https://doi.org/10.53656/str2024-5s-7-res

Education in the Information Society
Образованието в информационното общество

ИЗСЛЕДВАНЕ ПРИЛОЖИМОСТТА НА БЛОКОВИ ВЕРИГИ ОТ ПЪРВО НИВО (L1) В СИСТЕМА ЗА ЕЛЕКТРОННО ОБУЧЕНИЕ

Андриан Минчев, проф. Ваня Стойкова, гл. ас. д-р Галя Шивачева
Тракийски университет – Стара Загора
Доц д-р Анелия Иванова
Русенски университет „Ангел Кънчев“

Резюме. В статията е представено изследване на приложимостта на блокчейн технологията в система за електронно обучение. Проучени и оценени са техническите характеристики и оперативните разходи при употреба в помощ на избора на подходяща технология за конкретна платформа за електронно обучение. Направен е сравнителен анализ на водещи блокчейн платформи от първо ниво (L1), като са разгледани четири основни показателя: средно време за генериране на блок, цена на транзакция, време за финализиране на транзакция и пропускателна способност на веригата, измерена в брой транзакции в секунда за всяка верига. Целта е да се оценят и сравнят ключови параметри, които имат съществено значение при избора на конкретна блокова верига за записване на информация в реални условия в система за е-обучение. Приложени са методи за анализ на публично достъпна информация в комбинация с проверка на съвместимостта и съгласуваността на данните от различни източници.

Ключови думи: блокчейн технологии; блокови вериги от първо ниво; системи за е-обучение; сигурност и защита на данните

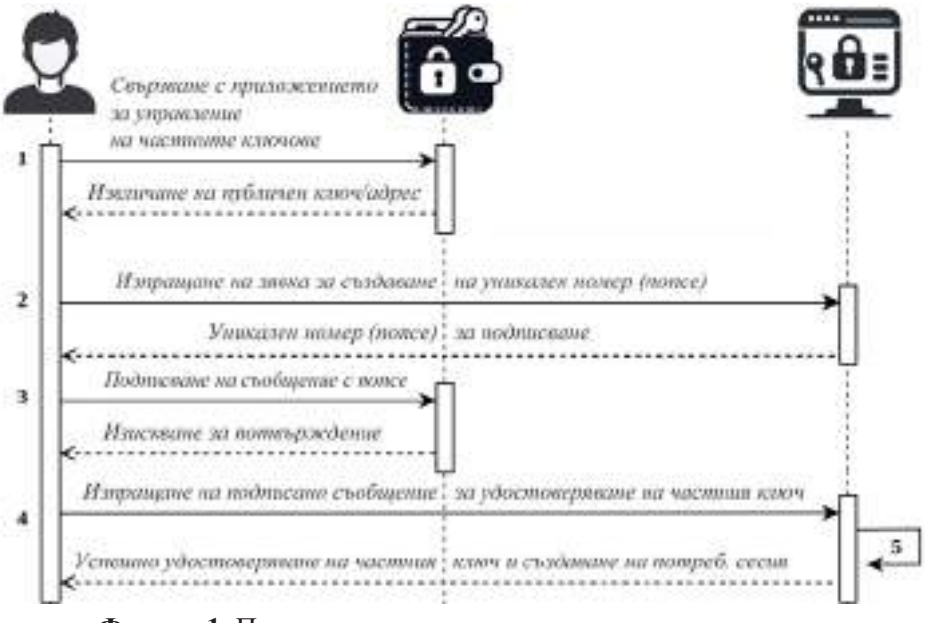
1. Въведение

Бързото развитие на компютърния хардуер предоставя все по-мощни инструменти на разположение на софтуерните специалисти. Дали тези възможности ще се насочат в положителна посока, зависи до голяма степен от самите разработчици. В допълнение изкуственият интелект (ИИ) позволява на всеки, дори и неспециалист, да създава програми за автоматизирани атаки срещу интернет сайтове и системи за удостоверяване на регистрирани потребители (Chio & Freeman 2018).

Системите за електронно обучение (СЕО) са източник на информация и лични данни за потребителите, които могат да бъдат от интерес за трети страни.

