Primjena tehnologije lanca blokova u financijama

Živković, Luka

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:406185

Sveučilište u Zagrebu

Ekonomski fakultet

Analiza i poslovno planiranje

Primjena tehnologije lanca blokova u financijama

Diplomski rad

Luka Živković

Zagreb, Lipanj, 2023.

Ekonomski fakultet

Analiza i poslovno planiranje

Primjena tehnologije lanca blokova u financijama

Application of blockchain technology in finance

Diplomski rad

Luka Živković, 0067571119

Mentor: Izv. prof. dr. sc., Danijel Mlinarić

Zagreb, Lipanj, 2023.

Sažetak i ključne riječi

Tehnologija lanca blokova je relativna novina, no nudi potencijalno rješenje za problem koji je star koliko i ljudsko društvo, a to je vremensko i prostorno prenošenje vrijednosti. Tijekom povijesti razvijali su se razni sustavi i standardi za izdavanje univerzalnog sredstva plaćanja te su nastojali zadovoljiti određene standarde sigurnosti i efikasnosti. Iako je za ljude najefikasnije i najjeftinije kada oni sami vladaju svojom imovinom te transakcije i druge financijske operacije obavljaju direktno s drugim osobama (bez posrednika) do sada je razvoj financijskog sustava obilježila centralizacija. Postoji više razloga zašto je sustav razvijan u tom smjeru poput sigurnosti, globalnog dosega te nepostojanja adekvatne tehnologije za sigurno i efikasno obavljanje financijskih aktivnosti bez posredništva. U svakom slučaju to je utjecalo na razvoj i dominaciju banaka i korporacija koje trenutno određuju standarde i pravila u poslovnom sektoru te imaju apsolutnu kontrolu nad svim informacijama. Po prvi puta nakon stoljeća korištenje istog sustava upravljanja novcem i imovinom, razvoj tehnologije omogućava prijelaz na alternativni financijski sustav. Njegov temelj je tehnologija lanca blokova (eng. *Blockchain technology*) koja omogućava razvijanje decentraliziranog financijskog sustava. On potpuno mijenja do sada ustaljene odnose u financijskome svijetu i otvara mogućnosti za izgradnju bržeg, sigurnijeg i efikasnijeg sustava. Potrebno je razumijevanje lanca blokova kao podloge i osnove na kojoj se razvija decentralizirani financijski svijet te se upravo time bavi ovaj rad. Uz detaljnu analizu protokola i sustava koji pokreću ovu tehnologiju poput pametnih ugovora, kriptografije, kriptovaluta, tokena i decentraliziranih aplikacija razmatraju se njezine prednosti i nedostaci te potencijalne mogućnosti primjene. Na primjeru postojećih decentraliziranih aplikacija u DeFi (eng. *Decentralized finance* – DeFi) sektoru te dosadašnje primjene nezamjenjivih tokena promatraju se trendovi njezina prihvaćanja te koristi koje je do sada pružila i potvrdila.

Ključne riječi: Tehnologija lanca blokova, decentralizirani financijski sustav, kriptovaluta, pametni ugovor, token, decentralizirane aplikacije

Summary and key words

Blockchain technology is a relatively new invention, but it offers a potential solution to a problem as old as human society, transfer of value through time and space. Throughout history, various systems and standards have been developed for the issuance of universal means of payment and they have sought to meet certain standards of security and efficiency. Although it is most efficient and cheapest for people when they manage their own property and perform transactions and other financial operations directly with other people (without intermediaries), until now the development of the financial system has been characterized by centralization. There are several reasons why the system was developed in this direction, such as security, global reach, and the lack of adequate technology for safe and efficient financial activities without intermediaries. Anyway, it influenced the development and dominance of banks and corporations, which currently determine the standards and rules in the business sector and have absolute power over all information. After the first century of using the same money and asset management system, the development of technology is enabling the transition to an alternative financial system. Its basis is blockchain technology, which enables the development of a decentralized financial system. It completely changes the relationships established so far in the financial world and opens up possibilities for building a faster, safer and more efficient system. It is necessary to understand the blockchain as the basis and foundation on which the decentralized financial world develops, and this is exactly what this work engages with. Along with a detailed analysis of the protocols and systems that drive this technology, such as smart contracts, cryptography, cryptocurrencies, tokens and decentralized applications, its advantages and disadvantages and potential applications are also considered. With existing decentralized applications in the DeFi sector and the current use of irreplaceable tokens as an example, the trends of its acceptance and the benefits it has provided and confirmed so far are observed.

Keywords: Blockchain technology, decentralized financial system, cryptocurrency, smart contract, token, decentralized applications

Sadržaj

1. Uvod

1.1. Predmet i cilj rada

Inovacije u svim sektorima, a posebno u financijskom, usmjerene su prema optimizaciji i većoj efikasnosti sustava. Do sada je financijski sustav, zbog specifičnih zahtjeva (visoka sigurnost i zaštita podataka), težio ka sve većoj centraliziranosti što je dovelo do dominacije banaka, institucija i velikih korporacija. Pojavljivanje disruptivne tehnologije lanca blokova otvorilo je vrata razvoju potpuno novog, decentraliziranog financijskog sustava kojim se mijenjaju dosadašnji odnosi do samih temelja. Iako je ovakav način funkcioniranja financijskog sektora još u svojim začecima i nije potpuno jasno hoće li i kada će doći do njegove šire primjene i općeg prihvaćanja, izaziva veliki interes ekonomista i laika zbog vrlo zanimljivih atributa i funkcionalnosti. Cilj ovoga rada je pojasniti tehnologiju lanca blokova kao temelja decentraliziranog financijskog sustava te ju približili široj publici.

1.2. Izvori podataka i metode prikupljanja

Za izradu teorijskog dijela diplomskog rada korišteni su sekundarni podaci. To uključuje izabrane stručne knjige, znanstvene i stručne internetske članke i publikacije te internetske stranice platformi i poduzeća koji se koriste kao ogledni primjeri u radu. Od metoda korištene su metode dedukcije, analize i deskripcije za definiranje i objašnjavanje tehnologije lanca blokova te metode komparacije za usporedbu decentraliziranog i centraliziranog financijskog sustava. Još su korištene i statističke metode kao dodatni materijal za upotpunjavanje usporedbe te prikaz intenziteta korištenja decentraliziranih sustava.

1.3. Sadržaj i struktura rada

Diplomski rad je podijeljen na šest poglavlja te svako poglavlje ima određeni broj potpoglavlja. U prvom poglavlju su definirani i opisane metode istraživanja, izvori, sadržaj i ostali tehnički aspekti rada. Drugo poglavlje se odnosi na teorijski okvir tehnologije. U tom su poglavlju detaljno objašnjeni svi osnovni pojmovi i principi funkcioniranja tehnologije lanca blokova kako bi se kasnije moglo diskutirati i proučavati njihove primjene. Treće poglavlje identificira i uspoređuje prednosti i nedostatke ove tehnologije te se provodi SWOT analiza. U četvrtom poglavlju obrađuju se sustavi, platforme i aplikacije

koje se izgrađuju na temelju lanca blokova te se posebno detaljno opisuju njihove primjene u financijama i potencijali izgradnje decentraliziranog financijskog sustava. Peto poglavlje se bavi opisivanjem postojećih primjera i primjene decentraliziranih aplikacija. U posljednjem poglavlju je na temelju informacija i spoznaja iznesenih u radu donesen zaključak o ključnim aspektima tehnologije lanca blokova u financijama.

2. Teorijski okvir tehnologije

Koncepti decentraliziranih baza podataka koji se temelje na kriptografiji i konsenzusu grupe sudionika razvijani su i diskutirani još 80-ih i 90-ih godina prošlog stoljeća. Međutim, prvi decentralizirani lanac blokova predstavljen je 2008. godine u dokumentu pod nazivom „*Bitcoin: A Peer-to-Peer Electronic Cash System*“. U njemu je opisana tehnologija na kojoj se zasniva Bitcoin te ju se u radu naziva lanac blokova (eng. *Block chain*). Autor ovog dokumenta se predstavlja kao Satoshi Nakamoto, no vjerojatno se radi o pseudonimu iza kojeg stoji više osoba. Prvi blok (eng. *Genesis block*) u Bitcoin-ov lanac blokova dodan je 3. siječnja 2009. godine od strane Satoshija Nakamota te je taj događaj službeni početak njegovog rada. Od 2011. godine na dalje počinju se pokretati novi lanci blokova koji nastaju na konceptu Bitcoina uz određene preinake i pokušaje proširenja funkcionalnosti. Najpoznatiji takav projekt predstavljen je 2013. godine po imenu Ethereum te pokrenut 2015. godine od strane Vitalika Buterina.

2.1. Definiranje lanca blokova i osnovnih pojmova

Osnova pokretačka snaga lanca blokova je mreža računala koja su međusobno neovisna (eng. *Nodes*) te pomoću sustava konsenzusa prihvaćaju i dokumentiraju transakcije (Tapscott, 2016.). Kažemo da se one dokumentiraju u lancu blokova zbog specifične arhitekture ovoga sustava u kojem se blokovi informacija međusobno povezuju tako da svaki sadrži identifikacijski broj prethodnoga te se na taj način stvara struktura koja podsjeća na karike u lancu (Agashe, 2019.). Svatko se može priključiti mreži tako da preuzme na svoje računalo softver od određenog lanca blokova te poduzme sve potrebne korake koji su potrebni za početak rudarenja (eng. *Mine*) ili odobravanja (eng. *Validate*) transakcija. Lanac blokova je inovativan način bilježenja i pohranjivanja transakcija koji se temelji na nekoliko osnovnih metoda i obilježja:

- Kriptografija

  Danas je kriptografija jedna od glavnih metoda kojom se razni sustavi štite od hakerskih napada. To je naziv za sve procese kojima se osiguravaju informacije i komunikacija tako da se konvertiraju iz razumljivog oblika, po nekom ključu i pomoću raznih algoritama, u kriptirani ili nerazumljiv oblik za sve one koji ne posjeduju znanje o ključu i procesu. Ona sustavu daje integritet, privatnost i neprobojnost za malverzacije i hakerske napade. U općenitom smislu

kriptografija pomoću matematičkih algoritama u procesu enkripcije pretvara običan tekst u kriptirani. Pritom se koristi nekim ključem, vitalnim i jedinstvenim pravilom ili komadom informacije koji se koristi u tom procesu te određuje transformaciju podataka (Bashir, 2017.). Kriptirani tekst se pomoću ključa može opet vratiti u svoj izvorni oblik. U kontekstu lanca blokova ona se koristi u njegovim fundamentalnim dijelovima i funkcijama, u sustavima konsenzusa u samom procesu određivanja identifikacijskog broja i dodavanja blokova te u kreiranju javnih i privatnih ključeva novčanika za kriptovalute.

- Kripto novčanik

Pomoću kripto novčanika korisnici čuvaju svoje privatne ključeve te vrše i odobravaju transakcije na lancu blokova. Oni su povezani s lancem te se u njih sprema kopija svih transakcija pa je korisniku uvijek vidljivo stanje na računu. Postoji više vrsta kripto novčanika na koje se mogu pohraniti i čuvati privatni ključevi, no najčešće je to softverski novčanik (program koji se preuzme na mobitel, računalo ili mu se pristupa preko web preglednika) ili hardverski novčanik koji pruža dodatnu razinu sigurnosti jer nije spojen na Internet.

- Javni i privatni ključevi

Važan aspekt tehnologije lanca blokova je zaštita privatnosti i anonimnost. To se postiže korištenjem kriptografije u procesima i protokolima lanca blokova te pomoću privatnih i javnih ključeva. Oni su automatski i nasumično generirani od strane novčanika za kriptovalute. Uvid u privatni ključ ima samo vlasnik te on služi za digitalno potpisivanje i autoriziranje transakcija pa je nužno da on bude skriven i tajan. Javni ključ je dobiven iz privatnog ključa pomoću matematičkih algoritama te je on vidljiv svima i služi kao adresa korisnika. Ovaj tip enkripcije se zove asimetrična enkripcija jer iako je javni ključ izveden iz privatnog, proces nije reverzibilan što znači da se iz javnog ključa ne može izvesti privatni (Bashir, 2017.). Međutim, nizom matematičkih i kriptografskih operacija može se potvrditi povezanost javnog i privatnog ključa te se ta veza koristi za potvrdu transakcija. To svojstvo javnih i privatnih ključeva je od vitalne važnosti za sigurnost korisnika. Kreiranje transakcija se odvija na sljedeći način:

1. Pošiljatelj daje nalog za transakciju u svojem kripto novčaniku te se zatim automatski stvara digitalni potpis koji je generiran kao kombinacija privatnog ključa i transakcija te služi kao potvrda da iza njih doista stoji vlasnik adrese.
2. Jednom kada je zahtjev za transakciju poslan u mrežu rudari ili odobravatelji na temelju javnog ključa pošiljatelja i transakcija koje se nalaze u zahtjevu potvrđuju digitalan potpis.
3. Javni ključ primatelja se koristi kao adresa na koju se šalju sredstva te jedino vlasnik odgovarajućeg privatnog ključa im može pristupiti .

