DOI: 10.5937/bankarstvo2501106R

Primljeno: 22.11.2024.
Odobreno: 24.01.2025.

ZLOUPOTREBE I NAPADI NA BLOKČEJN SISTEME

Aleksandra Radojević, istraživač saradnik, Ekonomski fakultet Univerziteta u Kragujevcu
email: aleksandra.radojevic@ekonomski.org
ORCID: https://orcid.org/0000-0001-8000-9248

Predrag Stanković, istraživač pripravnik, Ekonomski fakultet Univerziteta u Kragujevcu
email: predrag.stankovic@ef.kg.ac.rs
ORCID: https://orcid.org/0009-0004-6657-6544

Rezime

Blokčejn sistemi su sveprisutniji u svim sektorima poslovanja, ali kao primarni korisnik ovih tehnologija javlja se finansijska industrija. Radom se žele istražiti napadi na blokčejn sisteme, odnosno želi se utvrditi jačina ovih napada u prošlosti i obim njihovih posledica. Kroz istoriju vrste i načini napada na blokčejn sisteme su inovirani, a sa tim i jačina ovih napada je rasla. Rezultati napada na blokčejn sisteme su kratkoročne nestabilnosti koje izazivaju promenu cena kriptovaluta i smanjenje poverenja u iste, ali dugoročno posmatrano napadi i zloupotrebe nemaju jak uticaj. Zapravo, prisutan je napredak navedenih sistema nakon izvršenih napada i zloupotreba. Sprovedeno istraživanje pokazuje da se najčešće javljao napad 51%. Primarni cilj zloupotreba bio je prisvajanje sredstava, ali i dokazivanje slabosti sistema na koje su napadi izvršeni.

Ključne reči: blokčejn sistemi, kriptovalute, zloupotrebe i napadi, finansijski sektor, napad 51%.

JEL klasifikacija: O33, L86, D85

Uvodna razmatranja

Razvojne tendencije u svetu, pre svega jačanje i neizostavna implementacija informaciono-komunikacionih tehnologija bitno su uticale na sve sfere poslovanja i života. Blokčejn tehnologije privlače veliku pažnju i pokreću sve veći broj projekata u različitim industrijama, međutim, finansijska industrija se smatra primarnim korisnikom blokčejn koncepta (Nofer et al., 2017, 183). U sektoru finansijskih usluga neophodan je kontinuirani razvoj istovremeno sa razvojem poslovnih i organizacionih procesa kao i novih proizvoda i instrumenata (Sredojević, 2018, 84). Digitalni svet unapređuje se, posredstvom blokčejna, kroz donošenje nove perspektive o bezbednosti, otpornosti i efikasnosti sistema (Ahram et al., 2017, 137) i predstavlja novu, revolucionarnu tehnologiju. Navedeni sistem sačinjen je od niza blokova koji su međusobno povezani, pri čemu ne postoji centralna institucija koja bi vršila kontrolu ili bila odgovorna za povezivanje svih ostalih učesnika u sistemu. Tehnologija blokčejna je osnova kriptovaluta, a koja se zasniva na decentralizovanoj računarskoj mreži. Značajna odlika blokčejn sistema jeste i konsenzus, odnosno putem protokola konsenzusa vrši se validacija transakcija i dodaju blokovi u lanac.

Poslednjih godina, kriptovalute su privukle pažnju investitora na finansijskim tržištima iz celog sveta, a oblast kriptovaluta, odnosno virtuelnih valuta u platnim sistemima se ubrzano širi (Alihodžić, 2023, 129). Tokom vremena, ulaganje u kriptovalute donelo je izuzetno visoke stope prinosa, što prati visok rizik, bez ikakvih garancija i bez zaštite investitora (Tomić, 2020, 22-23). Potencijal koji imaju kriptovalute zasnovane na blokčejnu privlači veliki broj investitora, kao i zlonamernih pojedinaca. Razvoj blokčejn sistema, ali i poverenje u ovakav sistem može biti narušeno zbog napada koji su ka njemu usmereni. Brojni su oblici napada i načina na koji napadači žele da pristupe blokčejn sistemima u cilju ostvarivanja koristi.

Predmet istraživanja u radu su različiti oblici napada na blokčejn sisteme. Kao relativno mladi i sistemi sa velikim potencijalom za rastuću primenu u budućnosti, blokčejn sistemi su izloženi brojnim oblicima napada. U skladu sa definisanim predmetom istraživanja, cilj rada jeste izvođenje zaključka o veličini i snazi istorijskih napada na blokčejn sisteme. Sagledaće se efekti različitih oblika napada, njihove posledice, ali i mogućnosti ponavljanja napada. Dodatno će biti utvrđeno koji oblici napada na blokčejn sisteme su najučestaliji. U skladu sa definisanim predmetom i ciljem istraživanja, u radu će se poći od sledećeg istraživačkog pitanja: *Da li su napadi na blokčejn sisteme imali dugoročni uticaj na njihovu stabilnost?*

Osnovne odlike blokčejn sistema

Blokčejn sistem predstavlja lanac transakcija koji ne daje mogućnost korisnicima da vrše izmene ili brisanje ranije unetih podataka. Blokčejn se može definisati kao distribuirana baza podataka ili javna knjiga svih transakcija ili digitalnih aktivnosti koje su realizovane ili podeljene između učesnika (Martić, 2021, 337-338). Navedena baza podataka, u slučaju kriptovaluta, odnosi se na knjigu svih transakcija, odnosno sadrži spisak svih učesnika i iznose novca u njihovom posedu (Tomić i Todorović, 2020, 16). Lanac se održava mrežom čvorova, koji verifikuju validnost transakcija i dodaju ih novim blokovima u procesu koji se naziva rudarenje (Gatteschi et al., 2018, 63). Ako se većina učesnika (čvorova) u mreži putem mehanizma konsenzusa složi o validnosti transakcija u bloku i o validnosti samog bloka, blok se može dodati u lanac (Nofer et al., 2017, 184). Koteska et al. (2017, 3) objašnjavaju da kada se kreira novi blok, on se emituje na mrežu, zatim svi čvorovi primaju blok, potvrđuju blok i sve transakcije u njemu. U situaciji da je on validan, svi čvorovi ga stavljaju kao sledeći blok u svom lokalnom blokčejnu.

Blokovi u lancu zapravo predstavljaju stavke u kojima su sadržane informacije o izvršenim transakcijama. Blokčejn sistem se na osnovu transakcija koje se izvršavaju kontinuirano povećava. Svaka nova transakcija koja se pojavi mora biti usklađena sa postojećim informacijama u sistemu. Ukoliko je transakcija validna i ukoliko učesnici to potvrde nastaje novo stanje u sistemu.

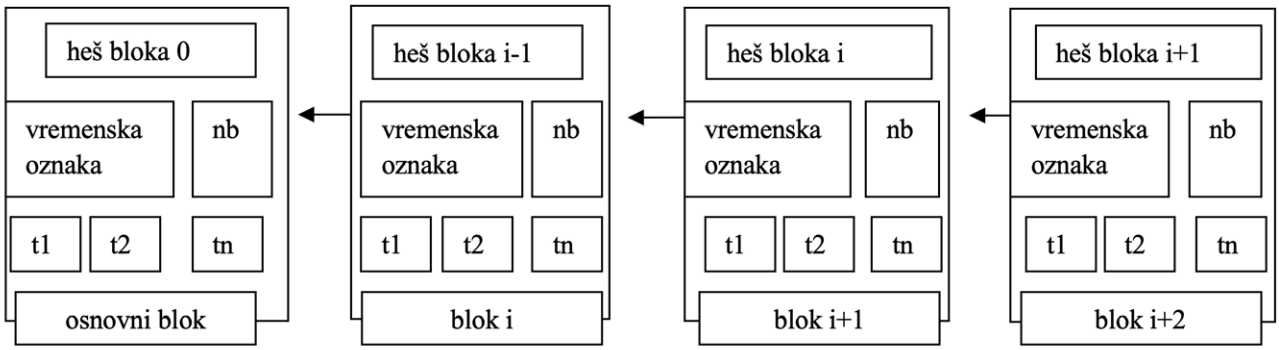
Blokčejn predstavlja tehnološku osnovu kriptovaluta, odnosno radi se o tehnologiji koja se do sada pokazala odličnom u očuvanju velikih baza podataka, jer istovremeno omogućava masovni pristup i sprečava zlonamerne napade (Tomić et al., 2020a, 41). Najznačajnije prednosti blokčejn tehnologije u poslovanju jesu sniženje troškova, brzina saldiranja transakcija, brzina i mogućnosti provere podataka, zaštita podataka, mogućnost provere krajnjeg korisnika i pouzdanost transakcija (Hadžić i Nedeljković, 2018, 153). U poređenju sa konvencionalnim, centralizovanim rešenjima, blokčejn koji se odlikuje decentralizacijom ima neke značajne prednosti kao što su nepromenljivost, poboljšana bezbednost, tolerancija grešaka i transparentnost (Fan et al., 2020, 126927).

Efikasnost blokčejn sistema zasniva se na tri elementa - decentralizovana mreža, konsenzus i kriptografija (Shetty et al., 2019, 5). Samo funkcionisanje blokčejn sistema podrazumeva nepostojanje centralnog autoriteta i postojanje potrebe za postizanjem konsenzusa za validaciju transakcija i dodavanje blokova u blokčejn lanac. Pored toga, kriptografija obezbeđuje sigurnost u funkcionisanju blokčejn sistema. Dva sastavna dela blokčejn sistema su konsenzus protokol i mehanizam transakcija (Kearney i Perez-Delgado, 2021, 2).

Konsenzus protokol se odnosi na donošenje odluka o dodavanju blokova u sistem i njihovoj validnosti. Mehanizam transakcija podrazumeva način na koji se prenose informacije u sistemu. Autori Hadžić i Nedeljković (2018, 154) kao osnovne karakteristike blokčejn tehnologije bitne za poslovnu implementaciju navode: Distribuirani podaci; Mogućnost da svi učesnici u direktnoj komunikaciji obavljaju transakcije koje međusobno validiraju na samom lancu; Anonimnost; Nepromenjivost zapisa; Mogućnost ugrađivanja računske logike i programiranje realizacije događaja ili transakcija u samoj strukturi lanca, koji se realizuju po ispunjavanju zadatih preduslova i postaju momentalno verifikovani – „pametni ugovori". Blokčejn tehnologija omogućava da se digitalna informacija distribuira između svih učesnika, pri čemu svaki učesnik održava sopstvenu kopiju svake relevantne informacije (Bolanča et al., 2018, 112). Svaki učesnik ima pristup celoj bazi podataka, a pri čemu ne postoji jedno centralno mesto u kome se podaci skladište i ne javlja se potreba da postoji centralna institucija za posredovanje i kontrolu u obavljanju transakcija. Transakcije koje su zabeležene u blokčejn sistemu su javne za učesnike.

Slika broj 1 prikazuje blokčejn lanac koji se sastoji od niza blokova. Sa Slike 1 se može videti da svaki novi blok sadrži heš prethodnog bloka, vremensku oznaku i više transakcija (od t1 do tn), kao i nasumični broj za verifikaciju heša (nb). Heš funkcija je matematička funkcija koja se efikasno može izračunati i koja vrši transformaciju ulazne poruke bilo koje veličine u izlaznu poruku fiksne veličine (Narayanan et al., 2016, 23). Korišćenje izlazne, fiksne veličine povećava bezbednost blokčejn sistema, odnosno pokušaj dešifrovanja heš vrednosti samo na osnovu izlazne veličine neće otkriti ulaznu veličinu (Frankenfield, 2022). Zapravo, heš se ne može upotrebiti za dobijanje ulaznih podataka, već isključivo za proveru validnosti.

Slika 1: Blokčejn sistem i niz blokova



Izvor: Zheng et al., 2018, 355

Svaki blok, sa izuzetkom prvog bloka, u blokčejn sistemu ukazuje na njegov neposredno prethodni blok (koji se naziva roditeljski blok) preko reference koja je u suštini heš vrednost roditeljskog bloka (Dai et al., 2019, 8078). Heš vrednosti su jedinstvene i prevara se može efikasno sprečiti pošto bi promene bloka u lancu odmah promenile odgovarajuću heš vrednost (Nofer et al., 2017, 184). Složen mehanizam validacije čini skoro nemogućim da čvor kontroliše većinu mreže, štaviše, činjenica da svaki validirani blok sadrži referencu na prethodni blok (obezbeđen korišćenjem metoda kriptografije) sprečava zlonamerne modifikacije snimljenih transakcija (Gatteschi et al., 2018, 64).

