Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.9
DOI: https://doi.org/10.24867/34BE06Ciric

RAZVOJ VIŠEPOTPISNOG DIGITALNOG NOVČANIKA NAD BLOKČEJN MREŽOM SOLANA
DEVELOPMENT OF A MULTI-SIGNATURE WALLET ON THE SOLANA BLOCKCHAIN NETWORK

Luka Ćirić, *Fakultet tehničkih nauka, Novi Sad*

OBLAST – PRIMENJENE RAČUNARSKE NAUKE I INFORMATIKA

Kratak sadržaj – *Ovaj rad predstavlja razvoj višepotpisnog digitalnog novčanika na Solana blokčejn mreži, sa fokusom na bezbednost, efikasnost i decentralizaciju. Kroz analizu arhitekture Solana mreže i implementaciju pametnih ugovora, demonstrira se kako se višepotpisni sistem može koristiti za zaštitu digitalne imovine u Web3 okruženju.*

Ključne reči: *Blokčejn, Solana, višepotpisni novčanik, decentralizacija, Web3*

Abstract – *This paper presents the development of a multi-signature digital wallet on the Solana blockchain network, focusing on security, efficiency, and decentralization. Through analysis of Solana's architecture and smart contract implementation, the paper demonstrates how multi-signature systems can be used to protect digital assets in a Web3 environment.*

Keywords: *Blockchain, Solana, multi-signature wallet, decentralization, Web3*

1. UVOD

U poslednjih nekoliko godina svedoci smo ogromnog napretka u svetu digitalnih tehnologija. Sve veći deo naših života, poslovanja i finansijskih aktivnosti preselio se na digitalni prostor. Sa tim razvojem pojavila se i potreba za novim načinima čuvanja i prenosa vrednosti na internetu bez posrednika i uz veću sigurnost. Upravo iz te potrebe nastala je blokčejn tehnologija, koja je promenila način na koji razmišljamo o poverenju, vlasništvu i decentralizaciji. Blokčejn (engl. blockchain) se najjednostavnije može opisati kao lanac blokova koji sadrže zapise o transakcijama, a koji su međusobno povezani i kriptografski zaštićeni. Za razliku od klasičnih baza podataka koje imaju centralni autoritet, blokčejn funkcioniše kao distribuirana mreža u kojoj svi učesnici imaju jednak uvid u informacije [1]. Na taj način, mogućnost zloupotrebe podataka je znatno manja, a poverenje između učesnika u sistemu ostvaruje se kroz transparentnost i verifikaciju transakcija od strane same mreže. Jedna od najpoznatijih i najrašireniji primena blokčejn tehnologije su digitalni novčanici, koji korisnicima omogućavaju da bezbedno čuvaju i koriste kriptovalute, tokene i druge digitalne vrednosti.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Dušan Gajić, red. prof.

Ipak, većina postojećih novčanika zasniva se na konceptu jednog privatnog ključa što znači da, ako se taj ključ izgubi ili kompromituje, korisnik gubi pristup svim svojim sredstvima. Da bi se ovakav rizik smanjio, razvijen je model višepotpisnih (engl. multisignature) novčanika, koji zahteva da više različitih korisnika (ili uređaja) potpiše transakciju pre nego što ona bude izvršena [2]. Na taj način postiže se dodatni nivo bezbednosti i poverenja, posebno u situacijama kada novčanik koristi više osoba ili organizacija. Tema ovog rada izabrana je upravo zbog aktuelnosti ove problematike i sve veće potrebe za bezbednim i efikasnim rešenjima u oblasti upravljanja digitalnom imovinom. Među brojnim blokčejn mrežama, Solana se istakla kao jedno od najbržih i najskalabilnijih rešenja. Zahvaljujući svom jedinstvenom mehanizmu konsenzusa nazvanom Dokaz istorije (engl. Proof of History – PoH), Solana je u stanju da obradi hiljade transakcija u sekundi, uz minimalne troškove [3][4]. Ove performanse čine je idealnom platformom za razvoj aplikacija koje zahtevaju brzinu, sigurnost i pouzdanost, upravo ono što je neophodno kod višepotpisnih novčanika. Cilj ovog rada je da istraži i prikaže proces projektovanja i razvoja višepotpisnog digitalnog novčanika na Solana mreži, uz poseban osvrt na način na koji se postiže bezbednost, efikasnost i jednostavnost korišćenja. Pored tehničkog aspekta, rad ima za cilj da doprinese boljem razumevanju mogućnosti koje Solana nudi za razvoj naprednih Web3 rešenja, kao i da ukaže na prednosti višepotpisnih sistema u zaštiti korisničke imovine.

