Decentralizirano financiranje

Vakanjac, Karlo

SVEUČILIŠTE U RIJECI
POMORSKI FAKULTET

KARLO VAKANJAC

DECENTRALIZIRANO FINANCIRANJE

ZAVRŠNI RAD

Rijeka, 2022.

SVEUČILIŠTE U RIJECI
POMORSKI FAKULTET

DECENTRALIZIRANO FINANCIRANJE
DECENTRALIZED FINANCE
ZAVRŠNI RAD

Kolegij: Elektroničko poslovanje
Mentor: doc. dr. sc. Dario Ogrizović
Komentor: doc. dr. sc Ozren Rafajac
Student: Karlo Vakanjac
Studijski smjer: Logistika i menadžment u pomorstvu i prometu
JMBAG: 0242046627

Rijeka, rujan, 2022.

Student: Karlo Vakanjac

Studijski program: Logistika i menadžment u pomorstvu i prometu

JMBAG: 0242046627

IZJAVA O SAMOSTALNOJ IZRADI ZAVRŠNOG RADA

Kojom izjavljujem da sam završni rad s naslovom Decentralizirano financiranje izradio/la samostalno pod mentorstvom doc. dr. sc. Daria Ogrizovića te komentorstvom doc. dr. sc. Ozrena Rafajca.

stručnjaka/stručnjakinje iz tvrtke _____
(naziv tvrtke).

U radu sam primijenio/la metodologiju izrade stručnog/znanstvenog rada i koristio/la literaturu koja je navedena na kraju završnog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo/la u završnom radu na uobičajen, standardan način citirao/la sam i povezao/la s fusnotama i korištenim bibliografskim jedinicama, te nijedan dio rada ne krši bilo čija autorska prava. Rad je pisan u duhu hrvatskoga jezika.

Student/studentica

(potpis)

Karlo Vakanjac

Student: Karlo Vakanjac

Studijski program: Logistika i menadžment u pomorstvu i prometu

JMBAG: 0242046627

IZJAVA STUDENTA – AUTORA
O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Izjavljujem da kao student – autor završnog rada dozvoljavam Pomorskom fakultetu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Pomorskog fakulteta.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Pomorskog fakulteta, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog ograničenja mog završnog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/licenses/

Student/studentica - autor

(potpis)

SAŽETAK

Decentralizirano financiranje (DeFi) u svijetu je još uvijek daleko od poznatog pojma, a naročito primjene u svakodnevnici. Razlog tome je trenutno uska mogućnost temeljnoga objašnjenja kako to zapravo funkcionira i zašto pojedinac ne bi više morao biti ovisan o svojoj banci. Glavni motiv decentralizacije jest oslobađanje „malih ljudi“ od velikih moćnika koji upravljaju masovnim količinama novaca i bankama. Putem Blockchain tehnologije svaka transakcija je vidljiva i transparentna u samome kodu. Dajući pojedincu pristup i kontrolu novaca na njegov izbor bilo kad i u bilo koje vrijeme. Tržišta su uvijek otvorena i nema centraliziranih tijela koja mogu blokirati plaćanja ili uskratiti pristup bilo čemu. DeFi je otvoreni i globalni financijski sustav izgrađen na internetu za svakoga. U kodu leži istina.

Ključne riječi: blockchain , financije, decentralizacija, kontrola

SUMMARY

Decentralization (Defi) in the world is still far from being known, especially for everyday use. The reason for this is the currently narrow possibility of a fundamental explanation of how this actually works and why the individual should no longer be dependent on his/her bank. The main motive of decentralization itself is the release of “small people” from large powers who manage mass amounts of money and banks. Through Blockchain technology, each transaction is visible and transparent in the code itself. It gives an individual access and control of funds to person's choice at any time. Markets are always open and there are no centralised bodies that can block payments or deny access to anything. Defi is an open and global financial system built online for everyone. The truth lays in the code.

Keywords: blockchain, finance, decentralization, control

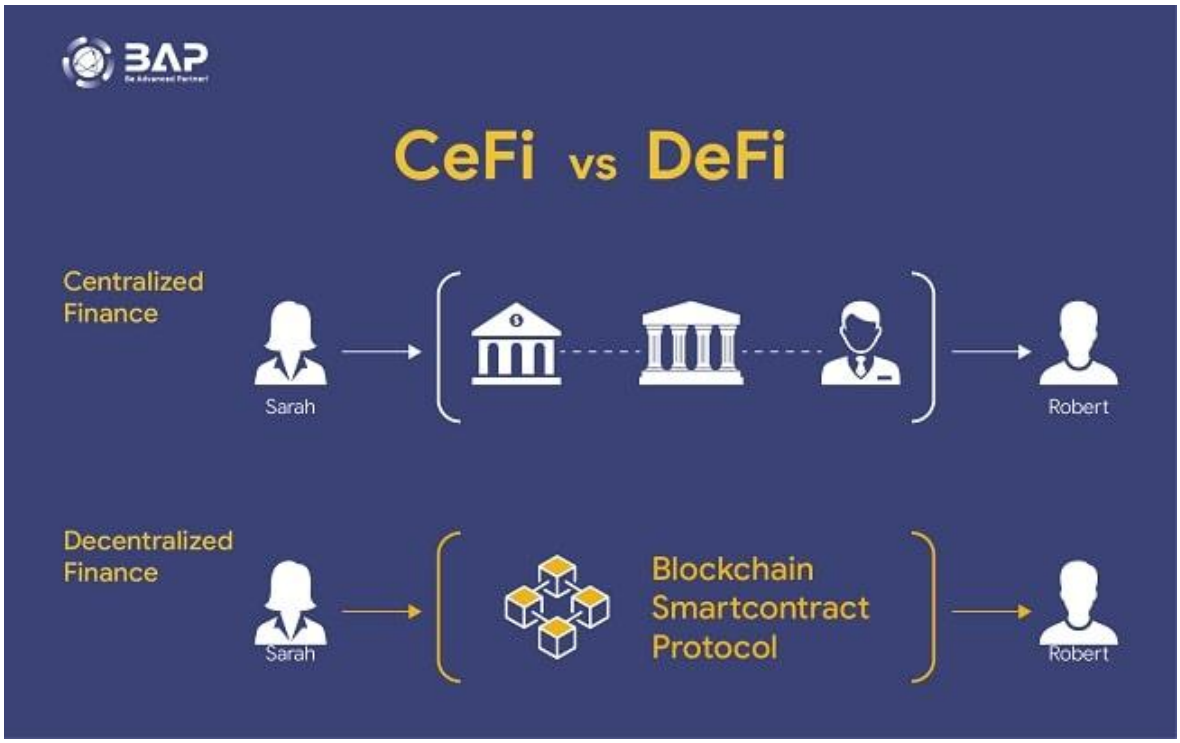
SADRŽAJ

1. UVOD

Stvaranjem novih tehnologija rezultiralo je dinamičnim pomakom u financijskim i tehnološkim sustavima. Ovaj pomak rezultirao je načinom na koji se razvijaju aplikacije i njihovom temeljnom strukturom u radu. Decentralizirane financije su dinamična i tehnološka evolucija tradicionalnog financijskog prostora. Stoga, da bi se adekvatno definirao taj termin mora se imati osnovno razumijevanje tradicionalnih financija. Pojam tradicionalnih financija funkcionira kao proces koji uključuje stvaranje, upravljanje, ulaganje novca i financijske imovine. Sve te aktivnosti kontrolira ili regulira središnja vlast. Interes decentralizacije bi bio rješavanje korupcije od strane središnjih vlasti i dobivanje potpune transparentnosti. Nova pojava modernog financiranja preko blockchaina koristi najnovije inovacije između kriptovaluta i pametnih ugovora za izgradnju poštenih, modernih i snažnih financijskih sustava, koji se ne oslanjaju na središnje financijske posrednike poput banaka. Navedene metode rješenja ujedno i narušavaju industriju tradicionalnih financijskih usluga dopuštajući ljudima da trguju financijskom imovinom bez posrednika.

2. UVOD U DEFI

Skraćeno za decentralizirane financije, DeFi je izraz za razne aplikacije i projekte u javnom blockchain prostoru sa glavnim ciljem mijenjanja tradicionalnog svijeta financija i trgovanja. Sustav je izgrađen na blockchain tehnologiji gdje se istovremeno omogućuju i odvijaju digitalne javne transakcije između više strana i protokola. Pritom ne narušavajući korisničku privatnost gdje korisnik pojedinac često može biti anoniman i čuvati svoje osobne podatke i identitet u tajnosti od usluga sa kojim se koristi. Pružatelji usluga nude širok izbor protokola koji se baziraju na posuđivanju, slanju, i ulaganju u kriptovalute. I što je najvažnije, sve se događa bez treće strane, ili uključivanja banaka i drugih tradicionalnih financijskih organizacija, dakle u potpunosti decentralizirano, slika 1.



Slika 1: Ilustracija između centralizirane i decentralizirane mreže.

Izvor: https://bap-software.net/en/knowledge/defi-finance/ (29.4.2022)

2.1. BLOCKCHAIN TEHNOLOGIJA

Blockchain (Lanac blokova) tehnologiju prvi su 1991 godine predstavili Stuart Haber i W. Scott Stornetta, dva istraživača koji su željeli implementirati sustav u kojem se ne mogu mijenjati vremenske oznake dokumenta. No, tek gotovo dva desetljeća kasnije, lansiranjem Bitcoina u siječnju 2009 godine, ta tehnologija je imala svoju prvu primjenu u stvarnom svijetu. Definirala je distribuiranu bazu podataka koja se dijeli među čvorovima računalne mreže. Umjesto da podatci budu pohranjeni na središnjem poslužitelju kojem pristupaju svi korisnici, blockchain zapisi se pohranjuju na računalima korisnika diljem svijeta. To čini blockchain distribuiranom bazom podataka s peer-to-peer arhitekturom. „Distribuirano" znači da su podaci pohranjeni na više lokacija, a „peer-to-peer" znači da ne postoji središnje tijelo koje drži glavnu kopiju podataka.[1]

Postoje tri glavne komponente koje definiraju blockchain:

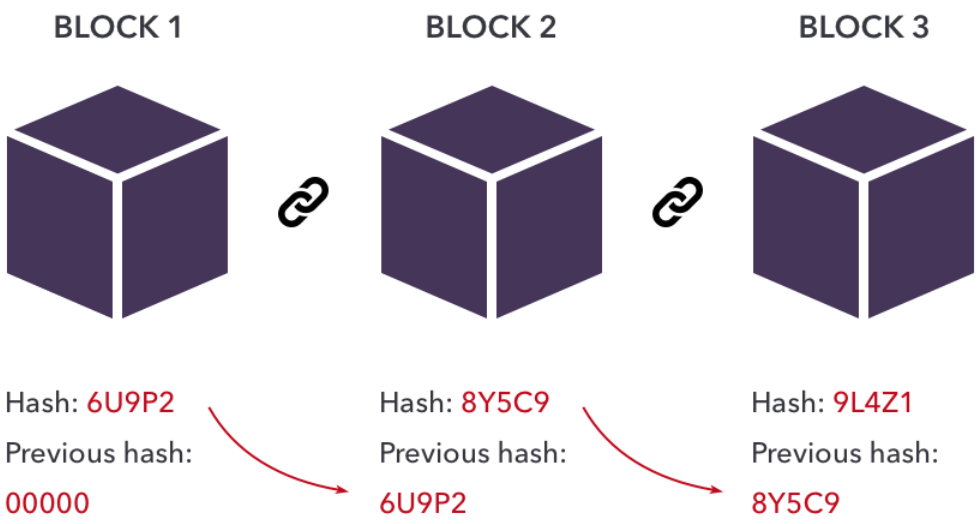
1. *Kriptografski ključevi* - ako dvije osobe žele obavljati transakcije putem interneta, svaka od njih treba imati privatni i javni ključ. Blockchain koristi ovaj koncept kako bi osigurao siguran digitalni identitet korisnika. Kombinacija privatnih i javnih ključeva može se promatrati kao vrsta privole stvaranjem jedinstvenog digitalnog potpisa.

2. *Distribuirana knjiga* - baza podataka koja se sporazumno dijeli i sinkronizira na više web-mjesta, institucija ili geografskih područja, kojoj pristupa više ljudi. Omogućuje da transakcije imaju javne "svjedoke".

3. *Kriptografski Hash* - podaci su strukturirani u blokove i svaki blok sadrži transakciju ili skup transakcija. Svaki novi blok povezuje se sa svim blokovima prije njega u kriptografskom lancu na takav način da ga je gotovo nemoguće mijenjati.