Konsenzus u blokčejn sistemima

Može se reći da je razvoj protokola konsenzusa sličan inženjeringu kriptografskih sistema i da bi programeri blokčejna trebalo da gledaju na uspostavljeno iskustvo u kriptografiji, bezbednosti i teoriji distribuiranih sistema za izgradnju sistema od poverenja (Cachin i Vukolić, 2017, 20). Ključna osobina blokčejn sistema je da čvorovi ne veruju jedni drugima, pri čemu se neki mogu ponašati na neadekvatan način (Dinh et al., 2018, 1368). U skladu sa ovom mogućnošću ispoljava se potreba za konsenzusom. Da bi se zadržao integritet sistema, podatke mora potvrditi i prihvatiti većina korisnika, ako ne i svi, što znači da svaki blokčejn mora imati ugrađeni konsenzus protokol (Tomić et al., 2020b, 366). Konsenzus je protokol u blokčejn mreži, koji specificira vremensku validnost i pravila kojih moraju da se pridržavaju svi učesnici da bi izvršili različite zadatke ili pridružene transakcije u mreži blokova (Bodkhe et al., 2020, 79772). Dakle, samo postojanje konsenzusa omogućava članovima blokčejn sistema da rade kao grupa i da teže zajedničkom cilju, čak i u situaciji postojanja zlonamernih učesnika.

Konsenzus je u skladu sa decentralizacijom blokčejn sistema, odnosno njime se uklanja potreba za centralnom institucijom koja bi garantovala validnost transakcija i održavala bezbednost blokčejn sistema. Narayanan et al. (2016, 54) objašnjavaju kako se zapravo dolazi do konsenzusa. Prema njima, u redovnim intervalima, recimo svakih 10 minuta, svaki čvor u sistemu predlaže sopstveni skup transakcija kao sledeći blok. Zatim čvorovi izvršavaju konsenzus protokol, gde je ulaz svakog čvora sopstveni predloženi blok. Neki čvorovi mogu biti zlonamerni i mogu stavljati nevažeće transakcije u svoje blokove, ali u takvoj situaciji treba uzeti u obzir da će drugi čvorovi biti iskreni. Ako konsenzus protokol uspe, validan blok će biti izabran kao izlaz. Čak i ako je izabrani blok predložio samo jedan čvor, to je validan izlaz sve dok je blok validan. U situaciji da postoji neka validna neizvršena transakcija koja nije uključena u blok, ona bi mogla samo da sačeka i uđe u sledeći blok.

Dve osnovne vrste blokčejn sistema jesu oni za koje nije potrebna dozvola (permissionless blockchains) i oni za koje je dozvola potrebna (permissioned blockchain) (Dinh et al., 2018, 1366). U prvom slučaju, stanje blokčejna i njegove transakcije, zajedno sa sačuvanim podacima je transparentno i dostupno svima, dok u slučaju blokčejn sistema za koje je potrebna dozvola, samo ovlašćenim entitetima je dozvoljeno da učestvuju u aktivnostima unutar blokčejna (Ferdous et al., 2020, 5). U skladu sa prethodno navedenom podelom blokčejn sistema prisutno je više protokola konsenzusa. Neki od protokola koji se primenjuju u blokčejn sistemima za koje je potrebna dozvola jesu: Paxos, Raft, Proof-of-authority, Practical Byzantine Fault Tolerance, Delegated Byzantine fault tolerance i Federated Byzantine Fault Tolerance (Tomić, 2021). S druge strane, protokoli koji se koriste u blokčejn sistemima za koje nije potrebna dozvola jesu: Proof-of-Work, Proof-of-Stake, Proof-of-Burn, Proof-of-Capacity, Proof-of-Importance, Proof-of-Activity (Tomić et al., 2020b). Može se reći da je najčešće spominjan, ali i najčešće primenjen konsenzus protokol Proof-of-Work. Ovaj konsenzus algoritam primenjuje se kod najpoznatije kriptovalute Bitcoin.

Napadi na blokčejn sisteme

Pored svih prednosti koje se vezuju za blokčejn sisteme prisutne su i određene manjkavosti koje se u vezi sa njima javljaju. Pri postojanju nedostataka u blokčejn sistemima uočava se mogućnost za napade i zloupotrebe u njima. Blokčejn je platforma koja teži obezbeđenju bezbednosti i sigurnosti, a kroz minimiziranje izloženosti zlonamernim napadima (Jiang et al., 2022, 1087).

U jednom od radova (Chen et al., 2022, 5-6) koji se bavi tematikom napada na blokčejn sisteme navodi se da postoje tri oblika napada: napad izazivanja konsenzusa (the attack of consensus protocol), napad srednjeg protokola (the attack of middle protocol), i napad servisa aplikacije (the attack of application service). Kod napada izazivanja konsenzusa cilj napadača je da ostvari dodatni prihod kroz umešanost u rezultate konsenzusa blokčejna. Kod ove grupe napada neke od metoda napada jesu: Block withholding napad, 51% napad, pool hopping napad, selfish mining napad i FAW napad. Napad srednjeg protokola podrazumeva uticaj napadača na komunikaciju čvorova i pametne ugovore. Kod napada na komunikaciju čvorova metode jesu: DdoS napad, Eclipse napad i Sybil napad, dok se kod napada na pametne ugovore može navesti reentrancy napad. Napad servisa aplikacije podrazumeva ponašanje napadača koje cilja na privatnost korisnika. Metode napada u ovom slučaju jesu: identity privacy i transaction information napadi.

Napadi na blokčejn sisteme su u jednom od radova (Kausar et al., 2022, 4301) podeljeni u dve grupe: napadi orijentisani na jezgro i napadi orijentisani na klijente. U grupu napada koji su orijentisani na jezgro mogu se ubrojati metode: Eclipse napad, Sybil napad, DNS napad, BGP hijacking and spatial partitioning, DDoS napad, Stress testing napad, Memory pool flooding napad, Block withholding napad, Finney napad, FAW napad, 51% napad, Selfish mining napad, Consensus delay i Timejacking napad. S druge strane, kod napada orijentisanih na klijente svrstavaju se Wallet theft, Cryptojacking napad, Double spending napad, Transaction malleability i Liveness napad.

U jednom od radova (Narayanan et al., 2016, 161) objašnjeno je da u situaciji kada se pronađe novi blok, podrazumevano ponašanje je da se to odmah objavi mreži. Međutim, napad Block withholding podrazumeva da se odstupi od takvog ponašanja i da napadač vrši dalje rudarenje u nadi da će pronaći dva bloka zaredom pre nego što ostatak mreže dođe do jednog. Dakle, napadač drži informacije u tajnosti sve vreme.

Napadači kroz napad 51% mogu da stvore duži lanac blokova u sistemu, a što podrazumeva da će sistem blokove poštenih učesnika učiniti nevažećim. Sayeed i Marco-Gisbert (2019, 5-6) objašnjavaju 51% napad kao napad koji se dešava kada napadač poseduje 51% snage heširanja. Ovaj napad počinje privatnim stvaranjem lanca blokova, koji je potpuno izolovan od prave verzije lanca. U kasnijoj fazi, izolovani lanac se predstavlja mreži da bi se uspostavio kao najduži lanac, a samim tim i kao pravi lanac. Kod ovog oblika napada nije neophodno da se dobije 51% moći heširanja, odnosno ako napadači dobiju manje procenata moći napad je moguć, ali sa manjom verovatnoćom uspeha.

Kod pool hopping napada napadač se pridružuje rudarskom pulu (mining pool) sa najvećim prihodom nakon analize prihoda više rudarskih pulova i na taj način poboljšava svoj prihod i utiče na efektivnu računarsku snagu u rudarskom pulu (Chen et al., 2022, 12). Drugim rečima, pool hopping podrazumeva vezivanje za rudarski pul u situaciji kada je njegova atraktivnost visoka i njegovo napuštanje kada ona nije, tj. usmeravanje računarske snage ka drugoj alternativi (Belotti et al., 2018, 2). Ovo znači da napadač iz rudarskog pula može da dobije više nego što mu doprinosi. U jednom od radova (Rosenfeld, 2011) pool hopping se objašnjava kao situacija u kojoj će napadač vršiti rudarenje u jednom pulu do određenog trenutka, a zatim će preći u drugi, pri čemu će dobiti nagradu za rudarenje u prvom pulu. Navedeno podrazumeva da će na osnovu preduzetih radnji napadač pre izlaska iz prvog pula dobiti određenu nadoknadu, iako su pošteni rudari završili rudarenje i došli do novog bloka nakon napadačevog izlaska iz datog rudarskog pula. Rudari koji napuštaju jedan rudarski pul utiču na smanjenje njegove ukupne heš snage, a što utiče na dalje rudarenje u smislu smanjenja uspešnosti ovog procesa (Singh et al., 2019, 1). Situacija u kojoj postoji veći broj učesnika koji prelaze iz jednog rudarskog pula u drugi je neodrživa. Svaki rudarski pul iz kog se može ovako izlaziti će doći u situaciju manje privlačnosti, a kada se ovo desi smanjiće se broj učesnika koji u njemu rudare i on će trajno zadržati ovakav status (Rosenfeld, 2011, 23).

U slučaju selfish mining napada, nepošteni rudari sakrivaju podatke i na taj način nanose štetu drugim poštenim rudarima (Vokerla et al., 2019, 5). U jednom od radova (Kausar et al., 2022, 4303) objašnjava se da napadač u slučaju selfish mining napada tajno dolazi do novih blokova i to ne objavljuje ostalim učesnicima sistema. Zatim, kada lanac blokova napadača postane duži od lanca blokova koji su kreirali pošteni učesnici on to objavljuje. Ovakav napad zapravo poništava blokove poštenih učesnika. Drugim rečima, u situaciji kada napadač prvi rudari blok on neće emitovati taj blok u lanac, ali će, kada pošteni rudari uspešno dođu do novog bloka, emitovati i svoj blok i prouzrokovati račvanje mreže (Chen et al., 2022, 12). Tada, pošto napadač ima skrivene blokove, lanac blokova koji on predlaže će biti duži i nadogradnja lanca će se nastaviti po liniji koju je predložio napadač prilikom račvanja.

DDoS je jedan od najčešćih napada u blokčejn mreži koji koriste napadači da ometaju autentične transakcije tako da se nevažeće transakcije mogu izvršiti (Sayeed i Marco-Gisbert, 2019, 5). Napadač preopterećuje mrežu velikim brojem zahteva, odnosno informacija, čime mrežne resurse čini nedostupnim korisnicima, odnosno dovodi do stanja da ona ne reaguje na transakcije (Aggarwal i Kumar, 2021, 406). U ovakvoj situaciji, zbog zagušenosti sistema, napadač može pokrenuti i druge vrste napada, kao što je, na primer, napad dvostruke potrošnje (Shetty et al., 2019, 58).

Aggarwal i Kumar (2021, 404) objašnjavaju Sybil napad kao situaciju u kojoj napadač stoji iza više učesnika istovremeno, odnosno napadač manipuliše mrežom i kontroliše celu mrežu kreiranjem više lažnih identiteta. Stvoreni različiti identiteti izgledaju kao pravi učesnici, ali zapravo nepoznati napadač kontroliše sve ove lažne učesnike. Napadač kroz lažne identitete uspeva da validira neadekvatne transakcije i uključi nove blokove u lanac blokova (Sayeed i Marco-Gisbert, 2019, 5). U ovom

slučaju napadač uspeva da nadglasa poštene učesnike mreže, odnosno kroz kreirane lažne identitete napadač stiče veliki uticaj na blokčejn sistem. Sybil napad predstavlja situaciju u kojoj napadač kontroliše onoliko identiteta koliko mu je potrebno da utiče na konsenzus i da izazove ishod koji ide u njegovu korist (Ferdous et al., 2020, 8) i zbog kog je pokrenuo napad. Napadač koristi lažne identitete za komunikaciju sa poštenim učesnicima, ovi učesnici zatim koriste vreme i resurse za komunikaciju sa napadačem i ne dobijaju na vreme validne informacije (Chen et al., 2022, 14). Dakle, u slučaju napada Sybil, napadači mogu da spreče validaciju određenih transakcija.

U slučaju eclipse napada, napadač izoluje žrtvu od ostatka svojih kolega na nivou mreže, kontrolišući njene dolazne i odlazne veze (Nayak et al., 2016, 305). Napadač prvo utiče na proces komunikacije između ciljnog čvora i okolnih poštenih čvorova, a kada se ciljni čvor poveže samo sa zlonamernim čvorom, napadač može da utiče na njega i dalje kontroliše efektivnu računarsku snagu ciljnog čvora (Chen et al., 2022, 14). Eclipse napad znači izolaciju i kontrolu ciljnog čvora, a što može dovesti do realizacije drugih napada (Yves-Christian, 2018, 4), odnosno suština ovog napada je u stvaranju mogućnosti za izvršenje drugih vrsta napada na blokčejn sisteme (academy.binance.com). Na osnovu navedenih aktivnosti, napadač može lako da izvrši napad dvostruke potrošnje (Aggarwal i Kumar, 2021, 405), odnosno na osnovu neadekvatnog pogleda na mrežu koji ima ciljni čvor omogućava se napad dvostruke potrošnje (Conti et al., 2018, 3431). Takođe, vršenje eclipse napada može se iskoristiti za stvaranje uslova za lakše sprovođenje napada 51% (academy.binance.com).

