Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.4
DOI: https://doi.org/10.24867/31BE13Jovicevic

ANALIZA PRETNjI I AUDITI U BLOCKCHAIN SISTEMIMA

THREAT ANALYSIS AND AUDITS IN BLOCKCHAIN SYSTEMS

Nikola Jovićević, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIČKO I RAČUNARSKO INŽENjERSTVO

Kratak sadržaj – *U radu su opisani osnovni koncepti blockchain tehnologije i procesa bezbednosnih audita, uključujući metodologije, izazove i specifične karakteristike. Zatim je predstavljena analiza pretnji koje ugrožavaju sigurnost blockchain sistema, kao i različite strategije za njihovu identifikaciju i ublažavanje. Date sz preporuke za efikasnije sprovođenje audita u blockchain okruženju, sa ciljem unapređenja ukupne sigurnosti i pouzdanosti sistema.*

Ključne reči: *blokčejn, distribuirani sistemi, auditi, bezbednost, kriptografija*

Abstract – *The paper describes the fundamental concepts of blockchain technology and the process of security audits, including methodologies, challenges, and specific characteristics. It then presents an analysis of threats to blockchain system security, as well as various strategies for their identification and mitigation. Recommendations are provided for more effective implementation of audits in a blockchain environment, with the aim of improving overall system security and reliability.*

Keywords: *blockchain, distributed systems, audits, security, cryptography*

1. UVOD

Blockchain tehnologija prvi put je u današnjoj formi predstavljena kada je neidentifikovani pojedinac ili grupa, sa pseudonimmom Satoshi Nakamoto, objavio dokument "Bitcoin: A Peer-to-Peer Electronic Cash System"[1]. U tom radu predstavljena je matematička osnova na kojoj funkcioniše bitcoin. Inicijalna primena ove tehnologije ogledala se u uvođenju decentralizacije u finansijski sistem, a koja bi dalje omogućila sprovođenje transakcija bez posredovanja nekog od centralizovanih autoriteta, dozvoljavajući ljudima da upravljaju svojim novcem po sopstvenoj volji, uz sopstvenu odgovornost.

Obzirom na svoju upotrebu i potencijal, ovakvi sistemi se smatraju jako kritičnim kada je u pitanju sigurnost njihovog funkcionisanja, jer bi i najmanji propust mogao jako puno koštati sisteme, ali i njihove korisnike. Veliki značaj u tome svakako imaju sigurnosni auditi, revizije projekata namenjene pronalaženju propusta nastalih tokom kreiranja dizajna i implementacije kako bi se na vreme otkrile i otklonile potencijalne pretnje.

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

Naravno, nemoguće je garantovati da je neki proizvod apsolutno bezbedan, stoga se u verifikaciji koriste različite tehnike kako bi se suzbila mogućnost za nastanak greške. Najsigurnija je detaljna analiza koda i protokola, odrađena od strane više ljudi i timova, mada postoje i različiti alati za statičku analizu koji su u stanju da prepoznaju neke od ustaljenih greški.

2. AUDITI

Proces auditovanja, odnosno sprovođenja audita, u generalnom pogledu može se definisati kao verifikacija ili pregled kvaliteta nekog procesa ili sistema, kako bi se osigurala njegova usklađenost za zahtevima[5]. Audit se može odnositi na celokupnu organizaciju, a može biti ograničen i na određenu funkcionalnost, proces ili korak u proizvodnji. Pored toga mogu se odnositi i na administraciju, gde uključuju revizije dokumenata, rizika, kao i praćenje sprovedenih korektivnih akcija.

U pogledu informacionih sistema, auditi imaju višestruku ulogu i obuhvataju sve aspekte provere bezbednosti, od fizičke konfiguracije i okruženja u kome će sistem funkcionisati, preko softverske arhitekture, implementacionih detalja, rukovanja informacijama, pa sve do načina kako se koristi od strane korisnika. Njima se vrši procena koliko dobro sistem ispunjava zadate kriterijume, što dalje omogućava pronalazak i rešavanje problema pre nego što sistem bude pušten u rad, a u čemu se uviđa njihova ključna uloga u osiguravanju bezbednosti i pouzdanosti krajnjeg proizvoda.