[1] https://kriptomat.io/hr/blockchain/sto-je-blockchain-tehnologija/ (29.4.2022)

Ovom tehnologijom postiže se decentralizirana sigurnost i povjerenje. Za početak, novi blokovi se uvijek spremaju linearno i kronološki. Odnosno, uvijek se dodaju na "kraj" blockchaina. Nakon što je blok dodan na kraj blockchaina, iznimno je teško vratiti se i promijeniti sadržaj bloka osim ako većina mreže ne postigne konsenzus (Dogovor) da to učini. To je zato što svaki blok sadrži svoj hash, zajedno s hash blokom prije njega, kao i prethodni vremenski žig. Hash kodovi su stvoreni matematičkom funkcijom koja pretvara digitalne informacije u niz brojeva i slova. Ako se te informacije uređuju na bilo koji način, mijenja se i hash kod, slika 2.



Slika 2: Primjer Hash-a u bloku.

Izvor: https://www.ig.com/en/trading-strategies/what-is-blockchain-technology--200710 (29.4.2022)

2.1.1. Bitcoin

31 listopada 2008. osoba ili grupa pod pseudonimom Satoshi Nakamoto objavila je tehnički dokument pod nazivom “Bitcoin: Peer-to-Peer Electronic Cash System”. Tehnički dokument je distribuiran na kriptografsku mailing listu, samo mjesec dana nakon što je investicijska banka Lehman Brothers podnijela zahtjev za najveći bankrot u povijesti SAD-a, a vlada odobrila financijsku pomoć od 700 milijardi dolara za ovu industriju**.** Nekoliko

mjeseci kasnije, 3. siječnja 2009., Bitcoin mreža pokrenula se, uvodeći novi sustav decentralizirane digitalne valute bez središnjeg posrednika.[2]

2013. godine, entuzijast bitcoina po imenu Laszlo Hanyecz napravio je post na oglasnoj ploči nudeći 10.000 BTC što je tada vrijedilo oko 25 dolara svakome tko bi dostavio dvije pizze u njegov dom u Jacksonvilleu na Floridi. Kako legenda kaže, te dvije pizze, koje je još jedan rani usvojitelj bitcoina kupio od lokalnog Papa John'sa, označile su prvu uspješnu kupnju nevirtualne robe koristeći bitcoin.[3]

Bitcoin je prva vrsta kriptovalute i koristi kriptografiju kako bi bio siguran. Ne postoje fizičke varijante bitcoina, samo stanja koja se vode u javnoj knjizi u kojoj svi imaju transparentan pristup. Sve Bitcoin transakcije provjerene su ogromnom količinom računalne snage putem procesa poznatog kao "rudarstvo". Bitcoin ne izdaje niti podupire nijedna banka ili vlada, niti je pojedini bitcoin vrijedan kao vrsta robe. Unatoč tome što nije zakonsko sredstvo plaćanja u većini dijelova svijeta. Bitcoin je vrlo popularan i pokrenuo je lansiranje stotinu drugih kriptovaluta, zajedničkih naziva Altcoini.

Bitcoina nema neograničeno. Količina je određena od strane Nakamota koji je mrežu postavio tako da broj nikada neće prijeći 21 milijun, osiguravajući kraj stvaranja novih tokena. Trenutno je još uvijek dostupno oko 3 milijuna bitcoina za rudarenje, što će se odvijati sve sporije i sporije. Posljednji blokovi će teoretski biti izrudareni 2140. godine.

Cijena 1 Bitcoina tijekom pisanja završnog rada iznosila je: 18,721$

Slika 3: Bitcoin logo

Izvor: https://bitcoin.org/en/ (29.4.2022)

[2] https://kriptomat.io/hr/kriptovalute/bitcoin/sto-je-bitcoin/ (29.4.2022)
[3] https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin (29.4.2022)

2.1.2. Pametni ugovori (Smart Contracts)

Pametni ugovori su računalni programi koji izvršavaju određene radnje, ako su izvršeni svi prethodno definirani uvjeti. Sve informacije i radnje iz pametnog ugovora se pohranjuju na blockchain.[4] Pametni ugovori funkcioniraju prateći jednostavne "ako/kada...onda..." komande koje su zapisane u kodu na blockchainu. Mreža računala izvršava te radnje ako su ispunjeni i unaprijed provjereni određeni uvjeti. Te radnje mogu uključivati slanje sredstava odgovarajućim stranama, registraciju vozila, slanje obavijesti ili izdavanje karte. Blockchain se zatim ažurira kada je transakcija dovršena. To znači da se transakcija ne može mijenjati i samo strane koje su dobile dopuštenje mogu vidjeti rezultate.

Prednosti pametnih ugovora:

Sigurnost - transakcije su šifrirane u blockchainu što čini pametni ugovor vrlo težak za hakiranje. Kada bi haker krenuo hakirati pametni ugovor, morao bi promjeniti cijeli lanac zbog jednog podatka.

Povjerenje i transparentnost - budući da nije uključena treća strana i budući da se šifrirani zapisi o transakcijama dijele među sudionicima, nema potrebe postavljati pitanje jesu li informacije izmijenjene za osobnu korist.

Brzina i učinkovitost – nakon što su uvjeti ispunjeni, ugovor se odmah izvršava. Razlog tome je to što su pametni ugovori digitalni i automatizirani pa nema potrebe za papirologijom.

Štednja – pametni ugovori uklanjaju potrebu za posrednicima. Što eliminira dodatne troškove naknade i vremenska kašnjenja.

Jednostavna metafora za pametni ugovor je automat za prodaju, slika 4, koji radi donekle slično kao i pametni ugovor, specifični ulazi jamče unaprijed određene rezultate.

- Korisnik bira proizvod
- Automat pokazuje iznos potreban za kupnju proizvoda
- Korisnik unosi ispravan iznos

[4] https://www.bitcoin-store.hr/blog/sto-je-pametni-ugovor/ (29.4.2022)

- Automat potvrđuje da je ubačen ispravan iznos
- Automat izdaje proizvod po izboru

Automat će izdati željeni proizvod tek nakon što se ispune svi zahtjevi. Ako se ne odabere proizvod ili ne unese dovoljno novca, automat neće izdati proizvod.

```
pragma solidity 0.6.11;

contract VendingMachine {

    // Declare state variables of the contract
    address public owner;
    mapping (address => uint) public cupcakeBalances;

    // When 'VendingMachine' contract is deployed:
    // 1. set the deploying address as the owner of the contract
    // 2. set the deployed smart contract's cupcake balance to 100
    constructor() public {
        owner = msg.sender;
        cupcakeBalances[address(this)] = 100;
    }

    // Allow the owner to increase the smart contract's cupcake balance
    function refill(uint amount) public {
        require(msg.sender == owner, "Only the owner can refill.");
        cupcakeBalances[address(this)] += amount;
    }

    // Allow anyone to purchase cupcakes
    function purchase(uint amount) public payable {
        require(msg.value >= amount * 1 ether, "You must pay at least 1 ETH per cupcake");
        require(cupcakeBalances[address(this)] >= amount, "Not enough cupcakes in stock to complete this purchase");
        cupcakeBalances[address(this)] -= amount;
        cupcakeBalances[msg.sender] += amount;
    }
}
```

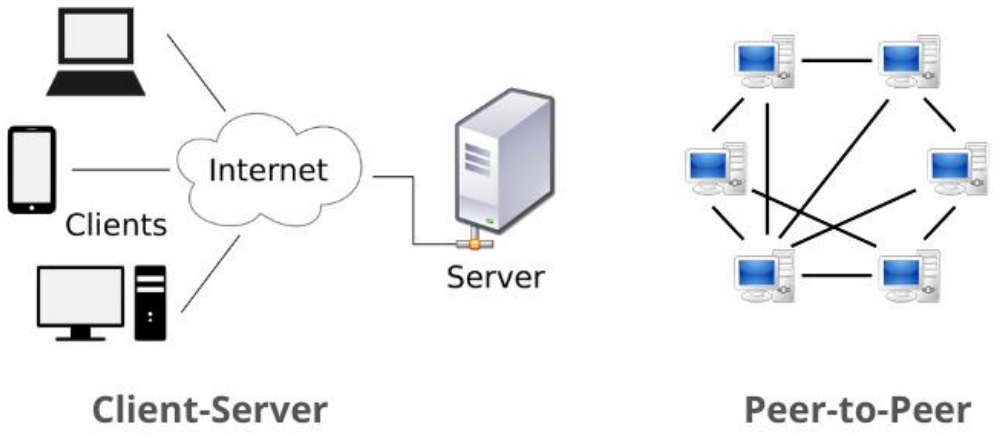
Slika 4: Primjer upotrebe Smart Contracta na automatu za prodaju

Izvor: https://morethandigital.info/en/what-are-smart-contracts-understanding-contracts-on-the-blockchain/ (29.4.2022)

2.1.3. Transakcije između korisnika (P2P)

U P2P mreži, korisnici su računalni sustavi i drugi uređaji koji su međusobno povezani putem Interneta, na primjer. Datoteke možemo dijeliti izravno putem mreže na koju su ti sustavi povezani. Za to nije potreban središnji poslužitelj. Računala ili uređaji koji su dio peer-to-peer mreže izravno su međusobno povezani i nazivaju se peers.. Drugim riječima, svako računalo u P2P mreži istovremeno postaje poslužitelj i klijent.[5] Peer-to-peer model održava distribuirana mreža računala. To znači da računala nemaju poslužitelja ili središnjeg administratora jer svaka strana drži kopiju datoteka – djelujući i kao poslužitelj i kao klijent, slika 5. Stoga svaka strana može učitavati datoteke za druge korisnike ili preuzimati datoteke s njih. Korisnici koriste vlastite tvrde diskove za pohranu podataka umjesto središnjeg poslužitelja.

Blockchain tehnologija koristi mogućnosti P2P mreža i pruža zajedničku i pouzdanu knjigu transakcija. Kao tehnologija distribuirane knjige, blockchain bilježi transakcije kao nepromjenjivi digitalni blok s vremenskim žigom koji označava pošiljatelje i primatelje. Nijedno centralizirano tijelo ne upravlja blockchain mrežama i samo sudionici mogu međusobno provjeravati transakcije. Tehnologija omogućuje ljudima i institucijama da vjeruju rezultatu bez povjerenja u ostale sudionike. Ovaj novi oblik distribuirane pohrane podataka i upravljanja djeluje kao digitalna knjiga koja javno bilježi sve transakcije i aktivnosti.



Slika 5: Usporedba Peer to peer mreže sa klijent-poslužitelj mrežom

Izvor: https://www.networkstraining.com/peer-to-peer-vs-client-server-network/ (5.5.2022)

[5] https://hr.itpedia.nl/2019/01/11/wat-is-p2p-peer-to-peer-en-wat-kan-je-er-mee/ (5.5.2022)

2.1.4. Vrste Konzensusa

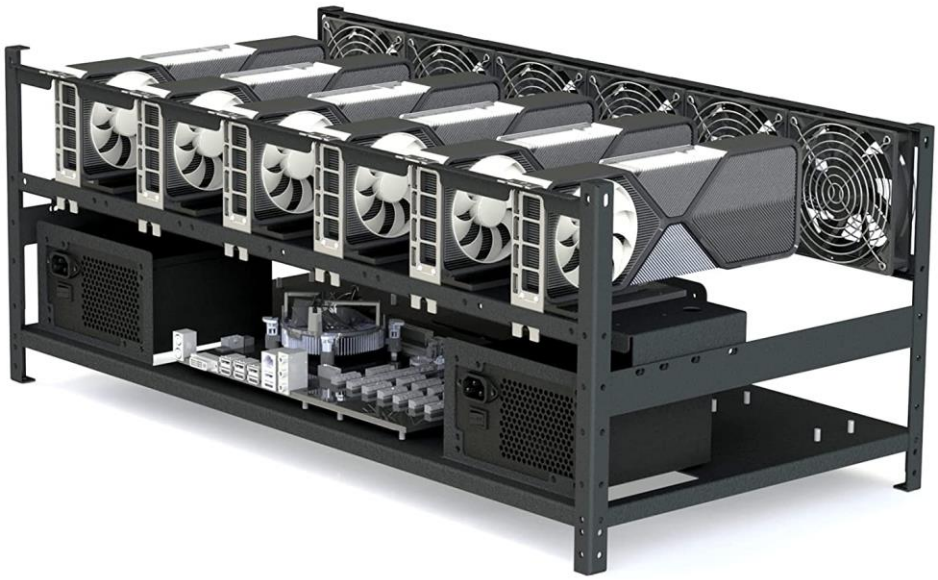
Konsenzus algoritam je postupak kroz koji svi sudionici blockchain mreže postižu zajednički dogovor o trenutnom stanju javne knjige. Na ovaj način algoritmi konsenzusa postižu transparentnost u blockchain mreži i uspostavljaju povjerenje između nepoznatih sudionika u distribuiranom računalnom okruženju.[6] U osnovi, konsenzus u blockchainu osigurava da svaki novi kreirani blok zadaje jedinu verziju istine na koji se slažu ostali zahtjevi.

