Platform. In 2021 International Conference on Intelligent Technologies (CONIT), Hubli, India, 2021, pp. 1-5, doi: 10.1109/CONIT51480.2021.9498537.

[153] Ocheja P, Agbo FJ, Oyelere SS, Flanagan B, Ogata H (2022) Blockchain in education: A systematic review and practical case studies. IEEE Access. 10, 99525-99540. https://doi.org/10.1109/ACCESS.2022.3206791

[154] Popa M, Stoklossa SM, Mazumdar S (2023) ChainDiscipline-Towards A Blockchain-IoT-Based Self-Sovereign Identity Management Framework. IEEE Transactions on Services Computing. https://doi.org/10.1109/TSC.2023.3279871

[155] Truong TC, Diep QB (2023) Technological Spotlights of Digital Transformation in Tertiary Education. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3270340

[156] Groschopf W, Dobrovnik M, Herneth C (2021) Smart contracts for sustainable supply chain management: Conceptual frameworks for supply chain maturity evaluation and smart contract sustainability assessment. Frontiers in Blockchain. 4, 506436. https://doi.org/10.3389/fbloc.2021.506436

[157] Liang Y, Samtani S, Guo B, Yu Z (2020) Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. IEEE Internet of Things Journal. 7(9), 9128-9143. https://doi.org/10.1109/JIOT.2020.3004077

[158] Kaushik K (2022) Blockchain enabled artificial intelligence for cybersecurity systems. In Big Data Analytics and Computational Intelligence for Cybersecurity. pp. 165-179. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-05752-6_11

[159] Luong DA, Park JH (2023) Privacy-Preserving Identity Management System on Blockchain Using Zk-SNARK. In IEEE Access, vol. 11, pp. 1840-1853, 2023, doi: 10.1109/ACCESS.2022.3233828.

[160] Guan Z, Wan Z, Yang Y, Zhou Y, Huang B (2022) BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs. In IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1446-1463, 1 May-June 2022, doi: 10.1109/TDSC.2020.3025129.

[161] Zheng P, Jiang Z, Wu J, Zheng Z (2023) Blockchain-based Decentralized Application: A Survey. IEEE Open Journal of the Computer Society. https://doi.org/10.1109/OJCS.2023.3251854

[162] Kushwaha SS, Joshi S, Singh D, Kaur M, Lee HN (2022) Ethereum smart contract analysis tools: A systematic review. IEEE Access. 10, 57037-57062. https://doi.org/10.1109/ACCESS.2022.3169902

[163] Firouzi F, Jiang S, Chakrabarty K, Farahani B, Daneshmand M, Song J, Mankodiya K (2022) Fusion of IoT, AI, edge–fog–cloud, and blockchain: Challenges, solutions, and a case study in healthcare and medicine. IEEE Internet of Things Journal. 10(5), 3686-3705. https://doi.org/10.1109/JIOT.2022.3191881

[164] Aldyaflah IM, Zhao W, Upadhyay H, Lagos L (2023) The Design and Implementation of a Secure Datastore Based on Ethereum Smart Contract. Appl. Sci. 13, 5282. https://doi.org/10.3390/app13095282.

[165] Samir E, Wu H, Azab M, Xin C, Zhang Q (2021) DT-SSIM: A decentralized trustworthy self-sovereign identity management framework. IEEE Internet of Things Journal. 9(11), 7972-7988. https://doi.org/10.1109/JIOT.2021.3112537

[166] A. Somasundar, M. Chilakarao, B. R. Krishnam Raju, S. Kumari Behera, C. V. Ramana and P. K. Sethy, "MongoDB integration with Python and Node.js, Express.js," 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2024, pp. 1-5, doi: 10.1109/ICAECT60202.2024.10469546.

[167] What is Python Used For? 7 Real-Life Python Uses, online (https://www.datacamp.com/blog/what-is-python-used-for), accessed: 04.04.2024.

[168] H. Ye, W. Chen, W. Dou, G. Wu and J. Wei, "Knowledge-Based Environment Dependency Inference for Python Programs," 2022 IEEE/ACM 44th International Conference on Software Engineering (ICSE), Pittsburgh, PA, USA, 2022, pp. 1245-1256, doi: 10.1145/3510003.3510127.

[169] B. Cherry, P. Benats, M. Gobert, L. Meurice, C. Nagy and A. Cleve, "Static Analysis of Database Accesses in MongoDB Applications," 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Honolulu, HI, USA, 2022, pp. 930-934, doi: 10.1109/SANER53432.2022.00111.

[170] N. Mansoor, K. F. Antora, P. Deb, T. A. Arman, A. A. Manaf and M. Zareei, "A Review of Blockchain Approaches for KYC," in IEEE Access, vol. 11, pp. 121013-121042, 2023, doi: 10.1109/ACCESS.2023.3328536.

[171] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, ‘‘Digital signature scheme for information non-repudiation in blockchain: A state of the art review,’’ EURASIP J. Wireless Commun. Netw., vol. 2020, no. 1, pp. 1–5, Dec. 2020, doi: 10.1186/s13638-020-01665-w.

[172] E. Andesta, F. Faghih and M. Fooladgar, "Testing Smart Contracts Gets Smarter," 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 2020, pp. 405-412, doi: 10.1109/ICCKE50421.2020.9303670.

[173] Zhang H., Gao P., Yu J., Lin J. and Xiong N. N. 2022. Machine Learning on Cloud With Blockchain: A Secure, Verifiable and Fair Approach to Outsource the Linear Regression," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 6, pp. 3956-3967, 1 Nov.-Dec, doi: 10.1109/TNSE.2021.3110101.

[174] Halili, F. and Rustemi, A., 2016. Predictive modeling: data mining regression technique applied in a prototype. International Journal of computer science and mobile computing, 5(8), pp.207-215.

[175] A. Rustemi, V. Atanasovski, A. Risteski, V. Angelkoska, "Legislation issues regarding the implementation of blockchain-based application in higher education institution in North Macedonia", 2nd International Scientific Conference : the Future of Science, University "Ukshin Hoti" Prizren, ISBN 978-9951-510-31-8.