Процедура № ФЕА56-НС1-026

Рецензията е постъпила във ФЕА на 11.X.2023г.
Секретар ФЕА:

РЕЦЕНЗИЯ

върху дисертационен труд за придобиване на образователна и научна степен „Доктор" в професионално направление 5.3 Комуникационна и компютърна техника, научна специалност „Компютърни системи, комплекси и мрежи", съгласно Заповед №: ОЖ-5.3-49 от 19.07.2023 г. на Ректора на Технически университет-София

Технически университет-София, ФАКУЛТЕТ „ЕЛЕКТРОНИКА И АВТОМАТИКА", филиал ПЛОВДИВ

Автор на дисертационния труд: **маг. инж. Георги Димитров Искров**

Тема на дисертационния труд: **„Изследване и реализация на мрежова сигурност, базирани на Blockchain технология"**

Рецензент: **проф. д-р Кольо Златанов Онков, катедра „Математика и информатика", Аграрен университет, Пловдив**

1. Актуалност на разработвания в дисертационния труд проблем в научно и приложно отношение.

Blockchain обобщава математически познания и елементи на информационни и криптографски технологии за да се гарантира сигурността при пренос на съобщения в публичните мрежи. В някои научни публикации Blockchain се определя като „еволюционна стъпка" в новото поколение информационни и комуникационни технологии. За актуалността на дисертационния труд може да се съди и от факта, че в редица свои документи, решения и дейности в периода 2016-2022г. Европейската комисия определя основно място на Blockchain технологията в развитието на електронното правителство и електронния бизнес, а също така поставя началото на изграждането на инфраструктура за Blockchain услуги (EBSI).

Без никакво съмнение, задълбочените научни изследвания относно използването на Blockchain технологията за повишаване нивото на сигурност на информацията в компютърните мрежи е от съществено значение за множество приложения в практиката. Всичко това определя високата степен на актуалност на разработвания в дисертационния труд проблем в научно и приложно отношение.

2. Степен на познаване състоянието на проблема и творческа интерпретация на литературния материал.

В дисертацията са цитирани 211 литературни източници: 206 на английски, 2 на български и 3 на руски език, като 202 от тях (над 95%) са публикувани в периода 2018-2021г.

Литертурният обзор има аналитичен характер и е разположен в **Глава I** „Дизайн, класификация и структура на Blockchain технологията" на дисертационния труд. **Маг. инж. Г. Искров** много добре познава Blockchain технологията и разбира научната и приложна същност на дисертацията. Видно е системното мислене на докторанта и способността му да извлича знание и информация от проучената литература.

Използван е стандартният за научни трудове в областта на информатиката и компютърните науки начин на позоваване чрез номера на източника в библиографията, което позволява на читателя по-лесно да установява връзка между референцията в текста и пълното описание на източника в библиографията.

3. Съответствие на избраната методика на изследване и поставената цел и задачи на дисертационния труд с постигнатите приноси.

Цел на дисертационния труд на **маг. инж. Г. Искров** е да се направи анализ на сигурността предоставяна от Blockchain технологията при предаване на съобщения в публични мрежи, да се анализират основните работни механизми и да се изведат предимствата и недостатъците на този динамичен и сложен процес. Приложен е интердисциплинарен подход, като най-важно място заемат емпирично-аналитичния метод, анализът на действието на консенсусите, системен и факторен анализ. Избраният подход е съобразен с поставената цел. Този подход изисква задълбочени познания относно поставените в дисертацията задачи и умения за творческото им прилагане. Избраните методи на изследване предоставят добри възможности за постигане на научни и приложни резултати.

4. Обща характеристика на дисертационния труд. Научни и приложни приноси.

Дисертацията съдържа нормативно изискваните структурни елементи – въведение, 3 глави с изводи към всяка от тях, насоки за бъдещо развитие, заключение, претендирани приноси, списък на публикациите по дисертационния труд и библиография.

В рамките на Литературния обзор в **Глава I** са разгледани принципите на действие на консенсусите Proof of work, Proof of stake, Proof of authority, Proof-of-capacity и Proof of burn. Представен е анализ на сигурността и защитата на данни при тяхната миграция от една към друга верига.