Konsenzuse u blockchainu djelimo na dvije osnovne vrste: Proof of Work (PoW) i Proof of Stake (PoS).

Proof of Work (PoW) je metoda koju osiguravaju i verificiraju virtualni rudari kriptovaluta diljem svijeta koji se utrkuju za rješavanje matematičkih zagonetki. Pobjednik može ažurirati blockchain s najnovijim potvrđenim transakcijama, a mreža ga nagrađuje unaprijed određenom količinom kriptovaluta. Proces rudarenja osim što potvrđuje transakcije na mreži, također je čini i pouzdanom.

Prilikom ovog procesa rudari koriste vrlo snažna i hardverski dobro opremljena računala pod imenom „Rigovi“, slika 6. Rigovi se grade ili s GPU karticama ili ASIC jedinicama koje su spojene zajedno. Najvažniji aspekti koje treba uzeti u obzir pri izgradnji rudarske opreme su potrošnja energije, učinkovitost procesa rudarenja, nagradu za izrudareni blok i vrijednost valute. Rudarenje kriptovaluta se odvija u rudarskim bazenima (slika 7) gdje zajednička skupina rudara kombinira svoje računalne resurse preko mreže kako bi povećali vjerojatnost pronalaska bloka postupkom pogađanja točnog broja zvanog „hash“. Rudari pogađaju ciljani hash tako što nasumično čine što više pogađanja što je brže moguće, što zahtijeva veliku računalnu snagu.

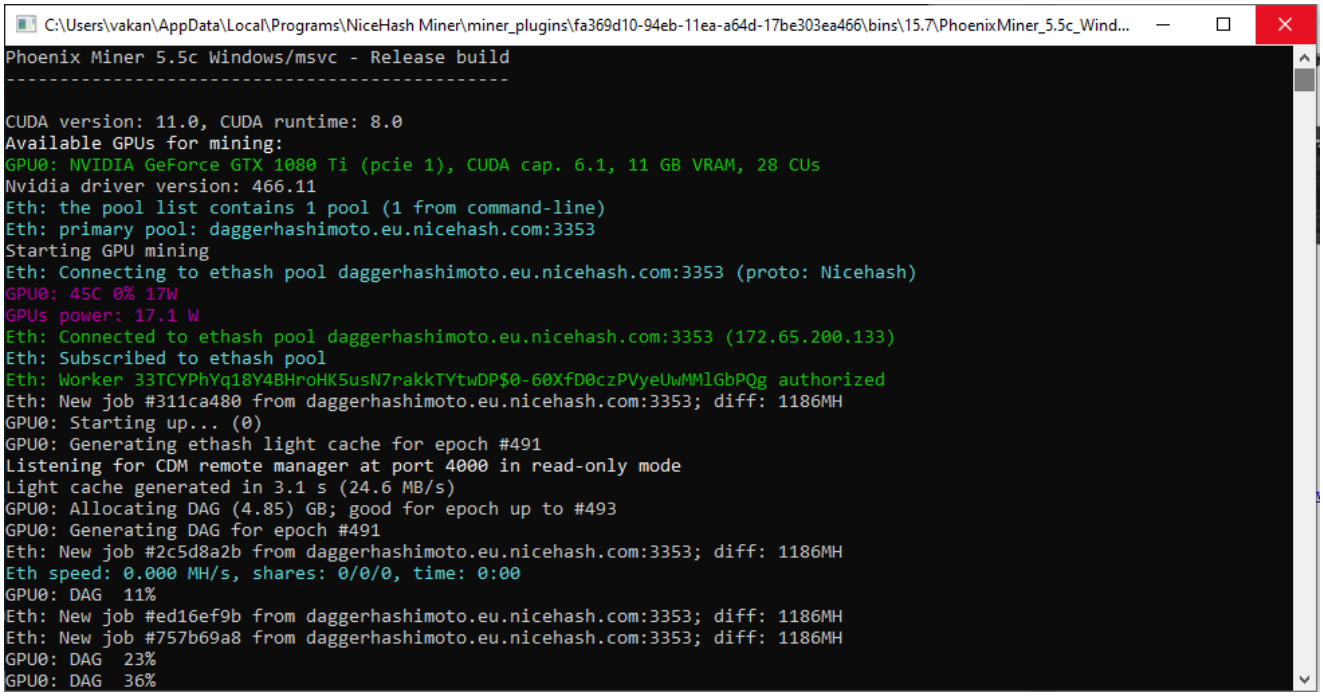
[6] https://crobitcoin.com/vrste-konsenzusa-na-blockchainu-proof-of-work-vs-proof-of-stake/ (8.5.2022)



Slika 6: Mining rig

Izvor: https://www.amazon.in/XtremeMiners-Mining-1GPU-Motherboard-Cooling/dp/B09645BYFW

(8.5.2022)



Slika 7: Primjer rudarenja valute ETH u bazenu daggerhashimoto

Izvor: Autor

Proof of Stake (PoS) metoda više ne koristi sustav za pogađanje teških kompleksnih jednadžbi i ujedno rješava problem prevelikog trošenja struje. PoS mijenja način na koji se blokovi verificiraju pomoću vlasnika valute. Vlasnici nude svoju valutu kao zalog za mogućnost provjere valjanosti blokova. Vlasnik s određenom uloženom kriptovalutom postaje "validator", slika 8. Validator ulaže dio sredstva koji je zadan od strane protokola i garantira da će ovjeriti i potvrditi sve nadolazeće transakcije, dok mu se pritom zaključavaju sredstva na određeno vrijeme. Za taj posao koji odrađuje, validator uzima transakcijske troškove (provizije) koje dolaze s transakcijama.

Slika 8: Ilustracija PoS-a

Izvor: https://www.chainbits.com/cryptocurrency-terms/proof-stake-definition/ (8.5.2022)

2.1.5. Vrsta i podjela lanaca mreže (Layers)

Blockchainova operativnost i sistematizacija lanaca djeli se na Layer-1 (Glavni protokol) i Layer-2 (Pomoćni protokol) mreže. To su sistemi osmišljeni kako bi blockchain mreže bile brže i prilagođenije brzo rastućoj bazi korisnika. Mnoge blockchain mreže istražuju kombinacije rješenja skaliranja Layer-1 i Layer-2 protokola kako bi postigle što izvrsniju skalabilnost bez žrtvovanja sigurnosti ili decentralizacije. Layer-1 (Glavni protokol) je skup rješenja koji poboljšava osnovni protokol nudeći rješenja problema decentralizacije, sigurnosti i skalabilnosti. Layer 2 (Pomoćni protokol) odnosi se na sekundarni sustav ili protokol koji je izgrađen na vrhu postojećeg blockchain sustava. Glavni mu je cilj riješiti probleme brzine transakcije i skaliranjem s kojima se susreću na mreži u kojoj je Layer-2 protokol pozicioniran.

Layer-1 mreža je izvorni unikatni sloj na blockchain decentraliziranom ekosustavu. Rješenja za skaliranje Layer-1 mreže moraju poboljšati skalabilnost, nadopunjavanjem osnovnog sloja toga protokola. Brojne metodologije se kontinuirano izgrađuju i implementiraju kako bi se izravno poboljšala i izgladila funkcija mreže.

Za poboljšanje učinkovitosti postoji Layer 2 blockchain koji radi na izvornom sloju (Layer-1). Layer-2 učinkovito rasterećuje transakcije prijenosom dijela transakcijskog tereta blockchaina Layera-1 na drugu arhitekturu sustava.

Opterećenje transakcija dakle preuzima Layer-2, koji mora onda informirati Layer-1 radi finalizacije rezultata. Budući da Layer-2 arhitektura nosi većinu opterećenja obrade podataka, zagušenje na glavnoj mreži je smanjeno što dovodi i do bolje skalabilnosti glavnoga protokola na kojem je Layer-2 nastanjen.

3. ETHEREUM

Ethereum nudi iznimno fleksibilnu platformu na kojoj se mogu izgraditi decentralizirane aplikacije koristeći izvorni skriptni jezik Solidity i Ethereum Virtual Machine. Najvažnija inovacija Ethereuma jest Turingov cjelovit softver koji radi na Ethereumovoj mreži nazvan Ethereum Virtual Machine (EVM)[7]. Omogućavanjem pristupa bilo kome kod pokretanja bilo kakvog programa, bez obzira na programski jezik. EVM čini postupak stvaranja blockchain aplikacija mnogo lakšim i učinkovitijim nego ikad prije. Umjesto da se mora izgraditi originalni blockchain za svaku novu aplikaciju, Ethereum omogućava razvoj potencijalno tisuće različitih aplikacija na jednoj platformi.

Protokol koristi valutu ETH za obavljanje transakcijskih poduhvata također nazvanim i "Gas fees" koji su neizbježni prema korisnicima i aplikacijama. Programeri koji razvijaju aplikacije na Ethereum mreži koriste pametne ugovore i imaju na odabir bogati ekosustav alata za korištenje. Korisnička baza potiče upravo te programere da implementiraju svoje aplikacije na mreži, što dodatno jača Ethereum kao primarni dom za decentralizirane aplikacije. Ethereum se često uspoređuje sa Bitcoinom, najčešće zbog toga što je trenutno druga najkorištenija kriptovaluta. No vizija i cilj Ethereuma nije samo da bude klasična valuta za trgovanje i transfer novaca, već da omogući daljnje razvijanje aplikacija na njemu kako bi se izgradio i osigurao bolji decentralizirani svijet.

Slika 9: Logo Ethereuma

Izvor: https://artistsatrisk.org/donations/ethereum-logo-2/?lang=ar (27.5.2022)

[7] https://electrocoin.hr/blog/sto-je-ethereum-i-kako-funkcionira (27.5.2022)

3.1. ETH TOKEN

Ether je transakcijski token koji olakšava operacije na blockchain mreži Ethereum. Svi programi i usluge povezani s mrežom Ethereum zahtijevaju računalnu snagu (a ta računalna snaga nije besplatna). Ether onda djeluje kao oblik plaćanja za sudionike mreže kako bi izvršili svoje tražene operacije na mreži.

Dok se Ether može smatrati kriptovalutom mreže Ethereum, metaforički rečeno točnije ga možemo nazvati "gorivom" mreže. Što znači da za svaku obavljenu transakciju na mreži, Ethereum uzima postotak provizije obračunat u valuti Ether. Ta provizija nije nikada fiksna, ona naime ovisi o zakrčenosti mreže. Strukturno gledano što više korisnika koristi mrežu u isto vrijeme, provizija će biti veća, a ako je mala korištenost onda će biti manja. Ovaj proces se značajno razlikuje od rada standardne kriptovalute što ga i odvaja od ostalih na tržištu i čini autentičnim.

U Ethereum mreži token ETH se koristi za:

TRANSAKCIJSKE PROVIZIJE - Svaka aplikacija na ethereumu traži proviziju ETH tokena što znači da korisnici moraju imati dovoljnu količinu tokena kako bi transakcija uspješno bila potpisana.

PLAĆANJE USLUGA – Također se koristi kao valuta za P2P plaćanja drugim stranama bez treće osobe.

POGONJENJE APLIKACIJA – Eth je potreban za bilo kakve aktivnosti unutar mreže što se tiče interakcija sa aplikacijama.

3.1.2. Transakcijske provizije

Naknade za transakcije (Gas fee) koriste se za kompenzaciju rudara Ethereuma, odnosno za njihov rad kod provjeravanja transakcija i osiguravanja mreže. Provizije također pomažu spriječiti da se mreža ne zaglavi zlonamjernim korisnicima koji šalju neželjenu poštu mreži s transakcijama. Gas je jedinica troška neke operacije koju računalo mora izvršiti, a izvršava je kada pošaljemo transakciju koja sadrži Ethereum program u sebi, kako bismo pokrenuli neku aplikaciju. Npr. zbroj dvije brojke košta 3 gasa. Množenje dvije brojke košta 5 gasa. Spremanje jedne riječi od 256 bita u blockchain košta 20,000 gasa, što znači da bi podaci duljine jednog kilobajta koštali 640,000 gasa.[8]

Ethereum koristi metrički sustav jedinica nazvan "wei", gdje je 1 ETH jednak 1 kvintilijunu wei-a. (Kvintilion je broj s 18 nula iza njega.). Jedna od najčešćih denominacija wei-a, koja se najčešće koristi za predstavljanje naknade za transakciju, je gigawei (gwei) ili 1 milijarda wei-a, slika 10. Stoga, kada provjerite na uređaju za praćenje gasa i vidite da je prosječni gas za transakciju 100 gwei, to znači da biste trebali očekivati da ćete platiti osnovnu naknadu od 0,0000001 ETH za određenu transakciju.