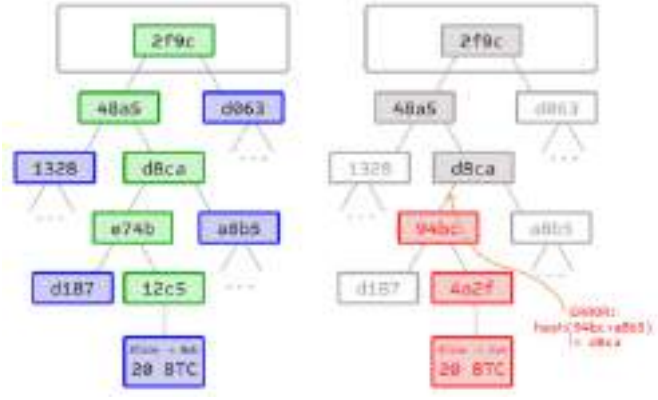
В тези системи могат да се издават и сертификати за успешно завършени курсове. Но дали неоторизиран потребител (хакер) може да се възползва от слабости в механизмите за удостоверяване и да създаде сертификати с невярно съдържание? Това става все по-вероятен сценарий, а системите са поставени пред нови предизвикателства по отношение на доказването на това кой стои от другата страна, кой е истинският притежател или издател на даден документ. Проблемите, свързани със сигурността на данните и достъпа до CEO, са разгледани от редица изследователи като (Beloev et al. 2023; Dimitrova 2023; Andreeva 2022).

Възможно решение на сложната задача, свързана с удостоверяването на самоличността на притежателя и издателя на сертификата/документа, е използването на блокчейн (БЧ) технологии и асиметрични криптографски ключове. Тези технологии предоставят висока степен на защита, като частните ключове се оказват изключително трудни за подправяне (Karaaslan & Konacakli 2020). На фиг. 1 е представен стандартен метод с използване на асиметрични криптографски ключове, който предоставя надежден начин за удостоверяване на потребителите. Процесът включва свързване на потребителя с портфейла, получаване на уникален *nonce* (произволно число, използвано еднократно, за да предотврати повторно подписване на стари транзакции) от системата, подписване на *nonce* с частния ключ на потребителя, изпращане на подписа обратно към системата за верификация и промяна на *nonce* след успешно удостоверяване.



Фигура 1. Процес на удостоверяване чрез частен ключ

В повечето случаи четенето на информация от блокчейн е бързо, тъй като самата технология имплементира специфични структури от данни, т. нар. дърво на Меркъл (фиг. 2) (Wattenhofer 2016; Antonopoulos 2018). Чрез този подход се достига изключително бързо до доказателство за наличие на определена информация в блокчейн. По отношение на записа на информация съществуват множество блокчейн разработки, които се фокусират върху различни технически параметри. В някои случаи се дава приоритет на сигурността, докато в други се работи за повишаване скоростта на записване на данни. Тази област е в непрекъснато развитие, като иновациите се внедряват ежедневно и ежечасно.



Фигура 2. Дърво на Меркъл

С оглед на успешно адаптиране на блокчейн технологията за нуждите на уеб базираните системи и услуги, вкл. системите за е-обучение, изискващи удостоверяване от своите потребители, е необходимо да се направи анализ на някои ключови параметри на БЧ, с което да се установи дали съответна верига има необходимите качества, за да се използва за интернет услуги. Поради някои особености при защитата на информацията, записана в блокови вериги, съществува т. нар. „*консенсусен механизъм*“, който се стреми да реши проблема, наречен „*блокчейн трилема*“, касаещ баланса между децентрализацията, сигурността и мащабируемостта (Karaaslan & Konacakli 2020; Shostak 1982) . Проблемът е, че при постигане по-висока скорост на създаване на нови блокове във веригата се получава негативно въздействие или върху сигурността, или върху децентрализацията. И трите индикатора на блокчейн трилемата са важни за осъществяване на сигурно и защитено записване на информация в блокови вериги, поради което се търси оптимално балансирано решение, предоставящо максимално висока скорост на взаимодействие, без това да повлиява съществено на сигурността и целостта на данните, съхранявани в БЧ.

Параметрите, които характеризират блоковите вериги, са много и разнообразни. В този труд е представен сравнителен анализ на водещи блокчейн платформи от първо ниво (L1) с фокус върху основни технически показатели: време за създаване на блок, цена на транзакция, време за финализиране на транзакция и пропускателна способност на веригата, измерена в брой транзакции в секунда за всяка верига. Ключов фактор за всяка интернет услуга е скоростта на взаимодействие с потребителите. Поради това един от разгледаните параметри е количественото измерване на броя взаимодействия с блокова верига, отнесени към единица време.