3. BLOCKCHAIN

3.1. Distribuirani sistemi

Distribuirani sistemi predstavljaju sisteme sačinjene od više samostalnih računara koji su geografski udaljeni, koordinisani i komuniciraju preko mreže delujući međusobno u postizanju zajedničkog cilja. Programi koji se na njima izvršavaju dele se na segmente koji se izvršavaju na različitim mašinama. Nastali su kako bi se prevazišli različiti problemi tradicionalne klijent – server arhitekture, konkretnije, kako bi se poboljšale performanse, skalabilnost i dostupnost kroz raspodelu obrade podataka i zadataka između više čvorova.

3.2. Koncept distribuiranog lanca blokova

U distribuiranom sistemu sa mnogo nezavisnih čvorova, očekuje se postojanje zlonamernih aktera, pa se međusobno poverenje isključuje[2]. Svaka pristigla informacija se proverava pre postizanja konsenzusa, koristeći kriptografske hash funkcije. Svaki čvor čuva

svoju kopiju lanca blokova, što omogućava visoku redundantnost i sprečava manipulaciju podacima. Blokovi se dodaju putem konsenzusa, gde većina čvorova mora potvrditi validnost novog bloka.

3.2.1. Struktura bloka

Blokovi najčešće sadrže zaglavlje sa verzijom protokola, hash prethodnog bloka, Merkle root, broj bloka, vremensku oznaku, ciljne vrednosti za rudarenje, i nonce. Telo bloka sadrži broj i listu transakcija[1].

3.2.2. Tok transakcije i konsenzus

Postizanje konsenzusa može se ostvariti raznim metodama, najčešće PoW (Proof of Work) i PoS (Proof of Stake). Transakcije se propagiraju kroz mrežu, a jedan čvor predlaže blok koji ostali čvorovi validiraju. U PoW sistemima se koristi *nonce* za izbor validatora koji predlaže blok, dok PoS sistemi biraju validatore na osnovu različitih faktora, najčešće na osnovu uloženih, odnosno delegiranih sredstava, ali i nasumičnim izborom.

Decentralizovani sistemi, sa druge strane, raspoređuju kontrolu na više nezavisnih čvorova, koji funkcionišu bez centralnog autoriteta. Oni nude prednosti kao što su otpornost na greške, otpornost na napade i skalabilnost, ali istovremeno uvode složenosti u koordinaciju i komunikaciju među čvorovima, kao i potrebu za algoritmima za sprovođenje konsenzusa.

3.4. Ograničenja i pravci unapređenja blockchain tehnologije

Kao i svaka druga tehnologija, blockchain ima svoja ograničenja u primeni, ali je sklon i evoluciji, promenama i unapređenjima. Brojni su razlozi zašto ne bi trebalo žuriti sa primenom ove tehnologije u svim sferama u kojima je ona primenjiva, a primarni je zato što je ona još uvek mlada i treba sačekati da se dodatno razvije. To će, naravno, zahtevati još vremena uloženog u razvoj tehnologija i algoritama koji će vremenom učvrstiti i verovatno proširiti spekar primene *blockchain*-a. Neki od problema sa kojima se ova grana industrije trenutno susreće i principi za njihovo prevazilaženje su[3]:

- **Nedostatak privatnosti**: Svi čvorovi održavaju celokupnu istoriju transakcija, što smanjuje privatnost. Rešenja poput ZK-SNARK, ZK-STARK, i L2 rešenja (npr. Lightning Network za Bitcoin i zk-Rollups za Ethereum) omogućavaju verifikaciju transakcija bez otkrivanja specifičnih podataka.
- **Visoki troškovi procesiranja transakcija**: Ovi troškovi štite od manipulacija, ali mogu povećati operativne troškove. *Layer 2* rešenja kao što su *rollup*-i i *sharding* smanjuju opterećenje glavnog lanca i poboljšavaju skalabilnost.
- **Bezbednosni modeli i gubitak sredstava**: *Blockchain* se oslanja na javne i privatne ključeve, bez rešenja za slučaj gubitka privatnog ključa. Korišćenje hardverskih i *multisig* novčanika smanjuje rizik od gubitka i zloupotrebe.
- **Kašnjenje**: Postizanje konsenzusa u distribuiranoj mreži može biti sporo. *Latency* se može smanjiti optimizacijom mrežnih protokola, korišćenjem PoS i DPoS pristupa, smanjenjem veličine blokova, *sharding*-om, i L2 rešenjima.

Blockchain sistemi takođe evoluiraju prema interoperabilnosti, omogućavajući komunikaciju između različitih *blockchain*-ova putem višelančanih protokola i mostova (*bridges*), kao što su Polkadot i Cosmos sa IBC protokolom.

4. AUDITI U BLOCKCHAIN-U

Blockchain tehnologija je vremenom ostvarila raznovrsnu primenu, ali pored svih benefita, rad u ovom okruženju sa sobom nosi i visoke rizike. S jedne strane je činjenica da je uglavnom u pitanju rad sa novcem, gde tačnost i bezbednost podataka ne smeju biti dovedeni u pitanje, dok je sa druge strane perspektiva i poverenje korisnika, čiji bi gubitak nepovoljno uticao na motivaciju za dalji razvoj. Ova kritičnost upravo naglašava potrebu za temeljnim revizijama projekata, koji se u celokupnom ekosistemu nameću kao ključni za identifikaciju potencijalnih pretnji i ranjivosti u sistemu, kao i generalnu validaciju projekata. Povećana odgovornost koju auditori preuzimaju potiče iz potrebe da se obezbedi integritet i sigurnost sistema koji radi sa finansijskim sredstvima i osetljivim podacima. Kako bi se to izvelo, svi učesnici u procesu moraju poslovati odgovorno.

4.1. Audit request dokument

Pri definisanju specifikacije audita, neophodno je jasno, jednoznačno i precizno definisati očekivanja, ali i osigurati da je relevantnim ljudima obezbeđen pristup do svih neophodnih izvora. Za ove svrhe, pre početka projekta, popunjava se zahtev za sprovođenje audita (*Audit Request*). On može predstavljati formu ili dokument kroz koji će klijent, odnosno softverska kuća koja zahteva audit, popuniti sa ciljem da se kroz kratak opis i obezbeđene resurse predstavi projekat, kako bi se mogla sprovesti precizna procena vremena i ljudstva potrebnog da se revizija sprovede. Dobro pripremljen zahtev za audit treba da sadrži:

1. Precizno definisan opseg audita (*scope*) – navesti delove sistema koji će biti pregledani, uključujući repozitorijume, module, biblioteke;
2. Resurse – lista relevantnih izvora (dokumentacija, kod, dijagrami) kako bi se audit tim bolje pripremio;
3. Željeno vreme do kada bi audit trebalo završiti (timeline) – razuman vremenski okvir na osnovu složenosti projekta;
4. Očekivanja od audita – definiše specifične zahteve i usluge;
5. Očekivani rezultat (output) – definiše šta će biti obezbeđeno na kraju audita (npr. izveštaj, issue-i na GitHub-u);
6. Relevantne kontakte sa obe strane – lista relevantnih osoba za komunikaciju između klijenata i auditora;

7. Dodatne napomene firme koja sprovodi audit – napomene o pripremi koda i resursa pre slanja zahteva.

Nakon razmatranja svih parametara, vrši se procena potrebnog vremena i resursa, a zatim se klijentu predstavlja procena i organizuje početni sastanak *(kick-off meeting*), gde će se razgovarati o detaljima neophodnim za početak posla. Nakon toga organizuju se sastanci po dogovoru, koji se sprovode jednom ili više puta nedeljno, a gde se diskutuje o projektu i potencijalno pronađenim problemima, sve do zaključivanja projekta i predstavljanja finalnog izveštaja o sprovedenoj reviziji na završnom (*closure*) sastanku.