2. POJAM BLOKČEJNA

Ideja o blokčejnu pojavila se kao odgovor na potrebu da se poverenje u digitalnom svetu zasnuje na tehnologiji, a ne na ljudskim ili institucionalnim autoritetima. Do pojave blokčejna, gotovo svi digitalni sistemi počivali su na nekoj vrsti centralizacije. Postojala je institucija, kompanija ili entitet koji je imao kontrolu nad bazom podataka i potvrdama transakcija. Takav model funkcioniše, ali ima očigledne nedostatke: mogućnost zloupotrebe podataka i potreba za poverenjem u centralni autoritet. Blokčejn je upravo odgovor na te probleme.

U najjednostavnijem smislu, blokčejn je distribuirana i decentralizovana baza podataka koja čuva zapise o transakcijama u nizu blokova koji su međusobno povezani. Svaki blok sadrži određeni broj transakcija i referencu na prethodni blok u lancu, što formira neprekidnu, hronološki uređenu strukturu podataka [1].

Kada se jednom doda u lanac, blok se više ne može menjati bez promene svih narednih blokova, što obezbeđuje visok nivo integriteta i otpornosti na manipulacije.

Ključni element koji omogućava ovaj sistem je kriptografija. Svaki blok u lancu ima svoj kriptografski potpis (heš), koji zavisi od sadržaja samog bloka i potpisa prethodnog bloka. Na taj način se stvara lanac poverenja u kojem svaka izmena podataka u bilo kom delu lanca automatski narušava sve naredne blokove.

2.1. Način funkcionisanja blokčejna

Svaka blokčejn mreža zasniva se na distribuiranoj glavnoj knjizi (engl. Distributed Ledger Technology - DLT) koju održavaju učesnici u mreži, poznati kao čvorovi (engl. nodes).

Proces potvrde transakcija obično se sprovodi kroz mehanizam konsenzusa – to je algoritam koji omogućava da se svi učesnici mreže usaglase oko trenutnog stanja baze podataka. Najpoznatiji mehanizmi konsenzusa su Dokaz posla (engl. Proof of Work - PoH), koji koristi Bitcoin mreža i Dokaz uloga (engl. Proof of Stake - PoS) koji koriste mnoge novije platforme, uključujući i Solanu [2]. Ovakvi mehanizmi omogućavaju mreži da funkcioniše bez centralnog autoriteta, jer se poverenje postiže matematičkim i kriptografskim pravilima.

2.2. Prednosti blokčejn tehnologije

Blokčejn je revolucionaran jer rešava jedan od najvažnijih problema u digitalnom svetu – problem poverenja bez posrednika. Zahvaljujući svojoj decentralizovanoj prirodi i kriptografskoj sigurnosti, blokčejn donosi niz ključnih prednosti:

Transparentnost i verifikacija – Sve transakcije na javnom blokčejnu su dostupne svima i mogu se proveriti u svakom trenutku. To omogućava visok nivo poverenja među učesnicima, jer niko ne može jednostrano menjati ili skrivati podatke.

Otpornost na manipulacije – Jednom kada se blok doda u lanac, njegovi podaci se ne mogu menjati bez saglasnosti većine učesnika u mreži. Time se postiže integritet sistema koji je gotovo nemoguće kompromitovati.

Decentralizacija – Ne postoji centralna tačka upravljanja ili kontrole. To znači da ne postoji entitet koji može jednostrano da utiče na sistem, što blokčejn čini otpornim na cenzuru i kvarove.

Sigurnost – Kriptografski algoritmi obezbeđuju da samo vlasnici odgovarajućih privatnih ključeva mogu izvršavati transakcije. Na taj način korisnici imaju potpunu kontrolu nad svojom digitalnom imovinom.

