Процедура № ФЕА56-НС1-026

Рецензията е постъпила във факултетна канцелария на ФЕА на 13.X.2023г.

РЕЦЕНЗИЯ

върху дисертационен труд за придобиване на образователна и научна степен „доктор”

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

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

от **проф. д-р Гриша Валентинов Спасов**
ТУ – София, Филиал Пловдив, **e-mail:** gvs@tu-plovdiv.bg

1.Актуалност на дисертационния труд.

Предложеният дисертационен труд е на безспорно актуална и важна тема свързана с изследване и анализиране на сигурността предоставяна от Blockchain технологиите и прилагането и при обмена на данни в публични компютърни мрежи. Обект на изследване са основните технологични възможности на различните консенсуси използвани във Blockchain технологията да защитават пренасяната поверителна информация, като данни за личност, адреси, съдържание на съобщенията, транзакции и т.н..

Решените конкретни задачи в дисертационния труд имат пряко практическо приложение при разработването на методи и средства за повишаване на сигурността при обмена на данни в рамките на Интернет на нещата (IoT), уеб услуги, интелигентно здравеопазване, интелигентен град (smart city), VANET, интелигентен дом (smart home), и други интернет системи базирани на обмен на данни и съобщения.

2. Степен на познаване състоянието на проблема.

Направеното литературно проучване (основно в глава 1) и направения анализ в него, показват едно много добро познаване на тематиката свързана с анализиране на мрежова сигурност базирана на Blockchain технологията. Литературните заглавия (общо 211) са свързани с тематиката на дисертационния труд, като в основната си част са на английски език, 3 на руски и 2 на български.

Литературното проучване завършва с анализ и изводи, на чиято основа е формулирана целта на дисертационния труд и са дефинирани задачите за нейното постигане.

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

Избраната от докторанта методика за научно изследване дава възможност да осъществи основната цел на дисертационния труд „да се изследва и анализира процеса на взаимодействие на Blockchain технологията при опериране със строго специфичните лични данни, като: транзакции, трансфери на парични средства, персонални IP адреси,

криптопортфейли, данни от бита и ежедневието събирани и съхранявани в рамките на концепцията за Smart Sity, Smart Home, VANET. Както и да се гарантира неприкосновеността на тези чувствителни и уязвими данни от кражба, присвояване, злоупотреба или агресивни хакерски атаки".

Методически дисертационният труд следва логическата последователност:

– Въведение в развитието на blockchain системите в сферата на криптовалутите и основните технологични възможности на различните консенсуси използвани в тях за защита пренасянето на поверителна информация. Както и предоставяното ниво на сигурност от Blockchain в сравнение с класическите методи за пренос на данни в рамките на концепцията Smart Home, въздействието на различните видове хакерски атаки и минимизирането на щетите причинени от тях.

– Функционален анализ на използването на Blockchain технологията в Интернет на нещата (IoT). Уязвимости, типови хакерски атаки и решения. Изследване на взаимодействащите процеси при трансфера на данни, съответно при използването на класическите протоколи за пренос на данни MQTT за IoT, и от друга страна при използването на Blockchain за същите цели.

– Анализ на използването на Blockchain при обмяната на съобщения във VANET с предхождащи консенсуси за повишаване на нивата на безотказност, надеждност, сигурност и мащабируемост.

– Анализиране устойчивостта на Blockchain на различни типове злонамерени хакерски атаки, като: DoS, DdoS, Ping-flooding, Sybil, Double-treasure-spending. Както и предлагане на методики и полезни практики за тяхното предотвратяване.

– Предлагане на математически модел, базиран на Blockchain технологии, при решаване на парадокса на Byzantine fault tolerance (BFT).

– Предлагане на експериментална система за избори с приложение на Blockchain технологии.

Считам, че използваната методика на изследване е в съответствие с поставената цел и задачи на дисертационния труд.

4. Характеристика на дисертационния труд.

Запознат съм с представеният вариант на дисертационния труд за пред-защитата. Намирам положително развитие и подобряване на материала с отработване на направените препоръки и забележки при обсъждането.

Изследванията в дисертационния труд са изложени в увод и 3 глави.

В увода се въвежда проблематиката на дисертацията.