Kada zlonamerni učesnici ciljaju na privatnost korisnika postoje dva pristupa. Kako Chen et al. (2022, 15-16) objašnjavaju identity privacy napad podrazumeva situaciju u kojoj napadač dobija informacije o drugim učesnicima sistema. Napadač kod ove vrste napada može da lažira identitet poštenih učesnika i time ih ugrozi. Isti autori napad transaction information objašnjavaju kao situaciju u kojoj zlonamerni učesnici dolaze do istorije transakcija na osnovu kojih stiču saznanja o ponašanjima učesnika.

Double spending napad ili napad dvostruke potrošnje je problem koji znači trošenje iste kriptovalute dva puta, a da bi se sprečilo nastajanje ovog problema potrebno je da mreža ostane decentralizovana tako da jedna strana ne može da preuzme kontrolu nad svim transakcijama u njoj (Aggarwal i Kumar, 2021, 400). U radu koji objašnjava vrste blokčejn napada (Kausar et al., 2022, 4303) naznačava se da dvostruka potrošnja podrazumeva korišćenje jednokratne transakcije dva ili više puta. Kao primer za ovu vrstu napada može se navesti situacija u kojoj osoba A želi da plati osobama X i Y istim novčićem.

Pregled istorijskih napada na blokčejn sisteme

Za istraživanje koje je sprovedeno korišćeni su prethodni radovi, akademske studije i članci koji su se bavili napadima na blokčejn sisteme i čiji su predmet posmatranja bile različite kriptovalute. Analizirana su istraživanja koja su ispitivala ove napade, a u obzir su uzeti i izvori koji detaljno prikazuju specifične oblike napada. Posmatrani slučajevi su raspoređeni prema vrsti napada (51% napad, DdoS napad i drugi), analizirana je njihova jačina, trendovi u napadima, kao i posledice koje su se ispoljile. U istraživanju je primenjeno sistemsko mišljenje, odnosno, oslanjajući se na teorijske osnove istraživanog problemskog područja izvedeni su zaključci o vezi svih elemenata blokčejn sistema. Korišćene su i metode indukcije i dedukcije. Polazeći od pojedinačnih napada, izveden je zaključak koji se odnosi na celokupno problemsko područje, dok se, s druge strane, pošlo od opšteprihvaćenih teorijskih saznanja kako bi se bolje razumeli pojedinačni oblici napada. U radu je korišćena kvalitativna ekonomska analiza u cilju boljeg razumevanja uzroka i efekata napada na blokčejn sisteme.

Tabela 1 - Pregled napada 51% kroz istoriju

Oblik		Meta napada-Kriptovalute	Posledice
51% Napad	2012.	CoiledCoin	Dvostruka potrošnja
	2013.	Terracoin i Feathercoin	Dvostruka potrošnja
	2016.	Shift i Krypton	Dvostruka potrošnja
	2018.	Bitcoin gold	18 miliona dolara dvostruke potrošnje
	2018.	ZenCash	550.000 dolara dvostruke potrošnje
	2018.	Vertcoin	100.000 dolara dvostruke potrošnje
	2019.	Vertcoin	Dvostruka potrošnja
	2020.	Ethereum Classic - kroz tri napada	Prvim napadom reorganizovano je 3.693 bloka, drugim 4.000 blokova i trećim 7.000 blokova
	2020.	Bitcoin gold	70.000 dolara dvostruke potrošnje
	2021.	Verge	Reorganizovano je više od 560.000 blokova i procenjeni iznos krađe je 1,7 miliona dolara
	2021.	Firo (ranije poznat kao Zcoin)	Reorganizacija blockchaina i dvostruka potrošnja

Izvor: Pregled autora

Tabelom 1 prikazani su neki od napada 51% u period od 2012. do 2021. godine. 51% napad je bio izuzetno redak pre 2018. godine, neki od napada jesu bili CoiledCoin 2012. godine, Terracoin i Feathercoin u 2013. godini, kao i mali projekti Shift i Krypton 2016. godine (Shanaev et al., 2019, 69). Štete koje su nastale ovim napadima su manjih vrednosti od onih koje se pojavljuju kasnije. Nakon 2018. godine, broj ovih napada se povećava. Neki od njih jesu napadi na Bitcoin gold, ZenCash, Bitcoin SV, Vertcoin, Ethereum Classic, Verge, Firo (Zcoin).

Kao napadi nakon 2018. godine mogu se navesti napadi na Bitcoin gold. Informacije koje govore o ovim napadima (Redman, 2018; Redman, 2020) prikazuju da je Bitcoin gold (BTG) sistem maja 2018. godine pretrpeo ovaj vid napada. Napad je doveo do ukupnog gubitka od 388.000 BTG (18 miliona dolara). Ponovni napad izvršen je januara 2020. godine. U ovom napadu uklonjeno je 29 blokova kroz blokčejn reorganizaciju, odnosno, prvo je uklonjeno 14 blokova i dodato novih 13, dok je drugog dana uklonjeno 15 i dodato 16 blokova. Ovi napadi uticali su na dvostruko trošenje BTG kriptovalute, odnosno potrošeno je više od 7.000 BTG (70.000 dolara) za dva dana. Nedostatak heš snage iza BTG mreže čini blokčejn izuzetno ranjivim na 51% napade. Rešenje za ovo vidi se u promeni algoritma konsenzusa čime bi se poboljšala sigurnost sistema. Nakon izvršenog napada, cena Bitcoin gold-a su porasle za 9%, što je suprotno od očekivanog.

Napad 51% izvršen je juna 2018. godine na ZenCash mrežu (Hrones, 2018; Avan-Nomayo, 2018). Ovim napadom izazvan je gubitak koji se procenjuje na 550.000 dolara, kroz dve transakcije. Napadač je reogranizovao lanac blokova nekoliko puta, odnosno napadom je obuhvaćeno oko 110 blokova, a što je trajalo manje od četiri sata. Procenjuje se da je napadač potrošio oko 30.000 dolara da bi izvršio ovaj napad. Iznos koji je potrošen odnosi se na troškove električne energije i troškove održavanja opreme potrebne za rudarenje (Molchan, 2018).

Mreža Vertcoin je takođe bila meta napada 51% u dva navrata 2018. i 2019. godine (Redman, 2019). Tokom prvog napada reorganizovano je 300 blokova od strane napadača, što je izazvalo 100.000 dolara duple potrošnje. Nakon ovog napada usledila je revizija algoritma po kome je mreža funkcionisala. Tokom drugog napada, iz lanca je uklonjeno 603 bloka i zamenjeno sa 553 napadačkih blokova. U slučaju drugog napada, izvršioci nisu imali značajne koristi od napada, pa se pretpostavlja da cilj nije bio zarada, već dokazivanje slabosti samog sistema.

Primer napada 51% jeste i Ethereum Classic - ETC (Voell, 2020a). Na ovaj sistem napadi su izvršeni tokom avgusta 2020. godine tri puta. Prvim napadom reorganizovano je 3.693 bloka, drugim napadom reorganizovano je 4.000 blokova, dok je trećim reorganizovano 7.000 blokova. Kod ovih napada, čini se da kriptovaluta nije pogođena u velikoj meri, odnosno cena nakon svih napada bila je 6,86 dolara, dok se tokom avgusta kretala u rasponu od 6 do 8 dolara. Nakon izvršenih napada, aktivnosti koje su preduzete da bi se sprečili ponovni napadi pre svega su usmerene na povećani monitoring i promenu algoritma. U slučaju prvog napada izvršena je dupla potrošnja u iznosu od 5,6 miliona dolara (Foxley, 2020). Kod drugog napada, napadač je pokušao da udvostruči 465.444 ETC, u vrednosti od približno 3,3 miliona dolara, ali je uspešno udvostručio 238.306 ETC u vrednosti od približno 1,68 miliona dolara (Voell, 2020b).

Još jedna od mreža kriptovaluta koja je bila pogođena napadom 51% jeste Verge (Redman, 2021). Sam napad dogodio se 2021. godine, a rezultirao je krađom od 1,7 miliona dolara. Smatra se da je ovo jedna od najdubljih reogranizacija lanca blokova koja se dogodila, odnosno reorganizovano je više od 560 hiljada blokova. Činjenica koja Verge mrežu čini podložnijom napadima jeste niža cena potrebna za postizanje 51% moći napadača u odnosu na druge blokčejn sisteme. Razlog niže cene za postizanje većinske moći napadača jeste manja potrebna brzina rudarenja (hashrate) u odnosu na jače sisteme kao što je, na primer, Bitcoin.

Kako je objavljeno (Garg, 2021) Firo, ranije poznat kao Zcoin je bio predmet napada 51% januara 2021. godine. Navodi se da osnovni motivi napada nisu finansijski, već je cilj bio narušiti reputaciju sistema. Napad je otkriven kada su ranije potvrđene transakcije postale nepotvrđene. Takvo stanje bilo je rezultat reorganizacije blokčejna od strane napadača, a što je dotaklo 306 ranijih blokova.

Zajedničko za sve pomenute slučajeve napada 51% jeste da su napadači iznajmljivali brzinu rudarenja (hashrate). Time je jačana njihova moć u odnosu na poštene učesnike sistema i omogućavalo se izvršenje napada. Brzina rudarenja predstavlja broj hešova koji se izračunaju u sekundi, pri čemu izolovanost više od 50% brzine rudarenja mreže stvara mogućnost napada 51% (Kausar et al., 2022, 4302). Kao strana koja je iznajmljivala snagu za rudarenje kriptovaluta kod većine napada navodi se platforma NiceHash. U slučaju napada 51%, napadači manipulišu vremenskim oznakama i proizvode blokove, pri čemu zarađuju na nagradama za rudarenje. U takvim situacijama napadači mogu kombinovati prethodne aktivnosti sa napadom dvostruke potrošnje da bi ostvarili veće koristi. Veličina blokčejna može biti prepreka za napad 51%, odnosno, manji blokčejn sistemi su podložniji ovom obliku napada. Napad na velike mreže iziskivao bi visoke iznose novčanih sredstava, što bi predstavljalo prepreku zlonamernim učesnicima, ili s druge strane ne bi obezbedio željene rezultate za napadače. Takođe, glavna prepreka ovom obliku napada mogu biti troškovi električne energije i troškovi održavanja hardvera (Avan-Nomayo, 2018). Utvrđeno je da je indikator rizika od pojave napada 51% veća koncentracija heš snage kod malog broja učesnika, kao i da postoji određeni obrazac ponašanja učesnika koji žele ovakav napad da sprovedu (Aponte-Novoa et al., 2021). Takođe, ukoliko se utvrdi namera za dvostrukom potrošnjom, pošteni učesnici će odbiti lanac blokova napadača, uspostaviće se okruženje bez dvostruke potrošnje i sprečiti sveukupni napad 51% (Babur et al., 2024).

Tabela 2 - Pregled ostalih napada na blokčejn sisteme kroz istoriju

Oblik napada	Godina	Meta napada-Kriptovalute	Posledice
DdoS napad	2021.	Arbitrum	Smanjenje brzine transakcija, smanjenje poverenja
	2021.	Solana	Privremeni zastoj mreže, smanjenje poverenja
Selfish mining napad	2018.	Minacoin	Šteta od 90.000 dolara
Sybil napada	2020.	Monero	Privremeno usporavanje transakcija

Izvor: Pregled autora

U Tabeli 2 prikazani su ranije izvršeni napadi DdoS, Selfish mining i Sybil. Tokom 2021. godine dogodila su se dva DdoS napada na blokčejn sisteme Arbitrum i Solana (Muchoki, 2021). U slučaju sistema Arbitrum, tokom napada, sekvencer je bio preplavljen transakcijama i bio je van mreže 45 minuta zbog preopterećenosti. Sekvencer je čvor koji ima ulogu da prima transakcije i razvrstava ih u red za uključivanje u blokčejn lanac. U ovoj situaciji, sve druge transakcije su bile ostavljene na čekanje dok se mreža ne oporavi, odnosno nove transakcije nisu uključivane i blokčejn sistem nije rastao kroz kreiranje novih blokova. Napad na sistem Solana izvršen je puštanjem 400.000 transakcija u sekundi, čime je sistem bio preplavljen, a što je otežalo njegovo dalje funkcionisanje. Sistem je bio blokiran satima, a napad je završen tek nakon ponovnog pokretanja celog sistema od strane programera. Posledice ovog napada jesu smanjenje poverenja u blokčejn sistem. Jedan od glavnih razloga za sprovođenje DdoS napada jesu protokoli koji su dizajnirani tako da ne uzimaju u obzir bezbednosna pitanja (Chaganti et al., 2022). A kao predlozi za zaštitu od ove vrste napada navodi se decentralizacija, kao i praćenje i pamćenje IP adrese napadača (Ibrahim et al., 2022).

