UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

RAZVOJ IN IMPLEMENTACIJA ŽETONA V OMREŽJU ETHEREUM

Ljubljana, julij 2023 MATEJ RENČELJ

IZJAVA O AVTORSTVU

Podpisani Matej Renčelj, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Razvoj in implementacija žetona v omrežju Ethereum pripravljenega v sodelovanju s svetovalcem doc. dr. Luko Tomatom

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu prek Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

11. da sem preveril verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne _____ Podpis študenta: _____

KAZALO

UVOD **1**
1 TEHNOLOGIJA VERIŽENJA BLOKOV **1**
1.1 Vrste tehnologije veriženja blokov **3**
1.2 Uporaba tehnologije veriženja blokov v podjetjih **3**
2 OPREDELITEV OMREŽJA ETHEREUM **3**
2.1 Zgodovina omrežja Ethereum **5**
2.2 Prihodnost pretočnosti omrežja Ethereum **7**
2.3 Ethereum virtualno izvajalsko okolje **8**
2.3.1 Ethereum računi 9
2.4 Metoda soglasja **10**
2.4.1 Dokaz o delu 10
2.4.2 Dokaz o deležu 10
2.5 Pametne pogodbe **11**
2.6 Decentralizirane aplikacije **12**
2.7 ERC-standard za podžetone **13**
2.7.1 ERC-20 13
2.7.2 ERC-721 13
2.7.3 ERC-1155 14
2.8 Programski jezik Solidity **14**
3 USTVARJANJE ERC-20 žetona **14**
3.1 OpenZeppelin **15**
3.2 REMIX IDE **15**
3.3 MetaMask **15**
3.4 Etherscan.io **15**
3.5 Ustvarjanje pametne pogodbe **16**
3.6 Lansiranje pogodbe na testno omrežje Sepolia **18**
SKLEP **19**
LITERATURA IN VIRI **20**
PRILOGE **26**

KAZALO SLIK

Slika 1: DLT-evolucija: od evidenčne zbirke podatkov do veriženja blokov 2
Slika 2: Prestop z metode soglasja »dokaz o delu« na metodo soglasja »dokaz o deležu« .. 7
Slika 3: Pregled transakcije na spletni strani Etherscan.io 16
Slika 4: Preizkus osnovnih ERC20-funkcij v lokalnem testnem okolju 17
Slika 5: Prehod z glavnega omrežja na testno omrežje Sepolia 18
Slika 6: Lansiranje pametne pogodbe 18
Slika 7: Uvoz nastavitev podžetona in stanje na računu 19

KAZALO PRILOG

Priloga 1: Nastavljanje OpenZeppelinove predloge za podžeton ERC-20 1
Priloga 2: REMIX IDE – virtualizacija Shanghai testnega omrežja 2
Priloga 3: REMIX IDE – transakcija podžetonov med računi, prenos 150.000 MidCoin žetonov 3
Priloga 4: REMIX IDE – preverjanje stanja na naslovljenem računu po transakciji 4
Priloga 5: Sepolia.etherscan.io – seznam opravljenih transakcij na testnem omrežju Sepolia 5

SEZNAM KRATIC

angl. – angleško
BLOB – (angl. Binary Large Objects); veliki binarni objekti
DAO – (angl. Decentralized Autonomous Organization); decentralizirana avtonomna organizacija
DAPP – (angl. Decentralized application); decentralizirana aplikacija
DLT – (angl. Distributed Ledger Tehnology); tehnologija razpršene evidence
EIP – (angl. Ethereum Improvement Proposals); predlog za izboljšanje Ethereuma
ERC – (angl. Ethereum Request for comment); Ethereum prošnja za komentar
ETH - Ether
EVM – (angl. Ethereum Virtual Machine); Ethereum virtualno izvajalsko okolje
ICO – (angl. Initial Coin Offering); prvotna ponudba kovancev
NFT – (angl. Non Fungible Token); nezamenljiv žeton
P2P – (angl. Peer-to-peer); omrežje enakovrednih vrstnikov

UVOD

Tehnologija veriženja blokov (angl. blockchain) je postala pomembno področje v sodobnem digitalnem svetu, ker naj bi omogočala decentralizacijo, preglednost, varnost in nespremenljivost podatkov. Tradicionalne podatkovne baze imajo za razliko od tega popoln nadzor nad podatki. Posledično je preglednost podatkov neobstoječa ali zelo omejena, podatki so shranjeni na manjšem številu različnih lokacij in obstaja možnost, da gostujoče podjetje propade, podatke izbriše ali z njimi manipulira, proda itd. Najpomembnejše je to, da uporabnik lastniku zaupa, da bo z njegovimi podatki previdno in pošteno ravnal (Budhi, 2022).

Veriženje blokov to potrebo po zaupanju teoretično odstrani. Vsi dogodki na javnih verigah blokov so transparentni in pregledni, podatki pa nespremenljivi in šifrirani. V večini različic implementacije verige blokov velja, da ko je podatek shranjen na verigi blokov, ga ne moremo več izbrisati ali spremeniti, lahko le dodamo nove (Hayes, 2023).

Namen zaključne strokovne naloge je raziskati in predstaviti omrežje Ethereum, ki temelji na tehnologiji veriženja blokov in že dlje časa sledi največji kriptovaluti v tržni kapitalizaciji – bitcoinu. Omrežje Ethereum je izbrano zaradi lahko dostopnih virov informacij in vrednot skupnosti.

Cilji naloge so:

- predstaviti osnove tehnologije veriženja blokov,
- predstaviti glavna dejstva in zgodovino omrežja Ethereum,
- na razumljiv način predstaviti tehnične gradnike omrežja,
- predstaviti in opredeliti metodi soglasja »dokaz o delu« in »dokaz o deležu«,
- predstaviti decentralizirane aplikacije in povezane gradnike,
- ustvariti in predstaviti lasten podžeton na testnem omrežju Ethereum.

Zaključna strokovna naloga je razdeljena na tri dele. V prvem delu raziščem in predstavim glavne lastnosti tehnologije veriženja blokov. V drugem delu predstavim glavne lastnosti in zgodovino verige blokov Ethereum. Posvetim se tudi tehničnim gradnikom omrežja, ki jih predstavim in obrazložim. V tretjem delu na Ethereum omrežju ustvarim svoj podžeton in ga preizkusim.

1 TEHNOLOGIJA VERIŽENJA BLOKOV

Tehnologija veriženja blokov (angl. blockchain) temelji na tehnologiji razpršene evidence (angl. Distributed ledger technology, v nadaljevanju DLT), ki je razpršeno evidentiranje šifriranih podatkov. Cilj tehnologije DLT je omogočiti decentralizacijo ter odpraviti kritične točke odpovedi (angl. single point of failure) in potrebe po osrednjem organu ali posredniku za avtentikacijo transakcij. Podjetja in organizacije uporabljajo DLT za obdelavo, potrditev

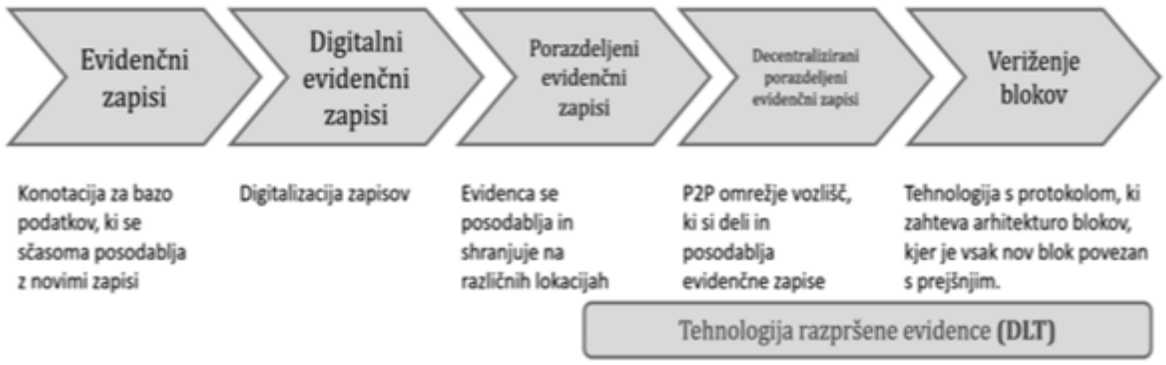
ali avtentikacijo transakcij in drugih vrst podatkovnih izmenjav. Zapisi se načeloma ne shranijo v glavno evidenco, dokler vpletene strani ne dosežejo dogovora (Marco Polo network, 2022). Evolucija evidence podatkov od preproste evidence do verige blokov je razvidna na sliki 1.

Tehnologija veriženja blokov je osnovana na DLT in vsaka veriga blokov uporablja DLT, ni pa vsaka uporaba DLT veriga blokov. Ta distinkcija je pomembna, ker veriženje blokov tudi omogoči razpršeno evidenco transakcij, ampak s to razliko, da je ta brana, odobrena in shranjena v verigi blokov.

Omrežja, ki temeljijo na tehnologiji veriženja blokov, delujejo porazdeljeno in vključujejo več omrežnih vrstnikov (angl. network peer), ki naj bi bili v večini sistemov implementacije veriženja blokov neodvisni drug od drugega in lahko uporabljajo komunikacijo vsak z vsakim (angl. peer to peer networking - P2P), s katero se strukturirajo v omrežno skupnost.

Omrežni vrstniki oziroma P2P-vozlišča (angl. P2P network nodes) hierarhije in vlog v številnih primerih implementacije veriženja blokov nimajo, zaradi tega pa lahko vsi omrežni vrstniki izvedejo vsako možno omrežno funkcijo (npr. transakcijo). Ker so omrežne funkcije decentralizirane in lahko vsi omrežni vrstniki opravijo vsako vrsto omrežne funkcije, je posledično omrežje samo decentralizirano in nima centralne oblasti (Belotti, Božić, Pujolle & Secci, 2019).

Slika 1: DLT-evolucija: od evidenčne zbirke podatkov do veriženja blokov



Prirejeno po Belotti, Božić, Pujolle & Secci (2019).