В края на тази глава са направени аргументирани изводи и са дефинирани цел и 6 задачи на дисертационния труд.

В **Глава II** „Blockchain и IoT" се разглеждат предимствата и недостатъците на класическата концепция за „Интелигентен град". Обсъждат се възможностите за използване на Blockchain технологията като начин да се предпазят личните данни от хакерска атака. Анализират се възможните хакерски атаки в „Интелигентен дом" като

част от концепцията за „Интелигентен град" и как Blockchain технологията би могла да минимизира техния ефект. Разгледана е принципна схема на приложението на Blockchain технологията в концепцията на IoT и комуникацията между трите слоя: възприемане на данните, комуникационен и мрежов. Реализиран е функционален анализ за приложението на Blockchain в IoT, свързан с видове хакерски атаки и техните цели в IoT.

Обсъдени са проблемите със сигурността при VANET – безжични мрежи, свързващи група движещи се или неподвижни превозни средства. Анализира се интегрирането на Blockchain към този тип мрежи за осигуряване на интелигентен контрол на трафика и предоставяне на полезна информация в реално време.

В **Глава III** „Анализ на сигурността предоставяна от Blockchain" са проведени анализи на устойчивостта на Blockchain технологията при злонамерени хакерски атаки (DoS, Sybil, и др.). Специално внимание е отделено на ролята на Blockchain при децентрализирания подход за предотвратяване на Double-spending (двойно харчене).

Подробно е представен и анализиран проблема на Византийската толерантност към грешки (Byzantine fault tolerance), познат още като дилемата на византийските генерали. Този проблем се решава в дисертацията чрез математическо-емпиричния метод. Това е важен въпрос отнасящ се до приносите на дисертацията, който ще бъде обсъден по-долу.

Оценявам високо способността на докторанта ясно и аргументирано да представи виждането си за развитие на получените резултати. Това виждане е в посока на изграждане на тестов алгоритъм към абстрактния модел на Blockchain в концепцията „Интелигентен град", тестов модел за VANET системата с възможности за интегриране с облачни структури и отдалечени изчислителни архитектури MEC (Mobile Edge Computing), задълбочено изследване на ефекта на различните типове хакерски атаки и въздействието им върху различни консенсуси. Реалистичният поглед върху бъдещото развитие на получените резултати е показател за професионализма и интелекта на автора на дисертационния труд.

Оценка на научните и приложни приноси.

А) Научен принос 1.

В началото авторът представя проблема на Византийската толерантност към грешки по описателен начин: генерали, армии, вземане на решения и съгласуваност. Това е необичайно за дисертация в областта на компютърните системи. Склонен съм да одобря този подход по две причини: а) проблемът става лесен за възприемане, включително от неспециалист в областта; б) авторът прави важна интерпретация на този проблем върху мрежа/разпределена система с основното значение на Blockchain.

Научният принос на докторанта се състои в математическо-емпиричното доказване на теоремата за невъзможност в рамките на проблема за Византийската толерантност към грешки. В настоящата работа се формализират условията отнасящи се до интерактивната съгласуваност между участниците в разпределената система/мрежа, за да може тя да продължи да функционира. Известните решения на споменатия проблем са на базата на графично-аналитичен подход. В тази дисертация за първи път е намерено решение на проблема на Византийската толерантност към грешки чрез математическо-емпиричния метод.

В Глава III.4.4. на дисертацията „Доказателство за невъзможност" е допусната неточност от докторанта. Изписан е израза (n < 3m+1), а трябва да се чете: (n > 3m +1). Докторантът уведоми своевременно членовете на журито с уверението, че е направена корекция в дисертацията и автореферата.

Б) Научно-приложни приноси.

