Катедри за рачунарство и информатику
Предмет: Сагласност за одбрану мастер рада.-

Одлуком Катедре и ННВ од 29.5.2020. именовани смо у комисију за одбрану мастер рада под насловом "Криптографски алгоритми у систему Биткоин" кандидата **Давида Ивића,** студијски програм Информатика.
Кандидат је 9.9.2020. доставио текст свог рада. Тема рада је биткоин, децентрализовани дигитални новац. Настао је 2008. године као пројекат отвореног кода, чији је аутор има псеудонимом Сатоши Накамото. Подржан је мрежом рачунара, која омогућује новчане трансакције без посредника. Основни проблем, спречавање двоструког трошења, решава се тако што се трансакције пакују у ланац блокова (blockchain), који се чува у свим чворовима мреже. Блокови се означавају временом креирања, потврђују хешираним доказом о извршеном обимном израчунавању и криптографски потписују.
Рад је подељен на осам поглавља. Прво поглавље је уводно. У другом поглављу излажу се криптографски елементи система, што омогућује да се прецизира шта је јавни кључ, односно адреса у овом систему. Трансакције су описане у трећем поглављу. Ланац блокова и могући напади на мрежу описани су у четвртом поглављу. Разне конструкције новчаника описане су у петом поглављу. Поступак формирања блока (рударење, mining) описан је у шестом поглављу. Основна реализација система, Bitcoin Core, описана је у поглављу седам; описани су експерименти са модификацијом овог програма. Осмо поглавље је закључак.

Мишљење.

Увидом у текст **Давида Ивића** "Криптографски алгоритми у систему Биткоин" дошли смо до закључка да приложени рад задовољава у потпуности захтеве који се постављају при изради мастер рада и предлажемо Катедри да одобри јавну одбрану рада.

У Београду, 23.9.2020.

Др Миодраг Живковић, ред. проф., ментор

Др Саша Малков, ванр. проф.

Др Филип Марић, ванр. проф.