Selfish mining napad izvršen je maja 2018. godine na Minacoin kriptovalutu (Gutteridge, 2018). Napadač je uspešno rudario i nadograđivao blokčejn sistem novim blokovima, a te informacije nisu bile dostupne ostalim rudarima. Napadač je stvorio novu granu lanca pre nego što je napad otkriven. Kako u blokčejn sistemima lanac sa najviše blokova ima veću snagu, poništavaju se svi blokovi drugih rudara. Napadač je u ovom slučaju pokušao da zameni stečenu kriptovalutu za druge valute pre nego što njegov tajni lanac bude otkriven. Izvršilac napada je imao dovoljno računarske snage da preuzme čak 57% brzine rudarenja (hashrate). Procenjeni iznos štete na blokčejn mreži kao posledica ovog napada iznosi 90.000 dolara. U jednom istraživanju (Zhou et al., 2023) navode se dve strategije koje treba da destimulišu nepoštene napadače i povećaju otpornost sistema na ovu vrstu napada, a to su povećanje poteškoća u rudarenju kada se otkrije nepošteno rudarenje i ograničavanje stope prihvatanja kada se istovremeno emituje veći broj blokova. Selfish mining napad prouzrokuje gubitak rudarske moći poštenih učesnika, a što kreira velike bezbednosne izazove u blokčejn sistemu na kome je napad izvršen (Wang et al., 2021).

Monero je bio predmet Sybil napada 2020. godine, ali ovaj napad nije imao značajnije posledice. Navodi se da je napadač pokušao da dobije informacije o učesnicima blokčejn sistema (Chipolina, 2020). Naime, napadač je pokušao da poveže transakcije sa IP adresom učesnika u sistemu, čime bi ugrozio njihovu privatnost. Napadač je namerno odbacivao određene transakcije, čime su one bile

neuspešne u samom sistemu. Zaključak je da ovaj napad nije bio dovoljno snažan da bi zadao veliki udarac Monero blokčejn sistemu. Sybil napad može narušiti kredibilitet sistema nad kojim se napad vrši, a prepoznavanje realnih identiteta zlonamernih učesnika, odnosno verifikacija njihovih indentiteta može sprečiti započinjanje ovakvog napada (Ul Haq i Saqlain, 2023).

Zaključna razmatranja

Prethodno navedena razmatranja u radu ukazuju na način funkcionisanja blokčejn sistema i osnovne postulate na kojima se ovi sistemi zasnivaju. Blokčejn sistemi su i dalje u razvoju i može se reći da je prisutna viša zainteresovanost za razumevanje osnovne svrhe blokčejna, ali i za moguće potencijalne koristi koje ovakvi sistemi donose. Blokčejn sistemi danas su svakako rasprostranjeniji nego na početku, ali može se reći da će se njihova primena tek proširiti, odnosno prepoznaje se veliki potencijal blokčejn tehnologije. Konsenzus kao značajna odlika svakog blokčejn sistema bitno utiče na donošenje odluka i samo kreiranje lanca blokova. Može se zaključiti, na osnovu teorijskih tvrdnji, da će u redovnim okolnostima, kod donošenja odluka, pošteni učesnici blokčejn sistema preovladati zlonamerne učesnike i samim tim neadekvatne transakcije neće biti prihvaćene i uključene u blokove sistema.

Blokčejn sistemi posmatrano kroz istoriju bili su više puta predmet napada, a ovi napadi su se vršili na različite načine. Kroz vreme broj napada se povećavao, i može se reći da je jačina tih napada rasla. Treba napomenuti da je napade lakše bilo izvršiti na sisteme koji su manji i kod kojih je napadačima bilo potrebno manje računarske snage kako bi sproveli svoje zlonamerne akcije. Najčešći oblik napada koji se u javnosti objašnjava jeste napad 51%. Najpoznatiji napadi ove vrste jesu napadi na Bitcoin gold i Ethereum Classic. Kod njih, zlonamerni učesnici su dobili većinsku snagu, time bitno uticali na transakcije i kreiranje blokova u sistemu. Napadi ove vrste su najčešće kombinovani sa napadom dvostruke potrošnje. Njihov cilj bio je prisvajanje sredstava, a iznosi su bili više hiljada dolara.

Na osnovu posmatranih istorijskih napada na blokčejn sisteme može se dati odgovor na postavljeno istraživačko pitanje, odnosno napadi na blokčejn sisteme nisu dugoročno uticali na njihovu stabilnost. Iz primera posmatranih istorijskih napada, može se zaključiti da su oni uticali na privremenu promenu cena kriptovaluta i nepoverenje u iste. Pored toga, izvršene zloupotrebe nisu imale dugoročnije posledice na postojanje kriptovaluta i funkcionisanje blokčejn sistema. Nakon završetka svakog od analiziranih napada funkcionisanje blokčejn sistema se vraćalo u redovno stanje, uz napore za poboljšanja i buduća usavršavanja u njihovom radu. Prisutni napori za unapređenje blokčejn sistema pre svega se odnose na promenu algoritma.

Osnovni doprinos rada ogleda se u celovitom prikazu različitih teorijskih osnova za posmatrano problemsko područje. Predstavljeni su različiti napadi koji su pogodili blokčejn sisteme u prošlosti. Iznete činjenice mogu ukazati na bitnost blokčejn sistema, ali i moguće značajne posledice napada na ove sisteme. Osnovna ograničenja rada odnose se na broj i vrste posmatranih napada na blokčejn sisteme. Različiti načini napada su otkriveni, odnosno različiti pristupi napadača kod zlonamernih akcija na blokčejn sisteme. Rad se bavi pojedinim oblicima napada, kao što su napad 51%, DdoS napad i slično. Da bi se stekla šira slika i izveli obuhvatniji zaključci o jačini i posledicama napada potrebno je posmatrati više njih. U skladu sa prirodom i karakteristikama blokčejn tehnologije i karakteristikama napada, ograničenje sprovedenog istraživanja jeste i nemogućnost involviranja svih aspekata posmatranih zloupotreba i napada. Takođe, manjkavost sprovedene analize jeste i nedostatak i nedostupnost svih podataka, odnosno, zbog prirode blokčejna, politike privatnosti i ostalih skrivenih podataka u istraživan-

je nisu mogli biti uključeni svi aspekti koji bi omogućili izvođenje sveobuhvatnijih zaključaka. Buduća istraživanja mogla bi obuhvatiti veći broj različitih pristupa napadima na blokčejn sisteme. Ovo bi omogućilo komparaciju posledica koje zlonamerni pojedinci izazovu svojim prodiranjem u blokčejn sisteme. Kako se napadi na blokčejn sisteme kontinuirano razvijaju, predmet budućih istraživanja mogu biti novi oblici napada, odnosno oni napadi koji su najučestaliji u proteklom period, ili oni koji su se po prvi put pojavili. Dodatno, značajno područje istraživanja mogu biti i tehnike i instrumenti za zaštitu od napada na blokčejn sisteme, odnosno koji su to načini i koje mehanizme treba razviti kako bi se napadi onemogućili ili bar učinili slabijim. Postavlja se pitanje da li su odbrambeni mehanizmi univerzalni za svaki oblik napada ili postoje određene razlike. Značajno pitanje jeste i prilagođavanje zakonodavstva i regulative u oblasti kriptovaluta i blokčejn tehnologije, kao i identifikovanje i sankcionisanje napadača na blokčejn sisteme.

Reference

1. Aggarwal, S. & Kumar, N. (2021). Attacks on blockchain. Advances in Computers, 121, 399-410

2. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. & Amaba, B. (2017). Blockchain technology innovations. 2017 IEEE technology & engineering management conference (TEMSCON). 137-141.

3. Alihodžić, A. (2023). Volatilnost bitkoina i rizičnost finansijskog portfolija. Bankarstvo, 52(2-3), 128-165.

4. Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R. & Wightman, P. (2021). The 51% attack on blockchains: A mining behavior study. IEEE access, 9, Doi: 10.1109/ACCESS.2021.3119291

5. Avan-Nomayo, O. (2018). 51% Attack: ZenCash the Latest Victim of a Suspected Double-Spend Attack. EWN. Pristupano: Februar 2022. Preuzeto sa: https://ethereumworldnews.com/51-attack-zencash-the-latest-victim-of-a-suspected-double-spend-attack/

6. Babur, S. M., Khan, S. U. R., Yang, J., Chen, Y. L., Ku, C. S. & Por, L. Y. (2024). Preventing 51% Attack By Using Consecutive Block Limits In Bitcoin. IEEE Access, Doi: 10.1109/ACCESS.2024.3407521

7. Belotti, M., Kirati, S. & Secci, S. (2018). Bitcoin pool-hopping detection. IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), 1-6.

8. Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N. & Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, 8, 79764-79800.

9. Bolanča, A., Pavlović, D. & Šijanović Pavlović, S. (2018). „Internet of Things" i „Blockchain" kao alati razvoja fleksigurnog energetskog sektora. Nafta i Plin, 38(153), 107-117.

10. Cachin, C. & Vukolić, M. (2017). Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873, 1-23.

11. Chaganti, R., Boppana, R., Ravi, V., Munir, K., Almutairi, M., Rustam, F., Lee, E. & Ashraf, I. (2022). A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. IEEE Access, 10, 96538-96555.

12. Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M. & Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. High-Confidence Computing, 2(2), 1-21.

13. Chipolina, S. (2020). Monero Hit by Sybil Attack from 'Incompetent Attacker'. Decrypt. Pristupano: Februar 2022. Preuzeto sa: https://decrypt.co/47798/malicious-nodes-attempt-sybil-attack-on-monero

14. Conti, M., Kumar, E. S., Lal, C. & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452.

15. Dai, H. N., Zheng, Z. & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094.

16. Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C. & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7), 1366-1385.

17. Fan, C., Ghaemi, S., Khazaei, H. & Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. IEEE Access, 8, 126927-126950.

18. Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A. & Colman, A. (2020). Blockchain consensus algorithms: A survey. arXiv preprint arXiv:2001.07091, 1-39.

19. Foxley, W. (2020). Ethereum Classic's Terrible, Horrible, No Good, Very Bad Week. CoinDesk. Pristupano: Februar 2022. Preuzeto sa: https://www.coindesk.com/tech/2020/08/10/ethereum-classics-terrible-horrible-no-good-very-bad-week/

20. Frankenfield, J. (2022). Hash. Invenstopedia. Pristupano: Februar 2022. Preuzeto sa: https://www.investopedia.com/terms/h/hash.asp

21. Garg, D. (2021). Is Firo (Zcoin) Completely Resistant to 51% Attacks Now?. Altcoinbuzz. Pristupano: Februar 2022. Preuzeto sa: https://www.altcoinbuzz.io/cryptocurrency-news/product-release/is-firo-zcoin-completely-resistant-to-51-attacks-now/

22. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. & Santamaria, V. (2018). To blockchain or not to blockchain: That is the question. It Professional, 20(2), 62-74.

23. Gkritsi, E. (2021). BSV Suffers 51% Attack: Report. CoinDesk. Pristupano: Februar 2022. Preuzeto sa: https://www.coindesk.com/markets/2021/08/04/bsv-suffers-51-attack-report/

24. Gutteridge, D. (2018). Japanese Cryptocurrency Monacoin Hit by Selfish Mining Attack. CCN. Pristupano: Februar 2022. Preuzeto sa: https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack/

25. Hadžić, M. & Nedeljković, N. (2018). Mogućnost primene blockchain tehnologije na tržištima kapitala. Sinteza 2018 - International Scientific Conference on Information Technology and Data Related Research, 153-159.

26. Hrones, M. (2018). ZenCash Target of 51% Attack; Loses More than $500k in Double Spend Transactions. Bitcoinist. Pristupano: Februar 2022. Preuzeto sa: https://bitcoinist.com/zencash-target-51-attack-loses-500k-double-spend-transactions/

27. Ibrahim, R. F., Abu Al-Haija, Q. & Ahmad, A. (2022). DDoS attack prevention for internet of thing devices using ethereum blockchain technology. Sensors, 22(18), Doi: 10.3390/s22186806

28. Jiang, S., Li, Y., Wang, S. & Zhao, L. (2022). Blockchain competition: The tradeoff between platform stability and efficiency. European Journal of Operational Research, 296(3), 1084-1097.

29. Kearney, J. J. & Perez-Delgado, C. A. (2021). Vulnerability of blockchain technologies to quantum attacks. Array, 10, 1-10.