Приемам **Принос 2**, но бих искал да отбележа неточност във формулирането му, цитирам „Разгледана е концепция за бъдещо развитие на изброените системи с помощта на облачни структури и отдалечени изчислителни архитектури MEC (Mobile Edge Computing)". Не е ясно кои са тези **„изброени системи"**. Идеята за съхраняване на данни в облачни структури и използване на отдалечени изчислителни архитектури MEC е развита в **Глава II** на дисертацията. **Принос 2** би могъл да се дефинира по-добре по следния начин: "Разгледана е концепция за бъдещо развитие на IoT и VANET мрежи с интегриране на Blockchain и използване на облачни структури и отдалечени изчислителни архитектури MEC (Mobile Edge Computing)".

Приноси 3-5 са много добре дефинирани и разкриват съществени страни на резултатите, постигнати в дисертационната работа. Те се отнасят до абстрактен модел на приложение на Blockchain технологията и различните типове консесуси в Smart Sity и Smart Home, функционален анализ на различни хакерски атаки в IoT, Smart Sity и Smart Home, както и анализ на устойчивостта на Blockchain технологията и модел за превенция и защита.

В) Приложни приноси.

Безспорни са приложните приноси на докторанта. Предложена е реализация на консенсуса PoA (Proof of authority) в рамките на VANET за контрол на пътната обстановка **(принос 6).** Разработени са структура на проект, цялостен програмен код и процедура на изпълнение с приложение на Blockchain технологията в система за провеждане на избори **(принос 7).** Звучат много актуално твърденията на автора, свързани с принос 7, относно възможностите на Blockchain за намаляване на бюрокрацията, разходите, корупцията и преди всичко повишаване сигурността на пренасяните данни при провеждане на избори.

В дисертацията не е дискутиран въпроса за наличието на резултати, които водят до пряк икономически ефект. Естеството на дисертационния труд е такова, че непряк икономически ефект със значителен потенциал се съдържа в практическите приложения на публичните компютърни мрежи на основата на Blockchain технологията с оглед на сигурността на преноса на данни и предоставяне на информационни услуги при някои функционалности на Smart Sity, Smart Home, VANET и др. Има логика в твърдението на докторанта за намаляване на разходите в приложението за провеждане на избори с използване на Blockchain. Това разбира се подлежи на бъдещи изследвания, финансов анализ и оценка.

5. Преценка на публикациите по дисертационния труд.

Представен е списък от пет научни публикации свързани с дисертацията. Една статия е на български език, останалите четири са на английски. Две статии са публикувани в списания, останалите в материалите на международни конференции. Личният принос на **маг. инж. Г. Искров** е безспорен. Той е единствен автор на четири от публикациите, а петата е в съавторство с научния му ръководител **доц. д-р Николай Каканаков**. Всички публикации отразяват важни изследвания и резултати на дисертационната работа.

Най-престижна е публикация [P2], представена в AIP Conference Proceedings (SJR = 0.164), която е самостоятелна и носи на автора 40 точки. Така е изпълнено изискването за придобиване на образователната и научна степен „доктор" за минимум 30 точки от група „Г" според „Правилник за прилагане на закона за развитието на академичния състав в Република България" за професионално направление 5.3. Комуникационна и компютърна техника.

6. Мнения, препоръки и критични бележки.

Преценката на докторанта **маг. инж. Г. Искров,** че цитирам (стр. 2): „Настоящият дисертационен труд няма претенции да представлява пълно и широкообхватно проблемите съпътстващи съвременното развитие на Blockchain технологията", е професионално направена. Това му е дало възможност да определи точно целите, задачите, методите на работа, като цяло мястото на дисертационния труд. В дисертационната работа има логическа последователност що се отнася до проведените изследвания.

Авторефератът отразява всички съществени елементи на дисертационния труд – структура, цели, задачи, основни резултати, приноси, приложения и публикации. Обемът му от 31 страници е на обичайно приетото ниво за дисертация в професионално направление 5.3 Комуникационна и компютърна техника.

Технически университет-София
ФАКУЛТЕТ „ЕЛЕКТРОНИКА и АВТОМАТИКА"
филиал ПЛОВДИВ

В някои приложения на Blockchain технологията би било уместно да се прави сравнителен анализ на основата на симулационни изчисления. Такъв е случаят с консенсусите PoW (Proof of work) и PoA (Proof of authority) в рамките на системата VANET за контрол на пътната обстановка.