Komunikacija in podatki, ki se shranjujejo na verigah blokov, so kriptografsko zavarovani. Omrežni vrstniki se morajo prek pravil, ki so določena s t. i. protokolom soglasja (angl. consensus protocol), strinjati oziroma voliti, katere podatke in v kakšnem zaporedju shraniti na omrežju in katerih ne (Belotti, Božić, Pujolle & Secci, 2019).

1.1 Vrste tehnologije veriženja blokov

Različnih omrežij, ki uporabljajo tehnologijo veriženja blokov, je v letu 2022 več kot tisoč, za njih pa v večini velja, da spadajo v eno od naslednjih štirih kategorij (Geeks for geeks, brez datuma, a):

- Javna veriga blokov (angl. public blockchain): V njih lahko kdorkoli s potrebno računalniško opremo in dostopom do interneta sodeluje, ta omrežja so decentralizirana, odprtokodna in transparentna. Primeri javnih verig blokov so Bitcoin, Ethereum, Cardano.
- Zasebna veriga blokov (angl. private blockchain): Ohranijo značilnosti tehnologije veriženja blokov, ampak vključujejo centralizacijo omrežnih vrstnikov. Uporabniki so izbrani in omrežja so bolj centralizirana kot javne verige blokov. Raven zasebnosti podatkov na omrežju je višja, ta tip omrežja je bolj primeren za interno uporabo v podjetjih oziroma v medpodjetniškem elektronskem poslovanju (angl. Business to business ali B2B). Primeri zasebnih verig blokov so R3 Corda, Hyperledger Fabric, Quorum.
- Hibridna veriga blokov (angl. hybrid blockchain): Del omrežja je pod vplivom organizacije in ostane zaseben ter ni dostopen javnosti, del pa ostane odprt in viden vsem. Primeri hibridnih verig blokov: IBM Hybrid Blockchain, Ripple Network.
- Konzorcijska veriga blokov (angl. consortium blockchain): Je delno javna, delno zasebna, tako kot hibridna veriga blokov, ampak jo upravlja in uporablja več organizacij. Primeri konzorcijskih verig blokov so Tendermint, Multichain, Hyperledger.

1.2 Uporaba tehnologije veriženja blokov v podjetjih

Tehnologija veriženja blokov je osnovana na podatkovni bazi, ki je decentralizirana, zanesljiva in dobro zaščitena pred zlorabo (Tasatanattakool & Techapanupreeda, 2018). Preden podjetje uvede in uporablja tehnologijo veriženja blokov, je pomembno, da se odloči, ali je sploh potrebna ali pa je smotrneje uporabiti tradicionalno obliko podatkovne baze. Te so z vidika shranjevanja podatkov običajno cenejše, veliko bolj preizkušene in dostopne. Z ozirom na zapisano je treba poudariti, da je uporaba tehnologije veriženja blokov smiselna le v primerih, ko podjetja lahko izkoristijo njene prednosti. Prednosti, ki jih ponuja tehnologija veriženja blokov, so zanesljivost, sledljivost, nespremenljivost, transparentnost ali zasebnost ter resničnost shranjenih podatkov na omrežju. Te lastnosti so še posebej zaželene v vladnih, finančnih, proizvodnih in zdravstvenih sektorjih (Ali, Jaradat, Kulakli, & Abuhalimeh, 2021).

2 OPREDELITEV OMREŽJA ETHEREUM

Ethereum je omrežje, namenjeno za gradnjo aplikacij, organizacij, lastništva digitalnih sredstev, omogočanja transakcij ter komunikacije brez osrednje avtoritete. Glavna

kriptovaluta omrežja je ether (v nadaljevanju ETH) in se uporablja za vsako plačljivo dejanje na omrežju (Ethereum, 2023a).

Omrežje Ethereum je bilo ustanovljeno z namenom izboljšave in združitve zasnov skriptiranja, alternativnih kovancev (angl. altcoins) ter verižnega upravljanja (angl. on-chain governance) (Vitalik, 2014).

Zasnova skriptiranja je uresničena prek objektno orientiranega programskega jezika Solidity, ki omogoča ustvarjanje in implementacijo pametnih pogodb (angl. smart contracts). Pametne pogodbe so programi, ki upravljajo pogodbene račune (angl. contract account) in njihovo stanje v Ethereum omrežju (Soliditylang, brez datuma). Pametne pogodbe so temelj za ustvarjanje Ethereum aplikacij.

Po angleški definiciji je alternativni kovanec katerakoli kriptovaluta, ki ni bitcoin, a v kontekstu Vitalikovega informativnega dokumenta o Ethereumu (angl. whitepaper) je tukaj zasnova alternativnega kovanca mišljena kot sposobnost omrežja, da podpira svoje alternativne valute oziroma podžetone (angl. token). Pametne pogodbe omogočajo obstoj, lastništvo in upravljanje Ethereum podžetonov znotraj Ethereum omrežja (Ethereum, 2022a). Zasnova verižnega upravljanja je obstoj sistema za upravljanje in implementacijo sprememb za omrežja verig blokov. Pravila za spremembe so vpisana v protokol omrežja. Razvijalci kode predlagajo spremembe s posodobitvami kode in vsak omrežni vrstnik glasuje, ali naj se sprememba sprejme ali zavrže (Becze & Jameson, 2015).

Več aplikacij in entitet decentraliziranih avtonomnih organizacij (angl. Decentralized autonomous organizations, v nadaljevanju DAO) znotraj Ethereum omrežja uporablja verižno upravljanje, proces za omrežje Ethereum pa poteka prek zunajverižnega upravljanja (angl. off-chain governance). DAO je nova oblika organizacijske strukture brez osrednjega upravnega organa, katere člani si delijo skupen cilj. Zunajverižno upravljanje je proces, ki poteka prek neuradne diskusije v sklopu forumov, kjer se deležniki skupaj odločijo, ali naj predlog za izboljšanje Ethereuma (angl. Ethereum Improvement Proposal, v nadaljevanju EIP) odobrijo ali zavrnejo (Ethereum, 2023d). Med deležnike štejemo nosilce Ethereum kovancev, uporabnike Ethereum aplikacij, razvijalce Ethereum aplikacij/orodij, upravnike vozlišč (angl. node operators), avtorje EIP, rudarje (angl. miners) in razvijalce protokola (angl. core developers). EIP je standard dokumenta preko katerega razvijalci predlagajo nove spremembe za Ethereum omrežje. (Ethereum, 2023d).

Cilji omrežja Ethereum so višja razširljivost (angl. scalability), varnost ter trajnost ob vzdrževanju decentralizacije, torej klasična trilema verige blokov. S posodobitvami se ob vzdrževanju ravnovesja teh lastnosti omrežje Ethereum premika v vse tri strani (Ethereum, 2023e).

2.1 Zgodovina omrežja Ethereum

Ustanovitelj omrežja Ethereum, Vitalik Buterin, se je začel ukvarjati s tehnologijo veriženja blokov in skupnostjo v letu 2011. Po dveh letih se je zavedel, da ima tehnologija veriženja blokov veliko več uporab, kot le za digitalno valuto. Tako je leta 2013 dobil idejo za Ethereum in takrat tudi izdal Ethereumov informativni dokument (angl. whitepaper). Ethereum omrežje naj bi bila platforma z lastnim programskim jezikom, s katerim naj bi razvijalci imeli omogočeno gradnjo različnih decentraliziranih aplikacij (Frank & Silverstein, 2021).

Za glavno financiranje projekta je v naslednjem letu, od julija do avgusta 2014, potekal ICO (angl. Initial coin offering, v nadaljevanju ICO). ICO je dogodek v katerem kriptoprojekt javnosti ponudi svoje podžetone v zameno za kriptovalute. Preko ICO dogodka je projekt prodal javnosti več kot 60 milijonov žetonov ETH in zbral 18,3 milijona ameriških dolarjev. Zbrani denar je bil namenjen za stroške, ki so nastali pred ICO (1,8 milijona ameriških dolarjev), ter za varnostni sklad (1 milijon ameriških dolarjev). Od preostalega denarja je 76,5 % šlo razvijalcem, 13,5 % za komunikacije in ozaveščanje skupnosti, 10 % pa za raziskave (Russo, 2020).

V letu 2014 je nastala Ethereum fundacija. To je neprofitna organizacija, ki podpira Ethereum ekosistem in je razvijalsko osredje omrežja, ki delno koordinira razvoj. Med člane so spadali Vitalik Buterin, Joseph Lubin, Gavin Wood in razni razvijalci. Ethereum fundacija je v tem obdobju v letih 2014 in 2015 ustvarila več prototipov omrežja Ethereum. Omrežje je bilo prvič javno lansirano v juliju leta 2015. Ta različica omrežja se je imenovala »Frontier« (Williams, 2022). Omrežje Ethereum je tako kot Bitcoin delovalo po metodi soglasja »dokaz o delu« (angl. Proof-of-Work Consensus Protocol). Za razliko od Bitcoina je bil cilj Ethereum omrežja v neki točki prestopiti na metodo soglasja »dokaz o deležu« (angl. Proof-of-Stake Consensus Protocol) (Ethereum, 2023b).