30. Kausar, F., Senan, F. M., Asif, H. M. & Raahemifar, K. (2022). 6G technology and taxonomy of attacks on blockchain technology. Alexandria Engineering Journal, 61(6), 4295-4306.

31. Koteska, B., Karafiloski, E. & Mishev, A. (2017). Blockchain implementation quality challenges: A literature review. 6th workshop of software quality, analysis, monitoring, improvement, and applications, SQAMIA 1-8.

32. Martić, V. (2021). Računovodstvena profesija u eri kripto valuta i globalne pandemije. Računovodstvena znanja kao činilac ekonomskog i društvenog napretka, Kragujevac: Ekonomski fakultet, 337-347.

33. Molchan, Y. (2018). ZenCash (Zen) Suffers 51 Percent Attack, Crypto Exchanges Warned. Pristupano: Februar 2022. Preuzeto sa: https://u.today/zencash-zen-suffers-51-percent-attack-crypto-exchanges-warned

34. Muchoki, S. (2021). Solana suffers network downtime, Ethereum demonstrates resilience as it shakes off attack. Crypto-news-flash. Pristupano: Februar 2022. Preuzeto sa: https://www.crypto-news-flash.com/solana-suffers-network-downtime-ethereum-demonstrates-resilience-as-it-shakes-off-attack/

35. Narayanan, K., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press

36. Nayak, K., Kumar, S., Miller, A. & Shi, E. (2016). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. 2016 IEEE European Symposium on Security and Privacy (EuroS&P), 305-320.

37. Nofer, M., Gomber, P., Hinz, O. & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187.

38. Redman, J. (2018). Bittrex to Delist Bitcoin Gold Over 51% Attack. Bitcoin.com. Pristupano: Februar 2022. Preuzeto sa: https://news.bitcoin.com/bittrex-to-delist-bitcoin-gold-over-51-attack/

39. Redman, J. (2019). Vertcoin Network Sabotaged by Another 51% Attack. Bitcoin.com. Pristupano: Februar 2022. Preuzeto sa: https://news.bitcoin.com/vertcoin-network-sabotaged-by-another-51-attack/

40. Redman, J. (2020). Bitcoin Gold 51% Attacked - Network Loses $70,000 in Double Spends. Bitcoin.com. Pristupano: Februar 2022. Preuzeto sa: https://news.bitcoin.com/bitcoin-gold-51-attacked-network-loses-70000-in-double-spends/

41. Redman, J. (2021). Privacy Coin Verge Suffers Third 51% Attack, Analysis Shows 200 Days of XVG Transactions Erased. Bitcoin.com. Pristupano: Februar 2022. Preuzeto sa: https://news.bitcoin.com/privacy-coin-verge-third-51-attack-200-days-xvg-transactions-erased/

42. Rosenfeld, M. (2011). Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 1-46.

43. Sayeed, S. & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, 9(9), 1-17.

44. Shanaev, S., Shuraeva, A., Vasenin, M. & Kuznetsov, M. (2019). Cryptocurrency value and 51% attacks: evidence from event studies. The Journal of Alternative Investments, 22(3), 65-77.

45. Shetty, S., Kamhoua, C. & Njilla, L. (2019). Blockchain for Distributed Systems Security. Wiley Blackwell

46. Singh, S. K., Salim, M. M., Cho, M., Cha, J., Pan, Y., & Park, J. H. (2019). Smart contract-based pool hopping attack prevention for blockchain networks. Symmetry, 11(7), 1-19.

47. Sredojević, S. (2018). Savremena uloga i značaj profesionalnih kvalifikacija u sektoru bankarstva. Bankarstvo, 47(1), 82-97.

48. Tomić, N. (2020). Measuring the effects of Bitcoin forks on selected cryptocurrencies using event study methodology. Industrija, 48(2), 21-36.

49. Tomić, N. (2021). A review of consensus protocols in permissioned blockchains. Journal of Computer Science Research, 3(2), 32-39.

50. Tomić, N. & Todorović, V. (2020). Potential negative implications of Libra cryptocurrency. Ekonomika, 66(1), 13-24.

51. Tomić, N., Todorović, V. & Čakajac, B. (2020a). The potential effects of cryptocurrencies on monetary policy. The European Journal of Applied Economics, 17(1), 37-48.

52. Tomić, N., Todorović, V. & Jakšić, M. (2020b). A survey on consensus protocols in permissionless blockchains. Contemporary Issues in Economics, Business and Management – EBM 2020, Kragujevac: Faculty of economics University of Kragujevac, 365-374.

53. Ul Haq, H. B. & Saqlain, M. (2023). An implementation of effective machine learning approaches to perform sybil attack detection (SAD) in IoT network. Theoretical and applied computational intelligence, 1(1), 1-14.

54. Voell, Z. (2020a). Ethereum Classic Hit by Third 51% Attack in a Month. CoinDesk. Pristupano: Februar 2022. Preuzeto sa: https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/

55. Voell, Z. (2020b). Ethereum Classic Attacker Successfully Double-Spends $1.68M in Second Attack: Report. CoinDesk. Pristupano: Februar 2022. Preuzeto sa: https://www.coindesk.com/markets/2020/08/07/ethereum-classic-attacker-successfully-double-spends-168m-in-second-attack-report/

56. Vokerla, R. R., Shanmugam, B., Azam, S., Karim, A., De Boer, F., Jonkman, M. & Faisal, F. (2019). An overview of blockchain applications and attacks. 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 1-6.

57. Yves-Christian, A. E., Hammi, B., Serhrouchni, A. & Labiod, H. (2018). Total eclipse: How to completely isolate a bitcoin peer. Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), 1-7.

58. Wang, Z., Lv, Q., Lu, Z., Wang, Y., & Yue, S. (2021). ForkDec: accurate detection for selfish mining attacks. Security and Communication Networks, 2021, Doi: 10.1155/2021/5959698

59. Zheng, Z., Xie, S., Dai, H. N., Chen, X. & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

60. Zhou, C., Xing, L., Liu, Q. & Wang, H. (2023). Effective selfish mining defense strategies to improve bitcoin dependability. Applied Sciences, 13(1), Doi: 0.3390/app13010422

61. Academy.binance.com, https://academy.binance.com/en/articles/what-is-an-eclipse-attack, Pristupano: Februar 2022.

Scientific review article

Bankarstvo, 2025, vol. 54, br. 1

DOI: 10.5937/bankarstvo2501106R

Reveived: 22.11.2024
Accepted: 24.01.2025

ABUSES AND ATTACKS ON BLOCKCHAIN SYSTEMS

Aleksandra Radojević, research associate, Faculty of Economics, University of Kragujevac
email: aleksandra.radojevic@ekonomski.org
ORCID: https://orcid.org/0000-0001-8000-9248

Predrag Stanković, research associate, Faculty of Economics, University of Kragujevac
email: predrag.stankovic@ef.kg.ac.rs
ORCID: https://orcid.org/0009-0004-6657-6544

Abstract

Blockchain systems are ever more ubiquitous in all business sectors, but the primary user of these technologies is the financial industry. This paper aims to explore attacks on blockchain systems, specifically determining the intensity of these attacks in the past and the extent of their consequences. Throughout history, the types and methods of attacks on blockchain systems have evolved, and with that, the intensity of these attacks has increased. The results of attacks on blockchain systems are short-term instabilities that cause changes in cryptocurrency prices and a decrease in trust in them, but in the long term, attacks and abuses do not have a strong impact. In fact, there is an improvement of these systems after the attacks and abuses. The research shows that the most common type of attack is the 51% attack. The primary aim of the abuses was the misappropriation of funds, but also proving the weakness of the system on which the attacks were carried out.

Keywords: blockchain systems, cryptocurrencies, abuses and attacks, financial sector, attack 51%.

JEL classification: O33, L86, D85.

Introduction

The development trends worldwide, above all the strengthening and indispensable implementation of information and communication technologies, have significantly impacted all spheres of business and life. Blockchain technologies are attracting a lot of attention and driving an increasing number of projects in various industries, however, the financial industry is considered the primary user of the blockchain concept (Nofer et al., 2017, 183). In the financial services sector, continuous development is essential, along with the development of business and organizational processes, as well as new products and instruments (Sredojević, 2018, 84). The digital world is being improved, through blockchain, by introducing a new perspective on security, resilience and system efficiency (Ahram et al., 2017, 137) and represents a new, revolutionary technology. The mentioned system consists of a series of blocks that are interconnected, with no central institution responsible for controlling or connecting all other participants in the system. Blockchain technology is the basis of cryptocurrencies, based on a decentralized computer network. An important characteristic of blockchain system is consensus, that is, through the consensus protocol, transactions are validated, and blocks are added to the chain.

In recent years, cryptocurrencies have attracted the attention of investors in financial markets worldwide, and the area of cryptocurrencies, or virtual currencies in payment systems, is rapidly expanding (Alihodžić, 2023, 129). Over time, investing in cryptocurrencies has yielded extremely high rates of return, accompanied by high risk, with no guarantees and no investor protection (Tomić, 2020, 22-23). The potential of blockchain-based cryptocurrencies attracts a large number of investors, as well as malicious individuals. The development of the blockchain system, as well as trust in such a system, can be damaged due to attacks directed at it. There are numerous forms of attacks and methods by which attackers want to access blockchain systems in order to gain benefits.

The subject of research in this paper is different forms of attacks on blockchain systems. As relatively young systems with great potential for growing applications in the future, blockchain systems are exposed to numerous types of attack. In accordance with the defined research subject, the aim of the paper is to draw a conclusion about the size and intensity of historical attacks on blockchain systems. The effects of different forms of attacks, their consequences, but also the possibility of repeated attacks will be analyzed. Additionally, the paper will identify which forms of attacks on blockchain systems are the most frequent. In accordance with the defined subject and aim of the research, the paper will start from the following research question: *Did attacks on blockchain systems have a long-term impact on their stability?*

Basic Characteristics of Blockchain Systems

A blockchain system represents a chain of transactions that does not allow users to modify or delete previously entered data. Blockchain can be defined as a distributed database or public ledger of all transactions or digital activities that have been realized or shared between participants (Martić, 2021, 337-338). The mentioned database, in the case of cryptocurrencies, refers to the ledger of all transactions, meaning it contains a list of all participants and the amounts of coins they hold (Tomić & Todorović, 2020, 16). The chain is maintained by a network of nodes, which verify the validity of transactions and add them to new blocks in a process known as mining (Gatteschi et al., 2018, 63). If a majority of participants (nodes) in the network agree on the validity of the transactions in the block and the validity of the block itself through a consensus mechanism, the block can be added to the chain (Nofer et al., 2017, 184). Koteska et al. (2017, 3) explain that when a new block is created, it is broadcast to the

network, then all nodes receive the block, verify the block and all transactions in it. If the block is valid, all nodes add it as the next block in their local blockchain.

Blocks in the chain actually represent entries that contain information about completed transactions. The blockchain system is continuously increasing based on the transactions being carried out. Each new transaction that appears must be reconciled with the existing information in the system. If the transaction is valid and participants confirm it, a new state in the system is created.

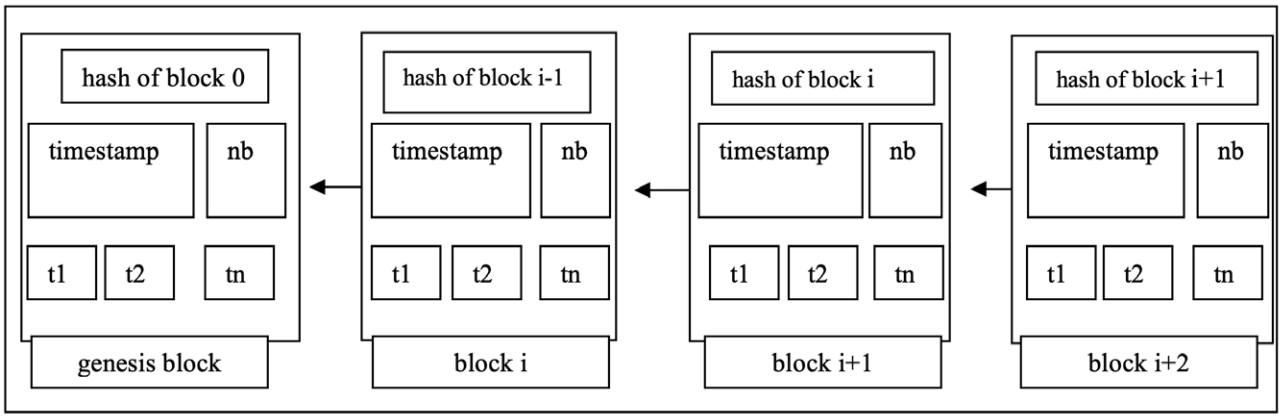
Blockchain is the technological basis of cryptocurrencies, i.e. it is a technology that has proven to be excellent in preserving large databases, as it simultaneously allows mass access and prevents malicious attacks (Tomić et al., 2020a, 41). The most significant advantages of blockchain technology in business are the costs reduction, transaction settlement speed, data verification speed and capabilities, data protection, the possibility to verify end-user and transaction reliability (Hadžić & Nedeljković, 2018, 153). Compared to conventional, centralized solutions, blockchain, which is characterized by decentralization, offers several significant advantages such as immutability, enhanced security, fault tolerance, and transparency (Fan et al., 2020, 126927).