В текста на дисертацията се забелязват някои технически неточности, но те не влияят съществено на добрия език и стил на автора.

ЗАКЛЮЧЕНИЕ.

Въз основа на направения анализ считам, че дисертационната работа на **маг. инж. Георги Димитров Искров** отговаря на изискванията на Закона за развитието на академичния състав в Република България и Правилника за неговото прилагане за получаване на образователна и научна степен **„Доктор”**.

Давам **ПОЛОЖИТЕЛНА** оценка на дисертационния труд и предлагам на членовете на уважаемото Научно Жури също да гласуват положително **маг. инж. Георги Димитров Искров да получи образователната и научна степен „Доктор” в професионално направление 5.3 Комуникационна и компютърна техника, научна специалност „Компютърни системи, комплекси и мрежи”.**

Дата: 11.10.2023 г.

Рецензент:

/ проф. д-р К. Онков /

REVIEW

on PhD thesis for receiving educational and scientific degree "Doctor" in professional field 5.3 Communication and computer technology, scientific specialty "Computer systems, complexes and networks", based on the order №: ОЖ-5.3-49 / 19.07.2023 of the Rector of Technical University-Sofia

Author of the PhD thesis: **M.Sc Eng. Georgi Dimitrov Iskrov**

Subject of the PhD thesis: **Research and implementation of Blockchain-based network security**

Reviewer: **Prof. PhD Kolyo Zlatanov Onkov, "Mathematics and Informatics" department, Agricultural University, Plovdiv**

1. Relevance of the problem developed in the PhD thesis in scientific and applied terms

Blockchain summarizes mathematical knowledge and elements of information and cryptographic technologies to ensure the security of message transmission in public networks. In some scientific publications Blockchain is defined as an "evolutionary step" in the new generation of information and communication technologies. The relevance of the PhD work is undoubted due to the fact that in the period 2016-2022 the European Commission in a number of its documents, decisions and activities has assigned a key place to Blockchain technology in the development of e-government and e-business, and also has initiated the construction of infrastructure for Blockchain services (EBSI).

Without any doubt, in-depth scientific research on the use of Blockchain technology to increase the level of information security in computer networks is essential for many applications in practice. All of this determines the high degree of actuality of the problem developed in the PhD work in scientific and applied terms.

2. Level of knowledge of the state of the problem and creative interpretation of the literary material

A total of 211 publications are referenced in PhD work: 211 in English, 2 in Bulgarian and in Russian language. 202 of them (more than 95%) are published in the period 2018-2021.

The literature review has analytical character and is located in **Chapter I** "Design, classification and structure of Blockchain technology" of the PhD thesis. **M.Sc Eng. G. Iskrov** knows Blockchain technology very well and understands the scientific and applied nature of the PhD work. The systematic thinking of the PhD student and his ability to extract knowledge and information from the studied literature are visible.

The standard reference method for scientific works in the field of informatics and computer science is used through the number of source in the bibliography, which allows the reader to establish more easily a connection between the reference in the text and the full description of the source in the bibliography.

3. Correspondence of the research methodology and the set aim and tasks of the PhD thesis with the achieved contributions

The PhD thesis of **M.Sc. Eng. G. Iskrov** aims at analyzing the security provided by Blockchain technology when transmitting messages in public networks, analyzing the main working mechanisms and bringing out the advantages and disadvantages of this dynamic and complex process. An interdisciplinary approach is applied. The most important place is occupied by the empirical-analytical method, the analysis of the action of consensuses, system and factor analysis. The chosen approach is consistent with the set goal. This approach requires in-depth knowledge about the tasks set in the PhD work and skills for their creative application. The selected research methods provide good opportunities for achieving scientific and applied results.

4. General characteristics of the PhD thesis. Scientific and applied contributions

The PhD thesis contains the legally required structural elements – introduction, 3 chapters with conclusions to each of them, directions for future development, conclusion, claimed contributions, list of publications on the PhD work and bibliography.