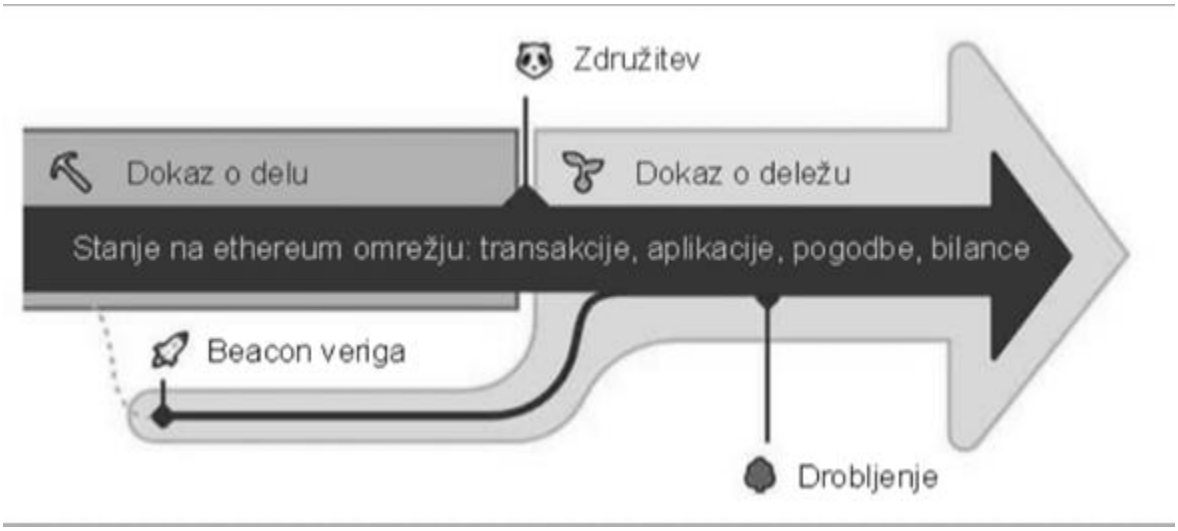
Leti 2015 in 2016 sta bili leti razvoja. Izdana je bila druga večja različica omrežja, imenovana »Homestead«, ki je vsebovala več sprememb na protokolu omrežja in omogočala nadaljnje nadgrajevanje platforme (Young, 2016). V letu 2016 je nastal prvi DAO. Za sprejemanje odločitev uporablja pristop upravljanja od spodaj navzgor. Prvi DAO je deloval kot sklad, v katerega je več kot 11.000 vlagateljev vložilo za takrat 150 milijonov ameriških dolarjev vrednosti v ethru. Tri mesece po zagonu, je zaradi varnostne napake napadalec premaknil za 60 milijonov ameriških dolarjev v Ethru. Ta incident je sprožil diskusijo v skupnosti o tem ali naj se sredstva vlagateljem povrnejo preko sprememb na omrežju, ali ne. Na koncu se je skupnost razdelila in nastalo je novo omrežje. Staro Ethereum omrežje se je preimenovalo v »Ethereum Classic«, tam je stanje glede DAO-napada ostalo enako. V novem omrežju, ki je podedovalo ime »Ethereum«, pa so se vložena sredstva vlagateljem povrnila (Williams, 2022).

V letu 2017 se je promet na omrežju Ethereum znatno povečal. Nekatere decentralizirane aplikacije, ki so delovale na Ethereum omrežju, so postale popularne in privabile promet. Med številne uspešne aplikacije spadajo igra »Cryptokitties«, platforma za samostojne delavce »EthLance« ter plačilna rešitev »TenX«. S pomočjo slednje so uporabniki lahko uporabljali fizično MasterCard in Visa kartico ter z njo pretvorili ETH v denar in ga uporabljali za nakupe (Duro, 2017). Omrežje se je zaradi povečanega prometa posledično zelo upočasnilo in transakcije so postale izjemno drage. Rešitev za skaliranje je bil čimprejšnji premik na metodo soglasja »dokaz o deležu«, saj je ta veliko bolj energetsko učinkovita in nadgradljiva v primerjavi z metodo soglasja »dokaz o delu«.

V tem obdobju je bilo Ethereum omrežje priljubljena izbira za gostovanje ICO-dogodkov. Do tega je prišlo zaradi preprostosti postopka kreacije novega podžetona standarda ERC-20, s pomočjo katerega so podjetja zbrala denar za svoje projekte in vlagateljem v zameno dala svoj podžeton. Vsak ICO-projekt se je od drugega lahko razlikoval po uporabnosti in lastnosti podžetona. V nekaterih primerih je podjetje izdalo svojo decentralizirano aplikacijo neposredno na Ethereum omrežju, za njeno uporabo pa je lahko uporabnik uporabljal podžeton kot plačilno sredstvo. Pogosto pa je izdani podžeton veljal kot začasno sredstvo, s katerim so lahko uporabniki podžeton zamenjali za drug, funkcionalen žeton ob lansiranju novega omrežja ali aplikacije na drugem omrežju (Gemini, 2022). Vlagatelj je lahko v veliko primerih ICO izdane podžetone takoj ob izdaji prosto prodajal in kupoval na odprtem trgu prek decentraliziranih kriptomenjalnic, pozneje pa tudi na centraliziranih kriptomenjalnicah. Regulacija trga je bila v tem obdobju pomanjkljiva, ponekod neobstoječa, in to je bilo tudi razvidno iz obsega prevar. V raziskavi Satis Group julija v letu 2018 je bilo ocenjeno, da je približno 80 % vseh ICO-projektov prevara. Vseeno pa je tudi omembe vredno tudi to, da je 70 % vsega vloženega denarja šlo v kakovostnejše projekte, kar nakazuje da je, kljub številnim prevaram večina vloženih sredstev šla v legitimne projekte (Dowlat, 2018).

Decembra leta 2020 je prišel v uporabo »Beacon Chain«. To je ime izvirne Ethereum blokovne verige, ki deluje prek mehanizma za doseganje soglasja z dokazom o deležu. Ustvarjena je bila z namenom preverjanja ustreznosti mehanizma soglasja in je delovala vzporedno z izvirnim Ethereum omrežjem. Po skoraj dveh letih nadgrajevanja in razvijanja se je v septembru leta 2022 zgodil dogodek, imenovan »Ethereum Merge«, na katerem se je Ethereum omrežje spojilo in prevzelo mehanizem za doseganje soglasja z dokazom o deležu, kot je prikazano na sliki 2. Ob spojitvi ni bilo izgube zgodovine transakcij in uporabnikom ni bilo treba nadgraditi ali storiti česarkoli za nadaljnjo uporabo Ethereum platforme (Ethereum, 2023b).

Slika 2: Prestop z metode soglasja »dokaz o delu« na metodo soglasja »dokaz o deležu«



Prirejeno po Ethereum (2023).

Spojitev je bila uspešna in omogoča številne nadgradnje na razširljivosti omrežja v prihodnosti. Posledično se je zaradi spojitve ocenjena letna energetska uporaba Ethereum omrežja zmanjšala z 78 TWh na 0,0026 TWH oziroma za kar 99,988 % (Ethereum, 2023b).

2.2 Prihodnost pretočnosti omrežja Ethereum

Trenutno je največja hiba omrežja Ethereum število transakcij, ki jih lahko obdela v določenem času. V trenutni različici je omrežje omejeno na 15 transakcij na sekundo oziroma milijon transakcij na dan. Ta omejitev obstaja na ravni plasti 1 (angl. Layer 1). Plast 1 je del Ethereum omrežja, ki je sestavljen iz omrežnih vrstnikov, omrežja proizvajalcev blokov, verige blokov in njenih podatkov ter metode soglasja. Plast 1 torej predstavlja temelj Ethereum omrežja (Ethereum, 2023f).

Trenutna Plast 2 (angl. Layer 2) predstavlja delno rešitev prej omenjeni omejitvi in je sestavljena iz ločenih stranskih verig blokov (angl. sidechains). Te verige blokov transakcije hitreje in ceneje obdelajo, zapakirajo več sto transakcij v eno in zapakirane transakcijske podatke podajo Plasti 1. Zapakirane transakcije se imenujejo zvitki (angl. rollups). Vsi pomembni podatki o transakcijah so shranjeni na Plasti 1, ki ima mehanizme, s katerimi lahko transakcije preveri in izpodbija. Ta rešitev zviša najvišje število transakcij omrežja s 15 na 45 transakcij na sekundo (Ethereum.org, 2023f). Cena povprečne transakcije prek Plasti 2 je tako desetkrat cenejša kot prek Plasti 1.

Za prestop na cenejšo uporabo omrežja in večje število transakcij na sekundo pa se predvideva, da bo čez nekaj let prevladovala tehnologija »Danksharding« ter njen predhodnik »Proto-danksharding«, ki je predviden za izdajo konec leta 2023. Cilj teh tehnologij je omogočanje kombinirane uporabe zvitkov in binarnih velikih objektov (angl.

Binary Large Objects, v nadaljevanju BLOB). BLOB se uporablja za shranjevanje podatkov in je v rabi v tradicionalnih podatkovnih bazah (Ethereum, 2023g).

Ethereum bo uporabljal »Proto-danksharding«, da lahko doda en BLOB oziroma 0,5 MB podatkov na vsak nov blok. Podatki so začasni in obstajajo le za od enega do treh mesecev. Ethereum virtualno izvajalsko okolje (angl. Ethereum Virtual Machine, v nadaljevanju EVM) do teh podatkov ne dostopa in notranjosti BLOB-ov ne preverja. Ker 90 % cene, ki jo uporabniki trenutno plačajo za uporabo zvitkov, prihaja iz stroškov shranjevanja podatkov, bo ta sprememba te stroške znatno zmanjšala in znižala obremenjenost omrežja. Ethereum omrežje ostane odgovorno zgolj za preverjanje, potrjevanje in shranjevanje transakcij, podatkovne vsebine BLOB-ov pa mu ni treba obdelati in trajno shranjevati, za to so odgovorni deležniki na Plasti 2.

Cilj »Danksharding« je zvišanje število BLOB-ov na blok z 1 na 64. Ta nadgradnja teoretično zviša število transakcij na sekundo na 100.000 in več (Ethereum, 2023g).

2.3 Ethereum virtualno izvajalsko okolje

EVM je temelj Ethereum omrežja. Gre za virtualni računalnik, za katerega velja, da je splošni Turingov stroj (angl. Turing Complete) in se izvaja na vsakem vozlišču v Ethereum omrežju. Zasnovan je na tak način, da omogoča izdelavo blokov, obdelavo transakcij in izvajanje pametnih pogodb, prek katerih lahko programerji razvijajo decentralizirane aplikacije (Ethereum, 2023h).

Zmožnost interpretacije pametnih pogodb ponudi razvijalcem razne inovativne opcije. Mednje spadajo ustvarjanje lastnih nezamenljivih domenskih imen (angl. Non-Fungible Token Domains), podžetonov, nezamenljivih žetonov (angl. Non Fungible Tokens, v nadaljevanju NFT), decentraliziranih finančnih aplikacij (angl. Decentralized Finance applications - De-fi) in DAO-entitet (Hedera, brez datuma).

