Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.9
DOI: https://doi.org/10.24867/30BE18Vukic

NAPADI VEZANI ZA REDOSLED I TEMPIRANJE NA L2 BLOCKCHAIN MREŽAMA

TIMING AND SEQUENCE ATTACKS ON L2 BLOCKCHAIN NETWORKS

Nikola Vukić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu će biti predstavljene L2 blockhcain mreže, napadi vezani za redosled transakcija, redosled instrukcija u transakciji, te napadi vezani za tempiranje na pomenutim mrežama. Rad uključuje i implementaciju jednostavnog pametnog ugovora za bolji prikaz efekata nekih od navedenih napada. Na kraju, dati su načini odbrambenih mehanizama za potpunu zaštitu, ili smanjivanje efektivnosti napada.*

Ključne reči: *blokčejn, problem skalabilnost, bezbednost*

Abstract – *This paper will present L2 blockchain networks, attacks based on transaction sequence, instruction sequence inside a transaction, and timing based attacks on said networks. The paper includes implementation of a simple smart contract to better show the effects of some of these attacks. Finally, the defense mechanisms, to completely mitigate the attacks, or reduce their effectiveness, are given.*

Keywords: *blockchain, scalability problem, security*

1. UVOD

Glavna primena blokčejna [1] (engl. *blockchain*) jeste u takozvanim decentralizovanim finansijama. Cilj osnivača jeste da se blokčejn koristi kao preferirani metod plaćanja opšte populacije u svakodnevnom životu.

Ova ideja ima dva problema, problem sigurnosti i problem skalabilnosti. Problem sigurnosti jeste taj što je logika na blokčejnu kontrolisana od strane pametnih ugovora, i ukoliko u njima postoji neka greška, sredstva mogu biti bespovratno ukradena. Problem skalabilnosti se ogleda u tome da je blokčejn mreža spora, te podržava svega oko 15 transakcija po sekundi. Ovo nije ni približno dovoljno da bi bila opšteprihvaćena, jer nije sposobna da podrži saobraćaj koji bi došao sa tolikim povećanjem broja korisnika mreže.

Još jedan dodatan problem jeste taj što skalabilnost na blokčjenu nije moguće povećavati u nedogled, jer se time smanjuje bezbednost sistema.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Veljko Petrović, docent.

[1]Postoji više vrsta i implementacija blokčejna, u daljem tekstu, termin *blokčejn* označavaće *Etirijum* (engl. *Ethereum) blokčejn mrežu*.

Zato što je blokčejn mrežu teško skalirati, odnosno povećati protok saobraćaja koji može da podrži, nastala su rešenja drugog sloja (engl. *Layer 2*, u daljem tekstu *L2*). Od svih vrste rešenja drugog sloja, najprimenjenija su rešenja zasnovana na namotavanjima (engl. *rollup*).

Osnovna ideja ovih rešenja jeste da bezbednost naslede od osnovne verzije blokčejna, takozvanog prvog sloja, a da povećaju skalabilnost tako što se transakcije vrše van samog prvog sloja, i s vremena na vreme, se više transakcija postavi na prvi sloj. Prvi sloj onda potvrdi njihovu ispravnost.

Kako uspešni napadi donose velike profite napadačima, veliki napori se ulažu da bi se ovi napadi analizirali, i da bi se stvorili odgovarajući bezbednosni mehanizmi. Neki od napada su omogućeni načinom funkcionisanja mreže, neki od njih su rezultat poslovne logike, a neki su jednostavno propusti pri programiranju pametnih ugovora. Napadi obrađeni u ovom radu pokrivaju sve tri od navedenih kategorija.

2. L2 BLOKCHAIN MREŽE

Kada se količina saobraćaja na mreži poveća, da bi se smanjilo zagušenje, transakcije postaju skuplje. Algoritam računanja cene transakcije je podešen da protok na mreži drži na oko pola njenog kapaciteta. Ako je mreža, zbog male skalabilnosti, zagušena, transakcije postaju izuzetno skupe, a samim time i nepristupačne za korisnike. Iz ovoga razloga bilo je neophodno da se napravi rešenje za problem manjka skalabilnosti. Iz ovoga su nastale L2 mreže [1].