In the frame of literature review as a part of **Chapter I**, the working principles of Proof-of-work, Proof-of-stake, Proof-of-authority, Proof-of-capacity and Proof-of-burn consensuses are discussed. An analysis of the security and protection of data during its migration from one chain to another is presented.

At the end of this chapter, well-reasoned conclusions are drawn and the aim and 6 tasks of the PhD work are defined.

Chapter II "Blockchain and IoT" examines the advantages and disadvantages of the classical concept "Smart City". The possibilities of using Blockchain technology as a way to protect personal data from a hacker attack are discussed. Possible hacker attacks in the

"Smart Home" as part of the "Smart City" concept and how Blockchain technology could minimize their effect are analyzed. Principal framework of the application of Blockchain technology in the concept of IoT and communication between the three layers: data perception, communication and network, is considered. Functional analysis for Blockchain application in IoT related to types of hacker attacks and their targets in IoT has been implemented.

Security issues with VANET – wireless networks connecting a group of moving or stationary vehicles, are discussed. The integration of Blockchain to this type of networks to ensure intelligent traffic control and provide useful real-time information is analyzed.

Analyzes of the resilience of Blockchain technology to malicious hacker attacks (DoS, Sybil, etc.) have been realized in **Chapter III** "Analysis of security provided by Blockchain". Special attention is paid to the role of Blockchain in the decentralized approach to prevent Double-spending.

The problem of Byzantine fault tolerance, also known as the Byzantine generals problem, is presented and analyzed in detail. In the PhD thesis this problem is solved through the mathematical-empirical method. This is an important issue concerning the contributions of the PhD work, which will be discussed below.

I highly appreciate the PhD student's ability to present clearly and reasoned his view for the development of obtained results. This view is in the direction of building a test algorithm to the abstract model of Blockchain in the "Smart City concept", a test model for the VANET system with opportunities to integrate with cloud structures and remote computing architectures MEC (Mobile Edge Computing) and as well as in-depth study of the effect of different types of hacker attacks and their impact on different consensuses. The realistic view on the future development of obtained results is an indicator of the professionalism and intelligence of the author of the PhD work.

Evaluation of the scientific and applied contributions

A) Scientific contribution 1

At the beginning, the author presents the problem of Byzantine fault tolerance in a descriptive way: generals, armies, decision-making and coherence. This is unusual for a PhD work in the field of computer systems. I am inclined to endorse this approach for two reasons: a) the problem becomes easy to perceive, including by a non-specialist in the field; b) the author makes an important interpretation of this problem on a network/distributed system with the main meaning of Blockchain.

PhD student's scientific contribution consists in the mathematical-empirical proof of the "impossibility theorem" within the Byzantine fault tolerance problem. In the present work, the conditions regarding the interactive coherence between the participants in the distributed system/network are formalized so that it can continue to function. Known solutions to the mentioned problem are based on a graphical-analytical approach. In this thesis, for the first time, the mathematical-empirical method is used to find a solution to the problem of Byzantine fault tolerance.

In Chapter III.4.4 of the PhD thesis "Proof of impossibility" an inaccuracy was admitted by the PhD student. The expression ($n < 3m+1$) is written, but it should be read: ($n > 3m+1$). The PhD student informed the members of the jury in a timely manner with the assurance that a correction was made in the PhD work and Author abstract.

B) Scientific-applied contributions

I accept **Contribution 2**, but would like to point out an inaccuracy in its wording, quote "A concept for future development of the listed systems was considered with the use of cloud structures and remote computing architectures MEC (Mobile Edge Computing)". It is not clear which these **"listed systems"** are? The idea of storing data in cloud structures and using remote computing architectures MEC is developed in **Chapter II** of the PhD thesis. **Contribution 2** could be defined better as follows: "Concept for future development of IoT and VANET networks with Blockchain integration and use of cloud structures and remote computing architectures MEC (Mobile Edge Computing) is considered".

