ФКСТ44 – НС1 – 048
23.08.2021г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ ФКСТ СОФИЯ

РЕЦЕНЗИЯ

на дисертационен труд за присъждане
на образователна и научна степен „**доктор**“
в Професионално направление 5.3 Комуникационна и компютърна техника,
научна специалност „Автоматизирани системи за обработка на информация и управление“

Тема на дисертационния труд:
Обработка и защита на информация в децентрализирани мрежи

Рецензент: проф. д-р инж. Румен Иванов Трифонов
Ръководител катедра ИТИ, ФКСТ, Технически Университет – София

Автор на дисертационния труд: маг. инж. Ивайло Симеонов Ченчев

I. Актуалност на дисертационния труд

Дисертационния труд разглежда една много актуална и бързо развиваща се област. Съвременните тенденции на развитие на блок-веригите показват изключителен теоретичен и практически интерес през последните няколко години. Свидетели сме на появата и все по-широкото навлизане на т.нар. „виртуални валути“ (или още крипто-валути, цифрови валути, цифрови пари). Нараства броя на фирмите в световен мащаб, които използват цифровите пари за продажба на стоки и услуги. Даже нещо повече: някои правителства разглеждат възможността за въвеждане на национална цифрова валута, докато например Китай тази година вече въведе в обръщение своя собствена цифрова валута – „дигитален юан“.

Безспорно, децентрализираните мрежи търпят бурно развитие. Доказателство за това е посочил и докторантът в направения предварителния анализ на научни публикации – от изследваните научни публикации, думата „блокчейн“ се среща най-много пъти и при това, нейната поява фигурира едва от 2016 година насам.

II. Степен на информираност на докторанта за състоянието на проблема

В дисертацията е извършен задълбочен анализ на постиженията в областта на децентрализираните мрежи. Добро впечатление прави подробното и детайлно изследване и анализа на методите за удостоверяване като са направени няколко класификации на методите за удостоверяване.

В дисертационния труд са цитирани 160 литературни източника в изследваната научна област в реномирани международни списания и научни форуми

и интернет източници, обхващащ периода от активно развитие на тази тематика. С това авторът показва отлична осведоменост и добро познаване на проблематиката.

На база обзорния анализ докторантът формулира целта и задачите на дисертационния труд. Считам, че докторантът има задълбочени познания в тематиката на проведените изследвания.

III. Съответствие на предложената методика на изследване и поставените цел и задачи на дисертационния труд

Целта на дисертационния труд е *да се изследват и предложат методи и алгоритми за подобряване на средствата за сигурно и защитено удостоверяване в децентрализирани мрежи, както и на средствата за обработка на информацията в частност при блок-веригите (блокчейн).*

За постигане на поставената цел правилно и адекватно са формулирани пет изследователски задачи за решаване, които включват: изследване на подходите, методите и алгоритмите за обработка, защита и съхранение на информацията в децентрализирани мрежи; подобряване на алгоритмите за обработка на информацията, достъпа до нея и подобряване на защитата на информацията чрез прилагане на различни криптографски алгоритми; проектиране и създаване на експериментален прототип на децентрализирана мрежа в лабораторни условия, който прилага предложените алгоритми за обработка и защита на информация; проектиране на софтуерна рамка за експериментален прототип за обработка, защита и съхранение на информацията в децентрализирани мрежи; валидиране на прототип за обработка, защита и съхранение на информацията в децентрализирани мрежи.

Докторантът е използвал разнообразие от взаимно допълващи се методи и алгоритми, които представят точни и надеждни резултати за анализиране и извеждане на изводи.

Избраните методи и алгоритми съответстват на основната цел и задачи, поставени за решаване от докторантът.

IV. Характеристика на естеството и оценка на достоверността на материала, върху който се градят приносите на дисертационния труд

Докторантът е направил обстоен анализ на множество литературни източници – научни публикации в световно известни издания, доклади в международни научни конференции, списания, книги и интернет източници.

При решаването на поставените задачи са използвани различни средства и похвати. Използвани са както стандартни методи и алгоритми, така и нови, предложени в дисертационния труд. Предложените методи и алгоритми са добре обосновани и не се забелязват грешки в тяхното представяне.

Експерименталните резултати от изследването се базират на проведени в различни инфраструктурни среди измервания. За целта са избрани стандартни типове виртуални машини в облачните среди на Амазон, Гугъл и Майкрософт. Направени са много голям брой практически измервания и изчисления, които са анализирани. На тяхна база са направени изводите и обобщенията.

Предложените идеи и основните резултати от измерванията и изчисленията са докладвани на международни научни конференции, както и на национални конференции.

V. Приноси на дисертационния труд

Приносите, формулирани в дисертационния труд, биха могли да се обобщят и категоризират с научен, научно-приложен и приложен характер.

Научни приноси:

(1) Направен е сравнителен анализ на основните характеристики в аспектите на реализацията, внедряването и техните свойствата на четирите вида блокчейн архитектури.