The efficiency of the blockchain system is based on three elements - a decentralized network, consensus and cryptography (Shetty et al., 2019, 5). The functioning of a blockchain system implies the absence of a central authority and the need to reach a consensus for transaction validation and adding blocks to the blockchain. Additionally, cryptography ensures security in the functioning of the blockchain system. The two components of a blockchain system are the consensus protocol and the transaction mechanism (Kearney & Perez-Delgado, 2021, 2).

The consensus protocol refers to making decisions about adding blocks to the system and their validation. The transaction mechanism involves the method by which information is transmitted within the system. Hadžić and Nedeljković (2018, 154) summarize the basic characteristics of blockchain technology important for business implementation as follows: distributed data; the ability for all participants to conduct transactions through direct communication, which are mutually validated on the chain; anonymity; immutability of records; the ability to embed computational logic and program the execution of events or transactions within the chain structure, which are carried out upon meeting specified conditions and become instantly verified – "smart contracts". Blockchain technology enables digital information to be distributed among all participants, with each participant maintaining their own copy of all relevant information (Bolanča et al., 2018, 112). Each participant has access to the entire database, and there is no central place where data is stored, nor is there a need for a central institution to mediate and control transactions. Transactions recorded in the blockchain system are public to participants.

Figure 1 illustrates a blockchain consisting of a sequence of blocks. From Figure 1, it can be seen that each new block contains the hash of the previous block, a timestamp, and multiple transactions (from t1 to tn), as well as a random number for hash verification (nb). A hash function is mathematical function that can be efficiently calculated and transforms an input message of any size into an output message of a fixed size (Narayanan et al., 2016, 23). Using an output, fixed size increases the security of the blockchain system, i.e. attempting to decrypt the hash value based on the output size alone will not reveal the input size (Frankenfield, 2022). In fact, the hash cannot be used to obtain input data, but only to check its validity.

Figure 1 – The Blockchain System and a Sequence of Blocks



Source: Zheng et al., 2018, 355

Each block, except for the first block in the blockchain system, points to its immediately preceding block (called parent block) via a reference that is essentially the hash value of the parent block (Dai et al., 2019, 8078). Hash values are unique, and fraud can be effectively prevented since block changes in the chain would immediately change the corresponding hash value (Nofer et al., 2017, 184). A complex validation mechanism makes it almost impossible for a node to control the majority of the network, moreover, the fact that each validated block contains a reference to the previous block (secured using cryptography methods) prevents malicious modifications of recorded transactions (Gatteschi et al., 2018, 64).

Consensus Protocols in Blockchain Systems

It can be said that the development of consensus protocols is similar to the engineering of cryptographic systems and that blockchain developers should consider the established experience in cryptography, security, and distributed systems theory to building trust-based systems (Cachin & Vukolić, 2017, 20). A key characteristic of a blockchain system is that nodes do not trust each other, with some potentially behaving inappropriately (Dinh et al., 2018, 1368). In line with this possibility, there is a need for consensus. To maintain the integrity of the system, data must be confirmed and accepted by the majority of users, if not all, which means that every blockchain must have an embedded consensus protocol (Tomić et al., 2020b, 366). Consensus is a protocol in the blockchain network, which specifies the temporal validity and rules that must be followed by all participants to perform various tasks or associated transactions in the blockchain network (Bodkhe et al., 2020, 79772). Therefore, the very existence of a consensus enables blockchain system members to work as a group and to pursue a common goal, even in the presence of malicious participants.

The consensus is in line with the decentralization of the blockchain system, that is, it removes the need for a central institution that would guarantee the validity of transactions and maintain the security of the blockchain system. Narayanan et al. (2016, 54) explain how consensus is actually reached. According to them, at regular intervals, such as every 10 minutes, each node in the system proposes its own set of transactions as the next block. Then the nodes execute a consensus protocol, where each node's

input is its own proposed block. Some nodes may be malicious and may put invalid transactions in their blocks, but in such a situation it should be considered that other nodes will be honest. If the consensus protocol succeeds, a valid block will be chosen as the output. Even if the chosen block was proposed by just one node, it is a valid output as long as the block is valid. If there is a valid unexecuted transaction that was not included in the block, it can simply wait and be included in the next block

The two main types of blockchain systems are permissionless blockchains and permissioned blockchains (Dinh et al., 2018, 1366). In the first case, the state of the blockchain and its transactions, along with the stored data, is transparent and accessible to everyone, while in the case of permissioned blockchains, only authorized entities are allowed to participate in activities within the blockchain (Ferdous et al., 2020, 5). In line with the previously mentioned classification of blockchain systems, there are several consensus protocols. Some of the protocols applied in permissioned blockchain systems are: Paxos, Raft, Proof-of-authority, Practical Byzantine Fault Tolerance, Delegated Byzantine fault tolerance and Federated Byzantine Fault Tolerance (Tomić, 2021). On the other hand, the protocols applied in permissionless blockchain systems are: Proof-of-Work, Proof-of-Stake, Proof-of-Burn, Proof-of-Capacity, Proof-of-Importance, Proof-of-Activity (Tomić et al., 2020b). It can be said that the Proof-of-Work consensus protocol is the most frequently mentioned, but also the most frequently applied one. This consensus algorithm is used in the most famous cryptocurrency - Bitcoin.

Attacks on Blokchain Systems

Along with all the advantages associated with blockchain systems, there are also certain shortcomings that arise in connection with them. When there are flaws in blockchain systems, there is a possibility for attacks and abuses in them. Blockchain is a platform aimed at ensuring security and safety, while minimizing exposure to malicious attacks (Jiang et al., 2022, 1087).

In one of the research (Chen et al., 2022, 5-6), which deals with the topic of attacks on blockchain systems, it is stated that there are three forms of attack: the attack of consensus protocol, the attack of the middle protocol, and the attack of application service. In an attack of consensus protocol, the attacker's goal is to achieve additional income through involvement in the blockchain consensus results. Within this group of attacks, some of the methods include: block withholding attack, 51% attack, pool hopping attack, selfish mining attack and FAW attack. An attack of the middle protocol involves the attacker's influence on node communication and smart contracts. In the case of attacks on the communication of nodes, the methods are: DdoS attack, Eclipse attack and Sybil attack, while in the case of attacks on smart contracts, a reentrancy attack can be mentioned. An attack of application service involves the attacker's behavior that targets the user's privacy. The attack methods in this case are: identity privacy and transaction information attacks.

Attacks on blockchain systems are classified into two groups in one of the studies (Kausar et al., 2022, 4301): core-oriented attacks and client-oriented attacks. The group of core-oriented attacks includes the following methods: Eclipse attack, Sybil attack, DNS attack, BGP hijacking and spatial partitioning, DDoS attack, Stress testing attack, Memory pool flooding attack, block withholding attack, Finney attack, FAW attack, 51% attack, Selfish mining attack, Consensus delay and Timejacking attack. On the other hand, client-oriented attacks include wallet theft, cryptojacking attack, double spending attack, transaction malleability and liveness attack.

One of the research projects (Narayanan et al., 2016, 161) explains that, in a situation where a new block is found, the default behavior is to publish it to the network immediately. However, a *block with-*

holding attack involves deviating from that behavior and having the attacker continue to mine in the hope of finding two blocks in a row before the rest of the network finds one. So, the attacker keeps the information secret all the time.

Through a *51% attack*, attackers can create a longer chain of blocks in the system, which results in the invalidation of the blocks produced by honest participants. Sayeed and Marco-Gisbert (2019, 5-6) describe a 51% attack as an attack that occurs when the attacker possesses 51% of the hashing power. This attack begins with creating a private block chain that is completely isolated from the legitimate version of the chain. In the later stage, the isolated chain is introduced to the network in an attempt to establish it as the longest chain, and thus as the valid one. With this form of attack, it is not necessary to obtain 51% of the hashing power, that is, if the attackers get a smaller percentage of the power, the attack is possible, but with a lower probability of success.

In a *pool hopping attack*, the attacker joins the mining pool with the highest income after analyzing the income of multiple mining pools, thus increasing their own income and influencing the effective computational power within the mining pool (Chen et al., 2022, 12). In other words, pool hopping implies affiliating with a mining pool in a situation when its attractiveness is high and leaving it when it is not, i.e. redirecting computing power to another alternative (Belotti et al., 2018, 2). This means that an attacker can get more from a mining pool than their actual contribution. In one study (Rosenfeld, 2011), pool hopping is explained as a situation in which the attacker mines in one pool for a certain period and then switches to another, receiving the mining reward from the first pool. This implies that based on the actions taken, the attacker will receive a reward before leaving the first pool, even though honest miners have completed mining and found a new block after the attacker exits the given mining pool. Miners leaving one mining pool affect the reduction of its total hash power, which affects further mining in terms of reducing the success of this process (Singh et al., 2019, 1). A situation where there is a large number of participants moving from one mining pool to another is unsustainable. Any mining pool from which participants can exit in this manner will become less attractive, and when this happens, the number of participants who mine in it will decrease and it will permanently retain this status (Rosenfeld, 2011, 23).

In the case of *selfish mining attacks*, dishonest miners hide data and thereby harm other honest miners (Vokerla et al., 2019, 5). One research (Kausar et al., 2022, 4303) explains that in the case of a selfish mining attack, the attacker secretly mines new blocks and does not announce it to other system participants. Then, when the attacker's blockchain becomes longer than the one created by the honest participants, they broadcast it. This kind of attack actually invalidates the blocks of honest participants. In other words, in a situation where an attacker first mines a block, he will not broadcast that block to the chain, but when honest miners successfully mines a new block, they will also broadcast their block and cause the network to fork (Chen et al., 2022, 12). Then, since the attacker has hidden blocks, the blockchain they propose will be longer, and the chain extension will continue along the path proposed by the attacker during the fork.

DDoS is one of the most common attacks in the blockchain network used by attackers to disrupt authentic transactions allowing invalid transactions to be executed (Sayeed & Marco-Gisbert, 2019, 5). The attacker overloads the network with a large number of requests, i.e., information, which makes network resources unavailable to users, that is, which leads to a state that it does not respond to transactions (Aggarwal & Kumar, 2021, 406). In this situation, due to system congestion, the attacker can launch other types of attacks, such as, for example, a double spending attack (Shetty et al., 2019, 58).

Aggarwal and Kumar (2021, 404) describe a *Sybil attack* as a situation in which an attacker is behind multiple participants simultaneously, that is, an attacker manipulates the network and controls the entire network by creating multiple false identities. The created identities appear as legitimate participants, but in reality, an unknown attacker controls all these fake participants. Through these false identities, the attacker manages to validate inadequate transactions and add new blocks to the blockchain (Sayeed & Marco-Gisbert, 2019, 5). In this case, the attacker manages to outvote the honest participants of the network, that is, through the created false identities, the attacker gains a great influence on the blockchain system. A Sybil attack is a situation in which the attacker controls as many identities as they need to influence the consensus and cause an outcome that benefits them (Ferdous et al., 2020, 8) and for which they launched the attack. The attacker uses fake identities to communicate with honest participants, these participants then use time and resources to communicate with the attacker and do not receive valid information in time (Chen et al., 2022, 14). Thus, in the case of a Sybil attack, attackers can prevent the validation of certain transactions.

In the case of an *eclipse attack*, the attacker isolates the victim from the rest of its peers at the network level, controlling its incoming and outgoing connections (Nayak et al., 2016, 305). The attacker first affects the communication process between the target node and the surrounding honest nodes, and when the target node only connects to the malicious node, the attacker can further manipulate it and control the effective computational power of the target node (Chen et al., 2022, 14). An eclipse attack means isolation and control of the target node, which can lead to the realization of other attacks (Yves-Christian, 2018, 4), i.e. the essence of this attack is in creating the possibility to execute other types of attacks on blockchain systems (academy.binance.com). Based on the activities described, the attacker can easily execute a double-spending attack (Aggarwal & Kumar, 2021, 405), that is, based on an inadequate view of the network that the target node has, a double spending attack is enabled (Conti et al., 2018, 3431). Also, performing eclipse attacks can be used to create conditions for easier execution of attacks 51% (academy.binance.com).

When malicious actors target user privacy there are two approaches. As Chen et al. (2022, 15-16) explain, an *identity privacy attack* involves a situation in which the attacker gains information about other system participants. In this type of attack, the attacker can spoof the identity of honest participants and thereby endanger them. The same authors explain the *transaction information attack* as a situation in which malicious participants access the history of transactions, on the basis of which they gain knowledge about the behavior of the participants.