- Tokenizacija

Tokenizacija je proces prenošenja vrijednosti i prava na imovinu iz realnog svijeta u digitalne tokene (Vigna, 2018.). Postoje različiti načini i svrhe njezina provođenja te se uvijek izvršava pomoću pametnih ugovora. Tokenizacija preko digitalnih tokena omogućuje jednostavno trgovanje i baratanje s udjelima u vlasništvu imovine ili nekih drugih prava vezanih uz imovinu na lancu blokova.

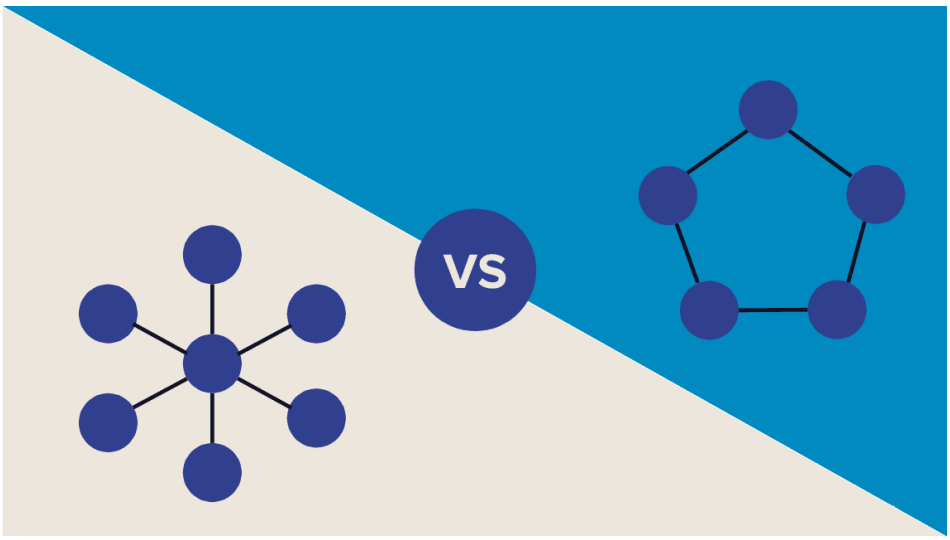
- Transparentnost

Mogućnost da svatko može vidjeti detalje transakcija je isto tako jedna od novosti te temelja lanca blokova. Transparentnost omogućava svim sudionicima mreže lanca blokova da potvrđuju transakcije što dodatno osigurava korisnike (Hayes 2022.). Iz podataka koji su vidljivi svima poput iznosa, vremena transakcije i javnih ključeva ne može se vidjeti tko stoji iza transakcija već se samo može potvrditi njihova legitimnost.

- Distribuirani zapisi

Jedna od inovacija tehnologije lanca blokova jest njegova distribuiranost. Sve što je zapisano na lancu blokova je istovremeno dokumentirano na tisućama računala različitih vlasnika koja sudjeluju u izgradnji P2P mreže (eng. *Peer to peer* – P2P). Upravo ovaj atribut omogućava tehnologiji lanca blokova da bude sigurna i inkluzivna za sve korisnike što joj daje potencijal da se koristi kao temelj za izgradnju decentraliziranog financijskog sustava (Ammous, 2018.).

Slika 1. Decentralizirani i centralizirani sustav



Izvor: https://perkuto.com/blog/centralization-vs-decentralization-why-you-need-a-hybrid-model-more-now-than-ever/ (Preuzeto 29. lipnja 2023. god.)

Vizualni prikaz decentraliziranog sustava pohrane podataka i mreže računala koja ga čini prikazan je na slici 1. U centraliziranom sustavu svi podaci su pohranjeni u izrazito velikim bazama podataka, odnosno podatkovnim centrima (eng. *Data center*). Te baze su u vlasništvu najvećih svjetskih kompanija (Google, Amazon, Meta, Apple itd.) te one imaju pristup svim podacima uključujući one privatne.

- Nemogućnost promjene pohranjenog sadržaja

Kriptografske metode i procesi koji se koriste prilikom dodavanja novih blokova i vršenja transakcija takozvani sustavi konsenzusa čine gotovo nemogućim bilo kakve izmjene ili malverzacije na lancu blokova koje bi štetile korisnicima (Antonopoulos, 2017.). Više o ovim procesima će se govoriti u slijedećem dijelu ovoga rada.

- Sigurnost i privatnost

Sve metode inkorporirane u softversku strukturu tehnologije lanca blokova osmišljene su kako bi omogućavale decentraliziranost te istovremeno zaštitile korisnike i njihovu privatnost.

2.2. Definiranje kriptovalute

Kriptovalute su digitalne valute koje ne ovise o niti jednom centralnom autoritetu (npr. centralnoj banci) poput svih ostalih valuta. Većina kriptovaluta je ograničene ponude te se distribuiraju mehanizmom lanca blokova na P2P mreži. Njihova svrha je ista kao i ona „običnog“ novca, a to je da služe kao sredstvo za vršenje transakcija (Antonopoulos, 2017.). Ono što karakterizira kriptovalute jest već spomenuta decentraliziranost, korištenje tehnologije lanca blokova, oslanjanje na kriptografiju i sustave konsenzusa kako bi se garantirala sigurnost i privatnost korisnika te omogućavanje vršenja sigurnih transakcija bez potrebe za posrednikom ili centralnim tijelom (bankom) (Casey, Vigna, 2015.). Za proces rudarenja potreban je veliki utrošak energije te su također potrebna sve naprednija i skuplja računala. Kako bi rudari bili motivirani izvršavati svoju dužnost, bez koje lanac blokova propada, svaki puta kada ugrade novi blok u lanac kao nagradu za svoj rad dobiju određenu količinu kriptovaluta. Kao i sve drugo u lancu blokova, kriptovalute postoje samo kao transakcijski zapis, što logično dovodi do pitanja koliko je njihova distribucija sigurna. Kao što je prethodno objašnjeno sustavi konsenzusa i distribucija zapisa, uz kriptografiju, čine izmjene zapisa gotovo nemogućim. Da bi se lažirala transakcija bilo bi potrebno promijeniti tu transakciju na barem pola računala u mreži te također zbog hash funkcije i svaki blok u lancu prije onoga koji se želi promijeniti.

2.2.1. Izvorne kriptovalute

Bitno je znati razliku između tokena i izvornog tokena. Iako oboje mogu imati ulogu digitalne valute te se ti pojmovi u određenom kontekstu koriste kao jednoznačnice, u pravilu samo oni tokeni koji imaju vlastiti lanac blokova u svojoj podlozi (Bitcoin, Ethereum, Ripple, Cardano itd.) se nazivaju izvornim tokenima ili kriptovalutama. Novčić (eng. *Coin*) je također naziv koji se koristi samo za izvorne tokene te se njime dodatno naglašava razlika između izvornih i ostalih tokena. Jedno od osnovnih obilježja kriptovaluta jest da se koriste kao sredstvo razmjene te za čuvanje vrijednosti. Također, ispunjavaju i druge kriterije poput standardiziranosti, široke prihvaćenosti, zamjenjivosti, djeljivosti na manje jedinice te prenosivosti koje su sve temeljne značajke novca pa možemo reći da one obnašaju njegovu ulogu u decentraliziranom sustavu (Agashe, 2019.). U tom kontekstu se često izvorni tokeni i tokeni plaćanja skupno nazivaju kriptovalutama. Tokeni imaju mnoštvo potencijalnih primjena, jedna od njih je i da se koriste kao sredstvo

plaćanja isto kao i kriptovalute, te su od velike važnosti za decentralizirani financijski sustav jer bi se pomoću njih izvršavale razne njegove funkcije. Iako se i kriptovalute i tokeni smatraju visoko rizičnom imovinom, kriptovalute su se do sada pokazale kao najtraženija kripto imovina jer potrošači vjeruju da su one sigurnije i da će im u dugom roku vrijednost rasti te da će opstati. S druge strane tokeni koji se koriste u svrhu plaćanja, odnosno koji imitiraju kriptovalute, najčešće propadaju i vrijednost im završi na nuli.

2.2.2. Token i nezamjenjivi tokeni

Tokeni su sva kripto imovina, uključujući kriptovalute, odnosno tokene koji se nalaze na vlastitom lancu blokova. Tokeni dolaze u raznim oblicima, ovisno o standardu i platformi na kojoj su izdani (npr. Ethereum, Solana ili Binance) te funkciji koja im je namijenjena. Izdaju se pomoću pametnih ugovora u kojima su definirani svi njihovi atributi (ime, naziv, svrha, količina, dodatne vrijednosti koje nose i ostalo) te uvjeti po kojima se novi tokeni izdaju. Da bi se olakšao proces njihovog izdavanja posljednjih nekoliko godina razvijeni su razni standardi za tokene, posebno na lancu Ethereum (ERC21, ERC20, ERC721 itd.), te kako bi se njima lakše rukovodilo i kako bi se postigla još jedna razina zaštite jer svaki standard definira određene atribute koje svaki token mora posjedovati (Agashe, 2019.). Popularno se umjesto izraza izdavanje tokena koristi izraz kovanje (eng. *Mint*). Osim kovanja, tokeni se mogu i spaliti (eng. *Burn*) tako da se pošalju na adresu ili pametni ugovor s kojeg ih više nije moguće vratiti u cirkulaciju. Izdavanje tokena se često koristi kao metoda prikupljanja sredstava za razvijanje i pokretanje novog projekta na lancu blokova u procesu zvanom ICO ili ITO (eng. *initial coin offering*, eng. *initial token offering*). Investitori kupuju tokene koji im najčešće garantiraju udio u projektu ili neke druge pogodnosti, dok projekt dobiva druge kriptovalute (Bitcoin, Ethereum itd.) ili čak fiducijarni novac koji su im potrebni za financiranje. Vidljiva je sličnost između ICO-a i standardnih IPO-a, međutim glavna razlika je u tome što poduzeća koja se odluče financirati pomoću inicijalne javne ponude moraju uzeti posrednika (najčešće banku ili fond) dok se ICO odvija bez posrednika. U jednu ruku to je bolje za poduzeća jer nema dodatnih troškova posrednika, no zbog nedostatka regulacije nosi povećane rizike prijevare ili propasti projekta. Prvi ICO je proveden 2013. godine za token Mastercoin (kasnije preimenovan u Omni Layer) koji je izdan na Bitcoin lancu blokova te se predstavljao kao poboljšana verzija Bitcoina i nudio mogućnost imateljima da izdaju vlastite tokene. Ovaj projekt je otvorio vrata i pokrenuo mnoštvo ICO-a između 2013. i 2017. godine. Investitori

su svjedočili velikom rastu cijena prvih tokena pa su počeli ulagati u razne projekte bez previše prethodnog istraživanja nadajući se naglom rastu cijena. Uz sva poduzeća i poduzetnike koji su vidjeli priliku za poprilično jednostavno prikupljanje velikih sredstava, u izdavanje tokena su se uključili i mnogi prevaranti s lažnim projektima. To je dovelo do konačnog kolapsa ICO projekata 2018. godine. (U posljednje vrijeme ova metoda prikupljanja sredstava se rijetko koristi te je zamijenjena s drugim sigurnijim metodama poput ponude sigurnosnih tokena (eng. security token offering - STO). To je također javni način prikupljanja sredstava koji kombinira pogodnosti koje pruža tehnologija lanca blokova s tržišnom vrijednošću realne imovine (Agashe, 2019.). U suštini ponuda sigurnosnih tokena je ista kao i inicijalna javna ponuda, no umjesto vrijednosnih papira se pomoću pametnih ugovora izdaju tokeni koji predstavljaju udio u imovini ili neka posebna prava u poduzeću. Dodatno, ponude sigurnosnih tokena poštuju zakone o vrijednosnicama u zemljama u kojima se odvijaju (pravila o zaštiti kupaca te izdavanju i prodaji vrijednosnih papira) što, uz sigurnosne tokene koji predstavljaju realnu imovinu, dodatno štiti investitore. Pokazalo se kako tokeni kao sredstvo plaćanja ne mogu konkurirati kriptovalutama te ih je do sada velika većina u potpunosti izgubila vrijednost i nestala s tržišta. Međutim, ističu se njihove druge primjene i koristi unutar financijskog sustava te se mogu klasificirati u nekoliko skupina:

- Uslužni tokeni (eng. *Utility tokens*)

  Vrijednost ovih tokena leži u posebnim povlasticama koje daju vlasniku. Ovisno o funkciji platforme koja izdaje ove tokene, to se može odnositi na ekskluzivno pravo na određene usluge, povoljnije uvjete poslovanja (npr. manje troškove transakcija ili konverzije), pravo na pristup posebnom sadržaju, pravo na glasanje u donošenju odluka povezanih s vođenjem platforme (u ovome slučaju dobivaju ulogu upravljačkih tokena) itd. Iz navedenih razloga, ovi tokeni imaju i svoju vrijednost pa se mogu koristiti i u razmjeni za drugu imovinu ili kao sredstvo plaćanja.