Kako je već ranije pomenuto, najzastupljeniji tip L2 mreže jesu namotavanja. Postoje dve vrste namotavanja, optimistična namotavanja, i namotavanja nultog znanja. Obe vrste su zastupljene i imaju svoje prednosti i mane. Ono što im je zajedničko, da obe izvršavaju transakcije van prvog sloja, a na prvi sloj postavljaju rezultat tih transakcija. Transakcije su grupisane u pakete (engl. *batches*), i na ovaj način se na stotine i hiljade transakcija postavi kao jedna transakcija, čineći paketirane transakcije jeftinijim.

2.1. Optimistična namotavanja

Naziv optimistična namotavanja (engl. *optimistic rollups*) potiče iz činjenice da kada se paket transakcija sa drugog sloja pošalje na prvi sloj, podrazumeva se da su sve transakcije validne. Da bi se dokazalo suprotno, neophodno je priložiti dokaz nevalidnosti. Dokaz se prilaže u takozvanom periodu izazivanja (engl. *challenge period*), koji ima varijabilne dužine trajanja, ali obično traje oko 7 dana.

Prednost optimističnih namotavanja jeste taj što su zahtevi za računarskom moći manji nego u slučaju namotavanja nultog znanja, ali je mana to što se na prvi sloj moraju postavljati sve transakcije, da bi se mogla utvrditi njihova validnost. Još jedna mana jeste ta što da bi transakcije bile konačne mora se sačekati da prođe period izazivanja.

2.2. Namotavanja nultog znanja

Namotavanja nultog znanja (engl. *zero-knowledge rollups*) su dobila naziv zbog toga što sekvenceri koriste tehnike dokaza nultog znanja da bi dokazali ispravnost transakcija u pakteima koje postavljaju na prvi sloj. Dakle, ni za jedan paket se ne smatra da je validan, nego se validnost mora dokazati pri postavljanju svakog paketa.

Prednost optimističih namotavanja je ta što su transakcije brže, zbog nepostojanja perioda izazivanja. Mana im je to što dokazi nultog znanja zahtevaju više računarske moći, što može da umanji broj učesnika.

3. PREGLED LITERATURE

Kako je glavna primena blokčejna u decentralizovanim finansijama, bezbednosni propusti neretko dovode do trajnog gubitka sredstava. Iz ovog razloga, postoje radovi [3-5] koji skreću pažnju na česte tipove napada na blokčejnu. Uprkos tome, svake godine, velike količine digitalnog novca biva ukradeno.

Sa druge strane, problemom unapređenja L2 mreža se bavi čitava zajednica, svako može da priloži predlog za poboljšanje Etirijuma (engl. *Ethereum Improvement Proposal*, u daljem tekstu *EIP*), koji dobije jedinstveni identifikator u formi broja.

Iako postoji više EIP-a koji su se bavili problemom unapređenja mreže, dva najbitnija su EIP-1559 [6] i EIP-4844 [7].

EIP-1559 je uveo model plaćanja za transakcije kakav danas postoji na mreži, čime je stabilizovao cene transakcija, što značajno pomaže L2 mrežama kada treba da se sinhronizuju sa prvim slojem, odnosno postave pakete.

EIP-4844 je predlog koji je direktno vezan za poboljšanje skalabilnosti L2 mreža i čijim usvajanjem je zajednica prihvatila mreže bazirane na namotavanjima kao budućnost Etirijuma. Osnovna ideja jeste da se podaci koji su neophodni za dokazivanje validnosti čuvaju samo određeni vremenski period, koji je dovoljan da bi se dokazala validnost, a onda se brišu.

4. NAPADI VEZANI ZA REDOSLED I TEMPIRANJE

Napadi koji su obrađeni u ovom radu, posledica su redosleda transakcija u bloku, redosleda instrukcija u transakciji, ili su vezani za tempiranje, odnosno mogućnost manipulacije vremenskim otiscima i premalim intervalima proteklog vremena između zahteva.

4.1 Napadi zasnovani na MEV-u

Maksimalna ekstraktibilna vrednost, odnosno MEV, jeste sva vrednost koju validator može da dobije uvrštavanjem bloka u lanac, pored standardne nagrade koja mu sledi za ovaj čin.

Pre nego što budu uvršćene u blok, transakcije dospevaju u bazen transakcija (engl. *mempool*) u kome borave dok ih neko od validatora ne uvrsti u svoj blok. Za vreme boravka u bazenu, svi detalji transakcije su potpuno javni. Ovo stvara priliku za napadača da pronađe transakciju koju može da napadne.