Iako su učinkovito sredstvo za poticanje rudara da nastave provjeravati transakcije i održavati sigurnost mreže, naknade za transakcije su ipak dio koji najviše odbija korisnike u Ethereumu. Korisnici mrze naknade za transakcije, ne samo zbog općeg prezira prema naknadama, već i zato što mogu biti apsurdno skupe kada je mreža zakrčena.

jedinica	wei
wei	1
kwei / ada / femtotether	1.000
mwei / babbage / picoether	1.000.000
gwei / shannon / nanoether / nano	1.000.000.000
szabo / microether / micro	1.000.000.000.000
finney / milliether / milli	1.000.000.000.000.000
ether	1.000.000.000.000.000.000

Slika 10: Vrijednosti Wei-a

Izvor: https://bitfalls.com/hr/2017/12/05/ethereum-gas-and-transaction-fees-explained/ (29.5.2022)

[8] https://bitfalls.com/hr/2017/12/05/ethereum-gas-and-transaction-fees-explained/ (29.5.2022)

3.1.3. ERC-20 tokeni

ERC-20 uvodi standard za zamjenjive tokene, drugim riječima, oni imaju svojstvo koje čini da svaki token bude potpuno isti (po vrsti i vrijednosti) kao i drugi token. Na primjer, ERC-20 token djeluje isto kao ETH, što znači da je 1 token i uvijek će ostati jednak svim ostalim tokenima. Standard tokena ERC-20 omogućuje programerima da kreiraju vlastite tokene unutar Ethereum mreže, slika 11. Tvrtkama je omogućen lakši put za razvoj blockchain proizvoda umjesto izgradnje vlastite kriptovalute.

Erc-20 tokeni se moraju pridržavati 6 obaveznih pravila i 3 opcionalnih.

Obavezna:

- *Total Supply* - pruža informacije o ukupnoj opskrbi tokenom, broj tokena mora biti fiksni.
- *BalanceOf* - osigurava stanje računa vlasnika
- *Transfer* - izvršava prijenos određenog broja tokena na određenu adresu
- *TransferFrom* - izvršava prijenos određenog broja tokena s određene adrese
- *Approve* - mora dopustiti potrošaču povlačenje skupa tokena s određenog računa
- *Allowance* - vraća vlasniku skup tokena od potrošača

Opcionalna:

- *Ime tokena* - Token bi trebao sadržavati ime kako bi lakše bio uočljiv na tržištu
- *Simbol* - Tokenima se može dodati simbol radi Estetike
- *Početna vrijednost* - Vrijednost tokena determinira njegovu poziciju na tržištu

Ostali Ethereum token standardi:

ERC-721 - Ovo je standard tokena za nezamjenjive tokene (NFT). Svaki je token jedinstven i ima vlastiti kod, što je dovelo do tržišta kripto kolekcionarskih predmeta, uključujući trgovačke kartice i digitalna umjetnička djela .

ERC-1400 - Ovo su sigurnosni tokeni (Securities) koji se mogu prodati kao vrijednosni papiri. To zahtijeva veću kontrolu nad time tko može pristupiti tokenima. Većinom se uvodi protokol poznavanja svog klijenta (KYC).

ERC-223 - Kada izvršite transakciju, naknade se trenutno plaćaju u Etheru. Ovaj standard omogućuje plaćanje naknada za transakcije korištenjem uključenih tokena u transakciji. To znači da bi prijenos Augura bio plaćen u Augur tokenima, sa simbolom tickera REP.

ERC-777 - Cilj mu je postati poboljšani ERC-20 token s ažuriranim značajkama i manjim troškovima.

Slika 11: Primjer ERC-20 tokena

Izvor:https://medium.com/@robinverderosa/bitgo-adds-support-for-erc20-tokens-ca8384779723 (29.5.2022)

3.1.4. ETH 2.0

Ethereum se sada priprema za pokretanje svoje važne nadogradnje na Ethereum 2.0 koja će značajno preustrojiti mrežu i rješavati pitanja kao što su skalabilnost, visoke cijene transakcija i zagušenja u mreži. To obilježava značajnu promjenu mreže koja se sastoji od shardinga i uzastopnih faza koje zaključuju prelazak s konsenzusa dokaza o radu na dokaz o udjelu, čineći mrežu skalabilnijom, sigurnijom i održivom. Sharding je proces cijepanja jednog blockchaina na više blockchaina poznatih kao „shardovi“. Čitavu mrežu čini učinkovitijom jer se jedan validator ne mora sam nositi s radnim opterećenjem, već svaki validator održava informacije vezane za "njegov" dio. Ovi se validatori također redovito miješaju između shardova kako bi se izbjegla bilo kakva manipulacija.

Najvažnija prednost Ethereuma 2.0 je njegova skalabilnost. Ethereum 2.0 imati će lance zbog kojih će moći provesti do 10.000 transakcija u sekundi dok Ethereum 1 može podržavati samo 30 transakcija u sekundi što dovodi do puno kašnjenja i zagušenja mreže. Implementacija lanaca shardova ubrzava mrežu i može se lakše skalirati jer se transakcije obrađuju u paralelnim lancima umjesto uzastopnim. Glavna ideja iza osmišljavanja nadogradnje postojećeg Ethereuma je ostvarivanje veće sigurnosti u cijeloj transakciji. Mnogi protokoli s konsenzusima o udjelu imaju vrlo mali skup validatora. Zbog toga može stradati sigurnost mreže no Ethereum 2.0 želi to izbjeći te zahtijeva veliki skup validatora, otprilike 16 384, što ga čini decentraliziranijim, sigurnijim i manje sklonim manipulaciji. Da bi korisnik postao ETH 2.0 validator potrebno mu je odvojiti minimalno 32 ETH-a. Za nagradu što postaje validator protokol mu obećava 10% APY (godišnji postotak prinosa) na njegov uloženi ETH.[9]

Slika 12: Ethereum 2.0 logo

Izvor: https://coingape.com/total-value-of-eth-in-2-0-deposit-contrcat-skyrockets-to-an-ath-of-8-9-million-eth/ (29.5.2022)

[9] https://www.bitcoin-store.hr/blog/ethereum-2-0-skaliranje-najpopularnije-blockchain-platforme/

4. AVALANCHE

Avalanche je decentralizirani sustav otvorenog koda koji se temelji na operacijama pametnih ugovora poput njegovog bliskog brata Ethereuma. Osmislila ga je pseudonimna grupa entuzijasta pod nazivom "Team Rocket koja je podijelila ideju na InterPlanetary File System-u (IPFS-u) u svibnju 2018 godine. Kasnije ga je razvio posvećen tim istraživača sa Sveučilišta Cornell. Istraživanje je vodio Emin Gün Sirer, profesor računalnih znanosti i softverski inženjer, uz pomoć Maofana "Ted" Yina i Kevina Sekniqija. Nakon faze istraživanja, Ava Labs je osnovan kako bi razvio mrežu prvenstveno za cilj zadovoljavanja složenih zahtjeva financijske industrije. U ožujku 2020. AVA kodna baza za Avalanche konsenzus protokol postala je otvorenog koda i dostupna javnosti.

Avalanche je prva platforma pametnih ugovora koja može finalizirati transakcije za manje od sekunde. Podržavajući cijeli komplet alata koji se koriste na Ethereum mreži, također sadrži i rekordan broj čvorova koji proizvode blokove na svom testnetu. Mreža ima potencijal obraditi preko 4500 transakcija u sekundi, što je čini jednim od najbržih blockchainova na tržištu.[10] Avalanche je dizajniran i programiran za rješavanje nekih ograničenja kod starijih blockchain platformi, uključujući spore brzine transakcija, centralizaciju i skalabilnost. Uz ta brojna efikasna rješenja također nudi i svojevrsne inovacije poput jedinstvenog Avalanche konsenzus protokola, koji obećava nisku latenciju, visoku propusnost i otpornost na napade od 51%. Napad od 51% odnosi se na napad na blockchain od strane grupe rudara koji kontroliraju više od 50% hash stope rudarenja ili računalne snage mreže. No Avax ne koristi metodu POW tako da ostaje u tom području siguran.

U svojoj srži Avalanche je izgrađen oko sustava od tri interoperabilna blockchaina: lanca razmjene (X-Chain), lanca ugovora (C-Chain) i lanca platforme (P-Chain). Ukratko, X-Chain se koristi za stvaranje novih digitalnih sredstava, dok je C-Chain implementacija Avalancheovog virtualnog stroja u Ethereum (EVM), a P-Chain se koristi za koordinaciju validatora i stvaranje podmreža.

[10] https://kriptomat.io/hr/kriptovalute/avalanche/sto-je-avalanche/ (8.6.2022)

Dva od ovih blockchaina (P-Chain i C-Chain) osigurana su konsenzusom "Snowman", pomažući u omogućavanju sigurnih pametnih ugovora visoke propusnosti, dok je X-Chain osiguran „DAG Avalanche“ optimiziranim konsenzusom za sigurnost i skalabilnost protokola zbog čega može postići konačnost transakcije u nekoliko sekundi.

Prema Ava Labs-u, platforma može podnijeti negdje oko 4500 transakcija u sekundi u usporedbi s 7 tx/sec za Bitcoin i 14 tx/sec za Ethereum . Također je u stanju postići konačnost transakcije za manje od 3 sekunde. Što platformu čini prikladnijom za masovno skaliranje decentraliziranih aplikacija.

Što se tiče gas naknada za transakcije tu je Avalanche znatno jeftiniji. Protokol naplaćuje standardnu naknadu za transakcije u iznosu od 26 nAVAX-a (0,000000026 AVAX-a) za razliku od Ethereuma koji trenutno naplaćuje standardnu naknadu za transakcije od 41 gwei-a (0,0000000547 ETH-a). Gledajući po vrijednosti ETH trenutno vrijedi 75x više od AVAX-a, tako da svaki gwei vrijedi 75x više od svakog nAVAX-a. To znači da su trenutne naknade za transakcije Ethereuma eksponencijalno veće od onih koje naplaćuje Avalanche. Čak i kad bi obje kriptovalute bile jednako vrijedne, Ethereum i dalje naplaćuje znatno veću naknadu za transakcije.

Slika 13: Avalanche logo

Izvor: https://medium.com/@bacool/on-the-economics-and-governance-of-avalanche-avax-b6beecff5d61 (8.6.2022)

4.1. AVAX TOKEN

Avax je matični token Avalanche ekosustava koji služi kao zajednički medij za razmjenu. Osim što se koristi kao valuta u protokolu, kupnjom Avax tokena i „hodlanjem“ osigurava se mreža i povratno nagrađuje dionike s više AVAX-a. Deflacijski mehanizam tokena povećava vrijednost dobivenu ulaganjem. AVAX tokeni koji se koriste za plaćanje transakcijskih naknada spaljuju se iz opskrbe, što trajno smanjuje količinu AVAX-a u optjecaju.

Avax token se može koristiti za više operacija kao na primjer:

Nagrade za ulaganje - Sve podmreže, uključujući primarnu mrežu, zahtijevaju validatore koji posjeduju i stavljaju AVAX tokene kao zajam ili kolateral. To ne znači da se nužno mora biti validator da bi se dobila nagrada za ulaganje u AVAX. Ako korisnik želi dobivatio nagrade za ulaganje u AVAX tokenima, mora delegirati svoj ulog validatoru kako biste zaradili postotak nagrada za ulaganje.

Plaćanje naknada za transakcije - AVAX je matična valuta mreže. Što znači da sve transakcijske naknade plaćaju se pomoću AVAX-a, a to je i zajednička valuta između podmreža, Korištenje AVAX-a između podmreža je važno jer pomaže interoperabilnosti između podmreža koje bi inače koristile vlastite interne kriptovalute.

Kreiranje tokena i dappova (Decentralized aplications) - Dva glavna slučaja korištenja Avalanchea su stvaranje novih tokena i novih blockchain platformi. Programeri mogu iskoristiti platformu za implementaciju NFT-a, DeFi protokola i igara. Koje se temelje na plaćanjima u AVAX-u.