- Sigurnosni tokeni (eng. *Security token*)

  Smisao ovih tokena je da imaju istu ulogu kao i vrijednosni papiri (dionice, obveznice itd.) te se izdaju u procesu zvanom ponuda sigurnosnih tokena. Najčešće se koriste za predstavljanje udjela u nekom poduzeću, projektu,

investiciji ili nekoj drugoj imovini. Podliježu regulacijama i zakonima o vrijednosnim papirima pa su znatno sigurnijih od drugih tokena.

- Tokeni plaćanja (eng. *Payment tokens*)

  Koriste se kao digitalne valute za vršenje svakodnevnih transakcija na lancu blokova. Najpoznatiji primjeri su kriptovalute kao što su Bitcoin, Ethereum i Ripple, no postoji i mnoštvo običnih tokena za plaćanje.

- Upravljački tokeni (eng. *Governance tokens*)

  Ova vrsta tokena daje mogućnost vlasniku da sudjeluje u demokratskim procesima odlučivanja o razvitku i poslovanju platforme. Tako vlasnici ovih tokena mogu sudjelovati u procesima odlučivanja o financiranju, vođenju, razvijanju i mijenjaju protokola i ostalim temama vezanim uz upravljanje poslovnim procesima.

Raznovrsnost tokena te mogućnost njihove prilagodbe shodno potrebama sustava ili novih platformi i aplikacija za izvršavanje i ostvarivanje financijskih odnosa otvara mogućnost njihovom stalnom razvijanju i prenamjeni. Iz tog razloga možemo pronaći tokene s čitavim spektrom vrijednosti i uloga koje nose ovisno o potrebama i ciljevima platforme. Isto kao i kod kriptovaluta, vrijednost tokena, osim iz njihove koristi, proizlazi i iz njihove količine, odnosno rijetkosti pa to otvara mogućnost platformama da manipulirajući njihovom ponudom (izdavanjem ili uništavanjem) pribavljaju potrebna sredstva.

Nezamjenjivi tokeni (eng. *Non fungible tokens* - NFT)

Definitivno najpopularniji i najtraženiji tokeni za vrijeme rastućeg tržišta u svijetu kriptovaluta krajem 2021. godine i početkom 2022. godine su bili nezamjenjivi tokeni (NFT). Oni služe kao garancija za jedinstvenost te u tome leži njihova vrijednost i svrha. Za razliku od drugih tokena koji su, jednom kada se definiraju u pametnom ugovoru i izdaju, svi jednaki i međusobno potpuno zamjenjivi, nezamjenjivi tokeni su svi različiti (Hayworth, 2021.). Najčešće su izdavani na lancu blokova Ethereum gdje je razvijeno nekoliko standarda za nezamjenjive tokene (ERC-721 i ERC-1155) ali postoje i drugi lanci blokova koji imaju razvijene standarde za izdavanje nezamjenjivih tokena popu Solane, Polygona i Binance Smart Chaina. U početnom razdoblju to njihovo svojstvo korišteno je

tako da su se tokeni vezali za razni sadržaj (najčešće jednostavan slikovni, audio ili video sadržaj) i prodavali na decentraliziranim platformama poput OpenSea-a i Magic Garden-a te je zbog utjecaja društvenih mreža i promocije od strane poznatih osoba njihova cijena dosegla izrazito visoke i nelogične cijene.

Slika 2. Bored Ape Yacht Club NFT

Izvor: https://www.rollingstone.com/culture/culture-news/bayc-bored-ape-yacht-club-nft-interview-1250461/ (Preuzeto 01. srpnja 2023. god.)

Nezamjenjivi tokeni sa sadržajem poput onoga na slici 2 prodavani su za višemilijunske iznose. Konkretan rekord za navedenu kolekciju postignut je u listopadu 2021. godine kada je jedan od tokena prodan za 3,41 milijuna dolara. Prilikom njihovog izdavanja određene informacije vezane uz njih (ime, opis, poveznica na imovinu, slika ili neki drugi atributi) se spremaju na decentralizirani sustav pohrane poput IPFS-a (eng. *InterPlanetary File System* – IPFS) ili na neki klasični centralizirani server. Te podatke zovemo meta podacima (eng. *Metadata*) te im je moguće pristupiti i bez vlasništva samog tokena na kojeg se ti podaci odnose. Za pristup meta podacima potrebna nam je adresa pametnog ugovora i jedinstveni identifikacijski broj nezamjenjivog tokena. Pametni ugovor sadrži poveznicu koja vodi do meta podataka svakog nezamjenjivog tokena pa se pomoću jedinstvenog broja dolazi do odgovarajuće poveznice. Međutim, bilo je primjera koji su pokazali i potencijalnu vrijednost koja bi se mogla stvoriti pomoću ove vrste tokena, a to je kao garancija jedinstvenosti i originalnosti za raznu realnu imovinu (npr. kolekcionarske predmete, karte

za koncerte ili bilo koje druge događaje, diskografske albume itd.). Vrijednost i upotreba ovih tokena bi doista mogla biti značajna ako se koriste na smislen način jer se pomoću njih likvidira potreba za trećim stranama u transakcijama koje uključuju virtualnu i fizičku imovinu.

2.3. Sustavi konsenzusa (eng. *Proof of stake* – POS / eng. *Proof of work* - POW)

Sustavi konsenzusa su metode kojima se dodaju novi blokovi u lanac te je njihov smisao i uloga da ga učine neprobojnim, odnosno sigurnim od malverzacija i zlouporabe (Swan, 2015.). Postoje dvije vrste sustava konsenzusa POW i POS, prvi od ta dva je onaj osnovni od kojeg se krenulo te i dalje dominira među lancima blokova pa će on prvi biti obrađen.

- Dodavanje novih blokova u lanac je svojevrsno natjecanje između rudara koji se nadmeću da bi prvi razriješili specifičan matematički problem određivanja jedinstvenog broja, odnosno identifikacijskog broja novog bloka (eng. *Hash*). Broj svakog bloka je kombinacija slova i brojeva koja nastaje na način da se pomoću *hash* funkcije kriptiraju određeni podaci (Drescher, 2017.). Mora sadržavati podatke o vremenu nastanka bloka te ovisi o transakcijama koje se u njemu nalaze, o identifikacijskom broju prethodnog bloka te o nasumično generiranom broju (eng. *Number only used once* - NONCE). NONCE je nasumično generiran broj od strane algoritma te se uzima kao jedan od inputa za dobivanje identifikacijskog broja. Također, on isto mora zadovoljavati određene kriterije poput maksimalne veličine i određene količine nekih brojeva koje mora sadržavati. Svaki puta kada se promijeni neki od inputa u algoritmu određivanja identifikacijskog broja on se mijenja (Drescher, 2017.). Upravo je nasumični broj onaj input koji rudar treba otkriti rješavanjem algoritma jer se ostali odnose na podatke o transakcijama u bloku i ostale podatke kako je prije objašnjeno. Ako identifikacijski broj dobiven uz određeni nasumični broj zadovoljava sve kriterije algoritma on se prihvaća, u suprotnom algoritam se ponavlja dok se ne pronađe nasumični broj uz koji će se zadovoljiti svi kriteriji (Frankenfield, 2022.). Sustav može regulirati težinu otkrivanja nasumičnog broja te na taj način smanjiti ili povećati broj i brzinu dodavanja novih blokova. Upravo ta nepredvidivosti i kompleksnost identifikacijskog broja te procesa kojima se on kreira je jedan od ključnih elemenata u sigurnosti ovog sustava. Kada prvi rudar razriješi problem svi drugi

odustaju i započinju rješavati sljedeći, dok sada novi blok koji se treba dodati u lanac prolazi još kroz proces odobravanja, odnosno više od pola računala koja se nalaze u mreži potvrđuju da se transakcije u bloku nalaze i u njihovim kopijama i odobravaju ga (tako da koriste nasumični broj koji je koristilo računalo koje je stvorilo blok te na vlastitom računalo provedu algoritam). Konačno, kada je novi blok dodan, rudar koji ga je dodao dobiva nagradu u obliku fiksnog iznosa kriptovalute (primjerice za Bitcoin ta nagrada u trenutku pisanja ovog rada, u lipnju 2023., iznosi 6.25 Bitcoina). Jedan od ključnih problema ovog sustava je upravo u nadmetanju i određivanju pravog nasumičnog broja jer se sva računala nadmeću za dodavanje istog bloka dok jedno ne pobijedi te je potrebno puno pokušaja rješavanja algoritma dok se ne pronađe odgovarajući NONCE. Takav sustav troši izrazito puno energije, posebice u trenutcima velike količine prometa na mreži što izaziva dodatne transakcijske troškove za korisnike koji plaćaju naknadu za utrošenu energiju računala rudara (eng. *Gas fee*). Ovi nedostaci predstavljaju prepreku i onemogućuju skaliranje sustava na višu razinu, odnosno na masovno prihvaćanje jer u tim uvjetima ne bi bio efikasan i isplativ. Iz tog razloga došlo je do razvijanja novog sustava konsenzusa koji ispravlja ove mane i poteškoće te je njegov razvoj predvodio lanac blokova Ethereum.

- Problematika vezana uz POW sustav konsenzusa potaknula je razvoj efikasnijeg sustava koji se naziva POS (eng. *Proof of stake)*. Ovaj sustav je izrazito inovativan te predstavlja veliki skok unaprijed za tehnologiju lanca blokova jer je njime riješena jedna od glavnih prepreka za masovno korištenje ove tehnologije. Ono što se u POW sustavu zvalo rudar u ovome sustavu je preimenovano u odobravatelj (eng. *Validator*). Sustav funkcionira tako da odobravatelji ulažu svoje kriptovalute (eng. *Stake*) u zajednički bazen (eng. *Pool*), odnosno fond, iz kojeg se onda prilikom dodavanja novog blokova nasumično bira jedan od njih ili skupina (ovisno o pravilima sustava) te dobivaju zadaću dodavanja novog bloka (Beck, 2020.). Proces nasumičnog biranja najčešće uzima u obzir faktore poput količine uloženih sredstava u fondu ili perioda koji je prošao od ulaganja, no svaki lanac blokova može odrediti i još neke dodatne kriterije. Sustav se od prijevare štiti tako da blok ne pregledava samo odabrani odobravatelj nego i drugi koji sudjeluju u fondu. Također, ako se utvrdi da su u blok dodani lažni podaci odobravatelj tog bloka ostaje bez svojih založenih sredstava te mu se može zabraniti daljnje sudjelovanje.

Kao nagradu za svoj rad odobravatelji dobivaju transakcijske naknade te ponekad i nagradu za dodavanje bloka po istom principu kao i u POW sustavu u obliku fiksnog iznosa kriptovalute. Još jedan problem koji ovaj sustav konsenzusa rješava je problem troška transakcije u razdobljima intenzivnog prometa i ušteda velike količine energije. Zbog navedenih promjena sustav je puno brži i efikasniji te su troškovi transakcija znatno manji. Očiti nedostatak kod ovog sustava je u mogućnosti preuzimanja fonda za odobravanje od strane jedne ili nekolicine vjerojatno imućnih osoba koje si mogu priuštiti veće količine kriptovalute, ako postignu znatan udio ili većinu uloženih kriptovaluta u fondu. U tome slučaju bi ostali sudionici izgubili motivaciju za sudjelovanjem te bi lancu blokova prijetila opasnost od centralizacije čime bi proces odobravanja i priznavanja transakcija bio kompromitiran.

