Зборник радова Факултета техничких наука, Нови Сад

**УДК: 4.9**
**ДОИ: https://doi.org/10.24867/35BE24Djordjevic**

# Децентрализовани приступ развоју друштвених мрежа коришћењем Урбит оперативног система

# *Decentralized development approach of social networks using Urbit operating system*

Михајло Ђорђевић, *Факултет техничких наука, Нови Сад*

**Студијски програм – СОФТВЕРСКО РЕИНЖЕЊЕРСТВО И ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ**

**Кратак садржај –** *Ovaj rad razmatra primenu decentralizacije u razvoju društvenih mreža, sa posebnim fokusom na Urbit tehnološki stek. Opisani su osnovni principi kriptografije i decentralizovanog identiteta, kao i uloga UrbitOS-a i UrbitID sistema u obezbeđivanju sigurne komunikacije. Rad takođe prikazuje pojednostavljenu arhitekturu decentralizovane društvene mreže zasnovane na Urbit platformi i razmatra prednosti i ograničenja ovog pristupa u odnosu na tradicionalne centralizovane modele.*
**Кључне речи:** *decentralizacija, društvene mreže, komunikacija, Urbit, kriptografija*

**Abstract** – *This paper explores the application of decentralization in social network development, with a particular focus on the Urbit technology stack. The core principles of cryptography and decentralized identity are outlined, along with the roles of UrbitOS and the UrbitID system in enabling secure communication. Additionally, the paper presents a simplified architecture of a decentralized social network built on the Urbit platform and discusses the advantages and limitations of this approach compared to traditional centralized models.*

**Keywords:** *decentralization, social networks, communication, Urbit, cryptography*

---

**НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Горан Савић, ред. проф.**

## 1. УВОД

Друштвене мреже су први пут популаризоване раних 2000-их, када је *MySpace* први пут постао познат. Он је омогућавао корисницима директну међусобну комуникацију преко интернет мреже као и способност сваког корисника да опишу себе путем свог профила. Из ових основних принципа настале су касније, популарније социјалне мреже као *Facebook* и *Twitter* које са својим функционалностима и лакоћом коришћења постала део свакодневнице већине људи на интернету.

Међутим, све велике функционишу на истом принципу централизације - тј. да се подаци свих њихових корисника налазе у рукама компанија које руководе овим платформама. Овакав приступ подиже питања у вези дигиталне приватности. Компаније прикупљају велике количине података о својим корисницима (које често и продају без сагласности корисника), контролишу алгоритме који диктирају који се садржај приказује и диктирају услове коришћења.
Децентрализација софтвера нуди решење овим бројним проблемима. Она представља имплементацију софтвера која се не заснива на монолитном серверу који управља пословном логиком, већ се ослања на саме кориснике - тј. сваки корисник је и сервер другим корисницима. Сваки корисник држи само своје податке, што им даје независност и потпуну контролу над својим подацима.
Овај рад нуди кратак увид у предности и мане децентрализованог приступа као и опис једног решења.

## 2. ДЕЦЕНТРАЛИЗАЦИЈА

Традиционалне апликације које се свакодневно користе – друштвене мреже, платформе за размену порука, сервиси за електронску пошту – функционишу кроз централизовану инфраструктуру. То значи да се сви подаци и интеракције корисника обрађују и складиште на серверима у власништву компанија попут *Mete* (*Facebook*), *Google*-а или *Twitter*-а. Овај модел има више проблема: централизована контрола над садржајем, експлоатација корисничких података, рањивост на хакерске нападе, као и могућност цензуре.
Управо због ових слабости, последњих година добија на значају концепт децентрализованих апликација (*dApps*) – софтверских решења која функционишу без централне тачке контроле, често ослањајући се на блокчејн технологију и криптографију као основне стубове безбедности и поверења.
*Mastodon* и *Bluesky* су међу најпознатијим примерима децентрализованих друштвених мрежа. Код обе платформе, уместо једнг централног ауторитета који

управља свим корисницима и подацима, мрежу чини више независних сервера (често названих инстанце или подови) које могу водити појединци, групе појединаца или организације. Овакав модел смањује ризик од цензуре и монопола, јер ниједан појединачни ентитет нема потпуну контролу над подацима.