В първа глава е направен обзор на развитието на blockchain системите в сферата на криптовалутите. Разгледани и анализирани са най-често използваните методи за консенсус при формиране на блокове във верига на Blockchain системи. Анализирано е използването на Blockchain веригите в рамките на концепциите Smart Sity (интелигентен град), Smart Home (интелигентен дом), VANET (Vehicular ad hocnetwork). Извършен е системен и факторен анализ на децентрализирана система за транзакции между различни криптовалути – Atomic Swaps с изтъкване на предимства и недостатъци при обмен на

данни между различните вериги. Главата завършва със съответните изводи, като е обоснована целта на дисертационния труд и задачите за нейното постигане.

В глава втора е направен анализ на Smart Home в рамките на концепцията за Smart Sity, възможните хакерски атаки и възможностите на Blockchain технологията да минимизира ефекта от тях върху системата. В главата е направен функционален анализ на приложението на Blockchain в IoT. Разгледана е примерна архитектура използваща консенсуси DpoS и PoA на Blockchain в рамките на Smart Home. Предложено е противодействие и превенция на хакерските атаки в рамките на използваните консенсуси на Blockchain за IoT, Smart Sity и Smart Home. Направен е факторен анализ на използването на Blockchain при обмяна на съобщения в VANET.

Глава трета е посветена на доказване устойчивостта на Blockchain технологията, както на DoS атаки, така и на Sybil атаки. С помощта на структурно-функционален анализ, посредством графичен подход се доказва непригодността и нецелесъобразността на атаката тип Double-treasure-spending при Blockchain веригите. Предложено е експериментално-математическо решаване и доказване на теоремата за невъзможност в рамките на отработване на парадокса на Bazantine fault tolerance (BFT) с използването на Blockchain технологий. В последната част на главата се демонстрира практическо приложение на Blockchain, като изборна система – посредством цялостно изложен програмен код (действаща програма).

След трета глава са представени обобщение и насоки за бъдещо развитие на изследванията в областта на дисертационния труд.

5. Приноси на дисертационния труд.

Приемам по принцип формулираните от докторанта приноси, които могат да бъдат класифицирани като научни, научно-приложни и приложни. Те са обобщени след последната глава на дисертационния труд. Считам, че формулираните приноси показват, че поставените задачи са изпълнени. Този подход за представяне на приносите е удачен, защото свързва формулираната цел и задачи на дисертационната работа с постигнатите резултати.

Научен принос:

- Предложено е доказателство на теоремата за невъзможността в рамките на парадокса Byzantine fault tolerance (BFT).

По-важните научно-приложни приноси са следните:

- Предложена е концепция за бъдещо развитие на изброените системи с помощта на облачни структури и отдалечени изчислителни архитектури MEC (Mobile Edge Computing).
- Предложен е абстрактен модел на приложение на Blockchain технологията в рамките на концепциите Smart Sity и Smart Home. Представена е примерна реализация на архитектура използваща консенсуси DPoS и PoA на Blockchain в рамките на Smart Home.
- Представен е функционален анализ на различните видове хакерски атаки и техните цели в IoT, Smart Sity и Smart Home. Предложено е противодействие и превенция на хакерските атаки в рамките на използваните консенсуси на Blockchain за IoT, Smart Sity и Smart Home.

- Представен е анализ на устойчивостта на Blockchain технологията на различни типове злонамерени хакерски атаки, като: DoS, DdoS, Ping-flooding, Sybil, Double-treasure-spending. Предложен е модел за превенция и защита.

Приложни приноси:

- Предложена е реализация на консенсуса PoA (Proof of Authority) в рамките на системата VANET (Vehicular ad hoc network) за контрол на пътната обстановка.
- Представено е експериментално практическо приложение на базата на Blockchain технологията под формата на изборна система. Изложен е пълния изходен код, структурата на проекта и процедурата на изпълнение.

Научно-приложните приноси се отнасят към следните две групи: доказване с нови средства на съществени нови страни в съществуващи научни проблеми и теории; създаване на нови модели, технологии и алгоритми. Характер на приносите за внедряване: методологии и алгоритми.

Считам, че постигнатите резултати, научно-приложните и приложни приноси са предимно лично дело на кандидата. Те доказват, че докторантът има капацитет да извършва самостоятелно изследователска и инженерна дейност.

6. Преценка на публикациите по дисертационния труд.