4.2. Očekivanja od audita

Jasno je da sprovođenje audita nije trivijalan proces, jer se ni audit sam po sebi ne svodi samo na analiziranje koda i traženje grešaka. Različite kompanije mogu koristiti različite tehnike i alate u pronalaženju problema, pa se stoga klijentima odmah treba skrenuti pažnja kakve usluge mogu da očekuju, i da u skladu sa tim odaberu šta im je od interesa. Ono što uglavnom spada u osnovne usluge audita su:

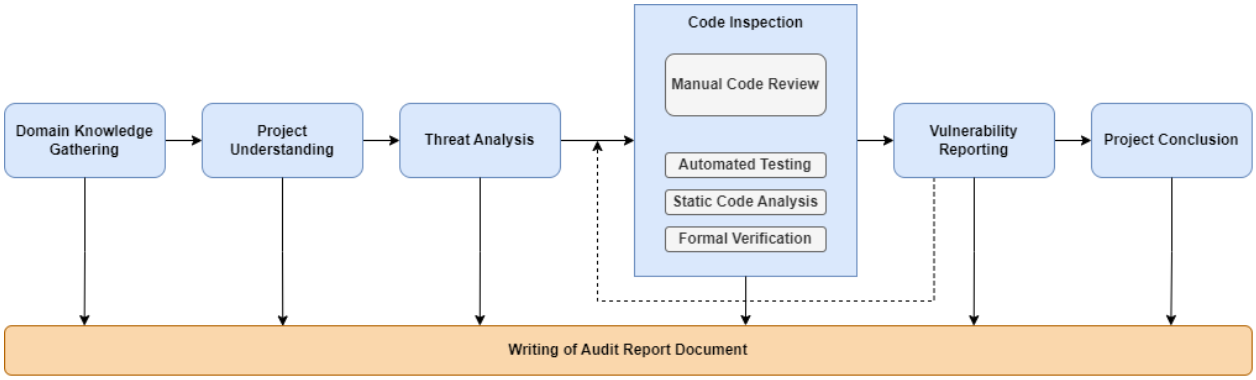
1. analiza specifikacije projekta;
2. pregled dokumentacije zbog potencijalnih nejasnoća i nekonzistentnosti sa kodom;
3. analiza koda i funkcionalnosti;
4. pregled ispravki problema prijavljenih u okviru audita.

Pored toga, neki alternativni pristupi uključuju i analizu arhitekture i protokola koja može obuhvatiti i sugestije za njihovo unapređenje, analizu i unapređenje testova, ali i pomoć pri odlukama u procesu dizajniranja rešenja za određene probleme, ili funkcionalnosti koje će tek biti implementirane. Tu se takođe mogu vršiti i neke od sofisticiranijih metoda, poput formalne verifikacije softvera, pisanjem matematičkih specifikacija upotrebom jezika kao što su TLA+ i Quint.

4.3. Tehničke složenosti i izazovi

Iako suštinski mogu biti nepredvidivi, auditi se mogu grubo podeliti na nekoliko faza (slika 1), gde za svaku treba izdvojiti dovoljno vremena kako bi dalji tok projekta mogao biti što bolje sproveden.

Prva faza nastupa pre početka same analize, gde se nakon utvrđivanja zahteva pristupa istraživanju relevantnih oblasti i tehnologija (izučavanje domena).