EVM podpira razne visokonivojske programske jezike, kot so Solidity, Vyper in Yul, ki jih razvijalci uporabljajo za ustvarjanje pametnih pogodb. Podana koda se ob uporabi prevede v nizkonivojsko bitno kodo (angl. Bytecode), ki jo lahko EVM izvede (Hedera, brez datuma).

EVM za izvajanje pametnih pogodb in transakcij zahteva gorivo (angl. gas), gorivo je enota, ki meri količino računskega napora, potrebnega za izvedbo določenih operacij na Ethereum omrežju. Vsaka Ethereum transakcija in pametna pogodba zahtevata računske vire za izvedbo, zato ima tudi vsaka svojo ceno v gorivu. Bolj kot je pametna pogodba in transakcija obsežna ali kompleksna, več goriva potrebuje (Ethereum, 2023h). Gorivo se plača z valuto ETH in meri v »gwei«. En gwei = 0,000000001 ETH.

Primer teoretične transakcije: Oseba A pošlje osebi B preprosto transakcijo, ta vsebuje 1 ETH. Iz enačbe (1) je razvidno kako se izračuna strošek preproste transakcije.

$$Cena\ transakcije = Zaželjena\ količina\ valute + količina\ plina \times (\ osnovni\ strošek + prednostni\ strošek) \quad (1)$$

ali:

$$1\ \text{ETH} + 21.000 \times (10\ \text{gwei} + 2\ \text{gwei}) = 1{,}000252\ \text{ETH}$$

Količina plina je odvisna od kompleksnosti izvedene transakcije ali pametne pogodbe. Osnovni strošek je spremenljiv in se samodejno izračuna glede na zasedenost omrežja v prejšnjih blokih. Prednostni strošek pa je neobvezen, z njim se da rudarjem pobuda, da transakciji dajo prednost in jo hitreje zapišejo v blok. V tem teoretičnem primeru bo oseba A za strošek transakcije plačala 0,000252 ETH in oseba B bo prejela 1 ETH.

2.3.1 Ethereum računi

Ethereum račun (angl. Ethereum account) je entiteta z ETH-bilanco, ki lahko pošilja transakcije na omrežju Ethereum. Račun lahko prejme, hrani ali pošlje ETH in komunicira s pametnimi pogodbami. Obstajata dve vrsti računa, EOA (angl. Externally-owned account, v nadaljevanju EOA) in pogodbeni račun (angl. contract account) (Ethereum, 2023c). EOA-račun lahko upravlja kdorkoli z izvirnem zasebnem ključem, primer EOA-računa je Ethereum račun katerega uporabniki lastijo in do njega dostopajo preko kriptodenarnice. Pogodbeni račun pa vsebuje pametno pogodbo s katero lahko kdorkoli komunicira, je živa koda ki obstaja na omrežju.

EOA-račun temelji na uporabi kriptografskega para ključev, zasebnega in javnega. Zasebni ključ je sestavljen iz 64 šestnajstiških znakov in se lahko šifrira z geslom. Uporablja se za ustvarjanje javnih ključev, za podpisovanje transakcij in kot geslo, s katerim prek kriptodenarnice (angl. Cryptowallet) dostopamo do Ethereum računa (Ethereum, 2023c).

Javni ključ se generira iz zasebnega ključa s pomočjo algoritma za digitalno podpisovanje (angl. Elliptic Curve Digital Signature Algorithm, v nadaljevanju ECDSA). ECDSA algoritem omogoči ustvarjanje javnega ključa iz zasebnega ključa, pri tem pa obraten postopek ni mogoč. Lastnik Ethereum računa lahko zaradi tega dokaže pristnost svojih transakcij s podpisom, ki je zapisan na poslani transakciji in ga je mogoče ustvariti le z zasebnim ključem istega Ethereum računa (Ethereum, 2023). Vsak Ethereum račun ima tudi svoj javni naslov, ki se uporablja kot javna identifikacija na Ethereum računu. Javni naslov nastane, ko se javni ključ ustavi v Keccak-256 zgoščevalno funkcijo in se pred zadnjih 40 znakov rezultata funkcije doda še »0x« (Geeksforgeeks, brez datuma, b).

2.4 Metoda soglasja

Metoda soglasja (angl. consensus mechanism) je skupek protokolov, pobud in idej, s pomočjo katerih omrežni vrstniki preverjajo in sinhronizirajo stanje na verigi blokov ter ga branijo pred napadalci. Metoda soglasja določa, kdo bo v omrežje dodal naslednji blok transakcij. Omrežje rudarje blokov (angl. miners) ali potrjevalce blokov (angl. validators) nagradi za njihovo delo, vendar morajo za to priložnost zastaviti določen lasten vir, npr. računsko moč, kriptovaluto, ugled, omrežno širino itd. Na tak način omrežje poskrbi, da se poizkusi prevare kaznujejo in delo nagradi. Različne metode soglasja dosežejo soglasje omrežja na različne načine in zahtevajo zastavitev različnih virov (Binance, 2018). Bitcoin na primer uporablja metodo soglasja »dokaz o delu«, enako je veljalo za Ethereum do prehoda na metodo soglasja »dokaz o deležu« v letu 2022 (Ethereum, 2023i).

Obstajajo še druge metode soglasja, ki se med seboj razlikujejo glede na obseg kompromisa na dostopnost omrežja, doslednosti podatkov, decentralizacije, hitrosti potrjevanja transakcij, energetske uporabe in drugih dejavnikov (Zhang & Lee, 2020).

2.4.1 Dokaz o delu

Pri metodi soglasja »dokaz o delu« (angl. Proof of Work) omrežje poda kriptografski račun, ki ga omrežni vrstniki z lastno računsko močjo poskusijo rešiti. Prvi omrežni vrstnik, ki ta kriptografski izziv uspešno reši, ima pravico zapisa naslednjega bloka transakcij v verigo blokov in je za to delo nagrajen. Omrežje težavnost kriptografskega računa čez čas spreminja glede na število dejavnih omrežnih vrstnikov in njihovo razpoložljivo računsko moč, ker želi omrežje v večini primerov obdržati enak pretečen čas med bloki. Verige blokov, ki uporabljajo metodo soglasja »dokaz o delu«, so energetsko drage, ker zahtevajo veliko računske moči (Zhang & Lee, 2020). Zaradi tega so velika omrežja relativno varna, saj mora napadalec imeti 51 % računske moči v omrežju, da lahko spremeni vsebino podatkov v zapisanih blokih (Frankenfield, 2023a). Ta metoda soglasja je preizkušena in je za vrsto let poskrbela za decentralizacijo in varnost Bitcoina in Ethereuma (Ethereum, 2023i).

2.4.2 Dokaz o deležu

Metoda soglasja »dokaz o deležu« (angl. Proof of Stake) uporablja potrjevalce blokov za preverjanje transakcij in dejavnosti, za glasovanje na odločitvah v omrežju in za vzdrževanje zapisov. Uporabnik postane potrjevalec, ko zastavi 32 ETH in vzdržuje Ethereum vozlišče (angl. Ethereum Node) oziroma ko se pridruži skupini potrjevalcev (angl. pool), ki skupno zastavi 32 ETH. Ethereum vozlišče je računalnik z omrežno povezavo, ki ima programsko opremo za potrjevanje blokov in shranjevanje stanja omrežja. Za zastavljen ETH so potrjevalci plačani v ETH. V primerjavi z metodo soglasja »dokaz o delu« metoda soglasja »dokaz o deležu« energetsko potratno rudarjenje zamenja z zastavljanjem ETH in zato porabi veliko manj energije in je bolj decentralizirana (Frankenfield, 2023b).

Do teoretično boljše decentralizacije omrežja pride, ker so omejitve za vstop manjše, saj potrjevalcem blokov ni treba vložiti veliko v opremo za rudarjenje in plačevati večjih stroškov elektrike. Posledično je večjih lastnikov manj in je omrežje tako bolj razpršeno. Kljub temu pa samo zato, ker vozlišča omrežja obstajajo na več lokacijah po svetu, še ne pomeni, da je omrežje popolnoma decentralizirano. Nevarnost še zmeraj obstaja v obliki »plutokracije,« kjer majhno število posameznikov drži veliko število kovancev in z njimi vpliva na odločitve v skupnosti (Bunin, 2019).

51 % napad je težje izveden, saj mora napadalec držati 51 % vseh zastavljenih žetonov, ob čemer tvega izgubo celotne vrednosti v žetonih, saj se lahko ob napadu drugi udeleženci odločijo odcepiti omrežje in starega zapustiti. Največja hiba metode soglasja »dokaz o deležu« leži v nepreizkušenosti tehnologije, zaradi česar obstaja nevarnost zlorabe še nepoznanih ranljivosti v kodi (Bunin, 2019).

Po mnogih zamikih se je Ethereum uspešno premaknil na metodo soglasja »dokaz o deležu« 15. septembra 2022 po dogodku »The Merge«. Za uporabnike premik sicer ni bil občuten, malenkostno pohitrila se je hitrost transakcij, stroški transakcij pa so ostali skoraj enaki. Največja takojšnja razlika je bila zmanjšanje električne porabe omrežja za ~99,95 % in postavitev pomembnih temeljev za prihodnje nadgradnje omrežja (Kessler, 2023).

2.5 Pametne pogodbe

Pametne pogodbe (angl. smart contracts) so računalniški programi, ki delujejo na tehnologiji veriženja blokov. So skupek funkcij in podatkov ter samodejno izvedejo lastno kodo, ko so izpolnjeni pogoji pogodbe. Obstajajo v obliki Ethereum računa in z njimi lahko drugi uporabniki, pametne pogodbe ali aplikacije komunicirajo s transakcijami (Ethereum, 2022a). Kdorkoli lahko ustvari pametno pogodbo in ko je ta implementirana v omrežje, njena osnovna logika ni več spremenljiva.

Obstajajo tudi nadgradljive pametne pogodbe (angl. Upgradeable Smart Contract), ki so razdeljene na dva dela. V prvem delu sta shranjena stanje in naslov drugega dela pogodbe, v drugem delu pa je shranjena glavna koda pametne pogodbe. Razvijalec lahko poljubno spremeni naslov do drugega dela pogodbe in tako spremeni osnovne funkcije pametne pogodbe. To lahko stori, ker lahko naslovi drugo pametno pogodbo, ki vsebuje drugačno kodo (Quicknode, 2023).