### 2.1. Предности и мане

Овакав приступ нуди корисницима бројне погодности. Пре свега, сваки корисник добија потпуну контролу над својим садржајем на интернету. Ова особина је кључна за дигиталну приватност. Тиме се може и заобићи цензура коју би иначе диктирале приватне компаније (или пак, диктаторска влада). Са таквом дигиталном слободом произилази и слобода изражавања која је иначе веома ретка у централизованим платформама.
Међутим, чак ни овај приступ није без својих мана. Пре свега, постаје теже гарантовати конзистентно корисничко искуство. Администрација корисникових података изискује техничко знање и искуство истог корисника. Поврх тога, постаје теже контролисати спам, и модерација садржаја се пребацује на локалне администраторе. Све ово има за последицу да постаје теже регулисати илегалан садржај.

## 3. КРИПТОГРАФИЈА

Пракса на којој се заснива сигурност свих дигиталних система, поготово децентрализованих, се зове криптографија. То је пракса развијања и коришћења алгоритама за заштиту и прикривање пренесених информација тако да их могу читати само они који имају дозволу (ауторизацију) и могућност да их дешифрују. Другим речима, криптографија прикрива комуникације тако да им неовлашћене стране не могу приступити [1]. Организације попут Националног института за стандарде и технологију (НИСТ) развијају криптографске стандарде за безбедност података.
Криптографија се заснива на четири главна принципа: поверљивост, интегритет, непорецивост и аутентичност.
Шифроване информације морају бити приступачне само особама којима су намењене и ником другом (поверљивост).
Шифроване информације не могу бити измењене током складиштења или преноса између пошиљаоца и примаоца без да било какве измене буду откривене (интегритет).
Пошиљалац шифрованих информација не може порицати своју намеру да пошаље информације (непорецивост).
Идентитети пошиљаоца и примаоца, као и порекло и одредиште информација су потврђени (аутентичност).

### 3.1. Криптографске методе

Једне од најзаступљенијих криптографских метода су методе базиране на асиметричној криптографији (парови јавних и приватних кључева) - које служе сигурној размени података - и хеш функције, тј. дигитални потписи, који служе обезвеђивању интегритета података.

### 3.2. Јавни и приватни кључеви

Асиметрична криптографија (која се такође назива криптографија јавног кључа) користи један приватни кључ и један јавни кључ. Подаци који су шифровани јавним и приватним кључем захтевају и јавни кључ и приватни кључ примаоца да би били дешифровани [1].
Криптографија јавног кључа омогућава безбедну размену кључева преко небезбедног медијума без потребе за дељењем тајног кључа за дешифровање јер се јавни кључ користи само у процесу шифровања, али не и дешифровања. На овај начин, асиметрично шифровање додаје додатни слој безбедности јер приватни кључ појединца никада није дељен.
Овакав приступ је безбедан и робустан (нуди поверљивост, непорецивост и аутентичност података) али је притом и скупа процесорска операција

### 3.3. Хеш функције

Дигитални потписи и хеш функције се користе за аутентификацију и обезбеђивање интегритета података. Дигитални потпис креиран помоћу криптографије обезбеђује непорецивост, гарантује да пошиљалац поруке не може порицати аутентичност свог потписа над подацима [2].
Хеш функције, попут Сигурног хеш алгоритма 1 (SHA-1), могу трансформисати улазне податке у низ знакова фиксне дужине, који је јединствен за оригиналне податке. Ова хеш вредност помаже у провери интегритета података чинећи рачунарски немогуће да два различита уноса произведу исту хеш вредност.