По дисертационния труд са представени пет публикации, една от тях в съавторсто с ръководителя на докторанта и четири самостоятелни. Четири публикации (P1, P2, P3, P4) са представени на международни конференции в България. P1, P2, P3 са публикувани на „TechSys" 2021 и 2022 и са индексирани в системата SCOPUS. Публикация P5 е пуликувана в списание в България. До момента няма открити цитирания на представените публикации.

Всички публикации имат пряко отношение към решаваните в дисертацията въпроси.

Броят на публикациите отговаря на изискванията за ОНС доктор в Научно направление 5.3.

7. Значимост на резултатите от дисертационния труд за науката и практика.

Докторантът е извършил голяма по обем работа, отличаваща се със задълбоченост и компетентност. Работата е значима не само заради научно-приложните постижения, но и заради възможността за пряко практическо приложение на Blockchain технологиите в концепциите за Smart Sity и Smart Home, VANET системите, системите за провеждане на избори.

8. Оценка на съответствието на автореферата с изискванията за изготвянето му.

Авторефератът в обем от 31 страници отговаря на изискванията и представя съдържанието, основните постижения, резултатите от изследванията и приносите в дисертационния труд.

9. Мнения, препоръки и бележки.

Образователните цели на дисертацията са изпълнени.

- Забележки:

В Дисертационния труд на стр. 89 изречение второ от текущия абзац има допусната грешка, изразяваща се в знака за неравенство: изписано е $n < 3m+1$, а трябва да се чете $n > 3m +1$. Същата грешка се повтаря и в Автореферата на стр. 23 ред № 7 - „Доказателство за невъзможност". След дискусия с докторанта е установено, че грешката е възникнала при оформяне на окончателния вариант на пуликация [P1]: „Analysis of the Protection Granted to Blockchain in the Operation of the Task of the Byzantine Generals (Byzantine Fault Tolerance (BFT), Byzantine Agreement Problem, Byzantine Generals Problem)".

- Препоръки:

Постигнатите резултати е добре да бъдат сравнени с други подобни, получени при алтернативни изследвания в областта на дисертацията.

Нямам забележки по отношение на количеството и качеството на извършената в дисертацията работа.

10. Заключение

Оценката ми за рецензирания дисертационен труд, автореферата и публикациите, отразяващи изследванията в дисертацията е положителна. Дисертацията съдържа научни, научно-приложни и приложни приноси в достатъчна степен и отговаря на изискванията на Закона за развитие на академичния състав в република България (ЗРАСРБ) и Правилника за неговото прилагане, както и на Правилника за условията и реда за придобиване на научни степени в ТУ-София.

В резултат на посочените до тук постижения в дисертационния труд, предлагам на уважаемото Научно жури да присъди на маг. инж. Георги Искров, образователната и научна степен „доктор" по специалност „Компютърни системи, комплекси и мрежи".

Дата: 13.10.2023 г.

Изготвил:

(проф. д-р инж. Гриша Спасов)

REVIEW

about the PhD thesis for acquisition of the scientific degree "doctor" in the professional field 5.3 "Communication and computer technics", doctoral program "Computer systems, complexes and networks",

Author of the PhD thesis: MSc eng. Georgi Iskrov

Topic of the PhD thesis: Research and implementation of blockchain-based network security

Reviewer: Prof. eng. Grisha Valentinov Spasov, PhD, TU – Sofia, Plovdiv Branch, Department of Computer Systems and Technologies, e-mail: gvs@tu-plovdiv.bg

1. Actuality of the problems in the PhD thesis

The proposed PhD thesis deals with an indisputably actual and important topic related to research and analysis of the security provided by Blockchain technologies and the application and exchange of data in public computer networks. The object of research is the main technological capabilities of the various consensuses used in Blockchain technology to protect the transferred confidential information, such as personal data, addresses, content of messages, transactions, etc.

The developed specific tasks solved in the dissertation work have a direct practical application in the development of methods and means of increasing security in data exchange within the Internet of Things (IoT), web services, intelligent healthcare, smart city, VANET, intelligent home (smart home), and other Internet systems based on data and message exchange.

2. Degree of knowledge of the state of the problem

The literature review in Chapter 1 and the analysis made in it show a very good knowledge of the topic related to analyzing network security based on Blockchain technology. The references (211 in total) are related to the subject of the dissertation work, with the main part being in English, 3 in Russian and 2 in Bulgarian.