Napadi zasnovani na MEV-u pripadaju tipu napada koji su vezani za redosled transakcija u bloku.

Tri osnovna tipa napada zasnovana na MEV-u jesu:

- **Prednjačenje** (engl. *frontrunning*) – napadač umeće svoju transakciju ispred one koju napada.
- **Zadnjačenje** (engl. *backrunning*) – napadač umeće svoju transakciju iza one koju napada.
- **Sendvič napad** (engl. *sandwich-attack*) – napadač umeće dve transakcije, jednu ispred, i jednu iza one koju napada. Predstavlja kombinaciju prednjačenja i zadnjačenja.

4.2. Napad na osnovu vremenske zavisnosti

Napadi na osnovu vremenske zavisnosti (engl. *timestamp dependence*) zasnivaju se na činjenici da sekvenceri mogu, u većoj ili manjoj meri, zavisno od konkretne L2 mreže, manipulisati vremenskim otiskom.

Iz ovog razloga ukoliko se vremenska zavisnost koristi kao izvor nasumičnih vrednosti, onda te vrednosti uopšte nisu nasumične nego su u potpunosti konotrlisane od strane sekvencera.

4.3. Napad ponovnim ulaskom

Napad ponovnim ulaskom (engl. *reentrancy attack*) je posledica neispravne sekvence instrukcija u transakciji. Ukoliko se eskterni poziv uputi ka određenoj adresi, pre nego što se ažurira stanje ugovora, onda, ukoliko je ova adresa pametni ugovor, može da iskoristi ovu činjenicu da izvrši napad ponovnim ulaskom.

Postoji više vrsta napada ponovnim ulaskom:

- **Ponovni ulazak u jednu funkciju** (engl. *single function reentrancy*) – najprostiji tip napada, napadaču se uputi poziv iz funkcije, on uputi poziv ka istoj funkciji.
- **Međufunkcijski ponovni ulazak** (engl. *cross-function reentrancy*) – napadaču se uputi poziv iz funkcije, on uputi poziv ka drugoj funkciji.
- **Međuugovorni ponovni ulazak** (engl. *cross-contract reentrancy*) – više ugovora deli stanje, ranjivi ugovor uputi poziv, pre nego što ažurira stanje, napadač pozove funkciju drugog ugovora. ugovora koji zahtevaju previše procesorkse moći, jer bi cena izvršavanja bila prevelika.
- **Međulančani ponovni ulazak** (engl. *cross-chain reentrancy*) – iako manje uobičajan, i dalje moguć. Slučaj u kome su ranjivi ugovori postavljeni na različite mreže.
- **Ponovni ulazak bez modifikacije stanja** (engl. *read-only reentrancy*) – poseban slučaj međuugovornog ulaska gde napadač uputi poziv

ugovoru, koji ne ažurira stanje pre upućivanja poziva napadaču, napadač napadne drugi ugovor, koji čita stanje iz prvog ugovora, koje nije ažurirano, i bude žrtva napada.

4.4 Napad onemogućavanja pružanja usluga

Efekat napada onemogućavanja pružanja usluga može biti privremen ili trajan. Trajan znači da ugovor više ne može da pruža neku uslugu, ili više njih, korisnicima. Privremen efekat onemogućavanja pružanja usluga nastaje kao rezultat premalo vremena između korisničkih zahteva.

Naime, ukoliko postoji uslov, nametnut stanjem ugovora, da bi se neka funkcionalnost započela, a ugovor još nije promenjen u to stanje, funkcionalnost se privremeno ne može izvršiti. Samim time se ne može pružiti usluga korisniku.

Nekada se ne može mnogo učiniti po pitanju privremenog onemogućavanja pružanja usluga, jer postoje situacije u kojima je spora promena stanja nametnuta logikom funkcionisanja ugovora.

5. PAMETNI UGOVOR

Napisan je pametni ugovor koji opisuje rad lutrije. Ugovor ima vlasnika, koji dobija 5% dobitka u svakom kolu, dok pobedniku ide ostatak. Svi učesnici uplaćuju jednaku cenu učešća. Sabiranjem svih cena učešća dobija se ukupni dobitak za kolo. Kolo traje minimalno sedam dana. Nakon sedam dana, pobednik se može izvući.

Dok ovaj period ne prođe, učesnik može da se povuče iz kola, čime dobija nazad uložena sredstva.