Slika 1. *Koncepti i faze audita*

Nakon nje započinje izučavanje konkretnog projekta i upoznavanje sa potrebnim segmentima sistema. U ovoj fazi veliku ulogu igraju projektne dokumentacije, slike, dijagrami, video prezentacije i sl. U slučaju nedostatka gorepomenutih izvora, pristupa se procesu reverzivnog inženjeringa.

Zatim se razmatraju potencijalni pravci napada, ustaljene pretnje relevantne za projekte koji imaju slične karakteristike, koncepte i namenu. Sumiraju se i flitriraju ranija iskustva kako bi se proverilo prisustvo ili nedostatak odgovarajućih mehanizama i algoritama koji bi ciljane pretnje adekvatno adresirali.

Analiza koda sprovodi se iterativno, prolazeći kroz iste segmente koda više puta od strane više auditora. Razlikujemo analizu koda „liniju po liniju“ i analizu upotrebom različitih alata za statičku analizu.

4.4. Modelovanje pretnji

Kako bi se sprovela detaljna analiza pretnji i razmotrili potencijalni vektori napada, neophodno je za analizirani sistem kreirati adekvatan model pretnji (*threat model*), koji bi trebalo da opisuje osnovne karakteristike pojedinih delova sistema ili korišćenih algoritama koji bi potencijalno mogli uvesti slabosti u sistem. Zbog ovoga se u obzir mora uzeti mnoštvo aspekata, poput učesnika i komponenti u sistemu, arhitekturu, tokove podataka, protokole za komunikaciju i konsenzus, njihova ograničenja i slučajeve upotrebe u odnosu na posmatrano okruženje i zahteve koje bi trebalo da ispunjavaju.

4.5. Raspodela i vektori napada

Analizom različite literature koja se bavila analizom napada na *blockchain* sisteme sa ograničenim pristupom, identifikovani su napadi i komponente koje su im podložne[4].

Neke od najučestalijih pravaca napada uključuju zloupotrebu ranjivosti pametnih ugovora, propusta u implementaciji matematičkih operacija i problema uzrokovanih pojavama *overflow*-a i *underflow*-a.

Velike probeleme mogu uzrokovati i kriptografske ranjivosti, koje ukoliko postoje, predstavljaju izuzetno ozbiljnu pretnju budući da integritet i neporecivost samog

blockchain-a zavisi od ispravnosti *hash* funkcija i digitalnih potpisa.

Kada su u pitanju *bridge* lanci namenjeni *cross-chain* komunikaciji i prenosu sredstava između različitih *blockchain* mreža, karakteristični su *replay* napadi, gde se koristi već izvršena, validna transakcija sa jedne mreže na drugu, pri čemu ona još uvek nije potpuno procesirana i evidentirana kao iskorišćena, uzrokujući *double minting*, odnosno *double burning*.

Prepoznatljivi DoS napadi, iako nisu previše zastupljeni, u *blockchain* okruženju ipak predstavljaju pretnju. Kako bi napadač izveo uspešan DoS napad, može pokušati da preplavi neke od čvorova karakterističnim zahtevima koje validator treba obraditi (npr. TCP SYN paketima). Ukoliko je napad usmeren na trenutnog lidera, može u značajnoj meri smanjiti ili potpuno obustaviti proces postizanja konsenzusa.

Segmentacija mreže (*network partitioning*), može se desiti ako se u sistemu pronađu zlonamerni validatori koji manipulacijom konsenzus protokola putem protokola na mrežnom nivou mogu particionisati mrežu koristeći napade poput BGP *hijacking*-a i DNS napada. Nakon što je mreža podeljena, sledi manipulacija procesom donošenja odluka, koja može uključivati stvaranje falsifikovanih blokova koji bi potom uticali na validnost i integritet lanca. Ovo se može sprovesti generisanjem lažnih čvorova ili izolovanjem određenog čvora u mreži koji bi video samo one podatke koje napadać želi da prikazuje, time omogućavajući manipulaciju podacima koje konkretan čvor vidi i šalje.