The literature review ends with an analysis and conclusions, on the basis of which the goal of the PhD thesis and the tasks for its implementation are defined.

3. Correspondence of the chosen research methodology with the set goal and tasks of the PhD thesis.

The research methodology chosen by the PhD student makes it possible to achieve the main goal of the dissertation "to study and analyze the interaction process of Blockchain technology when operating with strictly specific personal data, such as: transactions, money transfers, personal IP addresses, crypto wallets, household and daily life data collected and stored within the Smart City concept, Smart Home, VANET. As well as, ensuring the inviolability of this sensitive and vulnerable data from theft, misappropriation, misuse or aggressive hacking attacks".

Methodologically, the dissertation follows the logical sequence:

- Introduction to the development of blockchain systems in the field of cryptocurrencies and the main technological capabilities of the various consensuses used in them to protect the transfer of confidential information. As well as, the level of security provided by Blockchain compared to classic data transfer methods within the Smart Home concept, the impact of various types of hacker attacks and minimizing the damage caused by them;

- Functional analysis of the use of Blockchain technology in the Internet of Things (IoT). Vulnerabilities, types of hacking attacks and solutions. Study of the interactive processes of data transfer, respectively when using the classic data transfer protocols MQTT for IoT, and on the other hand when using Blockchain for the same purposes;

- Analysis of the use of Blockchain in the exchange of messages in VANET with prior consensuses to increase the levels of fail-safe, reliability, security and scalability;

- Analyzing Blockchain's resistance to various types of malicious hacking attacks, such as: DoS, DdoS, Ping-flooding, Sybil, Double-treasure-spending. As well as offering methods and useful practices for their prevention.

– Proposing a mathematical model based on Blockchain technologies in solving the Byzantine fault tolerance (BFT) paradox.

– Proposing an experimental system for elections with the application of Blockchain technologies.

I believe that the research methodology used is in accordance with the goal and objectives of the dissertation.

4. Characteristics of the PhD thesis

I was familiar with the presented version of the dissertation for pre-defense. I find a positive development and improvement of the material by working out the recommendations and remarks made during the discussion.

The PhD thesis is presented in an introduction and 3 chapters.

In the introductory part the problems of the dissertation are introduced.

In the first chapter, an overview of the development of blockchain systems in the field of cryptocurrencies is made. The most frequently used methods of consensus in the formation of blocks in a chain of Blockchain systems have been examined and analyzed. The use of chains in Blockchain systems within the concepts of Smart City, Smart Home, VANET (Vehicular ad hoc network) has been analyzed. A systematic and factor analysis of a decentralized system for transactions between different cryptocurrencies - Atomic Swaps, highlighting advantages and disadvantages of data exchange between different chains has been carried out. The chapter ends with the relevant conclusions, justifying the purpose of the dissertation work and the tasks for its achievement.

In the second chapter, an analysis of Smart Home within the concept of Smart City, possible hacker attacks and the possibilities of Blockchain technology to minimize their effect on the system is made. In the chapter, a functional analysis of the application of Blockchain in IoT is made. An example architecture using Blockchain DpoS and PoA consensus within Smart Home

is discussed. Countermeasures and prevention of hacker attacks are proposed within the used Blockchain consensuses for IoT, Smart Sity and Smart Home. A factor analysis of the use of Blockchain in VANET message exchange was done.

Chapter three is dedicated to proving the resilience of Blockchain technology to both DoS attacks and Sybil attacks. With the help of structural-functional analysis, by means of a graphical approach, the unsuitability and inexpediency of the Double-treasure-spending attack on Blockchain chains is proved. An experimental-mathematical solution and a proof of the impossibility theorem is proposed within the framework of working out the paradox of Byzantine fault tolerance (BFT) with the use of Blockchain technologies. In the last part of the chapter, a practical application of Blockchain, as an election system, is demonstrated by means of a completely exposed program code (working program).

After the third chapter, a summary and guidelines for future research in the field of dissertation work are presented.

5. Contributions to the PhD thesis

I accept in principle the contributions formulated by the PhD student, which can be classified as scientific, scientific-applied and applied. They are summarized after the last chapter of the dissertation. I believe that the formulated contributions show that the defined tasks have been fulfilled. This approach for presenting the contributions is appropriate because it connects the formulated goal and tasks of the dissertation with the achieved results.