Целта на анализа е да се направят оценка и сравнение на посочените погоре параметри, които имат съществено значение при избора на конкретна блокова верига за записване на информация в реални условия в системите за е-обучение. Приложени са методи за анализ на публично достъпна информация в комбинация с проверка на съвместимостта и съгласуваността на данните от различни източници.

2. Сравнителен анализ на блокови вериги от първо ниво

Предмет на анализа са параметрите на блокови вериги от първо ниво, тъй като те обикновено са защитени от злоупотреби чрез сложни криптографски алгоритми, които изискват значителна изчислителна мощност, за да произведат правилните хешове за продуциране на нови валидни блокове с информация (Chio & Freeman 2018; Bashir 2017; Shostak 1982). На фиг. 3 е представена тенденцията в нарастване на трудността за намиране на следващия валиден блок, измерена в терахеши за секунда (TH/s).

Фигура 3. Развитие на трудността за намиране на следващия валиден блок (TH/s)

Разгледана е публично достъпната статистическа информация относно ключовите показатели на блокчейн вериги от първо ниво, като следва да се отбележи, че ежедневно възникват нови блокови вериги от първо ниво и е почти невъзможно да бъдат сравнени всички. Фокусът ще бъде поставен върху някои от тях, като изборът ще бъде направен на база парична стойност, съхранена в съответната верига. За целта на анализа са проучени популярни каталози на блокови вериги. В каталога *CoinGecko* след филтриране по показателя „*ниво*“ са взети предвид първите 10 проекта от категория L1 (табл. 1), сортирани по метриката „*пазарен дял*“. По-нататък са събрани данни за избраните блокови вериги от публично достъпни източници относно показателите, предвидени за анализ в настоящото проучване: средно време за генериране на блок, теоретично максимален брой транзакции, средна цена за транзакция и средно време за финализиране на транзакция (Narayanan et al. 2016).

Таблица 1. Топ 10 блокови вериги по пазарен дял

Позиция по пазарен дял	Наименование	Символ
1	Bitcoin	BTC
2	Ethereum	ETH
4	BNB	BNB
5	Solana	SOL
10	Toncoin	TON
11	Cardano	ADA
13	Avalanche	AVAX
16	Bitcoin Cash	BCH
17	TRON	TRX
19	NEAR Protocol	NEAR
20	Internet Computer	ICP

Времето до издаване на следващ блок е приблизителна величина, която зависи от сложен механизъм за саморегулация на т. нар. *difficulty* – трудност на задачата, чрез която да бъде произведен следващият валиден хедър и хеш на блок в съответната верига от първо ниво (Antonopoulos 2017; Antonopoulos 2018; Narayanan et al. 2016).

В табл. 2 е представено сравнение на блокови вериги по показател „*средно време за генериране на блок*“. Трите мрежи с най-добри резултати спрямо скоростта са:

Internet Computer (ICP). Време за генериране на блок – 44,1 блока в секунда (или 1/44 s). Постига изключителна бързина и висока пропускателна способност, което я прави ефективна за бързо потвърждение на транзакции.

Solana (SOL). Средно време за генериране на блок – от 400 до 800 ms. Показва много висока скорост, позволявайки бързо потвърждение на транзакции и подходяща за приложения с висока натовареност.

Avalanche (AVAX). Време за генериране на блок – 1 s. Осигурява бързо и надеждно потвърждение на транзакции.

Тези резултати показват, че *Internet Computer*, *Solana* и *Avalanche* са водещи по отношение на скорост на продуциране на валидни блокове с информация.

Таблица 2. Средно време за генериране на блок

Наименование	Абревиатура	Средно време за генериране на блок
Bitcoin	BTC	10 m 45 s
Ethereum	ETH	12,07 s
BNB	BNB	3 s
Solana	SOL	400-800 ms
Toncoin	TON	5 s
Cardano	ADA	20 s
Avalanche	AVAX	1 s
Bitcoin Cash	BCH	7m 47s
TRON	TRX	3 s
NEAR Protocol	NEAR	1,3 s
Internet Computer	ICP	44,1 bps или 1/44 s

Параметърът TPS (транзакции за секунда) е от ключово значение за пропускателната способност на блоковата верига (табл. 3).

