



УНИВЕРЗИТЕТ У НОВОМ САДУ  
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА У  
НОВОМ САДУ



Мијановић Бојан

# Дизајн и имплементација *Blockchain* механизма са криптовалutom

ДИПЛОМСКИ РАД  
- Основне академске студије -

Нови Сад, 2024

# Садржај

<b>1</b>	<b>Увод</b>	<b>3</b>
<b>2</b>	<b>Основе <i>Rust</i> програмског језика</b>	<b>4</b>
2.1	Увод у <i>Rust</i> програмски језик . . . . .	4
2.2	Зашто <i>Rust</i> за <i>blockchain</i> ? . . . . .	4
<b>3</b>	<b>Увод у <i>blockchain</i> технологију</b>	<b>6</b>
3.1	Основни принципи и концепти . . . . .	6
3.2	Поређење са традиционалним базама података . . . . .	6
<b>4</b>	<b>Литература</b>	<b>8</b>

# 1 Увод

*Blockchain* технологија представља дистрибутивну, децентрализовану и јавну базу свих трансакција [1].

Први концепт *blockchain* технологије помиње се у 1982. години, када је Давид Чаум у својој дисертацији описао дистрибуирану базу података која користи криптографију [2]. Овај рани рад није био директно повезан са дигиталним валутама, али је поставио темеље за будући развој *blockchain* - а.

Права револуција долази 2008. године када Сатоши Накамото објављује рад "*Bitcoin: Peer-to-peer* електронски готовински систем", уводећи први модерни *blockchain* и криптовалуту *Bitcoin*. Генесис блок, први блок *Bitcoin blockchain* - а, ископан је 3. јануара 2009. године, означавајући почетак *blockchain* технологије какву данас познајемо [3].

*Ethereum*, лансиран 2015. године од стране Виталика Бутерина, увео је паметне уговоре који омогућавају сложеније трансакције и аутоматизацију различитих процеса. Овај развој проширио је примену *blockchain* технологије далеко изван дигиталних валута, омогућавајући креирање децентрализованих апликација.

*Blockchain* технологије су се од свог настанка имплементирале у различитим програмским језицима и окружењима. У својим раним фазама, *blockchain* технологије су се углавном развијале користећи језике као што су *C++* и *Java*, захваљујући њиховој ефикасности и широкој употреби у индустрији. Касније, с појавом паметних уговора, *Solidity* је постао стандард за развој на *Ethereum* платформи.

Овај рад се фокусира на имплементацију основних концепата *blockchain* технологије у програмском језику *Rust*, који је познат по својој сигурности, перформансама и могућности превенције грешака при руковању меморијом.

Рад је структуриран X целина

## 2 Основе *Rust* програмског језика

*Rust* је савремени програмски језик који је развијен да буде безбедан и брз. Развијен од стране *Mozilla Research*-а, *Rust* је од свог настанка привукао велику пажњу због својих изузетних безбедносних карактеристика и перформанси.

### 2.1 Увод у *Rust* програмски језик

*Rust* је системски програмски језик који наглашава безбедност и брзину. За разлику од неких других језика, *Rust* осигурава безбедност у раду са меморијом кроз свој јединствени систем власништва над подацима. То значи да *Rust* омогућава програмерима да пишу брз и ефикасан код без страха од уобичајених грешака као што су сегментација или тзв. „*dangling pointers*“. Поред тога, *Rust* нуди снажне алате за паралелно програмирање, што га чини идеалним за развој сложених и ресурсоинтензивних апликација.

Због своје компајлиране природе и минималног *runtime*-а, *Rust* програми се извршавају ближе нивоу машинског језика, што резултује високим перформансама. Ово је кључно за *blockchain* апликације где брзина обраде трансакција директно утиче на корисничко искуство и сигурност мреже.

### 2.2 Зашто *Rust* за *blockchain*?

Када је у питању развој *blockchain* апликација, *Rust* се истиче као одличан избор из неколико разлога:

1. **Безбедност меморије:** *Rust*-ов систем власништва и провера за време компилације осигуравају да програмери избегну уобичајене грешке у раду са меморијом, што је критично за сигурност *blockchain* система.
2. **Перформансе:** *Rust* је дизајниран да буде брз и ефикасан. Његов минималан *overhead* и високо оптимизован компајлер резултирају брзим извршавањем кода, што је важно за обраду великог броја трансакција у реалном времену.
3. **Паралелизам и конкурентност:** *Rust* нуди снажну подршку за паралелно и конкурентно програмирање, омогућавајући оптимално коришћење мулти-језгарних процесора.