Pomembne lastnosti pametnih pogodb so (Ethereum, 2022a):

– Samodejno izvajanje: To je ena od največjih koristi v primerjavi s klasičnimi pogodbami. Pogodba se samodejno izvede takoj, ko so izpolnjeni pogoji pogodbe, kar odstrani potrebo po zaupanju, da bo pogodba izvedena ob izpolnjenih pogojih.

– Javni zapis: Ker so pametne pogodbe javno dostopne na Ethereum omrežju, lahko vsakdo sledi prenosom sredstev in dogajanju v povezavi s pametno pogodbo. To omogoča revizijo in sledenje transakcij.
– Predvidljivi izidi: Pametne pogodbe se izvedejo, ko se izpolnijo točni pogoji, kar odstrani možnost različnih tolmačenj pogojev v pogodbi. Ta natančnost pomeni, da bo pametna pogodba v enakih okoliščinah vedno podala enak rezultat.
– Zaščita zasebnosti: Zasebnost uporabnika je varovana zato, ker je Ethereum psevdonimno omrežje. Transakcije so javno povezane s kriptografskim naslovom in ne z identiteto uporabnika.
– Vidni pogoji: Javna preglednost pogojev omogoča, da jih lahko uporabnik pregleda, preden sprejme pametno pogodbo.

2.6 Decentralizirane aplikacije

Decentralizirane aplikacije (angl. Decentralized applications, v nadaljevanju DApps) so aplikacije, ki povežejo uporabniški vmesnik s tehnologijo veriženja blokov prek pametnih pogodb (Coin telegraph, brez datuma). Glavne lastnosti decentraliziranih aplikacij so (Ethereum, 2023j):

– Decentralizacija: Decentralizirane aplikacije obstajajo na Ethereum omrežju, to je odprto javno omrežje, nad katerim noben posameznik ali skupina nima nadzora.
– Determinističnost: DApps zmeraj opravijo enako funkcijo ne glede na okoliščine, v katerih so izvedene.
– Splošni Turingov stroj: DApps lahko izvedejo katerokoli funkcijo glede na dane vire.
– Izolacija virtualnega okolja: DApps so izvedene v svojem virtualnem izvajalskem okolju, napake v kodi torej ne vplivajo na celotno omrežje.

Prednosti decentraliziranih aplikacij so številne ter imajo manj prekinitev in boljšo kontinuiteto omrežja, ker niso odvisne od enega strežnika ali enega ponudnika oblačnih virov. Prav tako so tudi bolj varne proti napadom, ker nimajo centralne strukture. Koda je odprtokodna in vidna vsem. Tudi cena lansiranja DApp je manjša, saj ne potrebuje lastnih strežnikov in kompleksne namestitve ter vzdrževanja strežnikov (Geeks for geeks, brez datuma, c).

Slabosti DApps pa so v trenutni počasnosti omrežja, saj je pretočnost omrežja veliko nižja v primerjavi s tradicionalnimi podatkovnimi bazami, hkrati pa je cena shranjevanja podatkov veliko višja v primerjavi s tradicionalnimi rešitvami. Vzdrževanje DAppa je tudi težje, ker mora razvijalec v veliko primerih ustvariti novo pametno pogodbo za vsako spremembo in popravek (Geeks for geeks, brez datuma, c).

Uporabniška izkušnja je v veliko primerih slabša, ker je pridobitev dostopa do DAppa bolj zapletena zaradi počasnih in nedodelanih vmesnikov. Te težave upočasnijo prihod novih

uporabnikov. Začasna ali delna rešitev obstaja v uporabi centraliziranih aplikacij kot uporabniški vmesnik (Geeks for geeks, brez datuma, c).

2.7 ERC-standard za podžetone

Ethereum prek pametnih pogodb omogoča ustvarjanje, uporabo in shranjevanje podžetonov na svojem omrežju. Razvijalci lahko pri ustvarjanju spremenijo lastnosti podžetona po svojih željah, a se morajo ob tem držati predlog in nekaterih pravil (Musharaff, 2021). Te predloge in pravila za ustvarjanje pametne pogodbe obstajajo v obliki ERC-standardov (angl. Ethereum Request for Comments, ERC), ki so uradno ustvarjeni prek procesa EIP. EIP spletna stran eips.ethereum.org/erc vsebuje seznam potrjenih ERC-standardov za podžetone in pametne pogodbe. Kdorkoli lahko ustvari svoj EIP in ga predlaga, prek neuradne diskusije pa se deležniki odločijo, ali naj predlagani EIP odobrijo ali zavrnejo (Becze & Jameson, 2015).

Obstaja več kot 300 sprejetih ERC-standardov. Trije glavni najbolj uporabljeni standardi so ERC-20, ERC-721 in ERC-1155 (Crypto, 2022). ERC-standardi večinoma podpirajo le osnovne lastnosti pri ustvarjanju in upravljanju podžetonov, razvijalec pa mora ustvariti ali uporabiti obstoječe pametne pogodbe, da podžetonu naknadno omogoči posebne funkcionalnosti v decentralizirani aplikaciji ali da jih razdeli deležnikom.

2.7.1 ERC-20

Trenutno je glavni model za ustvarjanje zamenljivih podžetonov (angl. fungible tokens) standard ERC-20. Zamenljivost podžetona pomeni, da je vsak podžeton enakovreden in neločljiv od drugega podžetona. Primerna analogija za to je denar – denarna vrednost petih evrov je pet evrov in na to oblika ne vpliva. Denarna vrednost ostane enaka, če je teh pet evrov v kovancih, gotovini ali na bilanci stanja v banki. ETH je prav tako zamenljiva valuta (Reiff, 2023).

2.7.2 ERC-721

Za NFT-je se veliko uporablja standard ERC-721. Za NFT-je velja, da je vsak žeton edinstven in nezamenljiv. Pogosto se uporabljajo za digitalno lastništvo zbirateljskih predmetov, digitalnih umetnosti, vstopnic, domenskih imen, predmetov v videoigrah ter kot evidenca lastništva fizičnih sredstev (Crypto, 2022). NFT-ji so postali sporna tema v javnosti, ker so neregulirani, pogosta tarča prevar in kraje intelektualne lastnine ter zaradi nepredvidljive spremenljivosti njihove cene (Singh, 2023).

Shranjevanje podatkov je na tehnologiji veriženja blokov relativno drago, zato NFT-ji redko vsebujejo medije, temveč vsebujejo le metapodatek oziroma povezavo do medija, ki je običajno gostovan na centraliziranem spletnem viru, kot npr. OneDrive, Google Drive,

Youtube itd. (Moreland, 2022). Če se bo v prihodnosti shranjevanje podatkov na Ethereum omrežju pocenilo, lahko pričakujemo, da bodo NFT-ji v celoti gostovani na verigi blokov.

2.7.3 ERC-1155

ERC-1155 je novejši standard, ki omogoča sočasno rabo različnih vrst žetonov. Razvijalcem omogoči, da v eno pametno pogodbo vključijo več vrst žetonov, kar posledično zniža kompleksnost in stroške pri projektih, ki uporabljajo več vrst žetonov. Standard ERC-1155 združi večino zmožnosti standardov ERC-20 in ERC-721 in doda nove lastnosti, kot so možnost več operacij ter sočasen prenos različnih žetonov v eni transakciji (Openzepellin, brez datuma).

2.8 Programski jezik Solidity

Solidity je objektno orientiran programski jezik za načrtovanje in programiranje pametnih pogodb na omrežjih, ki uporabljajo tehnologijo veriženja blokov. Glavni vplivi na programski jezik prihajajo iz JavaScripta in C++. Solidity uporablja spremenljivke, funkcije, razrede, aritmetične operacije, manipulacijo z nizi, knjižnice in številne druge zasnove. Podpira podatkovne tipe, ki so pogosto najdeni v objektno orientiranem programiranju kot npr. Booleanova spremenljivka, cela števila, znaki, nizi itd. (Simplilearn, 2023).

Programski jezik so ustvarili Gavin Wood in drugi razvijalci iz Ethereum Foundationa in je glavni programski jezik v uporabi za Ethereum (Simplilearn, 2023). Ethereum platforma podpira še druge programske jezike, specializirane za pametne pogodbe, kot na primer Yul in Vyper, in tudi bolj tradicionalno uporabljene programske jezike, na primer Java, JavaScript, Python itd. (Ethereum, 2022b).

Razvijalec lastno kodo razvije in preizkusi v raznih testnih okoljih, kot sta Truffle in Remix IDE. Obstaja tudi možnost preizkusa kode na javnih Ethereum testnih omrežjih Sepolia in Goerli. Pomembno je, da je vsaka pametna pogodba pregledana in testirana za napake in ranljivosti, enako velja tudi za povezave med njimi (Roan, 2020).

3 USTVARJANJE ERC-20 ŽETONA

V tem poglavju je predstavljen postopek ustvarjanja Ethereum podžetona standarda ERC-20. Opisana so uporabljena orodja in viri, ustvarjanje pametne pogodbe, preizkus in lansiranje pogodbe na Ethereum testnem omrežju. Povezave do vseh storjenih transakcij na testnem omrežju so dodane v prilogi.

3.1 OpenZeppelin

OpenZeppelin je odprtokodna platforma za gradnjo decentraliziranih aplikacij, ki ponuja tudi varnostne preglede kode in ima zgodovino pomembnih strank, kot so Ethereum Foundation in Coinbase. OpenZeppelinove knjižnice vsebujejo modularne in ponovno uporabljive pametne pogodbe, ustvarjene v programskem jeziku Solidity (Moralis, 2021). Uporabil bom njihovo predlogo za žeton ERC-20.

3.2 REMIX IDE

REMIX IDE je orodje za razvoj pametnih pogodb, ki podpira Solidity in Yul programske jezike. Obstaja v spletni obliki in kot namizna aplikacija (REMIX IDE, brez datuma). Prek tega orodja bom prilagodil, testiral in lansiral OpenZeppelinove predloge za podžetone.