Таблица 3. Теоретичен максимален брой трансакции

Наименование	Абревиатура	Теоретичен максимален брой трансакции
Bitcoin	BTC	7
Ethereum	ETH	119
BNB	BNB	2222
Solana	SOL	59400
Toncoin	TON	104715
Cardano	ADA	250
Avalanche	AVAX	4500

Bitcoin Cash	BCH	250
TRON	TRX	2000
NEAR Protocol	NEAR	100000
Internet Computer	ICP	11500

С оглед да се предотврати безцелното записване на ненужни данни в БЧ, съответно и атаки от този тип, е въведена такса за запис на данни. Таксата се определя динамично и е функция на броя желаещи да участват със запис в текущия блок и количеството информация, която трябва да бъде записана. В моменти на върхово натоварване цената на таксите за транзакции се увеличава и с това се поставят под въпрос устойчивостта, финансовата стабилност и непрекъсваемостта на услугата при реална експлоатация.

От табл. 3 е видно, че *Toncoin*, *NEAR Protocol* и *Solana* се отличават с най-висок теоретичен максимален брой транзакции, съответно 104 715, 100 000 и 59 400 транзакции в секунда, което може да се счита за предпоставка за поддържане на ниски и предвидими цени на транзакциите в тези блокови вериги. Блокчейнът на ICP е организиран в т. нар. подмрежи, всяка от които има максимална пропускателна способност за транзакции минимум 500 tps. Към месец април 2024 г. ICP оперира с 37 подмрежи, което се равнява на минимум 18 500 tps, и реално няма поставено ограничение за техния брой.

Цената на транзакциите в БЧ се определя въз основа на размера на транзакцията и броя на чакащите транзакции за включване в блок (натовареност на мрежата). Високият брой транзакции в секунда (TPS) и по-краткото време за генериране на блокове обикновено намаляват цената на таксите, тъй като увеличават пропускателната способност и намаляват натовареността на мрежата.

Данните от табл. 4 показват, че *NEAR Protocol* и *Internet Computer* имат най-ниските средни транзакционни такси, съответно 0,001 USD и 0,0000007885999 USD, което ги прави много по-достъпни за потребителите в сравнение с останалите блокчейн мрежи.

Таблица 4. Средна цена за трансакция

Наименование	Абревиатура	Средна цена за трансакция
Bitcoin	BTC	2-70 USD
Ethereum	ETH	около 1 USD
BNB	BNB	0,16-0,27 USD
Solana	SOL	$0,082 (0.00041 SOL)
Toncoin	TON	0.005 TON ~0.03 USD
Cardano	ADA	между 0,17 и 0,30 Ada

Avalanche	AVAX	75 nAVAX (gwei) и 225 nAVAX (gwei) 0,27 USD
Bitcoin Cash	BCH	0,000029 BCH (0,014 USD) 0,000000055 BCH/byte
TRON	TRX	0,002 TRX
NEAR Protocol	NEAR	0,001USD
Internet Computer	ICP	0,0000007885999 USD

Времето за финализиране представлява времето, необходимо на транзакцията, за да стане необратима и окончателно записана в блокчейн. От данните в табл. 5 е видно, че *Internet Computer* (ICP), *Avalanche* (AVAX), и *TRON* (TRX) имат най-кратко средно време за финализиране на транзакции, съответно 2, 2 – 3 и 3 секунди.

Необходимо е да бъде намерено решение, което дава сигурност чрез асиметрични криптографски алгоритми, без да повишава оперативните разходи за употреба на дадена система или поне да поддържа разходите в обозрими и предвидими граници (Mougayar 2016). С други думи, трябва да се гарантира сигурност при удостоверяване на потребителите и доказване валидността на издадени документи като сертификати, без това да води до прекомерни разходи за транзакции, особено в контекста на системите за електронно обучение (Bates 2019).