Efikasnost i automatizacija – Uvođenjem pametnih ugovora (engl. smart contracts) ili kako se drugačije zovu na Solana mreži programi (engl. programs), blokčejn omogućava da se procesi automatizuju i izvršavaju bez ljudske intervencije, čime se smanjuju troškovi i mogućnost greške.

2.3. Implementacije i primene blokčejna

Iako se blokčejn najčešće povezuje sa kriptovalutama poput Bitcoin i Ethereum, njegova primena je mnogo šira i raznovrsnija. Danas se blokčejn koristi u brojnim oblastima koje zahtevaju poverenje, transparentnost i verifikaciju podataka.

Finansijski sektor – Najveći broj implementacija vezan je upravo za finansije. Pored kriptovaluta, blokčejn se koristi za decentralizovane finansije (DeFi), koje omogućavaju korisnicima da pozajmljuju, ulažu i trguju digitalnom imovinom bez banaka i posrednika [5].

Lanci snabdevanja – U oblasti logistike i trgovine, blokčejn omogućava praćenje porekla i kretanja proizvoda od proizvođača do krajnjeg kupca. Time se smanjuju prevare i povećava transparentnost u globalnim lancima snabdevanja.

Zdravstvo – Medicinski podaci pacijenata mogu se čuvati na blokčejnu na bezbedan i transparentan način, uz potpunu kontrolu korisnika nad pristupom tim podacima.

Digitalni identitet – Blokčejn omogućava razvoj sistema za decentralizovani identitet (DID), gde korisnici sami upravljaju svojim identitetima bez potrebe za centralizovanim bazama podataka.

Upravljanje i glasanje – Neke zemlje i organizacije eksperimentišu sa blokčejn sistemima za elektronsko glasanje, kako bi se osigurala verodostojnost rezultata i sprečile manipulacije.

Umetnost i vlasništvo – Sa pojavom NFT (engl. Non-Fungible Token), umetnici i kreatori sadržaja mogu dokazati vlasništvo nad digitalnim delima i ostvarivati prihode bez posrednika.

3. ARHITEKTURA ČVORA I IZVRŠAVANJE MREŽE

Solana blokčejn mreža predstavlja jedno od najnaprednijih rešenja u domenu decentralizovanih sistema, zahvaljujući svojoj visoko optimizovanoj arhitekturi čvorova i inovativnim mehanizmima konsenzusa. U kontekstu razvoja višepotpisnih digitalnih novčanika, razumevanje unutrašnje strukture mreže i načina obrade transakcija od suštinskog je značaja za postizanje sigurnosti, pouzdanosti i skalabilnosti.

3.1. Struktura čvorova i distribuirana verifikacija

U Solana mreži, čvorovi (nodes) funkcionišu kao temelj decentralizacije. Svaki čvor poseduje kopiju blokčejna i učestvuje u validaciji transakcija. Posebno važni su validator čvorovi, koji formiraju nove blokove i obezbeđuju integritet mreže. Arhitektura čvora u Solani je projektovana za horizontalno skaliranje, što omogućava obradu hiljada transakcija u sekundi bez kompromisa po pitanju sigurnosti.

Solana koristi kombinaciju konsenzus mehanizama: Proof of Stake (PoS) i Proof of History (PoH). PoH omogućava vremensko redosledno obeležavanje događaja bez potrebe za sinhronizacijom među čvorovima, čime se značajno ubrzava obrada transakcija. Ova kombinacija omogućava

mreži da postigne izuzetno nisku latenciju i visoku propusnost.

3.2. Ključne komponente arhitekture

Arhitektura Solana čvora obuhvata niz specijalizovanih modula:

Gulf Stream: mehanizam za prosleđivanje transakcija unapred, čime se rasterećuju čvorovi i ubrzava validacija.

Turbine: protokol za distribuciju podataka u mreži, zasnovan na strukturi stabla, koji omogućava efikasno širenje informacija.

TPU (Transaction Processing Unit): jedinica zadužena za obradu transakcija, optimizovana za paralelno izvršavanje.

TVU (Transaction Validation Unit): komponenta koja verifikuje transakcije pre nego što se dodaju u blok.