3.3 MetaMask

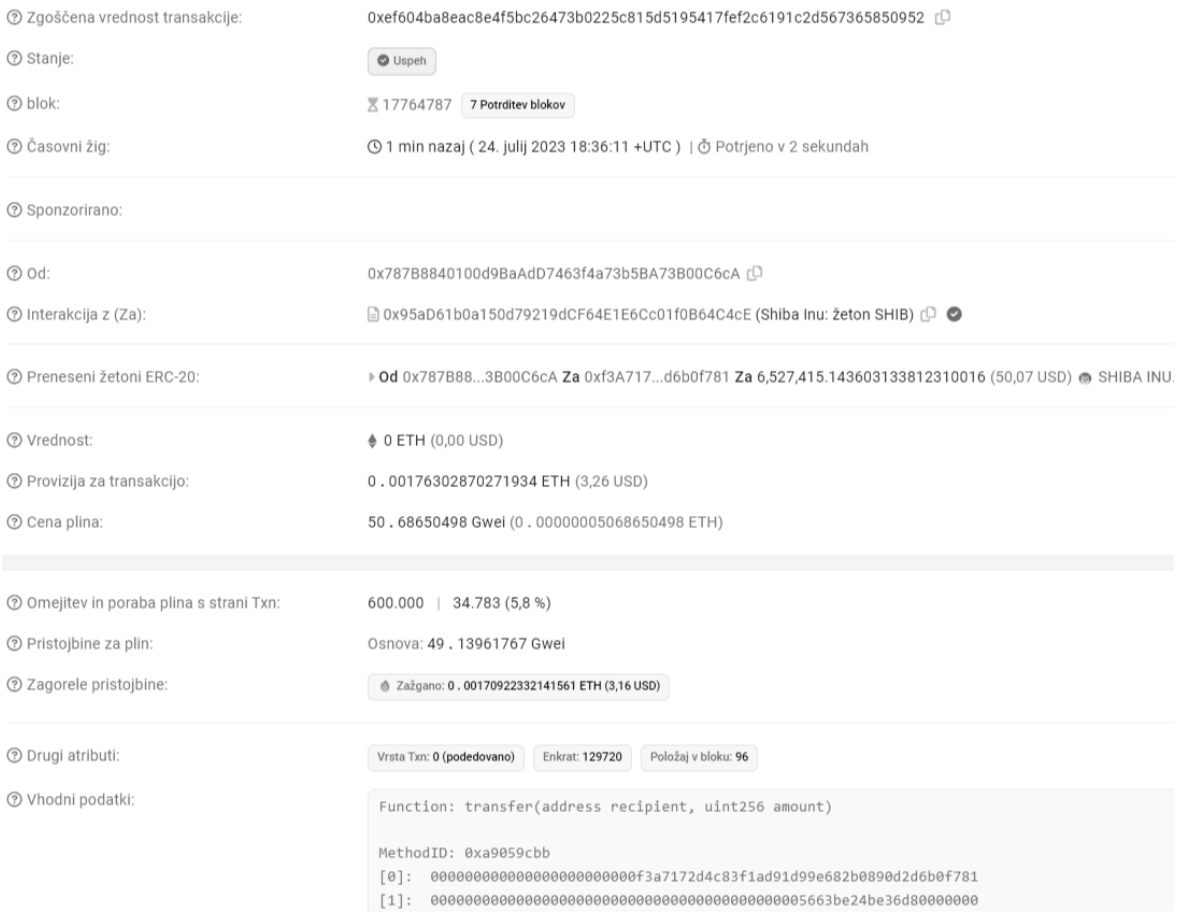
MetaMask je kriptodenarnica, dostopna kot razširitev brskalnika ali kot mobilna aplikacija. Podpira Ethereum omrežje in Ethereum podžetone ter druga omrežja, ki so združljiva z EVM, kot na primer Binance Smart Chain. Deluje kot vmesnik med uporabnikom in verigo blokov. MetaMask zasebnih ključev ne shranjuje na omrežju, ampak lokalno na uporabnikovi napravi, ki jih zaščiti z lokalnim geslom. Za dodatno varnost podpira tudi uporabo fizičnih denarnic za kriptovalute (Metamask, brez datuma).

3.4 Etherscan.io

Etherscan.io je neodvisen brskalnik verige blokov za Ethereum omrežje, ki uporabnikom omogoča pregled nad stanjem in preteklimi dogodki v omrežju. Omogoča pregled nad preteklimi in trenutnimi transakcijami, stanjem na Ethereum računih, pogled v pametne pogodbe ter izračun transakcijskih stroškov (Puggioni, 2022). Brskalnik verige blokov bom uporabil za pregled nad lastnimi podžetoni in transakcijami.

Na sliki 3 je prikazan primer pregleda transakcije na Etherscan.io. Glava vsebuje transakcijski identifikator (angl. Transaction Hash), stanje transakcije, številko bloka, v katerem je transakcija shranjena, ter kdaj se je transakcija zgodila. V naslednjem predelu je vidno, s katerega Ethereum računa je bila transakcija poslana in kam. V primeru, da uporabnik ne pošlje ethra, ampak podžeton, mora biti naslovljen račun tisti, ki vsebuje pametno pogodbo podžetona, to pa zato, ker moramo komunicirati s pametno pogodbo, da lahko upravljamo s podžetoni. Transakcija v predelu »Input Data« vsebuje podatke o naslovnem računu ter želeno vsoto podžetonov. Te podatke pametna pogodba prek transakcije sprejme in jih interpretira ter izvrši. Poleg predela »Input Data« je v drugi polovici slike razviden strošek transakcije. Etherscan tudi omogoči možnost pregleda kode pametnih pogodb

Slika 3: Pregled transakcije na spletni strani Etherscan.io



Vir: Etherscan (2023).

3.5 Ustvarjanje pametne pogodbe

V tem podpoglavju je opisan postopek ustvarjanja podžetona. Med prilogami (glej priloge) so navedene transakcije in slike postopkov ustvarjanja pametne pogodbe. Pametno pogodbo najprej preizkusim lokalno v virtualnem okolju s spletnem orodju REMIX IDE, za tem jo prek istega orodja lansiram in preizkusim na Sepolia testnem omrežju. Funkcije, ki jih podpira standard ERC20 in jih tudi preizkusim, so:

– totalSupply(). Vrne skupno zalogo ERC-20 podžetona;
– balanceOf(račun). Uporablja se za pridobitev stanja podžetona v izbrani Ethereum denarnici;
– transfer(naslovni račun, vsota žetonov). Omogoča prenos podžetonov med Ethereum računi;
– transferFrom(naslov računa pošiljatelja, naslovni račun, vsota žetonov). Podobna funkciji »Transfer«, pametni pogodbi omogoča prenos podžetonov v imenu uporabnika;

– Approve(naslov računa pošiljatelja, naslovni račun, vsota žetonov) (angl. Approve) & Dovoljenje (račun s podžetoni, račun porabnik) (angl. Allowance). Prva funkcija Ethereum računu dovoli omejen dovoljen dvig podžetonov, druga pa preveri, koliko podžetonov lahko premakne;
– Name(). Vrne ime podžetona (npr. MidCoin);
– Symbol(). Vrne kratico za ime podžetona (npr. MCOIN);
– Decimals(). Vrne podprto število »decimalk« podžetona.

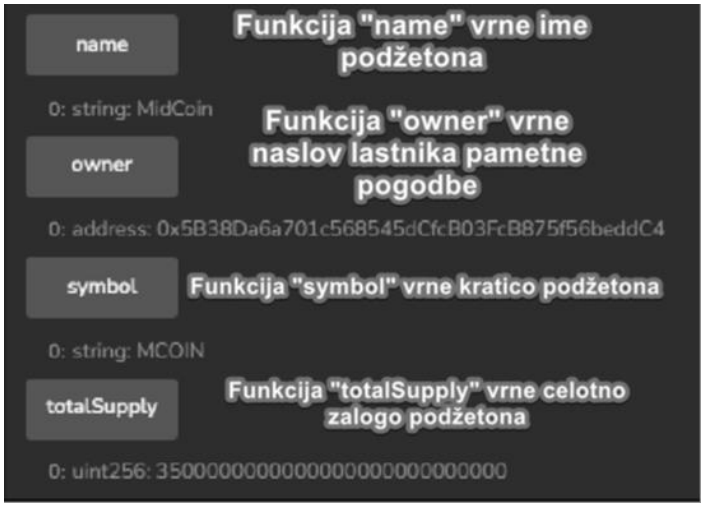
EVM uporablja cela števila (angl. integers) in ne podpira decimalnih števil. Nadomesti jih z uporabo spremenljive lastnosti »decimals«, ki doda določeno število podprtih celih številk na konec vseh številk (glej sliko 4 pod funkcijo »totalSupply«). V tem primeru je lastnost »decimals« na privzeti nastavitvi in doda 18 številk.

Za ustvarjanje pametne pogodbe uporabim OpenZeppelinovo predlogo, v njej spremenim osnovne lastnosti:

– Ime žetona: MidCoin.
– Kratica: MCOIN.
– Začetno število podžetonov: 350000000.
– Omogočeno ustvarjanje novih podžetonov (angl. Minting) in uničevanje obstoječih žetonov (angl. Token burning).

Pametno pogodbo nato uporabim v orodju REMIX IDE, kjer kodo preverim s kompilatorjem za programski jezik Solidity. Osnovne funkcionalnosti nato preizkusim na lokalnem virtualnem okolju, ki omogoči emulacijo testnega omrežja Shanghai. V tem virtualnem okolju preizkusim vse funkcije standarda ERC-20, nekaj jih je razvidnih na sliki 4. V prilogah 3 in 4 so slike, ki prikazujejo prenos podžetonov med dvema računoma in uporabo funkcije »balanceOf« za preverjanje stanja na računu.