Contributions 3-5 are very well defined and reveal essential aspects of the results achieved in the PhD work. They refer to an abstract application model of Blockchain technology and different types of consensus in Smart Sity and Smart Home, functional analysis of various hacker attacks in IoT, Smart Sity and Smart Home, as well as analysis of Blockchain technology resilience and model for prevention and protection.

C) Applied contributions

The applied contributions of the PhD student are indisputable. An implementation of the PoA (Proof of authority) consensus within VANET for traffic control is proposed **(contribution 6)**. A project structure, a complete program code and an implementation procedure with the application of Blockchain technology in an election system have been developed (**contribution 7**). The claims of the author related to contribution 7 about the possibilities of Blockchain to reduce bureaucracy, costs, corruption and foremost increasing the security of transmitted data when holding elections sound very relevant.

The issue of the presence of results that lead to a direct economic effect is not discussed in the PhD thesis. The nature of the PhD work is such that an indirect economic effect with

Технически университет-София
ФАКУЛТЕТ „ЕЛЕКТРОНИКА и АВТОМАТИКА"
филиал ПЛОВДИВ

significant potential is contained in the practical applications of public computer networks based on Blockchain technology with a view to the security of data transmission and providing information services in some functionalities of Smart Sity, Smart Home , VANET, etc. There is logic in the PhD student's claim of reducing costs in the election application using Blockchain. This is of course subject to future research, financial analysis and evaluation.

5. Evaluation of publications related to PhD thesis

A list of five scientific publications related to PhD work is presented. One article is written in Bulgarian language, the other four in English. Two articles have been published in journals, the rest in the proceedings of international conferences. The personal contribution of **M.Sc Eng. Georgi Iskrov** is indisputable. He is single author of four of the publications, and the fifth is co-authored with his scientific supervisor **Assoc. Prof. PhD Nikolay Kakanakov**. All publications reflect important research and results of the PhD work.

The most prestigious is a publication [P2], presented in the AIP Conference Proceedings (SJR = 0.164). This is single author publication of the PhD student and brings him 40 points. Thus, the requirement for acquiring the educational and scientific degree "doctor" for a minimum of 30 points from group "D" according to the "Regulations for the implementation of the law on the development of the academic staff in the Republic of Bulgaria" in professional field 5.3 Communication and computer technology is fulfilled.

6. Opinions, recommendations and critical notes

The assessment of PhD student **M.Sc. Eng. G. Iskrov** that I quote (page 2): "The present PhD thesis does not claim to fully and comprehensively represent the problems accompanying the modern development of Blockchain technology", is professionally done. This gave him the opportunity to define precisely the aims, tasks, methods of work and as a whole the place of the PhD work. There is a logical sequence in the PhD thesis as far as the research is concerned.

The Author abstract reflects all essential elements of the PhD work – structure, aims, tasks, main results, contributions, applications and publications. Its volume of 31 pages is at the usual accepted level for professional field 5.3 Communication and computer technology.

In some applications of Blockchain technology it would be appropriate to make a comparative analysis based on simulation computations. This is the case with the PoW (Proof of work) and PoA (Proof of authority) consensuses within the VANET traffic control system.

There are some technical inaccuracies in the text of the PhD work, but they do not significantly affect the good language and style of the author.

Технически университет-София
ФАКУЛТЕТ „ЕЛЕКТРОНИКА и АВТОМАТИКА"
филиал ПЛОВДИВ

CONCLUSION

On the basis of presented analysis, I consider that PhD thesis of **M.Sc Eng. Georgi Dimitrov Iskrov** fulfils the requirements of the Law of Academic Staff in Republic of Bulgaria and Regulations for its implementation to receive educational and scientific degree **"Doctor"**.

I evaluate **POSITIVELY** the PhD thesis and propose the members of Honorable Scientific Jury to vote positively for **M.Sc Eng. Georgi Dimitrov Iskrov to receive educational and scientific degree "Doctor" in the professional field 5.3 Communication and computer technology, scientific specialty "Computer systems, complexes and networks".**

October 11, 2023

Reviewer:

/ Prof. PhD Kolyo Onkov /