5. DECENTRALIZIRANE APLIKACIJE I PROTOKOLI

Decentralizirane aplikacije su poput normalnih aplikacija i nude slične funkcije, ali ključna razlika je u tome što se pokreću na peer-to-peer mreži, kao što je blockchain, koristeći pametne ugovore. Budući da su dapp-ovi decentralizirani, ne može ih kontrolirati niti jedna osoba ili entitet. Također često imaju sljedeće značajke:

- Oni su otvorenog koda i rade sami bez da ih itko kontrolira.
- Njihovi podaci i evidencija su javni.
- Koriste kriptografski token kako bi zaštitili svoju mrežu.

Iako mnogi u blockchain i kripto zajednici vjeruju da bi dapp-ovi trebali imati sve ove značajke, kako je industrija sazrijevala, postoje dapp-ovi koji koriste neke, kombinaciju ili ništa od gore navedenog.

5.1. CURVE FINANCE

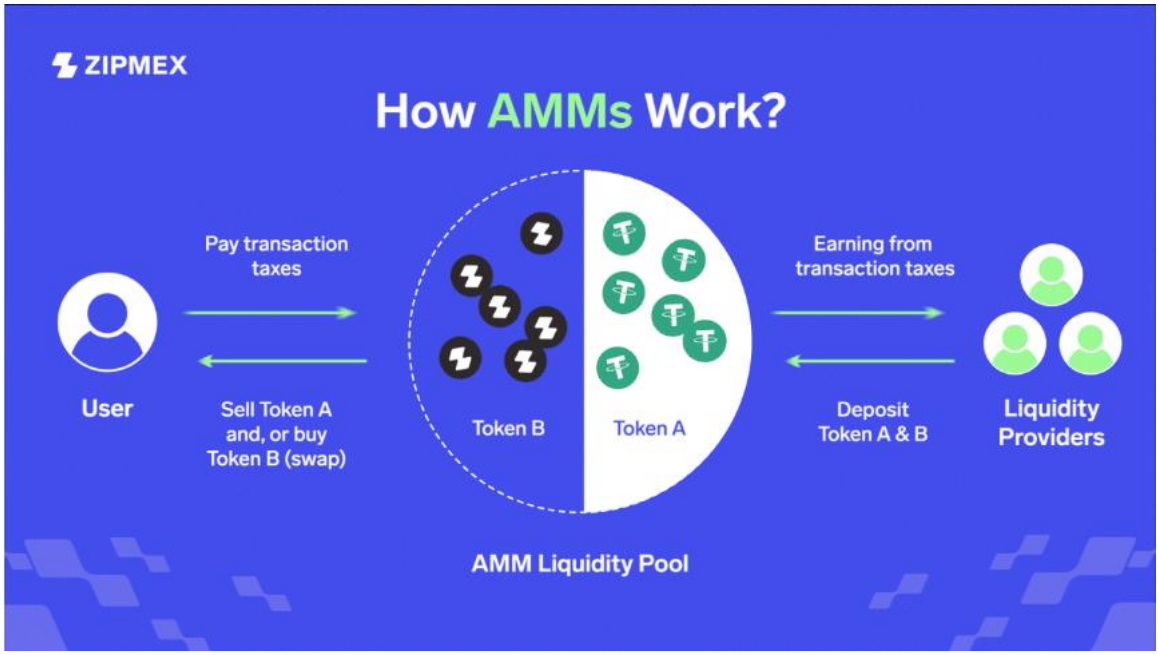
Curve je jedna od najpopularnijih platformi u DeFi-ju jer daje prednost kod sastavljanja stabilnog kapitala u odnosu na volatilnost i spekulacije ovog prostora**.** Curve Finance je decentralizirana burza za trgovanje kriptovalutama koja se usredotočuje na učinkovito trgovanje stablecoinima. Usredotočenost Curve-a na stablecoine omogućuje investitorima da izbjegnu nestabilnu kripto imovinu**.** Protokol funckionira kao AMM platforma, koja stvara bazene likvidnosti na bazi valuta sličnog ponašanja poput stablecoina ili omotanih verzija (Wrapped) slične imovine kao što su wBTC i wETH . Ovaj pristup omogućuje Curve-u da koristi učinkovitije algoritme i da ima najniže razine naknada od bilo koje decentralizirane burze (DEX-a) na Ethereumu.

Slika 14: Curve Finance logo

Izvor: https://moonbeam.curve.fi/ (13.6.2022)

Automatizirani market makeri (AMM) dopuštaju da se tokenima trguje bez dopuštenja koristeći strategiju implementiranja bazena likvidnosti umjesto trgovine između kupaca i prodavača. U općoj definiciji, bazen likvidnosti je zajednički lonac tokena. Korisnici opskrbljuju bazene likvidnosti tokenima, a cijene tokena u bazenu određuju se izračunavanjem matematičke formule. Podešavanjem formule, bazeni likvidnosti mogu se optimizirati za različite svrhe. Svatko s internetskom vezom i nekim ERC-20 tokenima može postati pružatelj likvidnosti izdvajanjem svojih tokena u bazen. Pružatelji likvidnosti obično zarađuju naknadu za takvu vrstu investicije i plaćeni su od strane trgovaca koji su u interakciji s platformom u želji da zamjene svoje tokene, slika 15.

AMM pomaže uspostaviti sustav likvidnosti u kojem svatko može pridonijeti tome. Time se uklanjaju sve posredničke transakcijske naknade za ulagače. Visoka likvidnost neophodna je za zdravo trgovanje u Defi-ju. Ako je likvidnost manja, može doći do visokog slippage-a. Slippage je uzrokovan količinom trenutne likvidnosti izabranih tokena za izdvajanje u bazen. Dakle, ako postoji niska likvidnost ili niska aktivnost trgovanja izabranog tokena u bazenu, tada će postotak slippage-a biti veći i protokol će nuditi korisniku zamjenu tokena uz veliku proviziju.



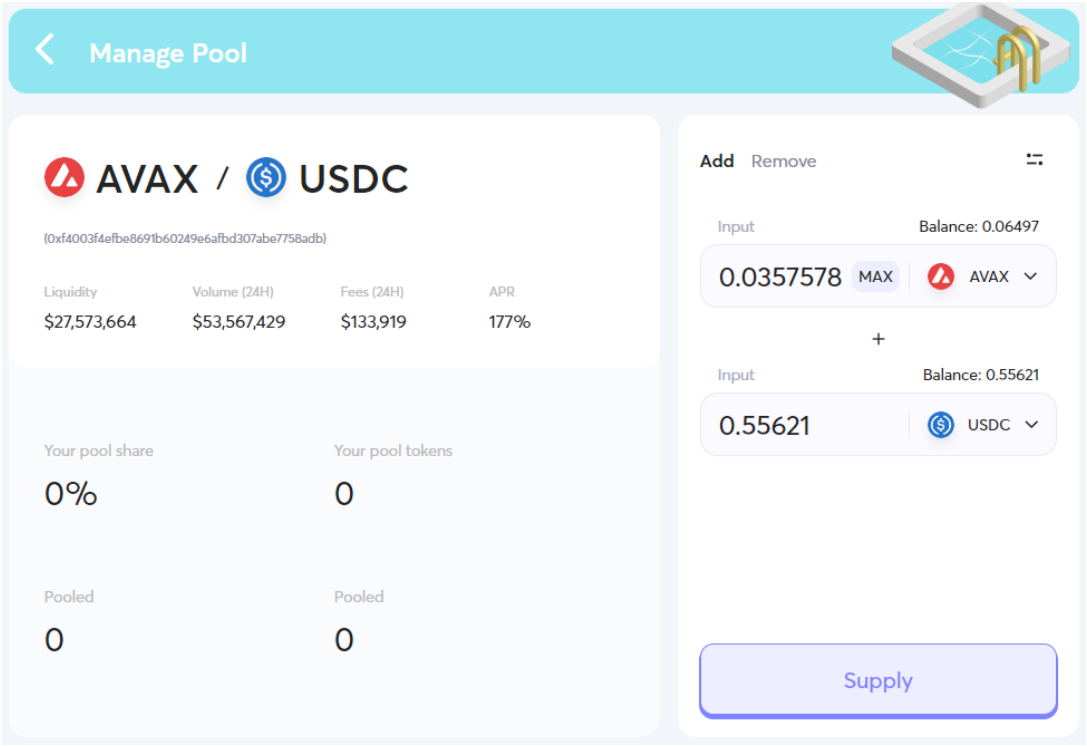
Slika 15: Primjer funkcije Automatiziranog market makera

Izvor: https://zipmex.com/learn/what-is-amm-automated-market-maker/ (13.6.2022)

5.1.1. Bazen likvidnosti (Liqudity pool)

Bazen likvidnosti je digitalna hrpa kriptovaluta zaključana u pametnom ugovoru. Metaforički izraženo bazen likvidnosti možemo zamisliti kao jedno veliko skladište svakakvih tokena koji su na raspolaganju. Svrha je da pruža likvidnost za sve tražene tokene kako bi se ostvarile brže transakcije. Osim pružanja likvidnosti bazeni potiču korisnike različitih kripto platformi da sudjeluju u procesu i postanu pružatelji likvidnosti radi nagrada. Za određeno vrijeme koliko su korisnici pružali likvidnost svojih tokena, nagrađuju se s djelićem naknada i poticaja, koji su ekvivalentni količini likvidnosti koju su pružili. Svaki pružatelj likvidnosti dobiva zauzvrat token pod nazivom „Token pružatelja likvidnosti“ (LPT). LPT tokeni se tada mogu koristiti na različite načine na DeFi mreži.

Postoji i nekoliko rizika pri pružanju likvidnosti u bazenu, kao na primjer Impermanent loss (Nestalni gubitak). Događaj kada korisnik osigura likvidnost u bazenu, a cijena tokena se promjeni u odnosu na vrijeme od kada je korisnik prvi put ušao u bazen. Što je promjena cijene veća, to je veća izloženost impermanent loss-u. U ovom slučaju gubitak znači manja vrijednost u dolarima u trenutku povlačenja nego u trenutku polaganja, slika 16.



Slika 16: Primjer pružanja likvidnosti u bazenu AVAX/USDC na mjenjačnici Trader Joe

Izvor: Autor

5.1.2. Stable coin

Stablecoin je most koji povezuje kriptovalute s klasičnim fiat valutama koje svakodnevno koristimo. Interes te valute je da zaštiti investitora od velikih promjena koje se događaju na tržištu. Iako se tržište kriptovaluta razvija velikom brzinom ono je još uvijek podložno većim promjenama u vrijednosti.[11] Stablecoin je jedna vrsta kriptovalute koja je dizajnirana da održava fiksnu vrijednost tijekom vremena. Vrijednost stablecoina obično je vezana uz određenu stvarnu valutu, često američki dolar. Budući da im je cilj pratiti imovinu, Stablecoini su često podržani specifičnom imovinom na koju su vezani. Na primjer, organizacija koja izdaje stablecoin obično postavlja pričuvu ili rezervu u financijskoj instituciji koja drži temeljnu imovinu. Dakle, stablecoin bi mogao držati 100 milijuna dolara u rezervi i izdati 100 milijuna tokena s fiksnom vrijednošću od 1 dolar po tokenu. Ako vlasnik stablecoina želi unovčiti token, pravi novac se u konačnici može uzeti iz pričuve.

Stablecoini obično nisu izloženi prevelikoj popularnosti kao druge kriptovalute, djelomično zato što ne nude istu vrstu mogućnosti za brzo stvaranje kapitala. No od mnogih Stablecoina izdvajaju se trenutna 3 najpopularnija i najsigurnija na tržištu.

- Tether (USDT): 82 milijarde dolara
- USD Coin (USDC): 49 milijardi dolara
- Binance USD (BUSD): 17 milijardi dolara

Rizici

Postoji nekoliko nedostataka Stablecoina koje treba imati na umu. Zbog načina na koji se stablecoini obično postavljaju, oni imaju različite bolne točke od ostalih kriptovaluta.

Ako su pričuve pohranjene kod banke ili neke druge treće strane, druga ranjivost je rizik druge ugovorne strane. Gdje onda dolazi do pitanja: Ima li subjekt stvarno kolateral za koji tvrdi da ima? Ovo je, na primjer, često postavljano pitanje Tetheru o tome održava li istinsku podršku 1-1 između USDT tokena i američkih dolara.

U najgorem slučaju, moguće je da bi rezerve koje podupiru token mogle biti nedovoljne za otkup svake jedinice, potencijalno poljuljajući povjerenje u taj token.