Scientific contribution:

- A proof of the impossibility theorem within the Byzantine fault tolerance (BFT) paradox is proposed.

The most important scientific and applied contributions are the following:

- A concept for future development of the listed systems using cloud structures and remote computing architectures MEC (Mobile Edge Computing) is proposed;

- An abstract application model of Blockchain technology within the Smart City and Smart Home concepts is proposed. An example implementation of an architecture using Blockchain DPoS and PoA consensus within Smart Home is presented;

- A functional analysis of the different types of hacker attacks and their targets in IoT, Smart City and Smart Home is presented. Countermeasures and prevention of hacker attacks are proposed within the used Blockchain consensuses for IoT, Smart Sity and Smart Home;

- An analysis of the resistance of Blockchain technology to various types of malicious hacker attacks is presented, such as: DoS, DdoS, Ping-flooding, Sybil, Double-treasure-spending. A model for prevention and protection is proposed;

Applied contributions:

- Implementation of the PoA (Proof of Authority) consensus within the VANET (Vehicular ad hoc network) system for traffic control is proposed.

- An experimental practical application based on Blockchain technology in the form of an election system is presented. The complete source code, project structure and implementation procedure are laid out.

Scientific and applied contributions belong to the following two groups: proving with new means of significant new features in existing scientific problems and theories; creating new models, technologies and algorithms. Nature of the contributions for implementation: methodologies, algorithms.

I believe that the achieved results, the scientific-applied and applied contributions are mainly a personal work of the candidate. They prove that the PhD student has the capacity to perform research and engineering activities independently.

6. Evaluation of the publications on the PhD thesis

Five publications are presented on the dissertation work, one of them co-authored with the supervisor of the doctoral student and four are with one author – the PhD student. Four publications (P1, P2, P3, P4) have been presented at international conferences in Bulgaria. P1, P2, P3 are published on "TechSys" 2021 and 2022 and are indexed in the SCOPUS system. Publication P5 was published in a journal in Bulgaria. To date, no citations have been found for the presented publications.

All publications are directly related to the issues addressed in the dissertation.

The number of publications meets the requirements for obtaining educational and scientific PhD Degree in Scientific field 5.3.

7. Significance of the results of the PhD thesis for science and practice

The PhD student has carried out a large volume of work, distinguished by thoroughness and competence. The work is significant not only because of scientific and applied achievements, but also because of the possibility of direct practical application of Blockchain technologies in Smart City and Smart Home concepts, VANET systems, and election systems.

8. Assessment of the conformity of the abstract with the requirements for its preparation

The abstract of 31 pages meets the requirements and presents the content, main achievements, research results and contributions to the dissertation.

9. Opinions, recommendations and notes

The educational goals of the dissertation are fulfilled.

Notes:

- In the Dissertation on page 89, the second sentence of the current paragraph, there is an error made in the inequality sign: $n < 3m+1$ is written, but $n > 3m+1$ should be read. The same mistake is repeated in the Abstract on page 23, line No. 7 - "Proof of impossibility". After a discussion with the PhD student, it was found that the error occurred when creating the final version of the publication [P1]: "Analysis of the Protection Granted to Blockchain in the Operation of the Task of the Byzantine Generals (Byzantine Fault Tolerance (BFT), Byzantine Agreement Problem, Byzantine Generals Problem)".

Recommendations:

• The achieved results should be compared with other similar ones obtained in alternative research in the field of the dissertation.

I have no remarks regarding the quantity and quality of the work done in the dissertation.

10. Conclusion

My assessment of the dissertation, the abstract and the publications reflecting the research in the dissertation is positive. The dissertation contains scientific-applied and applied contributions to a sufficient degree and meets the requirements of the Law for development of the academic staff in the Republic of Bulgaria and the Regulations for its implementation, as well as the Regulations for the conditions for acquiring scientific degrees in TU- Sofia.

As a result of the above-mentioned achievements in the dissertation, I propose to the Scientific Jury to award to MSc eng. Georgi Iskrov educational and scientific degree "Doctor", in the professional field 5.3. "Communication and computer technics", doctoral program "Computer systems, complexes and networks".

Date: October 13, 2023.

Reviewer:

(Prof. eng. Grisha Spasov, PhD)