Slika 4: Preizkus osnovnih ERC20-funkcij v lokalnem testnem okolju

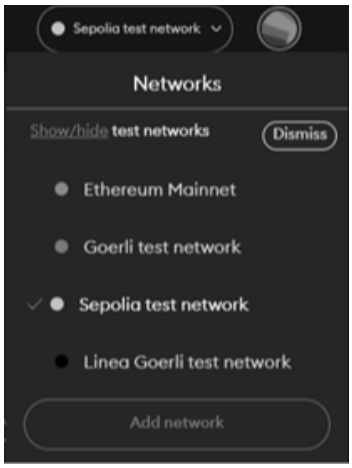


Vir: lastno delo.

3.6 Lansiranje pogodbe na testno omrežje Sepolia

Prek kriptodenarnice MetaMask ustvarim nov Ethereum račun in preklopim z glavnega omrežja na testno omrežje Sepolia, kot je razvidno na sliki 5. Prek spletne strani sepoliafaucet pridobim na lastni račun 0,5 Sepolia ETH, ki mi omogoči, da lansiram in preizkusim pametno pogodbo na testnem omrežju.

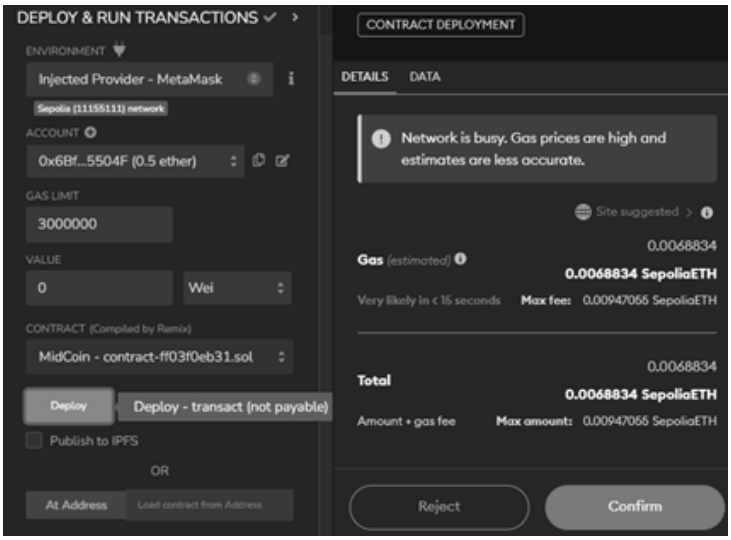
Slika 5: Prehod z glavnega omrežja na testno omrežje Sepolia



Vir: lastno delo.

V REMIX IDE izberem MetaMask kot ciljno okolje za zagon kode in pametno pogodbo, ki sem jo do sedaj uporabljal na lokalnem virtualnem okolju, ter jo preizkusim, kot je razvidno na levem delu slike 6. MetaMask kriptodenarnica me vpraša za potrdilo plačila transakcije, ki bo pametno pogodbo lansirala na testno omrežje, kot je razvidno na desni strani slike 6. Transakcijo potrdim.

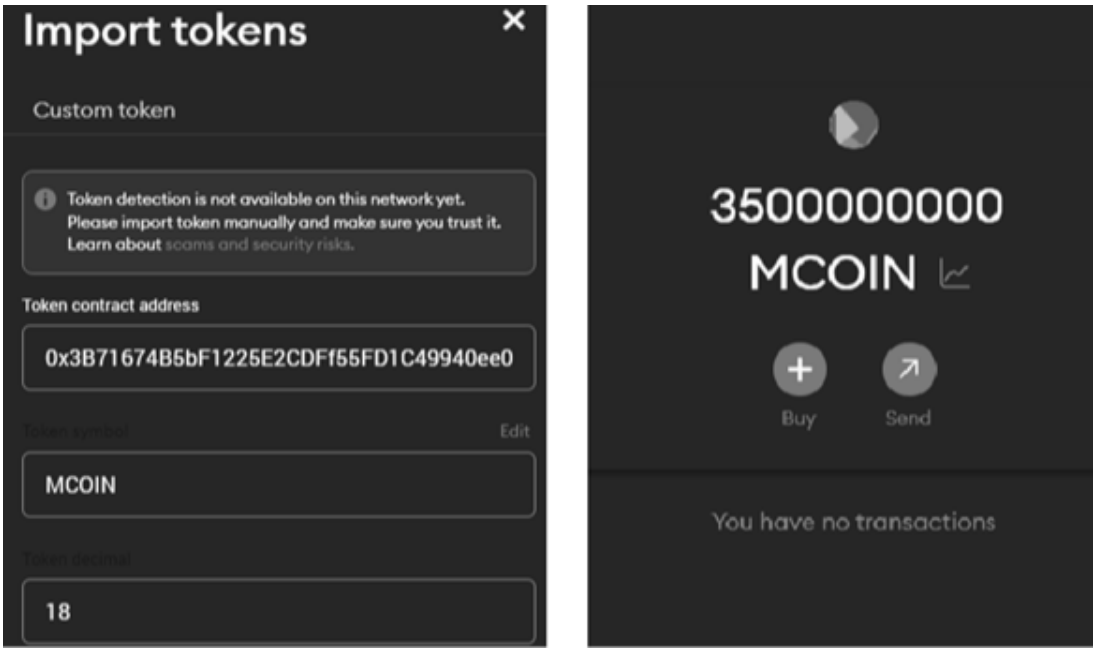
Slika 6: Lansiranje pametne pogodbe



Vir: lastno delo.

Podžeton MidCoin je uspešno lansiram na testnem omrežju Sepolia in postane viden na spletni strani sepolia etherscan. Celotna zaloga podžetonov je bila ustvarjena in dana na Ethereum račun, s katerim sem ustvaril pametno pogodbo. Da jih lahko vidim in z njimi upravljam s kriptodenarnico MetaMask, moram ročno uvoziti naslov računa, ki vsebuje pametno pogodbo podžetona, kot je razvidno v levem delu slike 7. Na desnem delu slike 7 je vidno stanje podžetonov na računu po uvozu nastavitev.

Slika 7: Uvoz nastavitev podžetona in stanje na računu



Vir: lastno delo.

Podžeton nato pošljem med dvema Ethereum računoma in preizkusim še funkcijo »Mint«, s katero ustvarim nove žetone. Da bi lansiral podžeton na glavno omrežje, bi moral skozi identičen postopek, s to razliko, da bi izbral glavno omrežje kot ciljno okolje. Pomembno je poudariti, da je uporaba testnega omrežja Sepolia brezplačna, lansiranje in preizkus pametne pogodbe na glavnem omrežju pa zahteva plačilo ethra.

SKLEP

Tehnologija veriženja blokov predstavlja nov decentraliziran in pregleden način shranjevanja in prenosa digitalnega lastništva in podatkov ter omogoči takojšen prenos plačil po vsem svetu brez dragih posrednikov. To naj bi predstavljalo osnovno idejo, na kateri je ta relativno mlada tehnologija nastala. A vendarle je realnost nekoliko drugačna. Tehnologija ni več tako mlada in implementacija v resnični svet ni tako preprosta, kot so si mnogi zamislili. Koda je lahko pogojna in objektivna, a človek, ki jo je napisal, ni. Kljub temu ima uporaba tehnologije veriženja blokov ob bolj zmernih pričakovanjih prihodnost in potencialno koristne primere uporabe.

Omrežje Ethereum, ki je v osredju moje zaključne strokovne naloge, je premagalo eno glavnih stigem tehnologije veriženja blokov, energetsko potratnost. Prehod na metodo soglasja »dokaz o deležu« je energetsko potrošnjo omrežja v primerjavi s prej praktično izničil. Uspeh tega je dal drugim verigam blokov pobudo, da se premaknejo na bolj energetsko učinkovite metode soglasja. Skupnost, ki obkroža Ethereum, je zelo dejavna in proaktivna v iskanju tehnoloških napredkov in menim, da ima platforma pred sabo še zanimivo prihodnost, ne glede na nihanje kriptotrga.

Med delom na nalogi sem raziskal in razumel veliko novih podrobnosti o omrežju Ethereum in dosegel zadane cilje ter spoznanja, med katere spadajo predstavitev in podrobnejše razumevanje lastnosti, dejstev, zgodovine ter tehnične podlage omrežja Ethereum in ustvarjanje lastnega žetona ERC-20. Ta izkušnja je bila pozitivna, vsa potrebna literatura in orodja so odlično pripravljena in dostopna, dostop do kakovostnih informacij pa je postal veliko lažji in tehnologija veriženja blokov prehaja iz obdobja nepredvidljive variabilnosti v obdobje zrelosti.

Učni viri, predloge, skupnost ter programska oprema za programiranje pametnih pogodb so vsi relativno lahko dostopni in prijazni do novih razvijalcev. Posledično sem tudi sam ustvaril in preizkusil lasten podžeton brez večjih zapletov in stroškov. Podobni viri informacij in programskih knjižnic ter predlog so dostopni tudi za bolj zapletene funkcije in druge ERC-standarde.