[11] https://www.bitcoin-store.hr/blog/sto-je-stablecoin-i-kako-funkcionira/ (17.6.2022)

5.2 TRADER JOE

Trader Joe je decentralizirana platforma za trgovanje na mreži Avalanche koja kombinira DEX usluge s DeFi pozajmljivanjem kako bi ponudila trgovanje s leverage-om. Platforma korisnicima omogućuje trgovinu, sudjelovanje u Yield farmingu, ulaganje i zaduživanje**.** Pokrenut 29. lipnja 2021 godine, Trader Joe je DEX, čija je glavna svrha pružanje usluga zamjene i trgovanja. Međutim, ovaj projekt također nudi druge osnovne značajke DeFi-ja kao što su Yield farming i posuđivanje. Osim toga, „ZAP“ je nova značajka projekta koja korisnicima omogućuje zamjenu za LP tokene u samo jednom kliku. Protokolom se odvijaju usluge i plaćanja u matičnom tokenu JOE. Trader Joe se brine o svojoj zajednici te nudi mogućnost ulaganja u token sJOE sa beneficijama i zaradom USDC tokena prikupljenih od likvidacija i transakcija koje se dešavaju na platformi.

Dugoročno, osnivači planiraju učiniti Trader Joe protokolom kojim upravlja zajednica, kao što je DAO (Decentralized autonomous organisation). JOE token će se koristiti za glasanje o prijedlozima zajednice, prijedlozi se mogu podnijeti na forumu za raspravu. Oni koji budu najviše prihvaćeni bit će u konačnosti izneseni na glasanje.

Glasanjem putem JOEVOTE sistema donositi će se odluke za daljnji razvoj protokola putem ovih načina:

1. Svaki JOE u JOE-AVAX bazenu vrijediti će 2 JOEVOTE-a
2. Svaki JOE koji je stejkan u sJOE token jednak je 1 JOEVOTE
3. Svaki JOE token vrijediti će 1 JOEVOTE

Slika 17: Trader Joe logo

Izvor: https://docs.traderjoexyz.com/en/marketing/brand-assets (17.6.2022)

5.3. ABRACADABRA MONEY

Abracadabra Money je DeFi platforma za pozajmljivanje koja omogućuje polaganje tokena iz drugih protokola kao zalog u zamjenu za stablecoin. Protokol podržava kretanje likvidnosti usluga kroz ostale mreže jer nije baziran na jednoj. Također omogućuje korisnicima da posude novac koristeći svoju kripto imovinu kao što su tokeni poput AVAX-a, WETH-a, yvUSD-a, FTM-a itd.

Abracadabra omogućuje svakom korisniku da založi svoju kriptovalutu kao kolateral, dajući mu zamjenu iz zalihe vlastitog stabilnog novca, koji se naziva Magic Internet Money (MIM). No taj stablecoin se izdaje u obliku zajma, jer se MIM na kraju mora vratiti protokolu ili će zajmoprimac snositi kazne. Evo dva moguća pravca djelovanja za zajam uzet u MIM-u:

- ✔ Uspješan zajam : Ako korisnik želi ponovno steći svoj kolateral založen u zamjenu za MIM, mora jednostavno vratiti MIM, uključujući unaprijed dogovorenu kamatu. Koji god kapital da je korisnik založio, nakon isplate potrebne sume MIM-a taj kapital se ponovno otključava. Ovo se smatra "uspješnim" zajmom.

- ✘ Neuspješan zajam: Ako korisnik ne uspije vratiti svoj posuđeni MIM prije određenog datuma ili ako mu kolateral padne ispod određene vrijednosti, automatski će izgubiti bilo koji oblik imovine koji je založio. No međutim, korisnik može zadržati svoj MIM koji je posudio. Ovaj oblik zajma smatra se „likvidacija“.

Slika 18: Abracadabra Money logo

Izvor: https://cryptoslate.com/how-abracadabra-became-one-of-the-fastest-growing-decentralized-protocols/ (18.6.2022)

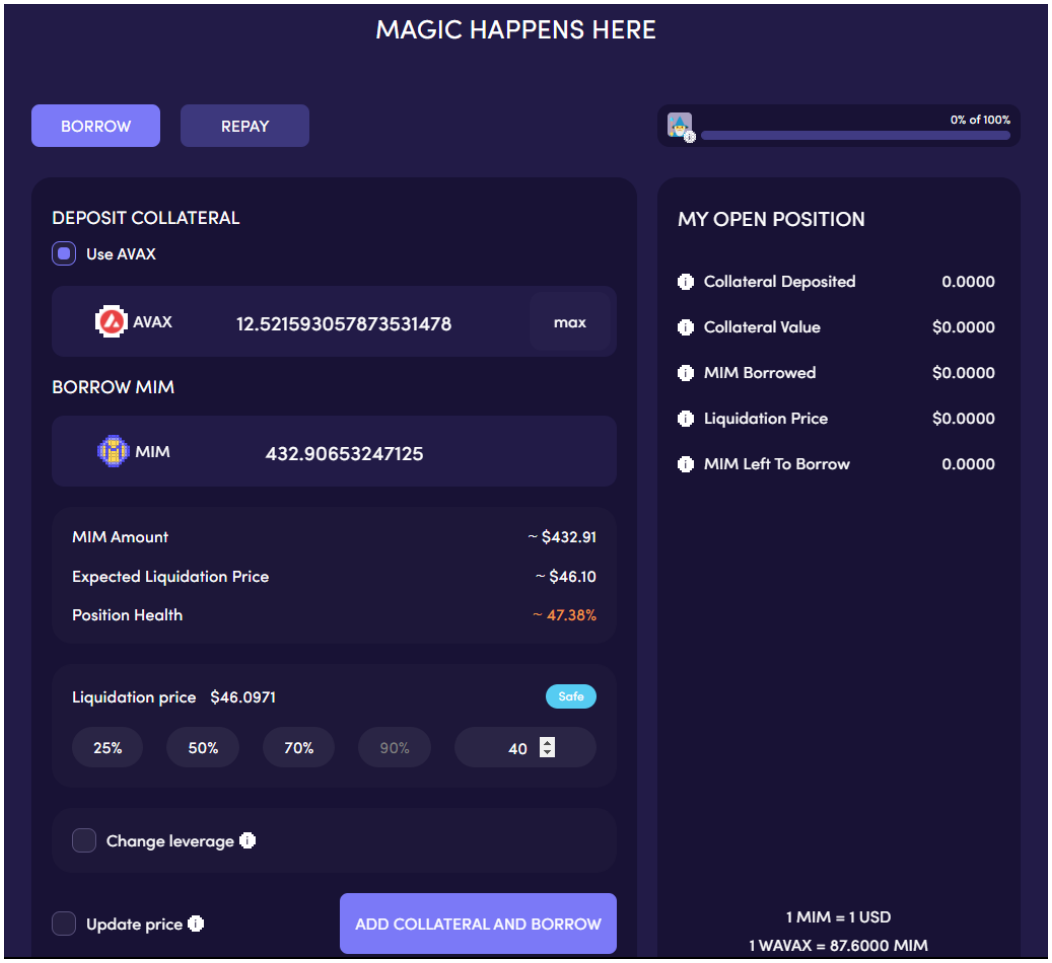
U sljedećim koracima objašnjena je procedura uzimanja zajma sa protokola, slika 19.

1. Korisnik posjeduje kriptovalutu AVAX koju zalaže u protokol i želi posuditi 40% od svoje založene imovine.

2. Protokol nudi korisniku 432 MIM-a koja se moraju onda naknadno vratiti u protokol kako bi korisnik ponovno otključao svojih 12.5 AVAX-a.

3. Korisnik mora paziti na polje „Expected Liquidation Price“ koje iznosi $46.10.

4. Ako cijena AVAX-a padne ispod $46.10 i korisnik nije vratio MIM, sredstva koja su založena se likvidiraju, a korisnik može zadržati posuđeni MIM.



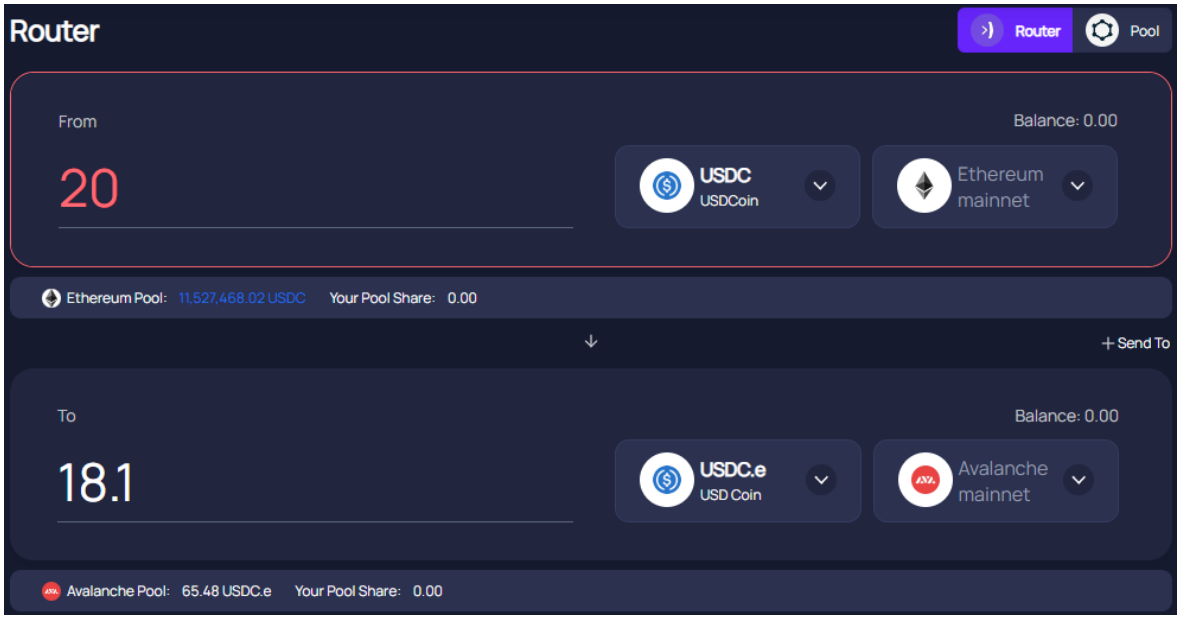
Slika 19: Primjer procedure uzimanja zajma na Abracadabra Money protokolu

Izvor: Autor

5.4. ANYSWAP BRIDGE

Anyswap je vrsta mosta koji djeluje kao potpuno decentralizirani protokol za međulančanu razmjenu tokena, temeljen na Fusion DCRM tehnologiji s automatiziranim cijenama i likvidnošću. Anyswap je decentralizirana aplikacija koja radi na Fusion, Binance Smart Chain, Ethereum, Fantom i Avalache blockchainu te i na mnogim drugim mrežama. Djelovajući kao blockchain most Anyswap pruža vezu koja omogućuje prijenos tokena ili podataka između dva različita blockchain ekosustava. Na primjer ako korisnik želi prebacitii USDC token sa Ethereum mreže na Avalanche mrežu, koristiti će značajku „Bridge ili Router“ i za tu uslugu će platiti određenu naknadu. Nakon što korisnik izdvoji svoje tokene za premošćivanje, USDC token nestaje sa Ethereum mreže i ponovno se pojavljuje na Avalanche mreži u kratkom periodu nakon što se transakcija dovrši.

Mostovi poput Anyswapa s značajkom „Bridge“ općenito koriste neku vrstu mint-and-burn protokola kako bi opskrbu tokena održavali konstantnom na svim platformama. Kada token napusti jedan blockchain, on se spaljuje ili zaključava, a ekvivalentni token se kuje na suprotnom blockchainu. Suprotno tome, kada se token vrati u svoju izvornu mrežu, "blizanac" se spaljuje ili zaključava. Dok sa druge strane značajka „Router“ koristi likvidnosti iz bazena koju protokol pruža kako bi se tokeni zamjenili, ali jedino ako ima dostupne likvidnosti za traženi token, slika 20.



Slika 20: Primjer korištenja usluge Router

Izvor: Autor

6. YIELD FARMING

Yield Farming, koji se također naziva i rudarstvom likvidnosti, način je za ostvarivanje zarade „holdanjem“ kriptovaluta. Jednostavno rečeno, to znači zaključavanje kriptovaluta i dobivanje kamata.[12] Korisnici posuđuju sebi ili drugima kriptovalute u svrsi za zaradom na pruženu uslugu u obliku tokena koje protokol nudi. Farmeri koji žele maksimalno povećati svoj prinos mogu primijeniti i složenije taktike. Na primjer, mogu stalno premještati svoje tokene između više platformi koje nude zajam kako bi optimizirali svoje dobitke.