PoH lanac: vremenski niz koji obezbeđuje deterministički redosled događaja.

Ove komponente zajedno omogućavaju mreži da funkcioniše sa izuzetnom efikasnošću, što je ključno za aplikacije koje zahtevaju visoku dostupnost i brzinu, poput višepotpisnih novčanika.

3.3. Model naloga i sigurnosna infrastruktura

Solana koristi model naloga zasnovan na strukturi ključ-vrednost u okviru AccountDB baze. Postoje dve vrste naloga: korisnički (user accounts) i programski (program accounts). Programske adrese se generišu pomoću PDA (Program Derived Address), što omogućava determinističko kreiranje sigurnih adresa koje ne zahtevaju privatne ključeve.

4. REŠENJE

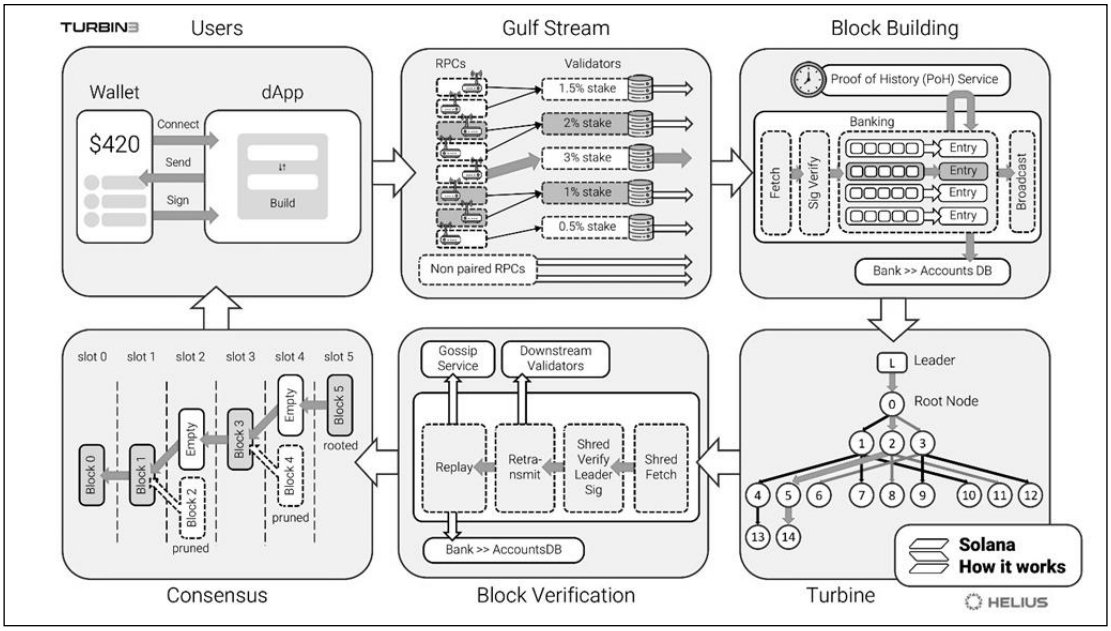
Implementacija višepotpisnog digitalnog novčanika na Solana mreži zasniva se na korišćenju Rust programskog jezika i Solana programskog okruženja. Rešenje je razvijeno kao programski modul koji omogućava kreiranje, upravljanje i izvršavanje transakcija koje zahtevaju više potpisa. Arhitektura sistema obuhvata jasno definisane funkcionalne komponente za inicijalizaciju novčanika, predlaganje transakcija i njihovo izvršavanje, uz podršku za konfiguraciju broja potpisnika i potrebnog praga.

Za razvoj su korišćeni standardni alati iz Solana ekosistema, uključujući *Anchor framework* za pojednostavljenu izradu pametnih ugovora, kao i *CLI* interfejs za testiranje i deployment. Projektna struktura organizovana je u više datoteka koje pokrivaju definiciju naloga, greške, konstante i funkcionalnosti za upravljanje novčanikom. Svaka funkcionalna jedinica je modularno implementirana i povezana kroz interni API programa.