*Rust* нуди низ алата и библиотека које олакшавају развој сложених апликација. Две од најзначајнијих библиотека за развој *blockchain* апликација су *Tokio* и *libp2p*. Ове библиотеке пружају подршку за асинхроне позиве и *peer-to-peer* комуникацију, што је кључно за функционалност и ефикасност *blockchain* система.

***Tokio*** је моћна асинхрона *runtime* библиотека за *Rust* која омогућава развој високоперформансних и високо доступних апликација. Кроз *Tokio*, програмери могу да имплементирају асинхроне позиве и да развију веб сервере који могу да обрађују велики број истовремених веза.

***libp2p*** је модуларни мрежни стек који омогућава *peer-to-peer* комуникацију. У контексту *blockchain*-а, *libp2p* се користи за омогућавање комуникације између различитих чворова у мрежи. Ова библиотека је флексибилна и подржава различите протоколе за пренос података, што је чини идеалном за развој децентрализованих апликација.

### 3 Увод у *blockchain* технологију

*Blockchain* технологија представља савремен приступ складиштењу и дистрибуцији података. Основни принципи и концепти *blockchain* технологије нуде дубоку промену у начину на који се информације похрањују, проверавају и дистрибуирају путем децентрализоване мреже рачунара.

#### 3.1 Основни принципи и концепти

*Blockchain* се може дефинисати као дистрибуисана дигитална књига трансакција. Основна идеја је стварање низа блокова који садрже податке. Блокови су криптографски повезани тако да је немогуће мењати податке у претходним блоковима без мењања свих следећих блокова.

Кључни елементи блокчејна укључују:

1. **Децентрализација:** Подаци се похрањују и управљају путем мреже чворова уместо централизованог ауторитета, што осигурава транспарентност и отпорност на цензуру.
2. **Дистрибуираност:** Сваки чвор у мрежи садржи комплетан или део *blockchain*-а, омогућавајући свима у мрежи да виде исте податке. Ово спречава појединачне тачке кvara и повећава отпорност на нападе.
3. **Сигурност:** Криптографски алгоритми осигуравају да је свака промена у *blockchain*-у лако проверљива, а трансакције се потврђују кроз консензус мреже.
4. **Неповратност:** Након што је трансакција забележена у *blockchain*-у, тешко ју је променити или обрисати без сагласности већине чворова у мрежи, чиме се осигурава поверење и интегритет података.

#### 3.2 Поређење са традиционалним базама података

Насупрот традиционалним базама података које су често централизоване и ослањају се на поверење у једну јединицу, *blockchain* нуди неколико кључних разлика:

1. **Централизација у односу на децентрализацију:** Традиционалне базе података често су централизоване под контролом једне организације. *Blockchain* дистрибуише податке широм мреже, елиминишући потребу за централним ауторитетом.
2. **Транспарентност и проверљивост:** *Blockchain* омогућава свим корисницима увид у све трансакције које су се догодиле, што повећава транспарентност и смањује могућност манипулације.

3. **Сигурност и отпорност:** Због своје дистрибуиране природе, *blockchain* је отпорнији на нападе и кварове у поређењу са традиционалним базама података које су осетљиве на појединачне тачке квара.
4. **Ефикасност и трошкови:** Иако *blockchain* може бити спорији у обради података у поређењу са централизованим базама података, његова сигурност и транспарентност могу надмашити трошкове и ризике традиционалних система.

## 4 Литература

- [1] Zheng, Zibin, Shaoan Xie, Hong Ning Dai, Xiangping Chen, i Huaimin Wang: *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. strana 1, Jun 2017.
- [2] Sherman, Alan, Farid Javani, Habin Zhang, i Enis Golaszewski: *On the Origins and Variations of Blockchain Technologies*. University of Maryland, Baltimore County (UMBC) Baltimore, Maryland 21250, Octobar 2018.
- [3] Nakamoto, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Cryptography Mailing list at <https://metzdowd.com>, Mart 2009.