2.4. Pametni ugovori

Kada se govori u kontekstu financija, kao i kod običnih ugovora, pametnim ugovorima su definirani odnosi između dviju ili više strana te njihove obveze i eventualne dobiti (u obliku novca ili neke druge imovine) ako se te obveze ispune. Ono što čini pametne ugovore posebnima jest to što su u potpunosti napisani u kodu te se izvršavaju preko platforme lanca blokova (najčešće Ethereum jer je Bitcoin limitiran u mogućnostima pametnih ugovora) gdje su i pohranjeni. Pošto se njihov kod nalazi na lancu blokova on automatski preuzima njegova bitna obilježja, a to su neprobojnost, odnosno nemogućnost izmjene, transparentnost i decentraliziranost (Frankenfield, 2022.). Postoji mogućnost implementacije posredničkih pametnih ugovora (eng. *proxy contract*) koji imaju mogućnost naknadne izmjene (koja je također transparentna), no najčešće se koriste klasični pametni ugovori koji nemaju tu mogućnost. Svaki pametni ugovor napisan je tako da sadrži osnovne uvjete koji moraju biti ispunjeni kako bi se ugovor izvršio te se u trenutku njihovog ispunjenja on automatski izvršava (Agashe, 2019.). U slučaju da uvjeti u ugovoru ovise o nekim parametrima iz realnog svijeta koriste se različiti vanjski izvori (eng. *Oracle*). Oni služe kao most između pametnih ugovora i informacija nedostupnih na lancu blokova te podataka u stvarnom vremenu poput tržišnih cijena tokena ili druge imovine, vremenske prognoze, kamatnih stopa ili bilo kojih drugih relevantnih parametara. Kao vanjski izvor najčešće se koristi određeni softver za dohvaćanje podataka s drugih web lokacija (financijska tržišta, vijesti, platforme za trgovanje itd.) ili hardver, odnosno

fizički instrument koji služi za mjerenje određenih podataka. Isto kao i obične transakcije na lancu blokova pametni ugovori su vidljivi svim sudionicima lanca te također prolaze kroz procese odobravanja pa je potreban konsenzus da bi se ugovor izvršio. Automatizam ovih ugovora uklanja potrebu za posrednikom, što u konačnici utječe na niže troškove provođenja ugovora i uštedu vremena, te također smanjuje mogućnost ljudske pogreške i nemoralnih radnji. Ova obilježja pametnih ugovora omogućavaju da se pomoću njih i tehnologije lanca blokova u njihovoj podlozi izvršavaju kompleksni financijski odnosi poput davanja kredita, investiranja u projekte, osiguranja imovine ili bilo kojeg drugog odnosa dokle god postoje barem dvije strane koje će sudjelovati u njemu. Pametni ugovori se koriste i za izdavanje tokena koji u decentraliziranom financijskom sustavu imaju veliku važnost i široku primjenu kako je detaljno objašnjeno u prethodnim poglavljima. Danas se ovi ugovori najčešće koriste za prebacivanje kriptovaluta ili tokena uz određene uvjete koje svaka stranka mora ispuniti kako bi došlo do transakcije te za njihovo izdavanje. Ovakvi ugovori su temelj decentraliziranog financijskog sustava jer su, uz decentralizirane aplikacije, ključni medij za financijske aktivnosti.

2.5. Decentralizirane aplikacije

Složenije infrastrukture koje koriste lanac blokova i sve što on nosi kao svoju podlogu jesu decentralizirane aplikacije. Odmah se postavlja pitanje kako postići decentraliziranost za aplikacije koje najčešće zahtijevaju velike količine memorijskog prostora na serverima. To se postiže kombinacijom pohrane podataka na lancu (eng. *On-chain storage*) i van lanca blokova (eng. *Off-chain storage*) na način da se mehanizmi izvršavanja transakcija, provođenja pametnih ugovora i drugih radnji vezanih uz lanac blokova i dalje odvijaju na njemu, dok se ostale funkcionalnosti poput baza raznovrsnih podataka, slikovni, audio ili drugi sadržaj pohranjuju van lanca (Antonopoulos, 2017.). Pohrana van lanca se odvija ili u klasičnim centraliziranim bazama podataka ili u decentraliziranim bazama podataka koje se sastoje od mreža računala (npr. IPFS sistem pohrane). Korisnici s decentraliziranom aplikacijom najčešće komuniciraju preko internetskih stranica ili mobilnih aplikacija koje se preuzimaju direktno na uređaje. Ovakva infrastruktura omogućava korisnicima da pomoću jednostavnih korisničkih sučelja (eng. *User-friendly*) pokreću transakcije ili aktiviraju pametne ugovore koji se zatim izvršavaju preko lanca blokova te utječe na još veću inkluzivnost u decentraliziranim financijama jer otvara vrata široj publici, koja ne mora nužno imati znanje o procesima i mehanizmima ove tehnologije, da se uključi i

sudjeluje u financijskim aktivnostima. Također, decentralizirane aplikacije se oslanjaju i na pametne ugovore i njihovo automatizirano izvršavanje uz predefinirana pravila i uvjete (Antonopoulos, 2017.). Pomoću njih se odvijaju sve funkcije i interakcije koje neka decentralizirana aplikacija omogućava i izvršava za svoje korisnike (poput plaćanja, razmjene, posuđivanja itd.). Pošto su pametni ugovori i lanac blokova temelji decentraliziranih aplikacija jasno je kako sve radnje i transakcije koje se odvijaju pomoću njih se također provjeravaju i dokumentiraju pomoću sustava konsenzusa na način kao što je objašnjeno u prethodnim poglavljima. Iz toga proizlazi još jedan pozitivan aspekt njihove decentralizirane prirode, a to je da jednom kada se ugovori napišu, čak i kada imaju mogućnost naknadne izmjene (posrednički pametni ugovor), zbog transparentnosti lanca blokova, svaka slijedeća promjena je vidljiva svima što daje dodatnu sigurnost i regulatornu ulogu korisnicima (Drescher, 2017.). Sudjelovanje u donošenju odluka i upravljanju ovisi od aplikacije do aplikacije, no najčešće sudjeluje cijela zajednica koja uključuje korisnike, investitore, programere, rudare i vlasnike kriptovaluta ili tokena. Zbog toga ne dolazi do otuđenja kao što je to slučaj s centraliziranim kompanijama i institucijama. Programeri su zaduženi za razvijanje pametnih ugovora i ostalih softverskih komponenti poput korisničkog sučelja te za njihovo stalno održavanje i unapređivanje. Rudari ne sudjeluju direktno u upravljanju, no svakako imaju važnu ulogu jer provode transakcije i pametne ugovore u sklopu lanca blokova što osigurava sigurnost i poštivanje protokola aplikacije. Korisnici su također važan dio upravljačkog ekosistema jer svojim zahtjevima utječu na odluke te je čest slučaj da decentralizirane aplikacije u svojim protokolima imaju sustave glasovanja u kojima sudjeluju vlasnici kriptovaluta i upravljačkih tokena što im daje dodatnu važnost i moć. Dodatno, decentralizirane aplikacije koje su razvijene od strane kompanija najčešće imaju timove koji su zaduženi za njihovo nadgledanje, usmjeravanje, promoviranje i drugo. Još jedna novost koju donosi ova tehnologija je izbacivanje posrednika i nemogućnost cenzure što je poželjno i korisno za financijski sustav. S druge strane problemi i prepreke koji se odnose na decentralizirane aplikacije su upitna mogućnost skaliranja (prvenstveno na POW sustavu), nedostatak regulacije i posljedice ljudskih grešaka. Posljednje se odnosi na potencijalne pogreške u pametnim ugovorima koje ako se dogode, zbog ireverzibilne prirode lanca blokova, se više ne mogu ispraviti te je nanesena šteta trajna. Vezano uz to javlja se i problem nemogućnosti izmjene pametnih ugovora koji se najčešće koriste, što znači da se poboljšanja vrlo teško implementiraju.

3. Karakteristike i specifičnosti tehnologije lanca blokova

U prethodnom poglavlju objašnjeni su mehanizmi i principi na kojima se temelji tehnologija lanca blokova te je njihovo razumijevanje potrebno kako bi se moglo raspravljati o pozitivnim i negativnim posljedicama ovog inovativnog i disruptivnog sustava provođenja transakcija i pohrane podataka. Na postojećem financijskom tržištu prilikom vršenja svake transakcije plaća se određena naknada posredniku (banci ili kartičaru) koji ih provodi. U svakodnevnom životu iznos toga troška po pojedinačnoj transakciji nije toliko značajan, no kada se radi o transakcijama velikog volumena te se uzme u obzir i njihova učestalost (posebice u poslovnom svijetu) on postaje itekako značajan. U poslovnome smislu transakcijski trošak je bitan faktor, posebice u granama financijske industrije koje su transakcijski intenzivne, poput sastavljanja i upravljanja portfolija dionica, brokerskih i dilerskih poslova, arbitraže ili bilo kojeg drugog posla koji uključuje trgovanje na burzi dionica, obveznica ili drugih vrijednosnih papira. Iz toga je vidljivo kako je vremenski i troškovno efikasnije poslove obavljati direktno, bez posredovanja trećih strana, no nedostatak povjerenja i zaštite od prijevare utjecali su na razvijanje banaka i raznih financijskih institucija te njegovu centralizaciju (Casey, Vigna, 2015.). Uz transakcijske troškove iz centraliziranosti sustava proizlaze i druge negativne posljedice poput upitne i ograničene inkluzivnosti, transparentnosti i privatnosti korisnika. Razvoj i dominacija banaka i ostalih institucija dodatno su potaknuti procesom globalizacije, odnosno uključivanjem i povezivanjem cijeloga svijeta u jedan opsežni i dinamični financijski sustav. Razvoj informatičke tehnologije u 21. stoljeću omogućio je razvoj i široku primjenu tehnologije lanca blokova koja ima potencijal za restrukturiranje financijskog sustava kakav danas poznajemo.

3.1. Prednosti tehnologije lanca blokova

Osnova iz koje proizlaze koristi ove tehnologije je decentraliziranost. To svojstvo lanca blokova, uz pomoć prije opisanih mehanizama rudarenja, enkripcije i sustava konsenzusa, čini ga otpornim na bilo kakve pokušaje promjena ili izmjena podataka što osigurava

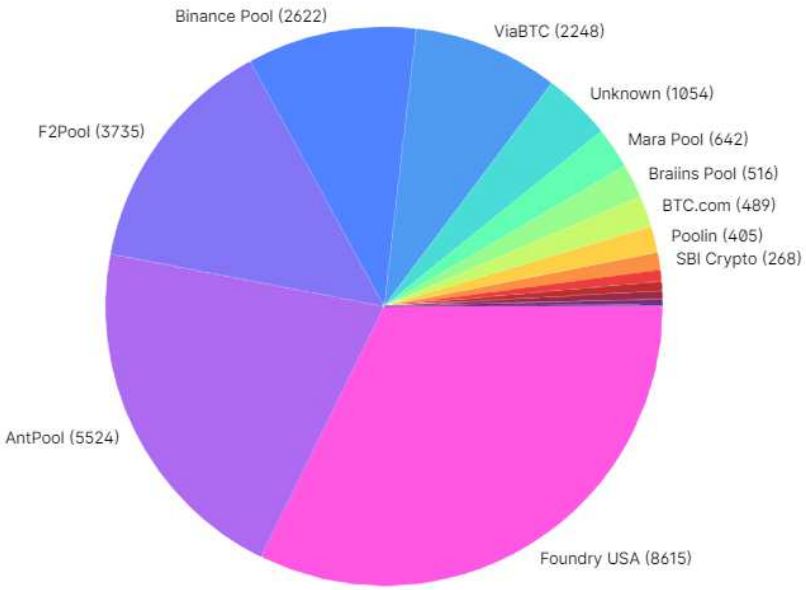
korisnike od prijevara. Pri tom ne postoji jedno ili nekoliko glavnih tijela koja kontroliraju te procese i posjeduje sve informacije nego su one distribuirane u mreži međusobno neovisnih računala. Podaci koji se nalaze na lancu blokova su javni što znači da su sve transakcije i pametni ugovori dostupni svakome te ih svatko može pregledavati i provjeravati što osigurava transparentnost. Pomoću asimetrične enkripcije, odnosno korištenja javnih i privatnih ključeva čuva se privatnost korisnika te ih se dodatno osigurava. Izbacivanje posrednika utječe na smanjenje ili potencijalno uklanjanje (u slučaju POS sistema konsenzusa) transakcijskih troškova. (Golosova, Romanovs, 2018.). Također, u slučaju financijskog sustava, dolazi do uštede vremena zbog automatiziranih pametnih ugovora te zbog nepostojanja birokratskih procesa koji inače zahtijevaju puno papirologije. Isto tako, transakcije se mogu odvijati u bilo koje doba jer ne postoji određeno radno vrijeme, kao što je to kod banaka ili burza, kada se transakcije mogu izvršavati što čini dodatnu vremensku uštedu. Generalno pojednostavljenje korištenja cijelog financijskog sustava i pristupačnost financijskih usluga utječe na njegovu veću inkluzivnost jer jedino što je potrebno kako bi im se pristupilo jest konekcija na Internet (Sundararajan, 2016.). Još jedno bitno svojstvo je veća internacionalna povezanost jer je moguće sudjelovati u investicijama, plaćanjima ili bilo kojoj vrsti poslovnih i financijskih odnosa s pojedincima iz drugih zemalja bez prepreka i potrebe za posrednikom.