Proces inicijalizacije novčanika podrazumeva kreiranje programskog naloga sa definisanim brojem potpisnika i pragom potrebnim za autorizaciju transakcija. Predlaganje transakcije uključuje evidentiranje predloga u okviru novčanika, dok se izvršenje vrši tek nakon što dovoljan broj potpisnika potvrdi predlog. Ova logika omogućava višeslojnu kontrolu pristupa i sprečava neautorizovano raspolaganje sredstvima.

Testiranje rešenja obavljeno je lokalno uz pomoć Solana testnet mreže, pri čemu su simulirane različite situacije — od inicijalizacije novčanika do izvršavanja transakcija sa nepotpunim brojem potpisa. Poseban fokus stavljen je na proveru sigurnosnih aspekata, kao što su validacija ulaznih podataka i zaštita od neovlašćenih poziva. Deployment je realizovan kroz *CLI* alatke, uz generisanje *IDL* fajla za dalju integraciju.

Rešenje je projektovano tako da bude proširivo i prilagodljivo za različite scenarije korišćenja, uključujući organizacione novčanike, DAO strukture i zajedničke fondove. Modularna arhitektura omogućava jednostavno dodavanje novih funkcionalnosti, dok korišćenje Solana mreže obezbeđuje visoku brzinu i niske troškove transakcija. Time se postiže balans između sigurnosti, efikasnosti i korisničke pristupačnosti u upravljanju digitalnom imovinom.



Slika 1. *Izvršavanje transakcije [6]*

5. ZAKLJUČAK

Razvoj višepotpisnog digitalnog novčanika na Solana mreži pokazao je kako se savremene blokčejn tehnologije mogu iskoristiti za unapređenje bezbednosti i pouzdanosti u upravljanju digitalnom imovinom. Kroz analizu arhitekture Solane, njenog jedinstvenog mehanizma konsenzusa i performansi, potvrđeno je da ova mreža predstavlja pogodno okruženje za implementaciju rešenja koja zahtevaju veliku brzinu obrade i niske troškove transakcija.

Implementacija višepotpisnog novčanika demonstrirala je praktične mogućnosti korišćenja programa u cilju postizanja višeg nivoa sigurnosti, jer se odluke o transakcijama ne oslanjaju na jednog korisnika, već na kolektivnu potvrdu više potpisnika. Time se značajno smanjuje rizik od kompromitovanja privatnih ključeva i gubitka sredstava, što je jedan od ključnih izazova u svetu digitalnih novčanika.

Pored tehničkog aspekta, ovaj rad ukazuje i na šire implikacije višepotpisnih sistema, od njihove primene u porodičnim i poslovnim finansijama, do uloge u decentralizovanim autonomnim organizacijama (DAO). Time se potvrđuje da višepotpisni modeli nisu samo tehničko rešenje, već i važan korak ka većem poverenju i decentralizaciji u digitalnoj ekonomiji.

Zaključno, rad potvrđuje da kombinacija Solanine arhitekture i višepotpisnog modela predstavlja snažan temelj za razvoj sigurnih i efikasnih Web3 aplikacija, čime se otvara prostor za dalji napredak u oblasti digitalnih finansija i decentralizovanih sistema.

LITERATURA

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. (Poslednji pristup: 19.10.2025) https://bitcoin.org/bitcoin.pdf

[2] A. M., & Wood, G. (2018). Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media.

[3] Yakovenko, A. (2020). Solana: A New Architecture for a High Performance Blockchain. [Online]. (Poslednji pristup: 19.10.2025) https://solana.com/solana-whitepaper.pdf

[4] Solana Foundation. (2023). Solana Documentation. [Online]. (Poslednji pristup: 19.10.2025) https://docs.solana.com

[5] Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review.

[6] Helius (2024). Solana Executive Overview. [Online]. (Poslednji pristup: 19.10.2025) https://www.helius.dev/blog/solana-executive-overview

Kratka biografija:



Luka Ćirić rođen je u Šapcu 2000. god. Diplomski rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Primenjeno softversko inženjerstvo odbranio je 2023.god. Nakon osnovnih strudija upisuje master studije na smeru Računarstvo i automatika, modul Računarstvo visokih performansi.
kontakt: ciric.e218.2023@uns.ac.rs