Pobednik se bira na osnovu rednog broja učesnika. Redni broj učesnika se bira kao ostatak pri deljenju vremenskog otiska bloka transakcije i broja učesnika u kolu. Nakon izvlačenja pobednika, pobednik se isplaćuje. Svi učesnici kola se brišu iz skupa učesnika, da bi se lutrija pripremila za naredno kolo. Onog momenta kada su svi dosadašnji učesnici obrisani, kreće se u novo kolo.

6. REZULTATI EKSPERIMENTA

Da bi se uporedile cene, radi pokazivanja prednosti cena na L2 mrežama, ugovor je bio postavljen na mrežu prvog, i drugog sloja.

Cena postavljanja na prvi sloj je bila, u protivvrednosti evra, 90 evra, dok je za drugi sloj bila 13 centi.

Pored ovoga, na ugovor su bili upućeni i napadi da bi se pokazali njihovi efekti. Na ugovor su bili upućeni:

- **Napad na osnovu vremenske zavisnosti** – simulira se da situacija u kojoj validator odabere vremenski otisak transakcije i bude pobednik.
- **Napad ponovnim ulaskom u jednu funkciju** – bilo koji učesnik povuče sredstva koja je dao kao cenu učešća i napadne ugovor.
- **Napad onemogućavanja pružanja usluga –** veliki broj učesnika onemogući njihovo čišćenje između dva kola.

TABELA 1: UPUĆENI NAPADI

Napad	Rezultat	Uzrok ranjivosti
Na osnovu vremenske zavisnosti	Deterministično izvlačenje pobednika, namešten ishod lutrije	Način funkcionisanja vremenskih otisaka na mrežnom nivou i način biranja nasumičnog broja
Ponovnim ulaskom	Ukraden sveukupan dobitak za kolo	Pogrešan raspored instrukcija u okviru transakcije
Onemogućavanja pružanja usluga	Onemogućavanje izvlačenja pobednika i nastavka funkcionanisanja ugovora	Način odbrane mreže od onemogučavanja pružanja usluga i logika sistema koji ugovor opisuje

7. ODBRANE

Prikazano je na koji način je neophodno izmeniti implementirani pametni ugovor da bi se zaštitilo, koliko je to moguće, od napada koji su bili upućeni.

7.1 Odbrane od napada zasnovanih na MEV-u

Kako implementirani pametni ugovor za lutriju nije bio podložan njima, prikazane su mrežne modifikacije koje implementiraju neke L2 mreže da bi se zaštitile od ovog tipa napada. Pored ovoga, dati su mehanizmi koji se mogu primeniti za zaštitu u određenim situacijama na mrežama koje ne implementiraju nikakve posebne mehanizme. Mrežne modifikacije postoje na L2 mrežama:

- **Arbitrum** – sekvencer nema mogućnost da menja redosled transakcija u bloku. Transakcije se isključivo redaju prema vremenskim otiscima pristizanja [8].
- **Optimism –** bazen transakcija je privatan, što onemogućava nadgledanje transakcija pre nego što budu uvrštene u blok [9].

Što se tiče ostalih mehanizama zaštite, opisana je potvrdi-otkrij šema, koja nudi odbranu u slučaju anonimnih glasanja ili aukcija, te mehanizam lomljenja transakcija u slučaju razmena na menjačnicama.

7.2 Odbrana od napada na osnovu vremenske zavisnosti

Ukoliko je neophodno generisati nasumičan broj, onda se za to ne može koristiti ni vremenski otisak, ni bilo kakva informacija vezana za blok, kojom validator može da manipuliše.

Sa druge strane, ukoliko je neophodno kontrolisati vreme trajanja nekog stanja, recimo trajanja glasanja, ili trajanja aukcije, onda je moguće da se, umesto samog vremenskog otiska, koristi broj blokova.

Blokovi se na različitim mrežama drugog sloja proizvode različitim brzinama, i shodno mreži na kojoj se postavi

ugovor, moguće je proračunati željeni broj blokova koji želimo da traje neko stanje.

7.3 Odbrana od napada ponovnim ulaskom

Za odbranu od napada ponovnim ulaskom su predložena dva mehanizma:

- **PEI šablon** – nastao kao skraćenica od principa redanja instrukcija: provere, efekti, interakcije (engl. *checks*, *effects*, *interactions*, to jest *CEI*). Podrazumeva prvobitnu proveru validnosti zahteva za transakciju. Potom, prvo se promeni stanje ugovora, odnosno izvrše se efekti transakcije. Tek na kraju se upućuju eksterni pozivi ka drugim adresama.