3.2. Nedostaci tehnologije lanca blokova

Uz mnoštvo novosti i prednosti koje pruža tehnologija lanca blokova, postoje i određeni rizici i nedostaci koje ona nosi. Najveće prepreke za široku uporabu tehnologije lanca blokova proizlaze iz POW sustava konsenzusa i nedostatka regulacije. Jedna od negativnih posljedica nedostatka regulacije je izrazito visoka volatilnost kriptovaluta i tokena koji se danas smatraju jednim od najrizičnijih imovina za ulaganje. Upravo to je jedna od glavnih prepreka razvijanja stabilnog decentraliziranosg financijskog sustava. S druge strane uključivanje regulatornih institucija i uvođenje opsežne kontrole ovog sustava moglo bi negativno utjecati na njegovu likvidnost i funkcionalnost jer bi ograničilo transakcijske mogućnosti što bi automatski demotiviralo pojedince da koriste decentralizirane platforme i aplikacije. Nije potpuno jasno kako bi se postojeći financijski zakoni i propisi mogli prenijeti na decentralizirani financijski sustav te ne postoji konsenzus oko toga u kojoj mjeri i kako bi se oni trebali mijenjati i prilagoditi. To je otvoreno pitanje koje tek treba razriješiti u skoroj budućnosti. Drugi problem koji proizlazi iz, za sada najraširenijeg,

POW sustava konsenzusa je nemogućnost skaliranja. Kao što je već prije spomenuto zbog mehanizma ovog sustava u trenutcima visokog prometa i uključenosti velikog broja korisnika dolazi do visokih transakcijskih troškova te duljeg vremena provođenja transakcija. Većina ovih nedostataka riješena je uvođenjem POS sustava konsenzusa (Ethereum 2.0, Polkadot, Cardano itd.), no oba sustava i dalje imaju jednu zajedničku manu, a to je postepena centralizacija i potencijalno preuzimanje većine mreže od jednog ili nekolicine velikih rudara (POW) ili odobravatelja (POS) što otvara mogućnost za tzv. 51% napad (Hayes, 2022.). U tom slučaju bi pojedinac ili skupina koja kontrolira većinu računala u mreži ili ima većinu sredstava u fondu za odobravanje, imala mogućnost izmjenjivanje ili krivotvorenja lanca blokova jer je potrebna većina za konsenzus pod njihovom kontrolom.

Slika 3. Količina dodanih blokova po kompanijama od 01. siječnja do 28. lipnja 2023.god.



Izvor: https://www.blockchain.com/explorer/charts/pools (Preuzeto 28. lipnja 2023. god.)

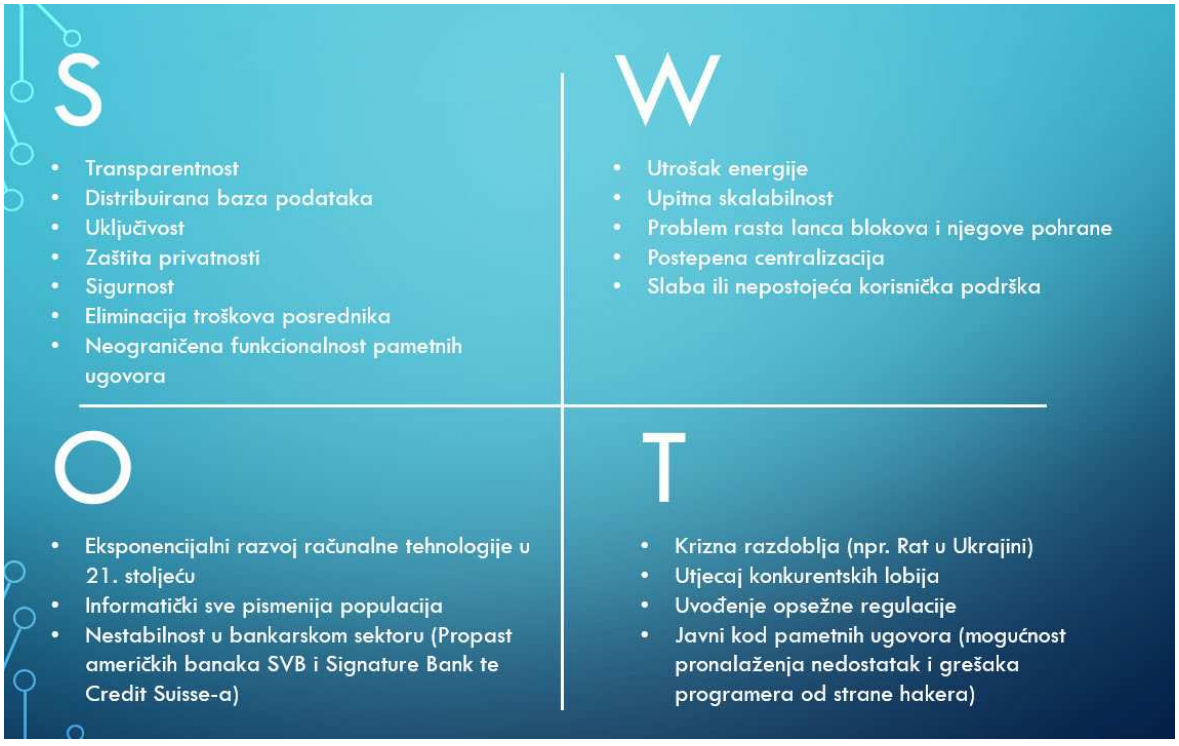
Ta potencijalna opasnost je jasno vidljiva na primjeru Bitcoina (Prikazano na slici 3) gdje postoji nekoliko velikih rudarskih kompanija, poput AntPool-a, Foundry USA-a i F2Pool-a koje trenutno u svojem zbrojenom vlasništvu imaju preko pola dodanih blokova u lancu u posljednjih šest mjeseci što postižu pomoću svojih farma za rudarenje (eng. *Mining farms*). Još jedan problem koji proizlazi iz postepene centralizacije je koncentracija bogatstva jer sav novo stvoren novac opet odlazi u vlasništvo nekolicine. Posljedica njihove koncentracije bogatstva i kontroliranja većine mreže može se odraziti i na njezin daljnji

napredak i razvitak jer se odluka o uvođenju novih procesa i protokola također donosi glasanjem većine pa postoji mogućnost manipuliranja i donošenja samo onih promjena koje njima koriste. S uključivanjem sve većeg broja korisnika i razvijanja sve više decentraliziranih aplikacija i pametnih ugovora do izražaja dolazi još jedna mana lanca blokova, a to jest limitirani kapacitet pohrane podataka (Buterin, Mogayar, 2016.). Pošto se radi o P2P mreži u kojoj svako računalo sadrži po jednu identičnu kopiju cijelog lanca blokova, odnosno svih podataka koji su na njemu spremljeni, dolazi do stanja da lanac postaje memorijski prezahtjevan za manja pojedinačna računala koja onda ne mogu više sudjelovati u mreži što opet utječe na njezinu centralizaciju. Iz tog razloga decentralizirane aplikacije koje imaju najveće memorijske zahtjeve se koriste kombinacijama pohranjivanja podataka na lancu i van lanca tako da se na lancu pohranjuju najbitniji i najosjetljiviji podaci zbog sigurnosti, a van lanca oni manje bitni.

3.3. SWOT analiza

SWOT analizom utvrđuju se snage (eng. *Strenghts*) i nedostaci (eng. *Weaknesses*) tehnologije lanca blokova te prilike (eng. *Opportunities*) i opasnosti (eng. *Threats*) iz njezine okoline.

Slika 4. SWOT tablica tehnologije lanca blokova



Izvor: Pripremio autor, 29. lipnja 2023. god.

Pošto su u prethodnom poglavlju detaljno analizirane snage i nedostaci fokus će biti na faktorima iz okoline, odnosno na prilikama i prijetnjama navedenim u SWOT tablici sa slike 4. Razvoj računalne tehnologije omogućio je razvoj tehnologije lanca blokova te njezin daljnji napredak će dodatno poboljšavati njegova svojstva. Napretkom računala, ona će biti sve efikasnija i cjenovno pristupačnija što znači da će usprkos rasta zahtjeva za računalnom snagom zbog veličine lanca blokova i dalje u sustavu moći sudjelovati šira zajednica. Nadalje, iako je opće uvriježeno mišljenje da su banke izrazito sigurne i praktički neuništive početak 2023. godine je pokazao kako je realno stanje ipak nešto drukčije. Kolaps dvije velike američke banke Silicon Valley Bank-a (SVB) i Signature Bank-a i poznate švicarske banke Credit Suisse te generalno loše performanse banaka u tom razdoblju pokazale su da ni one nisu imune na negativne ekonomske cikluse i eksterna zbivanja. Još jedna prilika za opće prihvaćanje tehnologije lanca blokova leži u mlađim generacijama koje odrastaju uz računala i pametne mobitele te su društvene mreže i računalne igrice neizostavan dio njihove svakodnevnice pa će puno lakše i rado prihvatiti tehnološke novine. S druge strane tijekom događaja poput ratnih ili globalnih kriza ljudi općenito „bježe“ prema realnoj imovini poput zlata i drugih plemenitih metala, nekretnina, gotovine, umjetnina i sličnog. Do sada je u takvim situacijama kripto tržište gubilo na vrijednosti. Druga navedena prijetnja je sputavanje od strane konkurentskih lobija (npr. bankarski) koji bi eventualnim općim prihvaćanjem decentraliziranog financijskog sustava značajno izgubili na vrijednosti. Oni mogu utjecati na provođenje određenih politika i donošenje zakona na štetu DeFi sektora. Iduća prijetnja je najkompleksnija za identificiranje jer je s jedne strane njezino uvođenje nužno, a s druge strane može potencijalno ozbiljno naškoditi prometu na DeFi platformama. Uvođenje regulacije mora biti provedeno tako da se uzme u obzir brzo napredujuća i dinamična struktura lanca blokova te nađe balans između zaštite potrošača i održavanja osnovnih principa decentraliziranih platformi. U slučaju da se pretjera s regulacijom ishod može potencijalno biti koban za decentralizirane financije. Zadnja prijetnja je javni kod pametnih ugovora koji otvara mogućnost da hakerima da ga detaljno testiraju te otkriju eventualne nedostatke i iskoriste ih. Zato je jako bitno da se korisnici dobro informiraju prije nego počnu koristiti neke od decentraliziranih aplikacija. Vrlo je bitno da se u interakciju ulazi samo s projektima iza koji stoje pouzdani i iskusni programerski timovi.

4. Analiza financijskog sustava na lancu blokova

Sama tehnologija lanca blokova i interakcije s njom zahtijevaju popriličnu razinu znanja o njoj od strane korisnika. U današnje vrijeme to predstavlja prepreku za velik broj ljudi jer iako su i mlađe i starije generacije informatički sve obrazovanije i dalje velika količina ljudi nije dovoljno digitalno pismena da bi se mogla brzo i intuitivno prebaciti na korištenje ove tehnologije. Iz tog razloga su decentralizirane aplikacije razvijene tako da budu pristupačne i upotrebljive „običnom“ čovjeku što je preduvjet za uporabu lanca blokova u široj ekonomiji

4.1. Primjena decentraliziranih aplikacija

Tijekom posljednjih godina razvijeni su mnogi pilot projekti koji su pokušali integrirati ovu tehnologiju u svoj posao. Iako atributi poput uklanjanja troškova posrednika, visoke sigurnosti, transparentnosti, efikasnosti, zaštite privatnosti te posebice lakoće u pronalaženju porijekla i nastanka transakcija ili bilo kojeg drugog zapisa na lancu blokova imaju potencijalne koristi i primjenu u gotovo svim sektorima, a ne samo u financijskom, za sada nije došlo do šireg prihvaćanja u niti jednom od njih (Tapscott, (2016.). Svakako, do sada je najveći fokus bio na poslovnom sektoru zbog same financijske prirode tehnologije lanca blokova koja je direktno povezana i ovisna o financijskoj imovini u obliku kriptovaluta. Najpoznatije kriptovalute poput Bitcoina i Ethereuma su dostigle popriličnu razinu korištenja te status legitimnog sredstva plaćanja, prvenstveno u financijskom i IT sektoru, ali i drugdje. Decentralizirane aplikacije su najviše korištene za razvijanje decentraliziranih mjenjačnica (eng. *Decentralized exchanges* - DEXES), platformi za posuđivanje i pribavljanje sredstava te decentraliziranih osiguranja.