Postoji nekoliko varijanta Yield-a:

1. Liqudity providing (Pružanje likvidnosti): Korisnici polažu dva tokena na DEX kako bi osigurali likvidnost trgovanja. Burze naplaćuju malu naknadu za zamjenu dvaju tokena koja se plaća pružateljima likvidnosti. Ova se naknada ponekad može platiti u novim tokenima fonda likvidnosti (LP).

2. Lending (Posuđivanje): Korisnici mogu posuditi svoje tokene zajmoprimcima putem pametnog ugovora i zaraditi prinos od kamata plaćenih na zajam.

3. Borrowing (Uzimanje zajma): Yield farmeri mogu koristiti jedan token kao kolateral i dobiti zajam drugog. Korisnici tada mogu obraditi prinos s posuđenim tokenima. Na taj način farmer zadržava svoj početni kapital u protokolu od kojeg je uzeo zajam, čija vrijednost s vremenom može rasti, a istovremeno zarađuje prinos na posuđenim tokenima.

Očekivani prinosi obično se računaju na godišnjoj razini. Dva često korištena mjerenja su godišnja postotna stopa (APR) i godišnji postotni prinos (APY). APR ne uzima u obzir nadopunjavanje i reinvestiranje dobitaka dok APY računa.

[12] https://crobitcoin.com/objasnjeno-defi-i-yield-farming/ (19.6.2022)

7. NFT

NFT (Non fungible token) je digitalna imovina koja predstavlja objekte iz stvarnog svijeta kao što su umjetnost, glazba, predmeti u igri i videozapisi. Kupuju se i prodaju putem interneta, često kriptovalutama, i općenito su kodirani istim temeljnim softverom kao i mnoge kriptovalute na blockchainu. Iako postoje od 2014 godine NFT-ovi trenutno dobivaju veću pozornost na tržištu jer postaju sve popularniji način kupnje i prodaje digitalnih umjetničkih djela. Tržište NFT- a vrijedilo je 41 milijardu dolara samo u 2021 godini, što je iznos koji se približava ukupnoj vrijednosti cjelokupnog globalnog tržišta likovne umjetnosti. NFT-ovi su također općenito jedinstveni, ili barem vrlo ograničeni, i imaju jedinstvene identifikacijske kodove što znači da niti jedan nije isti. Konkretno, NFT-ovi se obično drže na Ethereum blockchainu, iako ih podržavaju i drugi blockchaini korisnicima najviše ulijeva sigurnost Ethereum.

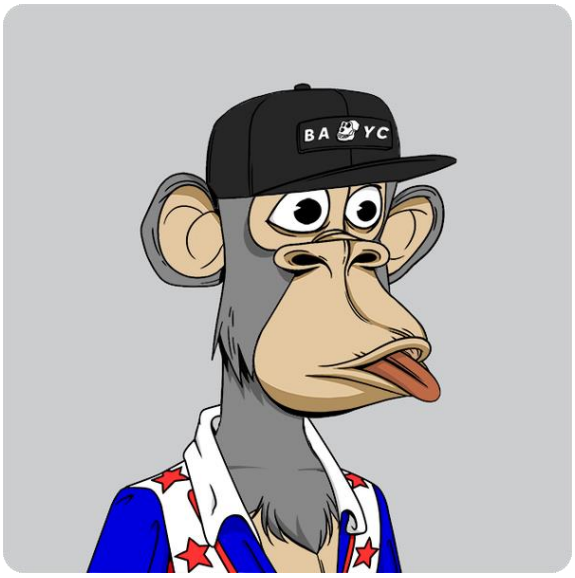
NFT se većinom stvara od digitalnih objekata koji predstavljaju materijalne i nematerijalne stavke kao na primjer:

- Grafička umjetnost
- GIF-ovi
- Videozapisi
- Kolekcionarski predmeti
- Virtualni avatari
- Dodatci za videoigre
- Glazba, te čak i dizajnerske tenisice

U suštini, NFT-ovi su poput fizičkih kolekcionarskih predmeta, samo digitalni. Dakle, umjesto da korisnik dobije stvarnu sliku livade koja će se objesiti na zid, kupac umjesto toga dobiva digitalnu datoteku. Također dobiva i ekskluzivna vlasnička prava. NFT-ovi mogu imati samo jednog vlasnika odjednom, a njihova upotreba kroz blockchain tehnologiju olakšava provjeru vlasništva i prijenos tokena između vlasnika. Kreator također može pohraniti određene informacije u metapodatke NFT-a. Na primjer, umjetnici mogu potpisati svoja umjetnička djela uključivanjem svog potpisa u datoteku. Na slici 21 prikazan je NFT iz kolekcije Bored Ape Yacht Club.

U krajnosti blockchain tehnologija i NFT daju umjetnicima i kreatorima sadržaja jedinstvenu priliku da prodaju svoje umjetnosti. Na primjer, umjetnici se više ne moraju oslanjati samo na galerije ili aukcijske kuće kako bi prodali svoju umjetnost. Umjesto toga, umjetnik može prodati svoje djelo izravno potrošaču kao NFT, što im također omogućuje da zadrže veći dio profita. Osim toga, umjetnici mogu programirati svoje umjetnine tako da dobivaju postotak od prodaje kad god se njihova umjetnost proda novom vlasniku. Ovo je atraktivna značajka budući da umjetnici uglavnom ne primaju budući prihod nakon što se njihova umjetnost prvi put proda.

Kupnja i prodaja NFT-ova se vrši na službeno verificiranim platformama poput Opensea, Rarible, Looksrare i Foundation aplikacija. Pored ovih javnih tržišta korisnici imaju i mogućnost obavljanja P2P transakcija koja se nazivaju OTC kako bi izbjegli dodatne naknade koje tržišta traže. No takva vrsta trgovanja je rizičnija jer se nikad ne zna ako će druga strana ispoštovati svoju riječ.



Slika 21: Bored Ape Yacht Club NFT

Izvor: https://opensea.io/assets/ethereum/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/4126 (19.6.2022)

8. NOVČANICI

Kripto novčanik je uređaj, fizički medij, program ili usluga koja pohranjuje javne i privatne ključeve.[13] Za razliku od normalnog novčanika, koji može držati stvarnu gotovinu, kripto novčanici tehnički ne pohranjuju kriptovalute. Posjedi praktički žive na blockchainu, ali im se može pristupiti samo pomoću tih privatnih ključeva. Ključevi dokazuju vlasništvo nad digitalnim novcem i omogućuju obavljanje transakcija. Ako korisnik izgubi svoje privatne ključeve, gubi i pristup svom novcu. Zato je važno čuvati svoj hardverski novčanik na sigurnom ili koristiti pouzdanog davatelja novčanika.

Kripto novčanici se kreću od aplikacija jednostavnih za korištenje do složenijih sigurnosnih rješenja. Glavne vrste novčanika koje korisnik može birati uključuju:

- Papirnati novčanici: ključevi su napisani na fizičkom mediju poput papira i pohranjeni na sigurnom mjestu. To naravno otežava korištenje kriptovaluta, jer se kao digitalni novac može koristiti samo na internetu.

- Hardverski novčanici: ključevi se pohranjuju u uređaj nalik USB-u koji se čuva na sigurnom mjestu i povezan je s računalom samo kada korisnik želi koristiti svoju kriptovalutu..

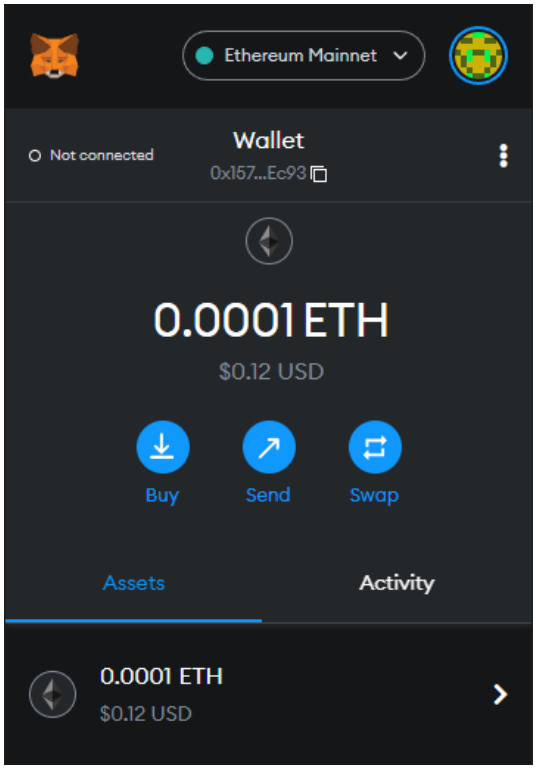
- Online novčanici: ključevi su pohranjeni u aplikaciji ili drugom softveru. To čini slanje, primanje i korištenje kriptovalute jednostavnim kao i korištenje bilo kojeg internetskog bankovnog računa, sustava plaćanja ili posredništva. Ali također ovakav novčanik može biti izložen hakerskim napadima.

[13] https://www.kriptovalute.hr/kripto-novcanik/ (19.6.2022)

8.1 METAMASK

MetaMask je jedan od poznatijih softver novčanika kojem se može pristupiti putem internetske ekstenzije na web browserima, slika 22. Nakon što se instalira, korisnicima pruža mogućnost pohrane Ethera i drugih ERC-20 tokena, te im omogućava transakcije s bilo kojom Ethereum adresom. Povezivanjem MetaMaska na dapp-ove temeljene na Ethereumu, korisnici mogu trošiti svoje tokene u igrama, ulagati tokene u aplikacije za kockanje, trgovati na decentraliziranim burzama te slati svoje kripto valute na druge adrese. Također korisnicima pruža ulaznu točku u novi svijet decentraliziranih financija.

Kada korisnik prvi put instalira MetaMask tražiti će se od korisnika da zapiše mix od 12 unikatnih riječi koje čine privatni ključ od tog novčanika. Korisnik ne smije izgubiti te riječi jer u protivnom će izgubiti i posjed nad svojom imovinom. Također svaki novčanik ima svoju jedinstvenu adresu koja služi za slanje i primanje kriptovaluta. S dijeljenjem te adrese treba postupati vrlo oprezno jer ako se zamijeni ili slučajno izbriše jedan broj ili slovo, sredstva će biti poslana na tuđi novčanik ili čak na ničiji i tad povrat nije moguć.



Slika 22: Izgled MetaMask novčanika

Izvor: Autor

8.2. LEDGER

Ledger je najsigurnija varijanta novčanika za pohranjivanje kriptovaluta, slika 23. Svojim izgledom podsjeća na USB sa ugrađenim tipkama za navigaciju i malim LCD ekranom. Ovaj novčanik je otporan na hakerske i malverske proboje jer uređaj zaključava privatan ključ svaki put nakon transakcije i traži ponovnu fizičku autentifikaciju vlasnika kod sljedeće transakcije. Takvom metodom se održava najveća razina sigurnosti, potpuno vlasništvo i privatnost nad svom imovinom koju korisnik posjeduje. Uz takve preventivne metode ledger također dodaje neke zgodne i prikladne funkcionalnosti, čineći hardverske novčanike efikasnijim.

Ledger je u svoju aplikaciju implementirao mogućnosti kupnje, prodaje i razmjenjivanja kriptovaluta, na siguran način, putem raznih pružatelja usluga izravno putem matične Ledger Live aplikacije. Neki primjeri uključuju protokole poput Wyre, Paraswap, Coinify, Changelly i još mnogo drugih. Ledger također pruža pristup tako da možete upravljati svojim NFT ili DeFi portfeljem putem drugih vanjskih pružatelja usluga, iz njegove aplikacije.

Slika 23: Ledger Nano S Novčanik

Izvor: https://www.jeftinije.hr/Proizvod/9905133 (19.6.2022)

9. PREVARE I KRAĐE

Prevaranti uvijek traže nove načine da ukradu ljudima novac, a ogroman rast kriptovaluta posljednjih godina stvorio je idealne prilike za prijevaru kakve bi svaki lopov mogao sanjati. Kriminal u kriptovalutama dosegao je rekordan broj u 2021 godini. Prevaranti su te godine ukrali preko 14 milijardi dolara kriptovaluta od korisnika koji su novi ili neiskusni u tom području. Korisnici DeFi usluga često budu namamljeni u razne vrste „Scam“ aplikacija koje nude lažne valute ili usluge koje obećavaju enormnu zaradu. Prevara ima mnogo i različitih su oblika i sastava, kako bi ih se izbjeglo korisnik mora obaviti svoje istraživanje, kratkim riječima nazvano DYOR (Do your own research).