Таблица 5. Средно време за финализиране на трансакция

Наименование	Абревиатура	Средно време за финализиране на трансакция
Bitcoin	BTC	варира от 60 min до над 200 min
Ethereum	ETH	15 min
BNB	BNB	6 min
Solana	SOL	16 sec
Toncoin	TON	6 sec
Cardano	ADA	2 min
Avalanche	AVAX	2-3 sec
Bitcoin Cash	BCH	60 min
TRON	TRX	3sec
NEAR Protocol	NEAR	4,6 sec
Internet Computer	ICP	1-2 sec

След анализ на разглежданите параметри, търсейки най-бързо време за генериране на блок, най-висок теоретичен максимален брой транзакции, най-ниска средна цена за транзакция и най-кратко време за финализиране на транзакция, може да се направи следното обобщение от съпоставената ин-

формация, а именно, че две от изследваните блокови вериги се открояват с най-добри резултати по няколко показателя, което ги прави подходящи за интернет приложения. Това са веригите NEAR и ICP, които постигат много добри резултати в три от четирите изследвани свойства на блоковите вериги. Освен това ICP може да се счита за най-добра и по четвъртия показател, „теоретично максимален брой транзакции", тъй като няма реално ограничение на броя транзакции, който може да се увеличава с добавянето на нови подмрежи.

Като фактор, даващ предимство в полза на ICP, може да се посочи, че TPS показателят зависи от броя на подмрежите, които обработват транзакции. ICP е платформа, чрез която се постига и безплатно за потребителите взаимодействие с блоковите вериги посредством *Reverse Gas Model*.

В резултат на анализа на представените по-горе данни могат да се направят следните допълнителни изводи.

Използването на блокчейн технологии за уеббазирани системи за електронно обучение е не само възможно, но и целесъобразно. Установено е, че ключови характеристики и показатели като скорост, мащабируемост и транзакционни такси са предвидими и стабилни, с което се постига удовлетворяване на нуждите на потребителите на системи за електронно обучение, както и на институциите, които ги поддържат и предоставят такава услуга.

Блокчейни като *Solana*, *Avalanche* и *Internet Computer* предлагат изключително кратко време за генериране на блокове и финализиране на транзакции (в рамките на секунди), което осигурява навременна обработка и актуализация на данни.

С висока пропускателна способност, каквато осигуряват *NEAR Protocol* и *Toncoin*, могат да се обработват голям брой транзакции и това ги прави подходящи за приложения с множество потребители и интерактивни функции. Тази способност за мащабиране гарантира, че системата може да поддържа голям брой едновременни потребители без забавяне или прекъсвания.

Ниските транзакционни такси при блокчейни като *NEAR Protocol* и *Internet Computer* ги правят финансово изгодни за системи за електронно обучение, които изискват чести и малки транзакции, като записване на оценки, удостоверяване на сертификати и други административни операции. Намаляването на оперативните разходи е основание за използването на блокчейн в СЕО и в образованието, като цяло.

3. Заключение

Блокчейн предлага висока скорост на обработка, мащабируемост, ниски разходи и висока сигурност, което е от съществено значение за ефективното функциониране на системите за електронно обучение. В резултат на това внедряването на блокчейн може значително да подобри надеждността по отношение на съхранение на данните и на удостоверяването на издателя и

притежателите на официални документи и сертификати за академични постижения.

Високата степен на сигурност и защита на данните, постигната чрез употребата на асиметрични криптографски алгоритми в комбинация с блокови вериги, е предпоставка за прилагане на технологията при съхранение на лични данни и проверка на достоверността на академичните записи в уеббазираните системи за електронно обучение.

По отношение на избора на блокова верига от L1, направеният сравнителен анализ води до заключението, че ICP е подходяща среда за разработка на приложения върху блокчейн. Времето, необходимо за окончателно записване на информация, създава усещане, аналогично на нормално уеббазирано взаимодействие, а потребителите дори не са в състояние да разберат, че системата за електронно обучение записва важна информация в блокчейн. Чрез *Reverse Gas Model* на ICP потребителите на CEO се освобождават от необходимостта да плащат такси за записване на информация. Уеббазираните системи разполагат със собствени портфейли за безпрепятствено използване от потребителите и в частност за CEO – за регистриране и удостоверяване на резултатите от учебен процес. Цената за записване на информация в рамките на ICP е предвидима и с тенденция за понижаване чрез допълнителна оптимизация. Посочените предимства на блокова верига от L1 ICP са основание за внедряването и експлоатацията на тази технология в университетска среда за електронно обучение.

Благодарности и финансиране

Това проучване е финансирано от Европейския съюз – NextGenerationEU, чрез Националния план за възстановяване и устойчивост на Република България, проект № BG-RRP-2.013-0001-C01.

Acknowledgments and funding

This study is financed by the European Union – NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, project № BG-RRP-2.013-0001-C01.