## 4. *URBITOS* И *URBITID*

*Urbit* представља један технолошки стек на којем се могу имплементирати децентрализовани системи (па и друштвене мреже), и главни је фокус овог рада. Два главна ентитета овог стека су *UrbitOS* и *UrbitID*. *UrbitOS* имплементира приступ заснован на идентиету (*UrbitID*), где сваки корисник има идентитет заснован на јавном и приватном кључу. Овај идентитет омогућава корисницима да комуницирају и извршавају трансакције са потпуним поверењем. Кроз криптографске технике, *UrbitOS* елиминише потребу за традиционалним аутентификацијама, као што су лозинке или биометријски подаци, који су склони нападима и злоупотребама [3].
Мрежа *UrbitOS*-а, као децентрализована платформа, користи ове сигурносне технологије за изградњу отпорности на нападе и за очување приватности. Са сваким корисником који има контролу над својим подацима и комуникацијама, систем омогућава високи ниво сигурности, док истовремено омогућава корисницима да задрже потпуну контролу над својим информацијама.
*UrbitOS* је софтверски стек који чине виртуелна машина, програмски језик (*hoon*) дизајниран да подржи развој апликација на *UrbitOS* и кернел дизајниран да покреће ове апликације. Сваки уређај са

оперативним системом налик *UNIX*-у може користити *UrbitOS* [3].

*UrbitOS* кернел, звани Арво, само је један од модула који служе да олакшају развој апликација. Остали модули имају различите функционалности који све заједно омогућавају сигурну и ефикасну комуникацију између корисника било којих *Urbit* апликација. Они такође чине посао програмера, који развија те апликације, лакшим - јер имплицитно рукују складиштењем података, сигурном комуникацијом, подизањем локалног сервера, итд.

*UrbitID* је инфраструктура јавног кључа опште намене заснована на *Ethereum* блокчејну (дистрибуирана база података, тј. књига дигиталних идентитета), и користи се за *Urbit* идентитете [4]. Пружа систем оскудних и непромењљивих идентитета који су криптографски безбедни.

Постоје три важне ствари које треба разумети о целокупном дизајну *UrbitID* система: оскудност, децентрализација и контрола.

Оскудност се постиже тиме што је број могућих *UrbitID* ограничен на $2^{32}$ (тј. на око 4 милијарде) идентитета. Поврх тога, пошто је заснован на *Ethereum*-у, идентитет такође кошта материјално, што значи да га људи мање користе за спам или зарад злоупотребе. Када се два корисника сретну са *UrbitID*, обе стране знају да друга има неки удео у игри (чак и без откривања личних података у било ком смеру).

Децентрализација се постиже тако што се *UrbitID* се дистрибуирају преко стабла спонзорства. Сваки спонзор издаје фиксиран број адреса. Пошто постоји много спонзора, постоји много начина да се добије *UrbitID* - не само један централни ауторитет. Када се једном добије ИД, постаје трајно власништво корисника.

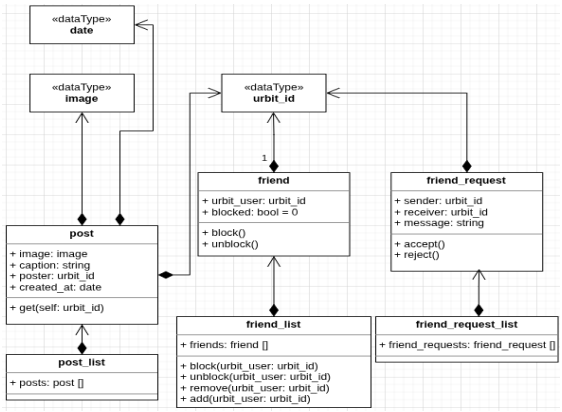
Под контролом се мисли на то да галаксије (тј. врх стабла спонзорства) формирају сенат који може да надгради логику *UrbitID* система већинским гласом.

Стабло спонзорства *UrbitID* није намењено да буде друштвени систем ни на који начин. Интеракције између људи и заједница на *Urbit* мрежи су директне (*peer-to-peer*), потпуно органске и потпуно неконтролисане од стране хијерархије адреса. *UrbitID* је једноставно аутентификациони субстрат на коме се могу градити системи за репутацију и комуникацију [4]. Због овога су се разматрали преименовања звезда и галаксија у "инфраструктурне" и "управљачке" чворове.