A double spending attack is a problem where the same cryptocurrency is spent twice, and to prevent this problem it is essential for the network to remain decentralized so that no single party can take control of all transactions within it (Aggarwal and Kumar, 2021, 400). A study explaining the types of blockchain attacks (Kausar et al., 2022, 4303) indicates that double spending involves using a single transaction two or more times. An example of this type of attack is a situation where person A wants to pay people X and Y with the same coin.

An Overview of Historical Attacks on Blockchain Systems

For the research conducted, the authors used previous works, academic studies, and articles that dealt with attacks on blockchain systems and focused on various cryptocurrencies. The research that examined these attacks was analyzed, and sources that provide detailed descriptions of specific types of attacks were also considered. The observed cases were categorized according to the type of attack

(51% attack, DDoS attack, and others), and their severity, attack trends, and the resulting consequences were analyzed. Systemic thinking was applied in the research, meaning that, based on the theoretical foundations of the investigated problem area, conclusions were drawn about the connection of all elements of the blockchain system. Inductive and deductive methods were also used. Starting from individual attacks, a conclusion was drawn that relates to the entire problem area, while, on the other hand, generally accepted theoretical knowledge was used to better understand individual forms of attacks. Qualitative economic analysis was employed in the study to gain a better understanding of the causes and effects of attacks on blockchain systems.

Table 1 - Overview of 51% Attacks Throughout History

Attack Type	Year	Attack Target - Cryptocurrencies	Consequences
51% attack	2012	CoiledCoin	Double spending
	2013	Terracoin and Feathercoin	Double spending
	2016	Shift and Krypton	Double spending
	2018	Bitcoin gold	18 milion dollars of double spending
	2018	ZenCash	550,000 dollars of double spending
	2018	Vertcoin	100,000 dollars of double spending
	2019	Vertcoin	Double spending
	2020	Ethereum Classic - through three attacks	The first attack reorganized 3,693 blocks, the second 4,000 blocks, and the third 7,000 blocks
	2020	Bitcoin gold	70,000 dollars of double spending
	2021	Verge	More than 560,000 blocks were reorganized, and the estimated theft amount is 1.7 million dollars
	2021	Firo (formerly known as Zcoin)	Blockchain reorganization and double spending

Source: Author's overview

Table 1 shows some of the 51% attacks that occurred between 2012 and 2021. The 51% attack was extremely rare before 2018, some of the attacks were CoiledCoin in 2012, Terracoin and Feathercoin in 2013, as well as smaller projects Shift and Krypton in 2016 (Shanaev et al., 2019, 69). The damages caused by these attacks are of smaller value compared to those that occurred later. After 2018, the number of these attacks is increasing. Some of them are attacks on Bitcoin gold, ZenCash, Bitcoin SV, Vertcoin, Ethereum Classic, Verge, Firo (Zcoin).

Attacks after 2018 include those on Bitcoin Gold. Information about these attacks (Redman, 2018; Redman, 2020) shows that the Bitcoin gold (BTG) system suffered this type of attack in May 2018. The attack resulted in a total loss of 388,000 BTG ($18 million). The attack was repeated in January 2020.

In this attack, 29 blocks were removed through blockchain reorganization, that is, first 14 blocks were removed, and 13 new ones were added, while on the second day 15 blocks were removed, and 16 blocks were added. These attacks resulted in a double spending of the BTG cryptocurrency, i.e. more than 7,000 BTG ($70,000) were spent in two days. The lack of hash power behind the BTG network makes the blockchain extremely vulnerable to 51% attacks. A solution to this issue is seen in changing the consensus algorithm, which would improve the system's security. After the attack, the price of Bitcoin Gold rose by 9%, which was contrary to expectations.

A 51% attack was carried out in June 2018 on the ZenCash network (Hrones, 2018; Avan-Nomayo, 2018). This attack resulted in a loss estimated at $550,000 through two transactions. The attacker reorganized blockchain several times, that is, the attack covered about 110 blocks, which lasted less than four hours. It is estimated that the attacker spent around $30,000 to carry out this attack. The amount spent refers to the costs of electricity and the maintenance of the mining equipment required for the attack (Molchan, 2018).

The Vertcoin network was also the target of 51% attacks on two occasions in 2018 and 2019 (Redman, 2019). During the first attack, 300 blocks were reorganised by the attackers, resulting in $100,000 worth of double spending. This attack was followed by a revision of the algorithm by which the network operated. During the second attack, 603 blocks were removed from the chain and replaced with 553 attack blocks. In the case of the second attack, the attackers did not benefit significantly from the attack, so it is assumed that the aim was not to make money, but to prove the weakness of the system itself.

An example of a 51% attack is also Ethereum Classic - ETC (Voell, 2020a). Attacks on this system were carried out three times during August 2020. The first attack reorganized 3,693 blocks, the second attack reorganized 4,000 blocks, while the third reorganized 7,000 blocks. In these attacks, the cryptocurrency was not significantly affected, the price after all the attacks was $6.86, while during August it was in the range of $6 to $8. After the attacks, measures taken to prevent further attacks focused primarily on increased monitoring and changes to the algorithm. In the case of the first attack, a double spending occurred in the amount of 5.6 million dollars (Foxley, 2020). In the second attack, the attacker attempted to double 465,444 ETC, worth approximately $3.3 million, but successfully doubled 238,306 ETC worth approximately $1.68 million (Voell, 2020b).

Another cryptocurrency network that was targeted by a 51% attack is Verge (Redman, 2021). The attack occurred in 2021 and resulted in the theft of $1.7 million. It is considered one of the deepest blockchain reorganizations to date, with more than 560,000 blocks being reorganized. The fact that makes the Verge network more vulnerable to attacks is the lower cost required to achieve 51% attacker power compared to other blockchain systems. The reason for the lower price for achieving the majority of the attacker's power is the lower required hashrate compared to stronger systems such as, for example, Bitcoin.

As reported (Garg, 2021) Firo, formerly known as Zcoin, was subject to a 51% attack in January 2021. It is stated that the main motives of the attack were not financial, but the aim was to damage the reputation of the system. The attack was discovered when previously confirmed transactions became unconfirmed. This situation was a result of a blockchain reorganization carried out by the attacker, affecting 306 blocks.

Common to all mentioned 51% attack cases is that the attackers rented the hashrate. This increased their power relative to the honest participants in the system, enabling the execution of the attack.

Hashrate represents the number of hashes calculated per second, where isolation of more than 50% of the network's hashrate creates the opportunity for a 51% attack (Kausar et al., 2022, 4302). NiceHash is frequently cited as the platform used for renting cryptocurrency mining power in many of these attacks. In the case of a 51% attack, attackers manipulate timestamps and produce blocks, thereby earning mining rewards. In such situations, attackers can combine these activities with a double spending attack to achieve greater benefits. The size of the blockchain can be a barrier to a 51% attack, that is, smaller blockchain systems are more vulnerable to this type of attack. An attack on large networks would require high amounts of financial resources, which could either discourage malicious actors or fail to yield the desired outcomes for the attackers. Also, the primary barriers to this form of attack can be cost of electricity and hardware maintenance (Avan-Nomayo, 2018). It has been established that an indicator of the risk of a 51% attack is the higher concentration of hash power among a small number of participants, as well as a certain behavioral pattern exhibited by participants intending to carry out such an attack (Aponte-Novoa et al., 2021). Additionally, if an intent for double-spending is detected, honest participants will reject the attacker's blockchain, creating an environment without double-spending and preventing the overall 51% attack (Babur et al., 2024).

Table 2 - Overview of Other Attacks on Blockchain Systems Throughout History

Attack Type	Year	Attack Target - Cryptocurrencies	Consequences
DdoS attacks	2021	Arbitrum	Reducing the speed of transactions, reducing trust
	2021	Solana	Temporary network outage, decrease in trust
Selfish mining attack	2018	Minacoin	The damage of 90,000 dollars
Sybil attack	2020	Monero	Temporary transaction delays

Source: Author's

Table 2 shows previously executed DDoS, Selfish mining and Sybil attacks. During 2021, there were two DDoS attacks on the Arbitrum and Solana blockchain systems (Muchoki, 2021). In the case of the Arbitrum system, during the attack, the sequencer was overwhelmed with transactions and was offline for 45 minutes due to overload. The sequencer is a node responsible for receiving transactions and sorting them into a queue for inclusion in the blockchain. In this situation, all other transactions were put on hold until the network recovered, that is, new transactions were not included and the blockchain did not grow through the creation of new blocks. The attack on the Solana system was carried out by flooding it with 400,000 transactions per second, which overwhelmed the system and made it difficult for it to function further. The system was blocked for hours, and the attack was only concluded after developers rebooted the entire system. The consequences of this attack are the reduction of trust in the blockchain system. One of the main reasons for conducting DDoS attacks is the existence of protocols designed without considering security issues (Chaganti et al., 2022). Proposed measures for protection against this type of attack include decentralization, as well as tracking and storing the IP addresses of attackers (Ibrahim et al., 2022).

A selfish mining attack was carried out in May 2018 on the Minacoin cryptocurrency (Gutteridge, 2018). The attacker successfully mined and upgraded the blockchain system with new blocks, and

that information was not available to other miners. The attacker created a new branch of the chain before the attack was discovered. As in blockchain systems the chain with the most blocks has more power, all blocks of other miners are invalidated. In this case, the attacker tried to exchange the mined cryptocurrency for other currencies before his secret chain was discovered. The attacker had enough computing power to take as much as 57% of the hashrate. The estimated amount of damage to the blockchain network as a result of this attack is $90,000. In one study (Zhou et al., 2023), two strategies are proposed to deter dishonest attackers and increase system resilience to this type of attack: increasing mining difficulty when dishonest mining is detected and limiting the acceptance rate when a large number of blocks are broadcast simultaneously. The selfish mining attack causes a loss of mining power for honest participants, creating significant security challenges in the blockchain system targeted by the attack (Wang et al., 2021).

Monero was subject to a Sybil attack in 2020, but this attack had no significant consequences. It is reported that the attacker tried to obtain information about the participants of the blockchain system (Chipolina, 2020). Namely, the attacker tried to connect the transactions with participants' IP addresses in the system, which would threaten their privacy. The attacker deliberately rejected certain transactions, which made them fail in the system itself. The conclusion is that this attack was not strong enough to deal a major blow to the Monero blockchain system. A Sybil attack can undermine the credibility of the system it targets, while identifying the real identities of malicious participants and verifying those identities can prevent the initiation of such an attack (Ul Haq & Saqlain, 2023).

Conclusion

The previous considerations in the paper highlight the functioning of blockchain systems and the basic postulates on which these systems are based. Blockchain systems are still in development, and it can be said that there is a greater interest in understanding the basic purpose of blockchain, but also in the possible potential benefits that such systems bring. Blockchain systems today are certainly more widespread than at the beginning, but it can be said that their application is only beginning to expand, recognizing the vast potential of blockchain technology. Consensus, as an important feature of any blockchain system, significantly affects decision-making and the creation of the chain itself. Based on theoretical assertions, it can be concluded that under regular circumstances, in decision-making processes, honest participants in the blockchain system will prevail over malicious actors, and thus, invalid transactions will not be accepted or included in the system's blocks.

Throughout history, blockchain systems have been the target of attacks numerous times, and these attacks were carried out in different ways. Over time, the number of attacks increased, and it can be said that the intensity of these attacks increased. It should be noted that it was easier to attack systems that were smaller and where attackers needed less computing power to carry out their malicious actions. The most common form of attack that in the public is the 51% attack. The most well-known examples of this type of attack are the attacks on Bitcoin Gold and Ethereum Classic. In these cases, malicious participants gained majority control, significantly affecting transactions and block creation in the system. Attacks of this type are most often combined with a double spending attack. Their aim was to seize funds, and the amounts were several thousand dollars.

Based on the observed historical attacks on blockchain systems, an answer to the research question can be provided, that is, attacks on blockchain systems did not affect their stability in the long-term. From the examples of the observed historical attacks, it can be concluded that they primarily caused

temporary fluctuations in cryptocurrency prices and a loss of trust in them. In addition, the abuses carried out did not have long-term consequences for the existence of cryptocurrencies and the functioning of the blockchain system. After the end of each of the analyzed attacks, the functioning of the blockchain system returned to its regular state, with efforts for improvements and future refinements in their operation. The ongoing efforts to enhance blockchain systems primarily relate to changes in algorithms.