REFERENCES

ANDREEVA, A., 2022. On Some Questions Of Academic Globalization And Synergy In Scientific Research. *Strategies for Policy in Science & Education-Strategii na Obrazovatelnata i Nauchnata Politika*, vol. 30, no. 3, pp. 227 – 243. Available at: https://doi.org/10.53656/str2022-3-1-glo.

ANTONOPOULOS, A. M., 2017. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* O'Reilly Media Inc. ISBN: 9781491954386.

ANTONOPOULOS, A. M., 2018. *Mastering Ethereum.* O'Reilly Media Inc. ISBN: 9781491971949.

BASHIR, I., 2017. *Mastering Blockchain: Deeper Insights into Decentralization Cryptography Bitcoin and Popular Blockchain Frameworks*. Packt Publishing. ISBN: 9781787125445.

BATES, T., 2019. *Teaching in a Digital Age: Guidelines for Designing Teaching and Learning*. BCcampus. ISBN: 9780995269255.

BELOEV, H., SMRIKAROV, A., VOINOHOVSKA, V., & IVANOVA, G., 2023. Determining the degree of digitalization of a higher education institution. *Strategies for Policy in Science & Education-Strategii na Obrazovatelnata i Nauchnata Politika*, vol. 31, no. 4s, pp. 9 – 21. https://doi.org/10.53656/str2023-4s-1-det.

CHIO, K. & FREEMAN, D., 2018. *Machine Learning and Security: Protecting Systems with Data and Algorithms*. O'Reilly Media. ISBN: 978-1491979907.

DIMITROVA, G., 2023. Competitive Positioning of Higher Education Schools and Digital Transformation. *Strategies for Policy in Science & Education-Strategii na Obrazovatelnata i Nauchnata Politika*, vol. 31, no. 4, pp. 351 – 373. DOI: 10.53656/str2023-4-1-com.

KARAARSLAN, E. & KONACAKLI, E., 2020. Data Storage in a Decentralized World: Blockchain and its Derivatives*. In book: Who Runs The World: DATA*, Ch.: 3, Istanbul University Press. DOI: 10.26650/B/ET06.2020.011.03.

MOUGAYAR, W., 2016. *The Business Blockchain: Promise, Practice and the Application of the Next Internet Technology*. Wiley. ISBN: 978-1-119-30031-1.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A. & GOLDFEDER, S., 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press. ISBN: 978-0691171692.

SHOSTAK, R., 1982. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382 – 401. DOI: 10.1145/357172.357176.

WATTENHOFER, R., 2016. *The Science of the Blockchain*. CreateSpace Independent Publishing Platform. ISBN: 978-1522751830.

EXPLORING THE APPLICABILITY OF LEVEL 1 (L1) BLOCKCHAINS IN E-LEARNING SYSTEMS

Abstract. This paper presents a study on the applicability of blockchain technology in an e-learning system. The technical characteristics and operational costs of using blockchain technology were examined and evaluated to select the appropriate technology for a specific e-learning platform. A comparative analysis of leading Level 1 (L1) blockchain platforms was conducted, focusing on four main metrics: average block generation time, transaction cost, transaction finalization time, and chain throughput measured in transactions per second for each chain. The objective is to assess and compare key parameters that are crucial when choosing a specific blockchain for recording information under real-world conditions in e-learning systems. Methods for analyzing publicly available information were applied, combined with verification of data compatibility and consistency from various sources.

Keywords: blockchain; level 1 blockchain networks; e-learning systems; data security and protection

✉ **Andrian Minchev**
ORCID iD: 0000-0001-7331-0331
✉ **Prof. Vanya Stoykova**
ORCID iD: 0000-0003-0940-3618
Trakia University – Stara Zagora
Yambol, Bulgaria
E-mail: andrian.minchev@trakia-uni.bg
vanya.stoykova@trakia-uni.bg
✉ **Dr. Galya Shivacheva, Assist. Prof.**
ORCID iD: 0009-0005-3766-5182
Trakia University – Stara Zagora
E-mail: galya.shivacheva@trakia-uni.bg
✉ **Dr. Aneliya Ivanova, Assoc. Prof.**
ORCID iD: 0000-0002-3859-2879
University of Ruse "Angel Kanchev"
7017, Ruse Bulgaria
E-mail: aivanova@uni-ruse.bg