



## УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Булевар краља Александра 73, 11000 Београд, Србија

Тел. 011/324-8464, Факс: 011/324-8681

### КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 28.08.2018. године, именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Видора Генцела под насловом „Софтверски систем за реализацију криптовалуте употребом блокчејн технологије“. Након прегледа материјала Комисија подноси следећи

### ИЗВЕШТАЈ

#### 1. Биографски подаци кандидата

Видор Генцел, дипл. инж. електротехнике и рачунарства, рођен 24.02.1994. године у Београду. Завршио је основну школу "Петар Петровић Његош" у Београду са одличним успехом. Уписао је Гимназију "Свети Сава" у Београду коју је завршио са одличним успехом. Уписао се 2012. г. на Електротехнички факултет у Београду, студијски програм Софтверско инжењерство, а дипломирао 2016. г. са просечном оценом 9.5. Дипломски рад на тему "Реализација софтверског агента за друштвене мреже коришћењем техника обраде природног језика" одбранио је у септембру 2016. године са оценом 10. Рад је објављен на Телфор конференцији 2016. године. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за Софтверско инжењерство уписао је у октобру 2016. године. Положио је све испите са просечном оценом 10.

#### 2. Опис мастер рада

Мастер рад обухвата 42 стране, са укупно 11 слика и 23 референце. Рад садржи увод, 4 централни поглавља и закључак (укупно 6 поглавља) и списак коришћене литературе.

Прво поглавље представља увод у коме су описаны предмет и циљ рада. Представљене су предности дистрибуираних система и мотивација за њихову употребу. Описане су околности под којима су се јавиле идеје о развијању дигиталног новца као и настанак две најпознатије криптовалуте - *Bitcoin* и *Ethereum*.

У другом поглављу су изложени основни криптографски алгоритми и концепти који су коришћени у развоју блокчејнова укључујући хеш функције, асиметричну криптографију засновану на елиптичним кривама, дигиталне потписе и структуре које омогућавају брзу проверу интегритета скупа података - *Merkle* стабла.

У трећем поглављу је дата оширене компаративна анализа *Bitcoin* и *Ethereum* блокчејнова. Изложени су сви делови архитектура, алгоритми и структуре података и посебни концепти. Наглашене су разлике као и предности и мање одређених приступа. Посебно детаљно су приказани алгоритми за постизање консензуса, њихова еволуција у приказаним блокчејновима као и предложене оптимизације. Представљене су методе функционисања криптовалута (енг. *Coin*) на овим блокчејновима као и криптовалуте које су резидентне на *Ethereum* платформи (енг. *Token*) и имплементиране су помоћу паметних уговора (енг. *Smart Contracts*).

У четвртом поглављу је изложена архитектура предложеног система, узимајући у обзир концепте употребљене у анализираним блокчејновима из 3. поглавља. Описана је архитектура, основни модули и функционалности, спецификација функционисања блокчејна као и истраживача блокчејна и интерфејса за интеракцију са њим. Образложене су донете одлуке уз опис предности и мања. Такође су детаљно описаны алгоритми на имплементационом нивоу. Приказане су основне функционалности система и начин његовог коришћења.

Пето поглавље даје опис имплементационих детаља укључујући: опис употребљених технологија, опис архитектуре система, дизајн базе података, опис комуникационог протокола, оптимизације процеса рударења и могућност конфигурације система.

У закључку је резимирано шта је анализирано у оквиру рада. Наведени су и предлози за будућа унапређења и проширења реализованог система. Образложена је мотивација употребе тренутне имплементације.

### **3. Анализа рада са кључним резултатима**

Мастер рад дипл. инж. Видора Генцела се бави проблемом реализације криптовалуте употребом блокчејн технологије. Детаљно су истражени основни криптографски концепти употребљени у блокчејновима и механизмима потврда извршених трансакција, начин рада *Bitcoin* и *Ethereum* блокчејнова и предложена је оригинална хибридна имплементација која је заснована на *Ethereum* платформи, али користи *Proof-of-work* концепт преузет од *Bitcoin* платформе. Све одлуке у спецификацији система су образложене уз анализу предности и мана. Детаљно је описан модификовани алгоритам којим се постиже консензус у имплементираном блокчејну. Поред блокчејна имплементација систем садржи и интерфејсе за интеракцију за друге апликације и кориснике у виду веб апликације која подржава функције за претраживање блокчејна као и дигитално потписивање трансакција.

Главни допринос рада представља реализација оригиналног дистрибуираног софтверског система који имплементира криптовалуту употребом истражених концепата.

### **4. Закључак и предлог**

Кандидат Видор Генцел је у свом мастер раду успешно представио софтверски систем за реализацију криптовалуте употребом блокчејн технологије. Током развоја је вођено рачуна о постојећим техничким решењима и блокчејн архитектурама, како би се реализовао оригинални хибридни систем који обједињује најбоље особине постојећих система. Тежило се ка томе да сваки део буде модуларан, лак за одржавање, изучавање и даље проширење. Рад и имплементација представљају добру полазну тачку за даље истраживање области дистрибуираних система и практичне примене блокчејн технологије.

На основу горе наведеног Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да прихвати рад „Софтверски систем за реализацију криптовалуте употребом блокчејн технологије“ дипл. инж. Видора Генцела као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 14. 09. 2018. године

Чланови комисије:

  
Др Павле Вулетић, доцент

  
Др Јарко Станисављевић, доцент