Научно-приложни приноси:

(1) Създаден е модел на дву-факторно удостоверяване между хостове, основан върху генерирани в реално време пароли, базирани на динамични хеш-вериги с променлива дължина.

(2) Предложен е алгоритъм за генериране на Merkle-root хеш-стойност за двоично дърво от транзакции, чрез използването на четири различни групи от изчисления с различни хеш-функции.

(3) Предложена е архитектура на система за генериране на пароли в реално време с цел валидиране на предложения метод и алгоритми.

Приложни приноси:

(1) Реализиран е софтуерен прототип с отворен код на клиент-сървър архитектура за удостоверяване по стандартния метод със записани пароли във файл, който може да се променя и развива за конкретни нужди.

(2) Реализиран е софтуерен прототип с отворен код на клиент-сървър архитектура за удостоверяване чрез предложения метод и алгоритми, постигайки подобрение на измереното време спрямо стандартния начин на удостоверяване, при който паролите са записани във файл, между 2.72 и 3.36 пъти при до 1 000 пароли, и между 5.32 и 7.89 пъти при до 10 000 пароли.

(3) Създадена е система с отворен код за автоматично генериране на тестови среди в облачната инфраструктура на Амазон AWS за валидиране на двата софтуерни прототипа за удостоверяване при клиент-сървър архитектура.

VI. Степен на личното участие на дисертанта в приносите

За личното участие на докторанта съдя по неговите 7 представени публикационни материали и лични наблюдения от участието му на научни конференции. Използва професионално графично оформление, както на фигурите, така и на цялостния труд. Докторантът убедително представя постигнатите резултати като демонстрира добра и задълбочена аргументация. Характерът на изследването предполага много добра и широка подготовка и определено считам, че се е справил успешно.

VII. Преценка на публикациите по дисертационния труд

Във връзка с разработването на дисертационния труд докторантът е представил общо 7 публикации – на шест от които е първи автор и една самостоятелна публикация. Две от публикациите са публикувани в ACM и в Springer, а трета е публикувана като глава от книгата „Information Security in Education and Practice“ (публикувана от Cambridge Scholars Publishing).

Не са представени данни за цитирания на тези публикации.

Публикациите отразяват по-съществените резултати, постигнати в дисертационния труд. Докладвани са на международни научни конференции, както и на национални конференции, което приемам за апробация в научните среди.

VIII. Съответствие на автореферата с изискванията за изготвянето му и адекватност на отразяване на основните положения и приносите на дисертационния труд

Авторефератът отразява обективно основното съдържание на дисертационния труд. Номерата на посочените таблици и фигури съответства на тези от дисертационния труд. Има ясна и логична композиция и много точно формулира основните постижения на дисертацията – основните алгоритми, резултатите, изводите и приносите. Дадох положително становище за отпечатването на автореферата в печатната база на ТУ - София.

IX. Мнения, препоръки и бележки

Нямам съществени забележки към представената дисертация. Оформлението на дисертационния труд говори за едно сериозно отношение към цялостния процес на събиране, обработка и анализ на резултатите.

Имам следния коментар, по отношение на обема на дисертационния труд:

(1) Глава 1 (Обзор на типовете мрежи, развитие и архитектура на блок-веригите и на механизмите за удостоверяване) е с най-голям обем (от 37 страници), спрямо Глави 2, 3 и 4 (поотделно). Но съдържателната част на дисертацията е съществена, което заслужава висока оценка.

Имам следните препоръки към докторанта:

(1) Да продължи работа по тематиката в областта на методите и алгоритмите за постигане на консенсус в блок-веригите;

(2) Да разшири изследването на бързодействието на изчисление на Merkle-root хеш-стойността с останалите алгоритми от двете фамилии SHA2 и SHA3.

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

X. ЗАКЛЮЧЕНИЕ

В заключение, маг. инж. Ивайло Симеонов Ченчев е съумял да направи един задълбочен научен труд. Темата е изключително актуална и изследването е добре организирано и структурирано. Той е успял да постигне поставените задачи като демонстрира изключително добро боравене с литературните източници и правещо отлично впечатление познаване и владеене на различни инфраструктурни компоненти и архитектури.

Качествата на дисертационния труд, постигнатите резултати и приноси, както и тяхното популяризиране, са достатъчно основание да дам ***положителна оценка*** на представения труд. Докторантът е постигнал поставените цели и задачи в него.

Дисертационният труд отговаря на изискванията на ЗРАСРБ, на Правилника за неговото приложение, както и на Правилника за развитие на академичния състав. Приложеният към него автореферат отразява същността на изследването и коректно представя приносите от него.

Всичко това ми дава достатъчно основание да предложа на членовете на уважаемото Научното жури да присъди на *маг. инж. Ивайло Симеонов Ченчев* образователната и научна степен „*доктор*".

23.08.2021 год.

Рецензент:.....

(проф. д-р инж. Румен Трифонов)