4.6. Audit Report dokument

Audit *report* dokument, predstavlja finalni izveštaj sa audit projekta koji obuhvata evidenciju o celokupnom poslu koji je urađen. Svaki dokument se razlikuje i zavisi od prakse audit kuće koja je autor. Centralni deo koji je svakako najvažniji predstavlja popis pronađenih problema i preporuka za njihovo rešavanje, ali on može sadržati i mnogo više, što je svakako dobra praksa. Sveobuhvatni izveštaj sa audita koji na transparentan način predstavlja i tok samog audita sadrži poglavlja za gotovo svaku fazu i uključuje:

1. Kratak pregled projekta (*Project Overview*);
2. Tehničke detalje vezane za audit (*Audit Dashboard*);
3. Analiza sistema (*System Overview*);
4. Analiza pretnji i invarijanti (Threat / Invariant Analysis);
5. Lista i opis pronađenih propusta (*Findings*);
6. Klasifikacija *finding*-a (*Findings Classification)*;
7. Odricanje od odgovornosti i dodatne napomene (Disclaimer).

5. ZAKLjUČAK

Potencijal *blockchain*-a postao je neupitan, i jedino se postavlja pitanje dokle će sezati granice njegove primene. Pred ovim konceptom ipak stoji još mnogo izazova, godina istraživanja i razvoja, a u svemu tome biće neophodna podrška u revizijama, verifikacijama kvaliteta i savetima za pravce unapređenja. Uloga audita u ovom celokupnom podvigu nije mala jer su upravo audit inženjeri oni koji dolaze u dodir sa raznovrsnim rešenjima i pristupima, i stiču široku sliku o tehnologijama koje se razvijaju. Iz tog razloga je ovaj poziv karakterističan, jer zahteva konstantno učenje novih tehnologija u kratkom vremenskom rasponu i doprinosi sticanju iskustva u mnogim domenima.

U okviru ovog rada, sumirani su ključni izazovi i specifične karakteristike audita u kontekstu *blockchain* tehnologije, kao i strategije za identifikaciju i ublažavanje pretnji koje ugrožavaju sigurnost *blockchain* sistema. Ovo je značajno jer pruža bolji uvid u kompleksnost bezbednosnih audita i nudi smernice za njihovo efikasno sprovođenje. Kroz analizu postojećih pretnji i potencijalnih napada, osvetljavaju se segmenti tehnologije u kojima je potrebno dodatno istraživanje, ali i kontinuirano unapređenje postojećih metodologija.

U svetlu sve brže evolucije blockchain tehnologije neophodno je nastaviti sa istraživanjem i razvojem novih pristupa u sprovođenju audita, kako bi nastavili sa obezbeđivanjem sigurnosti i pouzdanosti sistema. Ova istraživanja mogu dalje ići u različitim pravcima, baviti se analizama novih pretnji, razvojem automatizovanih alata za detekciju ranjivosti, ili unapređenjem procedura audita u skladu sa specifičnostima novonastalih protokola.

6. LITERATURA

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Satoshi Nakamoto* (2008).

[2] Chaum, David Lee. *Computer systems established, maintained and trusted by mutually suspicious groups*. Diss. University of California, Berkeley, 1982.

[3] Hughes, Laurie, et al. "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda." *International journal of information management* 49 (2019).

[4] Putz, Benedikt, and Günther Pernul. "Detecting blockchain security threats." *2020 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2020.

[5] https://asq.org/quality-resources/auditing (pristupljeno u septembru 2024)

Kratka biografija:

Nikola Jovićević rođen je u Užicu 1999. godine. Odrastao je u Požegi gde je završio osnovnu školu i gimnaziju. Osnovne akademske studije na Fakultetu tehničkih nauka Univerziteta u Novom Sadu upisao je 2018. godine. Diplomirao je u septembru 2022, i iste godine upisao master akademske studije.
kontakt: n.jovicevic999@gmail.com