4.2. Decentralizirana autonomna organizacija (eng. *Decentralized autonomous organization* - DAO)

Kao što joj samo ime govori, ovaj tip organizacije bi trebao biti decentralizirana verzija standardnih organizacija ili poduzeća. Kod ovih organizacija fokus je na razvijanju sustava upravljanja koji nema određenu hijerarhiju već se temelji na automatizmu pametnih ugovora i demokratskom glasanju pomoću upravljačkih tokena. Pomoću pametnih ugovora definiraju se sva pravila i odredbe te mehanizmi po kojima organizacija posluje što znači da su oni zapisani u kodu. Pošto se oni izvršavaju automatizmom, nema potrebe za centralnom upravom ili menadžerskim timom jer DAO posluje bez prekida neovisno o bilo

kojem ljudskom faktoru. Organizacijom se vodi i upravlja sustavom konsenzusa među imateljima upravljačkih tokena koje DAO izdaje. Svi takvi tokeni su identični te osim prava glasa nose i pravo na isplatu dividendi ili naknada u slučaju da organizacija posluje s dobitkom. Zbog tih koristi tokeni postižu određenu cijenu na tržištu te ih možemo usporediti s dionicama u klasičnom financijskom sustavu. Također, DAO je zamišljen tako da bude otvoren za sve pa ne postoje ograničenja i posebni zahtjevi koje netko treba ispuniti da bi mogao sudjelovati u glasanju, jedini zahtjev je da posjeduje odgovarajući token. Lanac blokova koji se nalazi u podlozi DAO-a osigurava im transparentnost pa svatko može vidjeti sve transakcije, mehanizme, pravila i promjene, uključujući sva dosadašnja glasanja. S druge strane, transparentnost ujedno predstavlja i slabost DAO-a jer omogućuje hakerima uvid u cijeli kod što im daje mogućnost da ga detaljno ispitaju te pronađu eventualne slabosti i iskoriste ih. Postoji mnoštvo prepreka za koje se još treba naći adekvatno rješenje (sigurnosni rizici, pitanje regulacije i efikasnosti), no decentralizirane autonomne organizacije imaju potencijal za razvijanje samoodrživih, automatiziranih poduzeća upravljanih direktno od same zajednice u kojoj djeluju.

4.3. Decentralizirane financije (eng. *Decentralized Finance* - DeFi)

Kako bi se mogao razviti financijski sustav temeljen na lancu blokova potreban je medij koji će povezati pojedince i omogućiti im korištenje financijskih usluga. Tu ulogu do sada su imale banke, a u decentraliziranom sustavu ju preuzimaju decentralizirane aplikacije te se pomoću njih vrše sve financijske aktivnosti. Svaka decentralizirana aplikacija temelji se na djelovanju jednog ili više pametnih ugovora koji su zapisani u njihovom kodu te omogućavaju izvršavanje njihovih predviđenih funkcija (Buterin, Mogayar, 2016.). Korisnici se pomoću svojih novčanika za kriptovalute povezuju s platformom, odnosno s pametnim ugovorom koji pokreće decentraliziranu aplikaciju te daju naloge za izvršavanje transakcija i ostalih aktivnosti koje ona nudi. U nastavku će se detaljnije objasniti kako funkcioniraju najkorištenije decentralizirane aplikacije.

- Stabilne kriptovalute (eng. *Stablecoin*)

  Izrazito bitan faktor za razvitak decentraliziranih financija su stabilne kriptovalute. To su kriptovalute čija je vrijednost vezana uz neku realnu imovinu ili najčešće uz fiducijarni novac i to u pravilu uz američki dolar (Benson, Rosen, 2022). Osmišljene su tako da u svakom trenutku budu zamjenjive za američki dolar i to prema tečaju 1

naprema 1. Na taj se način želi postići da korisnicima bude dostupno poznato sredstvo plaćanja sa stabilnom vrijednošću koje će koristiti za svakodnevne transakcije i operacije na decentraliziranom financijskom tržištu te da stabilne kriptovalute budu most između fiducijarnog novca i kriptovaluta (Hayes, 2022.). One doista jesu jedan od temelja decentraliziranog financijskog sustava te su glavno sredstvo za provođenje aktivnosti na svim DeFi platformama. Koriste se kao pričuva vrijednosti za vrijeme velikih tržišnih fluktuacija u cijenama kriptovaluta, kao referentna točka i katalizator njihovim trgovanjem te omogućuju pozajmljivanje novca. Stabilne kriptovalute svojom stabilnošću, na inače izrazito volatilnom tržištu, stvaraju uvjete za provođenje raznih poslovnih i financijskih aktivnosti. Više o njihovim konkretnim ulogama će se govoriti u slijedećim odlomcima. Najpoznatije stabilne kriptovalute su Tether, USDC i Dai.

- Povezivanje lanaca blokova

Općenito transakcije između dva različita lanca blokova su moguće samo uz pomoć posebnih posrednika ili mostova te uz pomoć pametnih ugovora. Tehnike i procesi koji omogućavaju interoperabilnost među lancima blokova uz pomoć posrednika ili mostova se uglavnom služe istim principima, a to je zaleđivanje sredstava, odnosno kriptovalute na jednom lancu te izdavanje jednake količine tokena koji predstavljaju zaleđenu kriptovalutu na drugom. Takvi tokeni se nazivaju omotani tokeni (eng. *Wrapped token*). Razmjena se može izvesti i pomoću pametnih ugovora bez potrebe za posrednikom tako da se na svakom lancu napravi po jedan pametni ugovor u kojem su dogovorena sredstva „zamrznuta“ te nakon toga dvije strane pomoću protokola razmjene ključeve koji im omogućavaju da „odlede“ i preuzmu sredstva. Ovakav tip razmjene se naziva atomska zamjena (eng. *Atomic swap*).

- Decentralizirane mjenjačnice (eng. *Decentralized exchanges* - DEX)

Poput svakodnevnih mjenjačnica koje služe za razmjenu različitih valuta, decentralizirane mjenjačnice služe za razmjenu različitih kriptovaluta. Koristeći se pametnim ugovorima one povezuju korisnike koji direktno sudjeluju u razmjeni te su kriptovalute kojima trguju u njihovom vlasništvu sve do samog trenutka izvršenja transakcije. Decentralizirane mjenjačnice omogućavaju trgovanje isključivo s kriptovalutama koje se nalaze na istom lancu blokova. Pametni ugovori su polazišna

točka svih decentraliziranih aplikacija pa tako i mjenjačnica te su pomoću njih definirana pravila i protokoli po kojima se vrše transakcije, a zapisani su u kodu u lancu blokova (Lewis, 2018.). U pravilu decentralizirane mjenjačnice funkcioniraju na jedan od dva načina, a to je pomoću knjiga narudžbe ili pomoću automatskih stvaratelja tržišta (eng. *Automated market makers* - AMM). Princip knjiga narudžbe je sličniji današnjem načinu funkcioniranja mjenjačnica, a odvija se tako da korisnici unose u knjigu, koja je u stvari pametni ugovor, količine i cijene kriptovaluta koje žele kupiti ili prodati. Zatim se preko pametnog ugovora automatizmom spajaju odgovarajuće ponude i preko lanca blokova odobravaju transakcije. Drugi princip rada decentraliziranih mjenjačnica (AMM) je češći te on funkcionira na temelju specijaliziranih pametnih ugovora koji se zovu fondovi likvidnosti (eng. *Liquidity pool*). Fondovi likvidnosti nastaju tako da investitori ulažu određene količine kriptovaluta u njih, a zauzvrat dobivaju udio u naknadama od svake transakcije u jednakom omjeru kao njihov udio u fondu. U početnom stanju, kada investitori pružaju likvidnost, uzimaju se kriptovalute tako da je udio u ukupnoj cijeni svake od njih jednak (najčešće 50:50), dok količine ovise o vrijednosti svake kriptovalute zasebno u tom trenutku. Na primjer u trenutku prikupljanja sredstava 1 Ether može vrijediti kao 10 Binance Coin-a pa će takav biti i omjer njihove količine u fondu. Cijene i odnosi po kojim se odvijaju transakcije se određuju automatski pomoću algoritma koji radi na principu konstantne jednakosti. To znači da se uvijek održavaju jednaki odnosi količina u fondu tako da se poštuje jednadžba $x*y = K$, gdje su x i y početna stanja količina različitih kriptovaluta, a K se dobiva kao njihov umnožak te ostaje konstantan. Pomoću te jednadžbe se dobiva količina izlazne kriptovalute koju treba isplatiti korisniku za određenu količinu ulazne kriptovalute. Svaka promjena količine određene kriptovalute na gore ili dolje utječe i na pomak svoje cijene u istom smjeru te količine i cijene druge kriptovalute u suprotnom. Tako se osigurava da udio svake od njih u ukupnoj vrijednosti uvijek bude jednak. U sustav trgovanja se može uključiti neograničen broj različitih kriptovaluta na način da se fondovi likvidnosti povezuju preko one zajedničke. Što je više sredstva u fondovima likvidnosti to je cijena kriptovaluta koje se nalaze u njima stabilnija jer svakodnevne transakcije imaju manji učinak na promjenu odnosa količine te posljedično, zbog načina na koji djeluje algoritam, i na promjenu cijene. Još jedan mehanizam koji utječe na stabilnost cijena u fondovima je djelovanje arbitražera. Oni djeluju identično kao i u klasičnom financijskom sustavu tako da

kupuju na tržištu gdje je cijena niža i prodaju tamo gdje je ona veća. U kontekstu fondova likvidnosti, ako je njihova cijena kriptovalute niža od tržišne, arbitražeri će ju kupovati kako bi je prodali uz profit te utjecati na algoritam tako da cijena u fondu raste.

- Decentralizirano zaduživanje i pozajmljivanje

Jedna od najbitnijih zadaća financijskog sustava je omogućavanje korisnicima da dođu do kapitala koji im je potreban da bi mogli vršiti poslovne aktivnosti. Potreba za zaduživanjem proizlazi iz svakodnevnih poslovnih aktivnosti, radilo se o pokretanju novog poslovnog pothvata, proširenju postojećeg ili bilo kojem drugom razlogu koji od poduzeća ili pojedinca zahtjeva nova kapitalna ulaganja. S druge strane, oni koji posjeduju višak kapitala imaju potrebu uložiti ga kako bi dodatno zaradili na kamatama ili jednostavno kako im kapital ne bi gubio na vrijednosti zbog inflacije. Do sada su glavni davatelji zajmova bile banke i investicijski fondovi, dok se u decentraliziranom financijskom sustavu, pomoću decentraliziranih aplikacija i pametnih ugovora direktno spaja korisnike (Casey, Vigna, 2015.). Slično kao i kod decentraliziranih mjenjačnica zajmodavci ulažu svoja sredstva u fondove likvidnosti iz kojih korisnici mogu pozajmiti sredstva, dok oni zauzvrat dobivaju kamatu. Sve se odvija automatikom preko pametnih ugovora u kojima su definirani svi detalji i odnosi (razdoblje i plan povrata, izračun kamatnih stopa, iznos zaloga itd.). Kamatne stope se računaju pomoću algoritama u sklopu pametnih ugovora te ovise o trenutnim razinama potražnje za sredstvima i drugim predefiniranim faktorima. Zbog izrazite volatilnosti kriptovaluta i općenito kriptoimovine postavljeni su posebni zahtjevi za kolateralom prilikom odobravanja kredita. Visina zaloga najčešće mora biti viša od samog iznosa koji se pozajmljuje te se postavlja određena granica likvidacije ispod koje ne smije pasti vrijednost založene imovine. Ovaj mehanizam se naziva prekomjerna kolateralizacija (eng. *Overcollateralization*). U slučaju pada vrijednosti imovine ispod likvidacijske granice pametni ugovor automatski zatvara pozajmicu tako što prodaje kolateralu te namiruje zajmodavca. Logično je da se nameće pitanje koji je smisao pozajmljivanja ako je potrebno založiti sredstva koja su vrjednija od same pozajmice. Korist ovakvog zaduživanja također proizlazi iz volatilnosti kripto imovine jer se pohranjivanjem njene određene količine u pametnom ugovoru čuva njihova vrijednost, dok se zauzvrat dobivaju sredstva u obliku stabilnih kriptovaluta koja se onda koriste za provođenje

financijske aktivnosti. Na ovaj se način štiti od potencijalnog gubitka koji bi nastao ako se vrijednost kriptovalute koja se koristila za financiranje poslovne aktivnosti poveća. Nadalje, ovakav princip pozajmljivanja nam omogućuje i korištenje financijske poluge u slučaju da pozajmljeni iznos stabilne kriptovalute ponovno reinvestiramo u kriptovalutu za koju smatramo da će cijena rasti. Kao i kod svakog korištenja poluge, veća mogućnost zarade znači i veći potencijalni gubitak tj. u slučaju negativnog kretanja cijena imovine u koju se investiralo gubi se višestruko.