### 4.1. Развој друштвене мреже на *UrbitOS* платформи

*UrbitOS* је децентрализова платформа, тако да не није могуће развити социјалну мрежу, или било коју другу апликацију на традиционалан начин (нпр. *Facebook*, *Instagram*, итд). Прво, да би се уопште користио *Urbit*, потребан је криптографски индентитет, што у принципу значи да је сваки корисник већ аутентификован као посебна јединка. Самим тим, имплементација аутентификације у социјалној мрежи је изостављива. Друго, пошто сваки корисник има потпуну контролу над својим подацима, имплементација ауторизације је такође већински изостављива. И треће, пошто сваки корисник чува искључиво само своје податке, не постоји потреба за (централизованом) базом података. Ове три олакшице чине развој друштвене мреже веома директним и поједностављеним подухватом.

Имајући ово у виду тај ограниченији скуп функционалности као и непостојање потребе за ауторизацијом, аутентификацијом и базом података, читав систем се може представити веома једноставним класним диаграмом:




Слика 1. Класни диаграм свих неопходних компоненти у једној децентрализованој друштвеној мрежи

Слика 1 показује идеју најједноставнијег облика друштвене мреже, заснован на *Urbit* технолошком стеку. Корисник има своју листу пријатеља, своју листу објава и захтеве за пријатељство. Објаве других корисника (пријатеља) се добављају помоћу њихових *UrbitID*. Захтеви за пријатељство се шаљу директном претрагом *UrbitID*. Корисник у сваком тренутку мозе да приступи захтевима који су му пристигли. "Пријатељство" се успоставља када се захтев прихвати, и тада се пријатељ додаје у листу пријатеља. Из листе се пријатељ мозе избацити и/или блокирати.

И коначно, пошто се сва стања се чувају локално на машини корисника, прјатељи им могу приступити само кад их затраже. Овакав принцип рада се пропагира и на компликованије и модерније функционалности садашњих друштвених мрежа (чет, слике, видеи, сторији, итд).

Дакле, децентрализоване апликације се суштински другачије развијају од монолитних, и *Urbit* постоји као једно од могућих решења над којим се могу имплементирати.

## 5. ЗАКЉУЧАК

Способности *UrbitOS*-а (његових модула и *hoon* програмског језика), чине развој децентрализованих апликација (као и друштвених мрежа) брзим и једноставним. Захваљујући модулима *UrbitOS*-а, програмер не мора да брине о размени кључева између корисника, нити о сигурности комуникације.

Међутим, ни овај приступ није без својих мана. Пре свега, *hoon* програмски језик за развој апликација је компликован, тешко се савладава и нечитак је. Чак би и искусан програмер морао провести пар недеља учећи га, што га чини неприступачним. Дебагер је такође нечитак и тешко се користи што успорава развој апликација. И поврх свега, терминологија коју

*Urbit* користи за своје модуле и програмерске појмове је неконвенционалан што додатно отежава учење технолошког стека и самим тим развој апликација. Све заједно, *urbit* оперативни систем чини нову примитиву развоја децентрализованих апликација.

## 6. ЛИТЕРАТУРА


[1] Johannes A. Buchmann, *Introduction to Cryptography*, vol. 335. New York: Springer, 2004.

[2] R. L. Rivest, "Cryptography," in Algorithms and Complexity, Elsevier, 1990, pp. 717-755.

[3] ‘Urbit — Leave the internet behind’. Приступљено: Окт. 09, 2025. [Online]. Доступно: https://urbit.org/overview/urbit-os

[4] ‘Urbit — Leave the internet behind’. Приступљено: Окт. 09, 2025. [Online]. Доступно: https://urbit.org/overview/urbit-id


**Кратка биографија:**


**Михајло Ђорђевић** рођен је у Београду, општини Савски Венац,, 2000. год. Мастер рад на Факултету техничких наука из области Софтверског инжењерства и информационих технологија машине одбранио је 2025.год.

**Контакт**:
mihajlodj@protonmail.com