9.1. RUGPULL

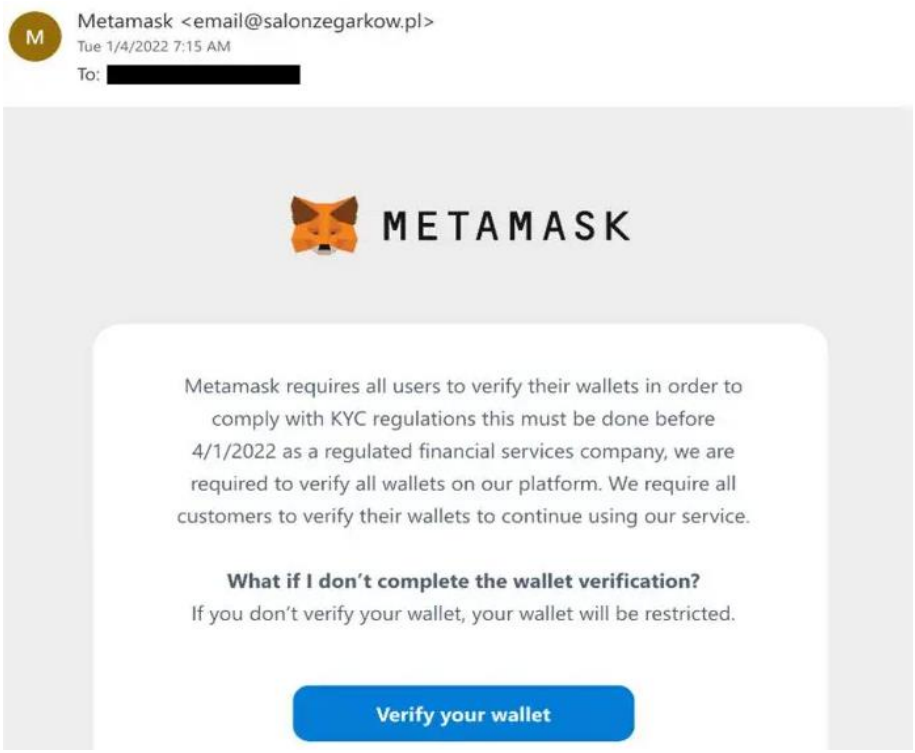
Rug Pull je vjerojatno najčešća prijevara s kriptovalutama u DeFi prostoru, ali može biti također jedna od lakših za uočavanje za one koji znaju kako početi. Rug Pull je izraz kada programeri promoviraju nešto što se čini kao novi, uzbudljivi i revolucionarni projekt kako bi stekli što više investitora. Kroz taj proces marketinga i promocije prikupljaju stotine tisuća, ako ne i milijune dolara. Onda, jednog dana, ti programeri jednostavno prodaju tokene i nestanu sa lica zemlje sa svim sredstvima od svojih investitora. Takvi programeri naravno nikada nisu ni namjeravali izgraditi projekt s tim novcem već su jednostavno htjeli provesti prijevaru. Investitori u krajnosti ostaju sa hrpom bezvrijednih tokena ili čak sa s ničime. Primjer RugPull-a i nagli pad vrijednosti tokena prikazan je na slici 24.

Slika 24: Primjer RugPull-a

Izvor:https://blog.cryptostars.is/crypto-scams-whats-a-rug-pull-f55e22f12cc2 (20.6.2022)

9.2. PHISHING

Phishing je taktika prevare stara koliko i Internet, ona se temelji na prevarantima koji se pretvaraju da su legitimne tvrtke i tako prikupljaju osobne podatke o svojim žrtvama. Kripto phishing često cilja na informacije koje se odnose na online novčanike. Pokušaj krađe se odvija putem e-pošte, pri čemu se prevarant pretvara da je predstavnik trgovačke platforme ili protokola. Prevarant će izmisliti pogrešku kao što je "vaš račun je kompromitiran. Pošaljite nam svoju e-poštu i lozinku kako bismo ga mogli zaštititi." Takve taktike mogu uključivati traženja privatnog ključa novčanika i lozinki ili zahtijevanje od žrtve da pošalje sredstva. Nakon što hakeri uspiju doći do tih informacija, kradu kriptovalute u tim novčanicima. Primjer Phishing e-maila prikazan je na slici 25.



Slika 25: Primjer Phishing e-maila

Izvor: https://news.trendmicro.com/2022/01/05/scam-alert-fake-metamask-crypto-wallet-security-alert-emails/ (20.6.2022)

9.3. HONEYPOT

Honeypots su pametni ugovori za koje se čini da imaju problem s dizajnom koji dopušta programeru koji ga je stvorio da isprazni Ether (nativnu valutu Ethereuma) iz ugovora ako korisnik ugovoru prethodno pošalje određenu količinu Ethera. Međutim, kada korisnik pokuša iskoristiti ovu zamku, otvara se drugi, još nepoznati otvor, sprječavajući uspjeh slanja ethera.

Najjednostavniji način za razumijevanje ovog složenog hakerskog programa je analiza stvarnog slučaja. U 2018 godini jedan haker je došao na prilično pametnu ideju za dobivanje kriptovaluta od neiskusnih korisnika. Naime haker je stvorio novčanik, stavivši 5000 USD u token $MNE (Minereum). Dotična kriptovaluta nije bitna ono što je relevantno je znati da je $MNE novčić koji se temelji na Ethereumu. Nakon što je to učinio, podijelio je svoj privatni ključ u javnom chatu. Nakon kratkog vremena korisnici su krenuli prebacivati te tokene sa njegovog walleta na svoji. Međutim, nitko nije znao da se operacija oslanja na vrlo mudro programirani pametni ugovor. Dogodilo se sljedeće:

1. Korisnici su povezali svoje novčanike s web-mjestom i pokušali poslati tokene na njihove wallete

2. Prije odobravanja transakcije korisnici su morali potvrditi naknadu za gas

3. Budući da su naknade za gas Ethereuma vrlo visoke, ključno je razumjeti da trošak transakcije nije jeftin

4. U nadi da će povući 5000 dolara, korisnici su razmišljali da potrošnja 100 dolara na gas za transakciju ne bi bila velika stvar jer će biti u profitu od 4900$

5. Nakon što su potpisali transakciju, inteligentni ugovor je uzeo naknade za gas i poslao u sekundarni novčanik

6. Na kraju bi transakcija propala jer sustav ne bi pronašao sredstva za naknadu za gas. Najpametniji trik ovdje je bio da u budućnosti nitko nije mogao povući originalnih 5000 dolara.

10. ZAKLJUČAK

DeFi predlaže rješenja za vraćanje ekonomske moći ljudima stvaranjem financijskog sustava koji je dostupan, učinkovit i transparentan. To je uzbudljiv razvoj za blockchain prostor koji svakome bilo gdje, donosi stvarne, korisne financijske usluge kao što su zaduživanje, pozajmljivanje, izdavanje imovine, ulaganje itd. No ne samo da funkcionira kao rješenje za ljude koji žele napraviti nešto više sa svojim novcem već je i rješenje za ostale velike tvrtke i korporacije. Nudeći unikatnu i brzu vrstu poslovanja i polaganja sredstva u protokole, DeFi bi riješio i nekolicinu problema s kojim se tvrtke suočavaju. Bitcoin je otvorio vrata ovog svijeta, on je začetnik ove vrste poslovanja i uvijek će biti cijenjena valuta, primarno jer je prva kripto valuta koja je stvorena, a sekundarno jer je „rastvorio“ svijet između primitivnog i moderno digitalnog financiranja. Da bi DeFi doživio svoj maksimalni publicitet i korisnost, mora doživjeti globalnu adaptaciju od strane ljudi. Najteži korak prema tome je objašnjavanje korisnicima kako ovo sve zapravo funkcionira i kako maksimalno osigurati svoja sredstva. No kako vrijeme ide, polako se ljudi navikavaju i na ostale modele digitalnog financiranja što znači da je samo pitanja vremena kada će se adaptacija dogoditi.

Oni koji žele započeti s DeFi-jem, izvan početnih osnova trgovanja sa kriptovalutama, trebali bi pažljivo nastaviti i biti sigurni da rade s pouzdanim protokolom. Iako su prinosi koje nudi DeFi primamljivi, korisnika ne smije zaslijepiti potencijalni povrat na uloženi rizik. Pad kretanja na tržištima kriptovaluta mogao bi brzo izbrisati sve male dobitke od prinosa, a izravne prijevare ili krađe mogle bi još brže izbrisati uloženo kripto bogatstvo.

LITERATURA

KNJIGE:

1. Dannen C; Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners 1st ed. Edition, Velika Britanija, 2018. God

INTERNETSKI IZVORI:

- Što su decentralizirane financije i koje su njihove prednosti? 19.1.2021 https://ecd.rs/blog/defi-sta-su-decentralizovane-finansije-i-koje-su-njene-prednosti/ (29.4.2022)
- Što je Blockchain tehnologija i kako funkcionira? https://kriptomat.io/hr/blockchain/sto-je-blockchain-tehnologija/ (29.4.2022)
- What is Blockchain technology? https://www.ig.com/en/trading-strategies/what-is-blockchain-technology--200710 (29.4.2022)
- What is Bitcoin? https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin (29.4.2022)
- Što je Bitcoin i kako funkcionira? https://kriptomat.io/hr/kriptovalute/bitcoin/sto-je-bitcoin/ (29.4.2022)
- Što je pametni ugovor i koja je njegova uloga u blockchainu? (2.1.2022) https://www.bitcoin-store.hr/blog/sto-je-pametni-ugovor/ (29.4.2022)
- Understanding smart contracts on the blockchain (22.3.2021) https://morethandigital.info/en/what-are-smart-contracts-understanding-contracts-on-the-blockchain/ (29.4.2022)
- Comparision of peer to peer vs client server netowork models https://www.networkstraining.com/peer-to-peer-vs-client-server-network/ (5.5.2022)
- Što je P2P i što možete učiniti s njom? https://hr.itpedia.nl/2019/01/11/wat-is-p2p-peer-to-peer-en-wat-kan-je-er-mee/ (5.5.2022)
- Vrste konsenzusa na blockchainu (9.1.2020) https://crobitcoin.com/vrste-konsenzusa-na-blockchainu-proof-of-work-vs-proof-of-stake/ (8.5.2022)
- Proof of stake definition (9.5.2018) https://www.chainbits.com/cryptocurrency-terms/proof-stake-definition/ (8.5.2022)
- Što je Ethereum i kako funkcionira? (27.2.2020) https://electrocoin.hr/blog/sto-je-ethereum-i-kako-funkcionira (27.5.20222)

- Što je to Ethereum gas i kako se određuju cijene transakcija u Ethereumu? (5.12..2017) https://bitfalls.com/hr/2017/12/05/ethereum-gas-and-transaction-fees-explained/ (29.5.2022)
- BitGo adds support for ERC20 tokens (17.4.2018) https://medium.com/@robinverderosa/bitgo-adds-support-for-erc20-tokens-ca8384779723 (29.5.2022)
- Ethereum 2.0 skaliranje napopularnije blockchain platforme (5.7.2021) https://www.bitcoin-store.hr/blog/ethereum-2-0-skaliranje-najpopularnije-blockchain-platforme/ (29.5.2022)
- Što je kriptovaluta Avalanche i kako funkcionira? https://kriptomat.io/hr/kriptovalute/avalanche/sto-je-avalanche/ (8.6.2022)
- Automated market maker (AMM) everything you need to know (10.2.2022) https://zipmex.com/learn/what-is-amm-automated-market-maker/ (8.6.2022)
- Što je stablecoin i kako funkcionira? Vodič za početnike (25.3.2022) https://www.bitcoin-store.hr/blog/sto-je-stablecoin-i-kako-funkcionira/ (17.6.2022)
- Što su NFT-I i zašto ljudi za njih daju milijune (14.3.2021) https://www.bug.hr/blockchain/sto-su-nft-i-i-zasto-ljudi-za-njih-daju-milijune-19244 (19.6.2022)
- What is a crypto wallet? A beginner's guide (26.4.2022) https://crypto.com/university/crypto-wallets (19.6.2022)
- Crypto scams- What's a Rug pull? (4.1.2022) https://blog.cryptostars.is/crypto-scams-whats-a-rug-pull-f55e22f12cc2 (20.6.2022)
- 9 common cryptocurrency scams in 2022 (13.6.2022) https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams (20.6.2022)

POPIS SLIKA