The main contribution of the paper is reflected in the comprehensive presentation of various theoretical bases for the observed problem area. Different attacks that have affected blockchain systems in the past are presented. The facts presented may indicate the importance of blockchain systems, but also the possible significant consequences of attacks on these systems. The main limitations of the paper relate to the number and types of attacks on blockchain systems that were observed. Different methods of attack have been discovered, that is, different approaches of attackers in malicious actions on blockchain systems. The paper addresses specific forms of attacks, such as 51% attack, DDoS attack and other. To gain a broader perspective and draw more comprehensive conclusions regarding the strength and consequences of attacks, it is necessary to observe a greater number of attacks. In accordance with the nature and characteristics of blockchain technology and the characteristics of the attacks, a limitation of the conducted research is the inability to involve all aspects of the observed abuses and attacks. Additionally, a shortcoming of the analysis lies in the lack and unavailability of all relevant data. Due to the nature of blockchain, privacy policies, and other hidden information, it was not possible to include all aspects in the research that would enable the drawing of more comprehensive conclusions. Future research could include a larger variety of approaches to attacks on blockchain systems. This would enable a comparison of the consequences caused by malicious individuals challenge with its entry into blockchain systems. As attacks on blockchain systems continue to evolve, future research could focus on new forms of attacks, particularly those that have been most frequent in the recent period or those that have appeared for the first time. Additionally, a significant area of research could involve techniques and tools for protecting blockchain systems, specifically identifying the methods and mechanisms that should be developed to prevent or at least mitigate attacks. This raises the question of whether defensive mechanisms are universal for all types of attacks or whether there are specific differences. Another important issue is the adaptation of legislation and regulations in the field of cryptocurrencies and blockchain technology, as well as the identification and sanctioning of attackers targeting blockchain systems.

References

1. Aggarwal, S. & Kumar, N. (2021). Attacks on blockchain. Advances in Computers, 121, 399-410

2. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. & Amaba, B. (2017). Blockchain technology innovations. 2017 IEEE technology & engineering management conference (TEMSCON). 137-141.

3. Alihodžić, A. (2023). Volatilnost bitkoina i rizičnost finansijskog portfolija. Bankarstvo, 52(2-3), 128-165.

4. Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R. & Wightman, P. (2021). The 51% attack on blockchains: A mining behavior study. IEEE access, 9, Doi: 10.1109/ACCESS.2021.3119291

5. Avan-Nomayo, O. (2018). 51% Attack: ZenCash the Latest Victim of a Suspected Double-Spend Attack. EWN. Pristupano: Februar 2022. Preuzeto sa: https://ethereumworldnews.com/51-at-

tack-zencash-the-latest-victim-of-a-suspected-double-spend-attack/

6. Babur, S. M., Khan, S. U. R., Yang, J., Chen, Y. L., Ku, C. S. & Por, L. Y. (2024). Preventing 51% Attack By Using Consecutive Block Limits In Bitcoin. IEEE Access, Doi: 10.1109/ACCESS.2024.3407521

7. Belotti, M., Kirati, S. & Secci, S. (2018). Bitcoin pool-hopping detection. IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), 1-6.

8. Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N. & Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, 8, 79764-79800.

9. Bolanča, A., Pavlović, D. & Šijanović Pavlović, S. (2018). „Internet of Things" i „Blockchain" kao alati razvoja fleksigurnog energetskog sektora. Nafta i Plin, 38(153), 107-117.

10. Cachin, C. & Vukolić, M. (2017). Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873, 1-23.

11. Chaganti, R., Boppana, R., Ravi, V., Munir, K., Almutairi, M., Rustam, F., Lee, E. & Ashraf, I. (2022). A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. IEEE Access, 10, 96538-96555.

12. Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M. & Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. High-Confidence Computing, 2(2), 1-21.

13. Chipolina, S. (2020). Monero Hit by Sybil Attack from 'Incompetent Attacker'. Decrypt. Pristupano: Februar 2022. Preuzeto sa: https://decrypt.co/47798/malicious-nodes-attempt-sybil-attack-on-monero

14. Conti, M., Kumar, E. S., Lal, C. & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452.

15. Dai, H. N., Zheng, Z. & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094.

16. Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C. & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7), 1366-1385.

17. Fan, C., Ghaemi, S., Khazaei, H. & Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. IEEE Access, 8, 126927-126950.

18. Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A. & Colman, A. (2020). Blockchain consensus algorithms: A survey. arXiv preprint arXiv:2001.07091, 1-39.

19. Foxley, W. (2020). Ethereum Classic's Terrible, Horrible, No Good, Very Bad Week. CoinDesk. Pristupano: Februar 2022. Preuzeto sa: https://www.coindesk.com/tech/2020/08/10/ethereum-classics-terrible-horrible-no-good-very-bad-week/

20. Frankenfield, J. (2022). Hash. Invenstopedia. Pristupano: Februar 2022. Preuzeto sa: https://www.investopedia.com/terms/h/hash.asp

21. Garg, D. (2021). Is Firo (Zcoin) Completely Resistant to 51% Attacks Now?. Altcoinbuzz. Pristupa-

no: Februar 2022. Preuzeto sa: https://www.altcoinbuzz.io/cryptocurrency-news/product-release/is-firo-zcoin-completely-resistant-to-51-attacks-now/

22. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. & Santamaria, V. (2018). To blockchain or not to blockchain: That is the question. It Professional, 20(2), 62-74.

23. Gkritsi, E. (2021). BSV Suffers 51% Attack: Report. CoinDesk. Pristupano: Februar 2022. Preuzeto sa: https://www.coindesk.com/markets/2021/08/04/bsv-suffers-51-attack-report/

24. Gutteridge, D. (2018). Japanese Cryptocurrency Monacoin Hit by Selfish Mining Attack. CCN. Pristupano: Februar 2022. Preuzeto sa: https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack/

25. Hadžić, M. & Nedeljković, N. (2018). Mogućnost primene blockchain tehnologije na tržištima kapitala. Sinteza 2018 - International Scientific Conference on Information Technology and Data Related Research, 153-159.

26. Hrones, M. (2018). ZenCash Target of 51% Attack; Loses More than $500k in Double Spend Transactions. Bitcoinist. Pristupano: Februar 2022. Preuzeto sa: https://bitcoinist.com/zencash-target-51-attack-loses-500k-double-spend-transactions/

27. Ibrahim, R. F., Abu Al-Haija, Q. & Ahmad, A. (2022). DDoS attack prevention for internet of thing devices using ethereum blockchain technology. Sensors, 22(18), Doi: 10.3390/s22186806

28. Jiang, S., Li, Y., Wang, S. & Zhao, L. (2022). Blockchain competition: The tradeoff between platform stability and efficiency. European Journal of Operational Research, 296(3), 1084-1097.

29. Kearney, J. J. & Perez-Delgado, C. A. (2021). Vulnerability of blockchain technologies to quantum attacks. Array, 10, 1-10.

30. Kausar, F., Senan, F. M., Asif, H. M. & Raahemifar, K. (2022). 6G technology and taxonomy of attacks on blockchain technology. Alexandria Engineering Journal, 61(6), 4295-4306.

31. Koteska, B., Karafiloski, E. & Mishev, A. (2017). Blockchain implementation quality challenges: A literature review. 6th workshop of software quality, analysis, monitoring, improvement, and applications, SQAMIA 1-8.

32. Martić, V. (2021). Računovodstvena profesija u eri kripto valuta i globalne pandemije. Računovodstvena znanja kao činilac ekonomskog i društvenog napretka, Kragujevac: Ekonomski fakultet, 337-347.

33. Molchan, Y. (2018). ZenCash (Zen) Suffers 51 Percent Attack, Crypto Exchanges Warned. Pristupano: Februar 2022. Preuzeto sa: https://u.today/zencash-zen-suffers-51-percent-attack-crypto-exchanges-warned

34. Muchoki, S. (2021). Solana suffers network downtime, Ethereum demonstrates resilience as it shakes off attack. Crypto-news-flash. Pristupano: Februar 2022. Preuzeto sa: https://www.crypto-news-flash.com/solana-suffers-network-downtime-ethereum-demonstrates-resilience-as-it-shakes-off-attack/

35. Narayanan, K., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). Bitcoin and Cryptocur-

rency Technologies. Princeton University Press

36. Nayak, K., Kumar, S., Miller, A. & Shi, E. (2016). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. 2016 IEEE European Symposium on Security and Privacy (EuroS&P), 305-320.

37. Nofer, M., Gomber, P., Hinz, O. & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187.

38. Redman, J. (2018). Bittrex to Delist Bitcoin Gold Over 51% Attack. Bitcoin.com. Pristupano: Februar 2022. Preuzeto sa: https://news.bitcoin.com/bittrex-to-delist-bitcoin-gold-over-51-attack/

39. Redman, J. (2019). Vertcoin Network Sabotaged by Another 51% Attack. Bitcoin.com. Pristupano: Februar 2022. Preuzeto sa: https://news.bitcoin.com/vertcoin-network-sabotaged-by-another-51-attack/

40. Redman, J. (2020). Bitcoin Gold 51% Attacked - Network Loses $70,000 in Double Spends. Bitcoin.com. Pristupano: Februar 2022. Preuzeto sa: https://news.bitcoin.com/bitcoin-gold-51-attacked-network-loses-70000-in-double-spends/

41. Redman, J. (2021). Privacy Coin Verge Suffers Third 51% Attack, Analysis Shows 200 Days of XVG Transactions Erased. Bitcoin.com. Pristupano: Februar 2022. Preuzeto sa: https://news.bitcoin.com/privacy-coin-verge-third-51-attack-200-days-xvg-transactions-erased/

42. Rosenfeld, M. (2011). Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 1-46.

43. Sayeed, S. & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, 9(9), 1-17.

44. Shanaev, S., Shuraeva, A., Vasenin, M. & Kuznetsov, M. (2019). Cryptocurrency value and 51% attacks: evidence from event studies. The Journal of Alternative Investments, 22(3), 65-77.

45. Shetty, S., Kamhoua, C. & Njilla, L. (2019). Blockchain for Distributed Systems Security. Wiley Blackwell

46. Singh, S. K., Salim, M. M., Cho, M., Cha, J., Pan, Y., & Park, J. H. (2019). Smart contract-based pool hopping attack prevention for blockchain networks. Symmetry, 11(7), 1-19.

47. Sredojević, S. (2018). Savremena uloga i značaj profesionalnih kvalifikacija u sektoru bankarstva. Bankarstvo, 47(1), 82-97.

48. Tomić, N. (2020). Measuring the effects of Bitcoin forks on selected cryptocurrencies using event study methodology. Industrija, 48(2), 21-36.

49. Tomić, N. (2021). A review of consensus protocols in permissioned blockchains. Journal of Computer Science Research, 3(2), 32-39.

50. Tomić, N. & Todorović, V. (2020). Potential negative implications of Libra cryptocurrency. Ekonomika, 66(1), 13-24.

51. Tomić, N., Todorović, V. & Čakajac, B. (2020a). The potential effects of cryptocurrencies on monetary policy. The European Journal of Applied Economics, 17(1), 37-48.

52. Tomić, N., Todorović, V. & Jakšić, M. (2020b). A survey on consensus protocols in permissionless blockchains. Contemporary Issues in Economics, Business and Management – EBM 2020, Kragujevac: Faculty of economics University of Kragujevac, 365-374.

53. Ul Haq, H. B. & Saqlain, M. (2023). An implementation of effective machine learning approaches to perform sybil attack detection (SAD) in IoT network. Theoretical and applied computational intelligence, 1(1), 1-14.

54. Voell, Z. (2020a). Ethereum Classic Hit by Third 51% Attack in a Month. CoinDesk. Pristupano: Februar 2022. Preuzeto sa: https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/

55. Voell, Z. (2020b). Ethereum Classic Attacker Successfully Double-Spends $1.68M in Second Attack: Report. CoinDesk. Pristupano: Februar 2022. Preuzeto sa: https://www.coindesk.com/markets/2020/08/07/ethereum-classic-attacker-successfully-double-spends-168m-in-second-attack-report/

56. Vokerla, R. R., Shanmugam, B., Azam, S., Karim, A., De Boer, F., Jonkman, M. & Faisal, F. (2019). An overview of blockchain applications and attacks. 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 1-6.

57. Yves-Christian, A. E., Hammi, B., Serhrouchni, A. & Labiod, H. (2018). Total eclipse: How to completely isolate a bitcoin peer. Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), 1-7.

58. Wang, Z., Lv, Q., Lu, Z., Wang, Y., & Yue, S. (2021). ForkDec: accurate detection for selfish mining attacks. Security and Communication Networks, 2021, Doi: 10.1155/2021/5959698

59. Zheng, Z., Xie, S., Dai, H. N., Chen, X. & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

60. Zhou, C., Xing, L., Liu, Q. & Wang, H. (2023). Effective selfish mining defense strategies to improve bitcoin dependability. Applied Sciences, 13(1), Doi: 0.3390/app13010422

61. Academy.binance.com, https://academy.binance.com/en/articles/what-is-an-eclipse-attack, Pristupano: Februar 2022.