Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:
P2P протокол за праћење јединствених криптографски потписаних ентитета

Значај теме и области:
Уз огроман степен цензуре, плагијата и фалсификата, аутентичност и следљивост постају примарни захтеви у најразличитијим сферама друштва (новинарство, уметност, модна индустрија, итд.). Идеја је да се свим корисницима мреже омогући да поуздано, брзо и економично провере аутентичност и власништво било ког криптографски потписаног ентитета који се налази у мрежи. Ентитет може бити у дигиталном формату (документ, видео, аудио, уговор), као и у физичком формату уз јединствени идентификатор (*QR, NFC*) који га одређује.
Како се за решавање оваквог типа проблема природно намеће коришћење ланца блокова, у овом случају Етеријум, протокол ипак настоји да минимизује или комплетно избаци његову употребу. Сваки чвор мора да садржи цео ланац свих трансакција, док протокол корисницима нуди опцију да чувају и прате информације само о оним ентитетима који су за њих значајни. Такође, како је могуће да неки ентитет има учестале и многобројне промене стања коришћење Етеријум мреже би се могло испоставити као прескупо, а сама цена чувања информације би била јако непредвидива што је још једна велика мана у оваквим системима.

Специфични циљ рада:
Циљ рада је дефинисање и реализација новог протокола који елиминише потребу за управљање комплексном инфраструктуром и омогући једноставан интерфејс за повезивање различитих типова апликација на хоризонтално скалабилну децентрализовану P2P мрежу. Целокупна архитектура је подељена у три независна слоја: снабдевач, апликативни и клијентски слој. Снабдевач, најнижи слој протокола, чине чворови у *Kademlia* мрежи који служе за обрађивање, верификацију и снабдевање виших слојева. У апликативни слој спадају све апликације које желе да користе протокол са својом специфично дефинисаном логиком док у клијентски слој спадају сви крајњи корисници апликација из апликативног слоја, нпр. корисници *iOS* или *Android* уређаја. За потребе складиштења ентитета, биће коришћена нека од децентрализовано дистрибуираних база података попут *IPFS*, *OrbitDB*.

Литература:

1. *Schollmeier, R. (2001, August). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications.*
2. *Jakobsson, M., & Juels, A. (1999). Proofs of work and bread pudding protocols.*
3. *Maymounkov, P., & Mazieres, D. (2002, March). Kademlia: A peer-to-peer information system based on the xor metric.*

Андрија Новаковић 1016/2021, Информатика

(својеручни потпис студента)

(датум подношења молбе)

Сагласан ментор доц. др Александар Картељ

(својеручни потпис ментора)

Чланови комисије

1. проф. др Миодраг Живковић
2. проф. др Саша Малков

Катедра за рачунарство и информатику је сагласна са предложеном темом.

(*шеф катедре*)

(*датум одобравања молбе*)