- Platforme za osiguranje

Slično kao i s prethodnim decentraliziranim aplikacijama, platforme za osiguranje pomoću svojih pametnih ugovora definiraju sve odnose i obveze (odredbe i uvjeti police osiguranja, iznos premije, razina zaštićenosti, uvjeti i isplata sredstava u slučaju nastupanja događaja od kojeg se štiti) koje imaju osiguratelj i osiguranik. Sredstva investitora, koje u ovom slučaju nazivamo osiguratelјima, se skupljaju u fondove koji služe za eventualnu isplatu po policama osiguranja, dok oni zauzvrat za uložena sredstva dobivaju naknade u obliku premija koje plaćaju osiguranici. Specifičnost ovih platformi je u tome što postoji potreba za konstantnim praćenjem uvjeta u stvarnome svijetu kako bi se moglo utvrditi nastupanje događaja od koji se korisnici osiguravaju (npr. Visoke ili niske temperature, požari, oluje, krize itd.). U tu svrhu se koriste vanjski izvori informacija koji se koriste kako bi se mogli utvrditi i pratiti uvjeti iz stvarnog svijeta. Ti izvori su definirani u pametnom ugovoru te svaka strana koja sudjeluje u njemu, pošto je on transparentan, može vidjeti koji su to izvori te odlučiti želi li sudjelovati u takvom ugovoru. Primjerice ako je u ugovoru definirano da će osiguraniku biti nadoknađena šteta koja nastaje u slučaju elementarne nepogode, kao izvor može biti određena stanica za mjerenje temperature i praćenje vremena te će se njezine informacije koristiti kao izvor za utvrđivanje nastupanja definiranog događaja.

4.4. Primjena nezamjenjivih tokena

Uz sve mogućnosti standardnih tokena te načine na koje se mogu primjenjivati, nezamjenjivi tokeni dodaju još i dimenziju jedinstvenosti što dodatno proširuje spektar potencijalne primjene (Lewis, 2018.). Njihova garancija autentičnosti i jedinstvenosti ima mnoštvo potencijalnih primjena i u financijskom sustavu.

- Otvaranje mogućnosti za poduzetnike da svoje proizvode prodaju direktno kupcima bez potrebe za posrednikom. Na ovaj način se može stvoriti značajna ušteda pošto su poduzećima s velikim obujmom prometa ukupni transakcijski troškovi izrazito visoki, dok ona s manjim obujmom najčešće plaćaju veće naknade po transakciji.
- Mogućnost implementacije tantijema u pametni ugovor što znači da nakon izdavanje od svake iduće prodaje izdavatelj dobiva određenu naknadu (Hayworth, 2021.). Ovo svojstvo se može potencijalno primijeniti u raznim poslovnim ugovorima i za privlačenje investitora koji često zahtijevaju ugovore tog tipa dok im se ne vrati određeni iznos uloženog.
- U slučaju garancije vlasništva nad imovinom nezamjenjivi tokeni se potencijalno mogu koristiti kao kolaterala pri zaduživanju i financiranju.
- Tokenizacija kolekcionarskih predmeta. Zbog svojstva tehnologije lanca blokova i nemogućnosti izmjene zapisa nezamjenjivi tokeni bi služili kao dokaz originalnosti (satovi, umjetnine, knjige ili bilo koja druga imovina).
- Svestrane mogućnosti pametnih ugovora i jedinstvenost nezamjenjivih tokena otvaraju mogućnost za razvijanjem raznih financijskih instrumenata poput opcija, izvedenica ili nekih novih špekulativnih instrumenata (Lewis, 2018.).

5. Primijenjena tehnologija lanca blokova

Svjedočili smo da je početkom 2022. godine ovaj sektor doživio veliki pad te nije dosegnuo niti približnu razinu prihvaćanja kao što se to u nekim trenutcima činilo da će biti. S druge strane, opće je poznato da su nove tehnologije sklone velikim tržišnim oscilacijama te s obzirom na količinu kapitala koja se odjednom i bez pokrića počela ulagati u ovaj sektor, možemo reći da ni ne čudi to što se u konačnici dogodio kolaps. No, ono što je pozitivno jest tehnologija koja je ipak napredovala u ovom razdoblju te se pokazalo kroz primjere raznih platformi da ona doista ima realnu primjenu i mogućnost pružanja medija za razvijanje decentraliziranog financijskog sustava.

5.1. Primjeri financijskih platformi

Iako postoji mnoštvo lanaca blokova koji podržavaju razvijanje decentraliziranih financijskih platformi, Ethereum se nametnuo kao uvjerljivi lider u tom sektoru. Od ukupnih sredstava uloženih u protokolima decentraliziranih financijskih platformi na svim lancima u 2022. godini, čak 58% je na Ethereumu[1]. Pošto su najpoznatije platforme s najvećim volumenima transakcija upravo na ovom lancu u nastavku će se analizirati neke od njih.

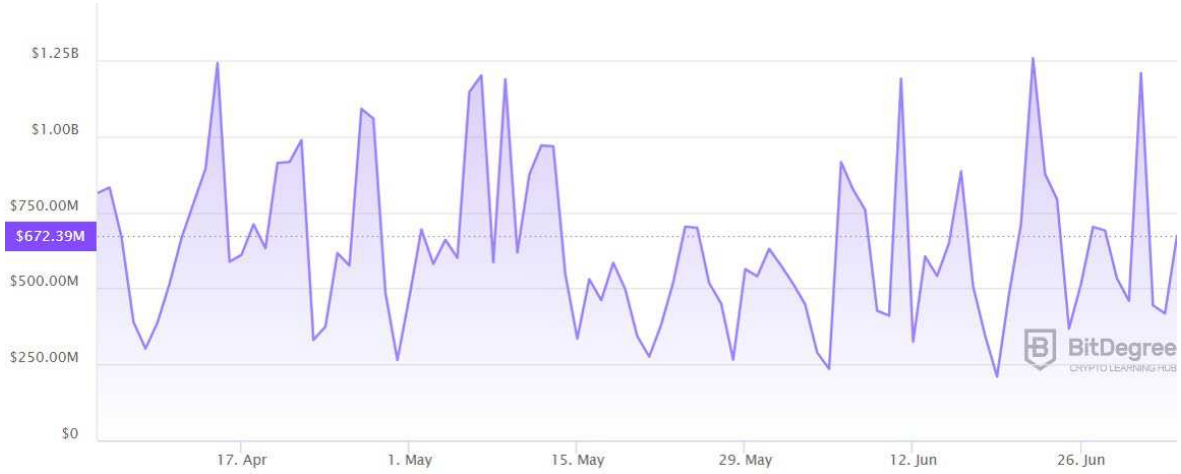
- Uniswap i SushiSwap

  Uniswap je prva decentralizirana mjenjačnica pokrenuta 2018. godine na lancu blokova Ethereum te je vrlo brzo postigla veliku popularnost zbog jednostavnog korisničkog sučelja i velikog broja tokena u ponudi (u prosjeku više od 900). Ona funkcionira po principu automatskih stvaratelja tržišta (eng. *Automated market makers* - AMM) te pruža mogućnost trgovanja tokenima tipa ERC-20 izdanim na lancu blokova Ethereum pomoću pametnih ugovora. Prilikom trgovanja naplaćuje se fiksna naknada od 0,3% te svatko tko uloži u fond likvidnosti zauzvrat dobiva tokene pružanja likvidnosti (eng. *Liquidity provider token* – LP token) koji reprezentiraju njihov udio u fondu i naknadama. Uniswap je 2020. godine po prvi puta izdao svoj upravljački token Uni.

Izvor: https://www.banklesstimes.com/defi-statistics/ (pristupljeno: 02. srpnja 2023. god.)

On omogućuje glasanje prilikom donošenja odluka o unaprjeđenjima i promjenama na decentraliziranoj aplikaciji. Posljednja verzija V3 pokrenuta je u svibnju 2021. godine.

Slika 5. Volumen trgovanja na Uniswap (V3) mjenjačnici u travnju, svibnju i lipnju 2023. god.



Izvor: https://www.bitdegree.org/top-crypto-exchanges/uniswap-v3 (Preuzeto 02. srpnja 2023. god.)

Iz grafikona prikazanog na slici 4 vidimo da prosječan dnevni volumen trgovanja u razdoblju između travnja i lipnja 2023. godine iznosi oko 600 milijuna dolara uz nerijetke prijelaze preko jedne milijarde dolara. Za usporedbu prosječni dnevni volumen trgovanja na NYSE-u (eng. *New York Stock Exchange* – NYSE) iznosi 18,9 milijardi američkih dolara. Druga popularna decentralizirana mjenjačnica pokrenuta u kolovozu 2020. godine koja je nastala na bazi koda Uniswap-a s idejom da poboljša neke njegove aspekte je Sushiswap. Isto kao i Uniswap, ona funkcionira na principu AMM-a te je vođena od strane zajednice pomoću upravljačkih Sushi tokena. Zanimljiva novost koju je Sushiswap uveo je nagrada za pružanje likvidnosti, odnosno za investiranje u njihove fondove u obliku Sushi tokena koji se onda mogu koristiti za glasovanje ili ponovno investirati u fond (tako zvani *Yield farming*) što je dodatan motiv korisnicima da ulažu u ovu decentraliziranu aplikaciju. S druge strane, Sushiswap si ovom metodom osigurava dodatnu likvidnost. Druga bitna promjena je vezana uz transakcijske naknade, dok je na Uniswap-u ona fiksna i iznosi 0,3% na Sushiswap-u ona ovisi o ponudi i potražnji Sushi tokena. Ovo su samo dvije poznatije među mnoštvom decentraliziranih mjenjačnica te se na svima zajedno ostvaruje prosječni dnevni volumen od približno 2,34 milijarde dolara. Kada usporedimo ukupni

volumen samo s NYSE vidimo da trenutno decentralizirane mjenjačnice te općenito financije se ne koriste niti približno intenzivno kao tradicionalne. S druge strane, može se reći da je volumen njihovih transakcija dovoljno značajan da može služiti kao potvrda da je ovakva financijska infrastruktura održiva.

- Aave

Jedna od najpoznatijih decentraliziranih aplikacija u DeFi sektoru koja služi za zaduživanje i pozajmljivanje raznih kriptovaluta te je također postavljena na lancu blokova Ethereum. Djeluje na principu pametnih ugovora koji omogućuju zajmodavcima da ulažu sredstva u fondove likvidnosti koja se zatim mogu posuditi drugim korisnicima tj. zajmoprimcima, dok zajmodavac zauzvrat dobiva kamatu. Platforma se dodatno osigurava sa sustavom prekomjerne kolateralizacije. Na taj se način štiti zajmodavce u slučaju da zajmoprimac ne može vratiti dug ili nastupi likvidacija. Ova platforma također ima svoje upravljačke tokene koji se izdaju i kao nagrada za zajmodavce (Aave token). Kao i kod svih drugih decentraliziranih aplikacija vlasnici tih tokena mogu sudjelovati u upravljačkim procesima te nude još neke dodatne, nestandardne mogućnosti. Aave tokeni se mogu koristiti za plaćanje transakcijskih troškova i troškova kamata, mogu se uložiti u rezervni ASM (eng. *Aave Safety Module*) fond koji služi za dodatno osiguranje zajmodavaca te se mogu uložiti u jedan od fondova likvidnosti. Još jedna specifična funkcija ove platforme su brzi krediti (eng. *Flash loans*). Oni omogućavaju da se posude veliki iznosi bez davanja kolaterale i uz niske naknade uz uvjet da budu otplaćeni u sklopu iste transakcije (na lancu blokova Ethereum proces odobravanja najčešće traje 10-15 sekundi). To se postiže pomoću kombiniranja više pametnih ugovora koji su međusobno povezani u kodu. Proces započinje tako da zajmoprimac definira količinu kriptovalute koju želi posuditi te adresu i način na koji će ju iskoristiti. Zatim pametni ugovor pomoću kojega se provodi funkcija brzog kredita provjerava ispunjavaju li navedene transakcije zahtjeve, odnosno hoće li se moći vratiti dug i kamate. Ako su uvjeti zadovoljeni, brzi kredit se odobrava i sredstva se prebacuju na navedenu adresu u ugovoru. Nakon provođenja definiranih transakcija zajmoprimac vraća posuđena sredstva uvećana za kamate zajmodavcu, odnosno platformi. Pošto su sve transakcije povezane pomoću pametnih ugovora one se na lancu blokova mogu zapisati kao jedna skupna transakcija. U slučaju da nakon odrađenih transakcija zajmoprimac nema dovoljno sredstava da bi

vratio dug aktivira se mehanizam storniranja transakcije (eng. *Transaction reversal*). U tom slučaju pametni ugovor vrši operacije potrebne za vraćanje početnog stanja poput vraćanja originalnog novca platformi i poništavanja svih transakcija i promjena koje su se događale u procesu pomoću raznih tehnika. Nakon toga mreža računala u lancu blokova briše transakciju (eng. *Roll back*) i time osigurava da se sva stanja na računima vrate u početno stanje. Storniranje transakcije je moguće samo u kratkom periodu, ovisno o pravilima lanca blokova na kojem se one vrše, no najčešće je to vremensko razdoblje od svega nekoliko do desetak sekundi. Brzi krediti omogućavaju kratkoročni pristup velikoj količini sredstava što otvara vrata raznim kompleksnim financijskim operacijama te iskorištavanju kratkoročnih prilika i anomalija na tržištu.