- **Modifikator za zaključavanje funkcije** – u ugovor se dodaje logika kojom se onemogućuje da isti korisnik uputi još jedan zahtev ka ugovoru, pre nego što se prethodni zahtev ne izvrši.

7.4 Odbrana od napada onemogućavanja pružanja usluga

Kao što je ranije pomenuto, trajno onemogućavanje pružanja usluga svedeno je na privremeno mehanizmom paketiranja. Osnovna ideja je da se ograniči broj iteracija u petljama i na taj način se onemogući prebacivanje maksimalne cene gasa koju transakcija može da ima.

Na ovaj način se izbegava da se neka transakcija ne može izvršiti nikada. Međutim, iako je razbijena na više transakcija, od kojih se svaka može izvršiti, dok se sve ne izvrše, korisnici neće moći biti usluženi.

8. ZAKLJUČAK

U radu su predstavljene osnove blokčejna, i objašnjeno je zašto su neophodne L2 blokčejn mreže. Objašnjene su osnove rada L2 mreža zasnovanih na namotavanjima.

Zatim, analizirani su napadi koji su vezani za redosled, kako transakcija u bloku, tako i redosleda instrukcija u transakcijama. Pored ovoga, predstavljeni su i napadi vezani za tempiranje: korišćenje vremenskih otisaka blokova, i premalo vremena između zahteva ka ugovorima.

Za napade koji su navedeni predstavljeni su mehanizmi odbrane koji, zavisno od prirode logike pametnog ugovora, mogu da umanje ili negiraju efekat napada.

9. LITERATURA

[1] Ethereum Foundation. Layer 2. https://ethereum.org/en/layer-2/ (pristupljeno u septembru 2024.)

[2] Merkleovo stablo https://en.wikipedia.org/wiki/Merkle_tree/ (pristupljeno u septembru 2024.)

[3] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. 2020. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Comput. Surv. 53, 3, Article 67 (May 2021), 43 pages. https://doi.org/10.1145/3391195.

[4] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur and H. -N. Lee, "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract," in ***IEEE Access***, vol. 10, pp. 6605-6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[5] P. Daian ***et al***., "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability," ***2020 IEEE Symposium on Security and Privacy (SP)***, San Francisco, CA, USA, 2020, pp. 910-927, doi: 10.1109/SP40000.2020.00040.

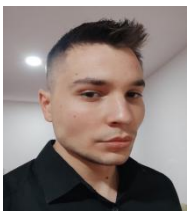
[6] Rick Dudley (@AFDudley) Matthew Slipper (@mslipper)-Ian Norden (@i-nor-den) Abdelhamid Bakhta (@abdelhamidbakhta) Vitalik Buterin (@vbuterin), Eric Conner (@econoar). "eip-1559: Fee market change for eth 1.0 chain," ethereum improvement proposals, no. 1559. https://eips.ethereum.org/EIPS/eip-1559, April 2019. (pristupljeno u septembru 2024.)

[7] Diederik Loerakker (@protolambda) George Kadianakis (@asn-d6) Matt Garnett (@lightclient) Mofi Taiwo (@Inphi) Ansgar Dietrichs (@adietrichs) Vitalik Buterin (@vbuterin), Dankrad Feist (@dankrad). "eip-4844: Shard blob transactions," ethereum improvement proposals, no. 4844. https://eips.ethereum.org/EIPS/eip-4844, February 2022.
(pristupljeno u septembru 2024.)

[8] Arbitrum. Gas and fees: Tips in l2. https://docs.arbitrum.io/how-arbitrum-works/gas-fees#tips-in-l2
(pristupljeno u septembru 2024.)

[9] Optimism. Rollup protocol overview - block production. https://docs.optimism.io/stack/protocol/rollup/overview#block-production
(pristupljeno u septembru 2024.)

Kratka biografija:



Nikola Vukić rođen je u Tesliću 2000. godine. Osnovnu školu i gimnaziju završio u Doboju. Diplomski rad na Fakultetu tehničkih nauka u Novom Sadu odbranio je 2023. god.

kontakt: nikola.vukic@uns.ac.rs