Sve decentralizirane financijske aplikacije imaju zajedničku namjeru da omoguće korisnicima veću kontrolu nad vlastitom imovinom, bolje uvjete poslovanja i veću uključenost. Usprkos tome, korisnici moraju biti svjesni rizika koje one nose poput izrazite volatilnosti, potencijalnih nedostatak pametnih ugovora i nedostatka likvidnosti.

5.2. Primjeri primjene i platformi za trgovanje nezamjenjivim tokenima

Nakon početnog razdoblja izdavanja nezamjenjivih tokena vezanih isključivo uz slikovni sadržaj bez nekih drugih osobitih značajki ili potencijalnih povlastica, počeli su se razvijati i projekti sa zanimljivim i potencijalno korisnim idejama. Većina tih projekata je pokrenuta samo s ciljem iskorištavanja izrazito volatilnog tržišta koje se nalazilo na povijesnom vrhuncu te su koristi tih nezamjenjivih tokena ostali samo obećanja. Nakon što je „balon“ pukao u svibnju 2022. godine velika većina projekata je propala te su njihovi nezamjenjivi tokeni postali bezvrijedni. Međutim, bilo je i dobro organiziranih projekata koji su do neke mjere i pokazali potencijalne upotrebe i mogućnosti nezamjenjivih tokena. U nastavku će se izdvojiti neki od najpoznatijih takvih projekata.

NBA topshot – platforma pokrenuta od strane američke Nacionalne košarkaške zajednice (eng. *National basketball association* – NBA) koja izdaje digitalne kolekcionarske zbirke u obliku nezamjenjivih tokena. Svaki nezamjenjivi token je vezan uz kratki video koji

prikazuje neki istaknuti isječak iz utakmice. Ova platforma je zanimljiva jer je uz određene kolekcije ili pojedinačne nezamjenjive tokene počela vezati i druge koristi poput ulaznica na utakmicu ili upoznavanja poznatih košarkaša.

Veefriends – kolekcija od poznatog američkog poduzetnika, govornika i autora. Ova kolekcija nezamjenjivih tokena je vrlo upitne umjetničke vrijednosti pošto je slike vezane uz nezamjenjive tokene nacrtao sam Gary Vee. No, ono što je zanimljivo je to što posjedovanje ovog tokena omogućava prisustvovanje na njegovim javnim govorima i seminarima za koje se inače ulaznice naplaćuju i po nekoliko stotina dolara.

OpenSea – najveća decentralizirana platforma za trgovanje s nezamjenjivim tokenima. U ponudi se mogu pronaći nezamjenjivi tokeni svih vrsta poput originalnih slikovnih kolekcija, raznih predmeta namijenjenih video igricama, sportskih i drugih kolekcionarskih sličica te virtualnih zemljišta (popularizirano za vrijeme raznih projekata metaversa). Privukla je mnoštvo korisnika zbog jednostavnosti kreiranja nezamjenjivih tokena pomoću platforme i njihovog plasiranja. Posebno je zanimljiva opcija određivanja tantijema od svake iduće prodaje nakon izdavanja tokena. Svoj vrhunac je doživjela krajem 2021. i početkom 2022. godine kada je mjesečni volumen trgovanja prelazio 3 milijarde dolara.

6. Zaključak

Današnje društvo je naviknuto na dominaciju banaka i velikih korporacija koje su postale sinonim za poslovni i financijski svijet. Na njih se gleda kao na nezaobilazan autoritet koji održava i osigurava cijeli financijski sustav. Iz tog razloga potrebno je puno napora i dokazivanja da bi došlo do prihvaćanja nekog alternativnog sustava poput decentraliziranih financija od šire populacije. Tehnologija lanca blokova koja je podloga za razvijanje tog sustava je prvi put predstavljana javnosti 2009. godine s pojavljivanjem Bitcoina. Međutim, prve decentralizirane aplikacije i složenije financijske strukture počele su se razvijati tek s pojavom lanca blokova Ethereum 2015. godine koji je proširio mogućnosti i doseg pametnih ugovora. Zato se može reći da je ova tehnologija relativno nova te se na temelju do sada razvijenih financijskih rješenja ne može definitivno prosuditi njezina budućnost u financijskom sektoru. Činjenica je da je u svojim počecima obilježena izrazitom volatilnosti te negativnim financijskim ishodom za veliku većinu investitora i projekata, no to je proces kojem je društvo kroz povijest svjedočilo već više puta te je jedan od najpoznatijih u posljednjih nekoliko desetljeća „pucanje“ .com balona (eng. *.com Bubble*) pokrenutog uzletom interneta. Dodatno, zbog određenih mogućnosti koje pruža ova tehnologija poput baratanja s izrazito velikom količinom sredstava bez regulacije, izdavanja raznih kriptovaluta i tokena omogućeno je prevarantima da se lako uključe i zarađuju na strahu od izostavljanja u zaradi (eng. *Fear of missing out*) i naivnosti ljudi. Isto tako, zbog navedenih transakcijskih mogućnosti (posebice međunarodnih), te zbog nedostatka regulacije kripto sektor je služio za pranje novca i druge financijske malverzacije. S druge strane, određeni projekti poput onih o kojima se govorilo u ovome radu su pokazali da se s kvalitetnom infrastrukturom na lancu blokova mogu odvijati vrlo složeni financijski procesi i odnosi uz još neke dodatne koristi i novosti koje on nosi. Postoji mnoštvo prepreka koje se još moraju nadvladati da bi došlo do općeg prihvaćanja ove tehnologije, počevši od direktnog konkuriranja bankarskom sektoru za kojeg je opće poznato da je jedan od najmoćnijih, ako ne i najmoćniji sektor u svijetu. Uz taj problem postoje još i razne tehničke poteškoće koje se moraju razriješiti poput konzumacije energije, tendencije da se s vremenom sustav centralizira te vječno pitanje regulacije. Ovo posljednje je ključna odrednica za razvoj DeFi-ja te predstavlja dvosjekli mač jer s jedne strane pruža sigurnost koja je krucijalna u privlačenju šire populacije na ovaj sustav, no s druge strane ograničava neke njegove funkcionalnosti zbog kojih je i postao popularan (anonimnost, neregulirano međugranično prebacivanje sredstava, lako dizanje kapitala

pomoću ICO-a itd.). Ono što je sigurno i što kriptovalute poput Bitcoina dokazuju jest da je decentralizirani sustav, iako relativno mlad, pokazao određenu otpornost te da ima popriličnu bazu stalnih korisnika i ljudi koji vjeruju i špekuliraju na njegov napredak i uspjeh. Također, sektor je i dalje vrlo aktivan te se svakodnevno javljaju novi projekti i nadogradnje koji sve češće uključuju i najpoznatije svjetske kompanije iz svijeta sporta, tehnologije i mode.

Popis literature

1. Ammous S. (2018.), The Bitcoin standard, Wiley; 1st edition
2. Antonopoulos A. (2017.), Mastering Bitcoin, O'Reilly Media; 2nd edition
3. Agashe A. (2019.), Blockchain Bubble or Revolution: The Future of Bitcoin, Blockchains, and Cryptocurrencies, Paravane Ventures
4. Bashir I. (2017.), Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks, Packt Publishing
5. Beck J. (2020.), The Ethereum beacon chain 2.0 is here, preuzeto s https://consensys.net/blog/blockchain-explained/the-ethereum-2-0-beacon-chain-is-here-now-what/
6. Benson A., Rosen A. (2022.), Stablecoin Definition: What Are They and How Do They Work?, preuzeto s https://www.nerdwallet.com/article/investing/stablecoin
7. Buterin V., Mogayar W. (2016.), The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, Wiley; 1st edition
8. Casey M., Vigna P. (2015.), The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order, St. Martin's Press
9. Drescher D. (2017.), Blockchain Basics: A Non-Technical Introduction in 25 Steps, Apress; 1st ed. edition
10. Frankenfield J. (2022.), Proof of work, preuzeto s https://www.investopedia.com/terms/s/stablecoin.asp
11. Frankenfield J. (2022.), Smart Contracts, preuzeto s https://www.investopedia.com/terms/s/smart-contracts.asp
12. Golosova J., Romanovs A. (2018.), The advantages and disadvantages of the blockchain technology, Institute of Electrical and Electronics Engineers
13. Hayworth M. (2021.), The Ultimate Non Fungible Token Guidebook: A Practical Guide to Everything NFT in Everyday Language, Kindle
14. Hayes A. (2022.), What is a blockchain ?, preuzeto s https://www.investopedia.com/terms/b/blockchain.asp
15. Hayes A. (2022.), Stablecoin, preuzeto s https://www.investopedia.com/terms/s/stablecoin.asp
16. Lewis A. (2018.), The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography,

Derivatives Investments, Futures Trading, Digital Assets, NFT), Mango; Illustrated edition

17. Paszke A. (2021.), Layer 2 blockchain, preuzeto s https://academy.binance.com/en/glossary/layer-2
18. Sundararajan A. (2016.), The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism, Cambridge; London
19. Swan M. (2015.), Blockchain: Blueprint for a New Economy, O'Reilly Media; 1st edition
20. Tapscott D., Tapscott A. (2016.), Blockchain revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Portfolio
21. Vigna P. (2018.), The truth machine: The Blockchain and the Future of Everything, St. Martin's Press

Popis slika

Luka Živković

Curriculum Vitae

Adresa: Hercegovačka 32, 10000 Zagreb

Broj telefona: +385 91 595 3323

E-mail adresa: luka.zivkovic98@gmail.com

Datum rođenja: 07.10.1998.

Vještine

- Rad na računalu - MS Office (Word, Excel, Powerpoint, Outlook)
- Programiranje (C, C++)
- Interpersonalne vještine, upravljačke vještine, integritet, kritičko razmišljanje

Radno iskustvo

PricewaterhouseCoopers / Student u reviziji

Studeni 2022 - Svibanj 2023, Zagreb

Studentski posao u odjelu revizije.

ECOMED d.o.o. / Voditelj webshopa i prodaje

Rujan 2021 - Trenutno, Zagreb

Exterra Pharma d.o.o. / Studentski posao

Svibanj 2019 - Listopad 2021, Zagreb

B4B d.o.o. / Studentski posao

Listopad 2018 - Ožujak 2019, Zagreb

Zmajsko pivovara d.o.o. / Studentski posao

Lipanj 2017 - Kolovoz 2017 - Listopad 2021, Zagreb

Obrazovanje

Ekonomski fakultet Sveučilišta u Zagrebu / Fakultet

Listopad 2017 - Trenutno

Student pete godine na smjeru analize i poslovnog planiranja

Prirodoslovno-matematički fakultet - istraživačka matematika, Sveučilište u Zagrebu / Fakultet

Listopad 2020 - Trenutno (mirovanje studijskih obveza)

VII. gimnazija / Srednja škola

Rujan 2013 - Lipanj 2017, Zagreb

—

Jezici

- Hrvatski (materinji jezik)
- Engleski - tečnost u govoru i pismu
- Njemački - praktično znanje

—

Interesi

- Financijska tržišta
- Jezici
- Politika
- Futsal (član EFZG futsal momčadi)

—

Tečajevi/Smjerovi

- Delf A2
- Erasmus + razmjena mladih