LITERATURA IN VIRI

1. Ali, O., Jaradat, A., Kulakli, A. & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access*, *9*, 12730–12749.
2. Becze, M. & Jameson, H. (2015). *EIP-1: EIP Purpose and Guidelines*. Pridobljeno 9. junija 2023 iz https://eips.ethereum.org/EIPS/eip-1#what-is-an-eip
3. Belotti, M., Božić, N., Pujolle, G. & Secci, S. (2019). A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys & Tutorials, 21*(4), 3796–3838.
4. Binance academy. (2018). *What is a Blockchain Consensus Algorithm?* Pridobljeno 30. maja 2023 iz https://academy.binance.com/en/articles/what-is-a-blockchain-consensus-algorithm
5. Budhi, V. (2022). *Advantages and Disadvantages of Blockchain Technology.* Pridobljeno 24. junija 2023 iz https://www.forbes.com/sites/forbestechcouncil/2022/10/20/advantages-and-disadvantages-of-blockchain-technology/?sh=78314d2e3453
6. Bunin, V. (2019). *Proof of Stake's security model is being dramatically misunderstood.* Pridobljeno 7. junija 2023 iz https://viktorbunin.medium.com/proof-of-stakes-security-model-is-being-dramatically-misunderstood-4ed7b19ca419

7. Coin telegraph. (brez datuma). *What are DApps? Everything there is to know about decentralized applications.* Pridobljeno 9. junija 2023 iz https://cointelegraph.com/learn/what-are-dapps-everything-there-is-to-know-about-decentralized-applications
8. Crypto.com. (2022). *What Are Token Standards? An Overview*. Pridobljeno 9. junija 2023 iz https://crypto.com/university/what-are-token-standards
9. Dowlat, D. (2018). *Cryptoasset market coverage initiation: Network creation.* Pridobljeno 16. maja 2023 pridobljeno iz https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ
10. Ethereum. (2022a). *Introduction to smart contracts.* Pridobljeno 26. oktobra 2022 iz https://ethereum.org/en/developers/docs/smart-contracts/
11. Ethereum. (2022b). *Programming languages.* Pridobljeno 13. junija 2023 iz https://ethereum.org/en/developers/docs/programming-languages/
12. Ethereum. (2023a). *What is ethereum*. Pridobljeno 16. maja 2023 iz https://ethereum.org/en/what-is-ethereum/
13. Ethereum. (2023b). *Spojitev*. Pridobljeno 16. maja 2023 iz https://ethereum.org/sl/roadmap/merge/
14. Ethereum. (2023c). *Ethereum accounts*. Pridobljeno 30. maja 2023 iz https://ethereum.org/en/developers/docs/accounts/
15. Ethereum. (2023d). *Introduction to Ethereum Improvement Proposals (EIPs)*. Pridobljeno 30. maja 2023 iz https://ethereum.org/en/eips/
16. Ethereum. (2023e). *Mission and vision*. Pridobljeno 30. maja 2023 iz https://ethereum.org/en/contributing/translation-program/mission-and-vision/
17. Ethereum. (2023f). *Ethereum for everyone.* Pridobljeno 16. maja 2023 iz https://ethereum.org/en/layer-2/
18. Ethereum. (2023g). *Danksharding*. Pridobljeno 16. maja 2023 iz https://ethereum.org/en/roadmap/danksharding/
19. Ethereum. (2023h). *Ethereum Virtual Machine (EVM)*. Pridobljeno 16. maja 2023 iz https://ethereum.org/en/developers/docs/evm/
20. Ethereum. (2023i). *Consensus mechanisms*. Pridobljeno 19. maja 2023 iz https://ethereum.org/en/developers/docs/consensus-mechanisms/
21. Ethereum. (2023j). *Ethereum-powered tools and services.* Pridobljeno 9. maja 2023 iz https://ethereum.org/en/dapps/
22. Frank, J. & Silverstein, S. (2021). *Ethereum co-founder Vitalik Buterin on how he created one of the world's largest cryptocurrencies in his early twenties*. Pridobljeno 29. aprila 2023 iz https://www.businessinsider.com/vitalik-buterin-created-ethereum-one-of-the-worlds-three-largest-cryptocurrencies-2019-1
23. Frankenfield, J. (2023a). *51% Attack: Definition, Who Is At Risk, Example, and Cost.* Pridobljeno 30. maja 2023 iz https://www.investopedia.com/terms/1/51-attack.asp
24. Frankenfield, J. (2023b). *What Does Proof-of-Stake (PoS) Mean in Crypto?* Pridobljeno 7. junija 2023 iz https://www.investopedia.com/terms/p/proof-stake-pos.asp
25. Geeks for geeks. (brez datuma, a). *Types of Blockchain.* Pridobljeno 13. oktobra 2022 https://www.geeksforgeeks.org/types-of-blockchain/

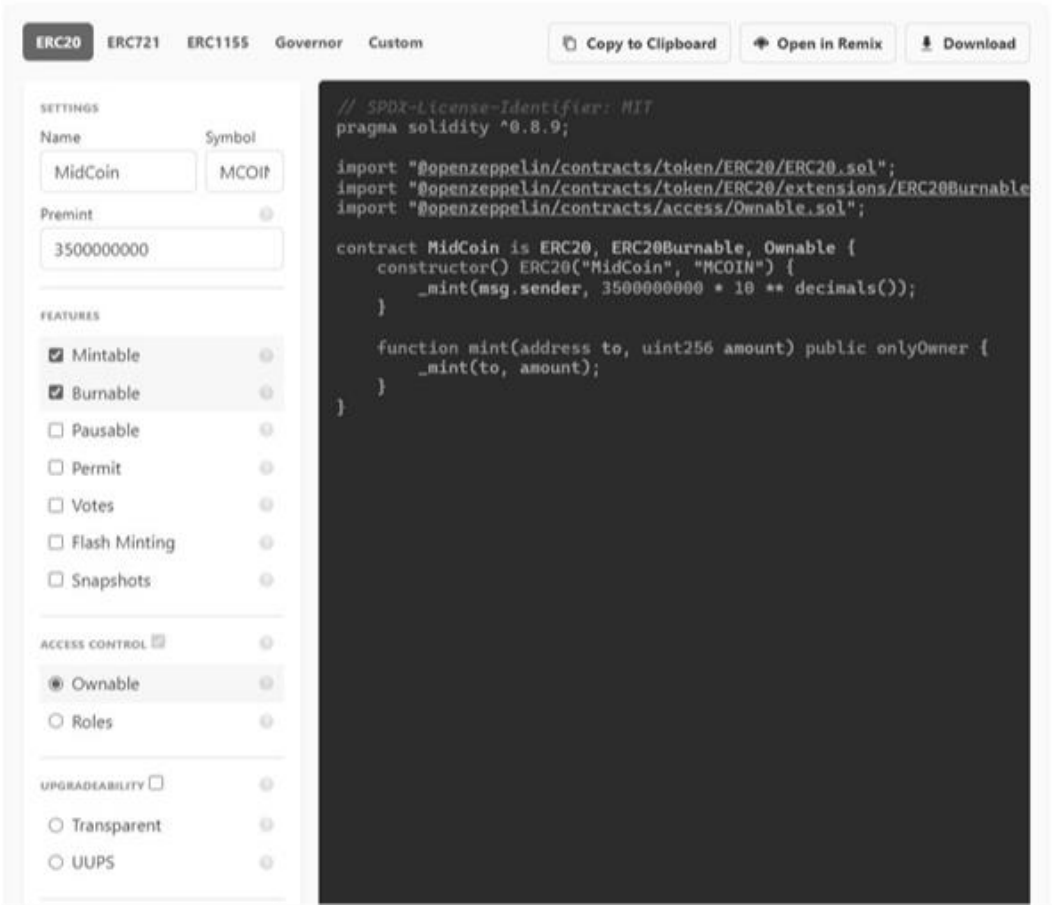
26. Geeks for geeks. (brez datuma, b). *Difference Between SHA-256 and Keccak-256.* Pridobljeno 30. maja 2023 iz https://www.geeksforgeeks.org/difference-between-sha-256-and-keccak-256/
27. Geeks for geeks. (brez datuma, c). *Pros, Cons, and Examples of Dapp*. Pridobljeno 9. junija 2023 iz https://www.geeksforgeeks.org/pros-cons-and-examples-of-dapp/
28. Hayes, A. (2023). *Blockchain Facts: What Is It, How It Works, and How it Can Be Used.* Pridobljeno 24. junija 2023 pridobljeno iz https://www.investopedia.com/terms/b/blockchain.asp
29. Hedera. (brez datuma). *What is the Ethereum Virtual Machine & How Does it Work?* Pridobljeno 29. maja 2023 iz https://hedera.com/learning/smart-contracts/ethereum-virtual-machine
30. Duro, K. (2017). *Top Applications Based on Ethereum Network* Pridobljeno 9. junija 2023 iz https://imperiumapps.com/top-applications-based-ethereum-network/
31. Kessler, S. (2023). *Ethereum Merge Explained: What Investors Should Know About the Shift to Proof-of-Stake*. Pridobljeno 9. junija 2023 iz https://www.coindesk.com/learn/ethereum-merge-explained-what-investors-should-know-about-the-shift-to-proof-of-stake/
32. Marco Polo network. (2018). *Difference Blockchain and DLT*. Pridobljeno 13. oktobra 2022 iz https://marcopolonetwork.com/distributed-ledger-technology/
33. Metamask. (brez datuma). *The Web3 101 course*. Pridobljeno 2. maja 2023 iz https://learn.metamask.io/overview
34. Moralis. (2021). *What is OpenZeppelin? The Ultimate Guide.* Pridobljeno 21. junija 2023 iz https://moralis.io/what-is-openzeppelin-the-ultimate-guide/
35. Moreland, K. (2022). *NFT Metadata: What and Where is it?* Pridobljeno 9. junija 2023 iz https://www.ledger.com/academy/wheres-your-nft-image-not-on-the-blockchain
36. Musharraff, M. (2021). *What are ERC Tokens and Why Do We Use Them?* Pridobljeno 9. junija 2023 iz https://www.ledger.com/academy/what-are-erc-tokens-and-why-do-we-use-them
37. OpenZeppelin. (brez datuma). *ERC1155*. Pridobljeno 13. junija 2023 iz https://docs.openzeppelin.com/contracts/3.x/erc1155
38. Puggioni, V. (2022). *What is Etherscan, and how does it work?* Pridobljeno 22. junija 2023 iz https://cointelegraph.com/news/what-is-etherscan-and-how-does-it-work
39. Quicknode. (2023). *An Introduction to Upgradeable Smart Contracts.* Pridobljeno 7. junija 2023 iz https://www.quicknode.com/guides/ethereum-development/smart-contracts/an-introduction-to-upgradeable-smart-contracts
40. Reiff, N. (2023). *What Are ERC-20 Tokens on the Ethereum Network?* Pridobljeno 26. oktobra 2022 iz https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/
41. Remix-IDE. (brez datuma). *Welcome to Remix's documentation!* Pridobljeno 21. junija 2023 iz https://remix-ide.readthedocs.io/en/latest/
42. Roan, A. (2020). *How to Test Ethereum Smart Contracts.* Pridobljeno 13. junija 2023 iz https://betterprogramming.pub/how-to-test-ethereum-smart-contracts-35abc8fa199d

43. Russo, C. (2020). *Sale of the Century: The Inside Story of Ethereum's 2014 Premine*. Pridobljeno 29. aprila 2023 iz https://www.coindesk.com/markets/2020/07/11/sale-of-the-century-the-inside-story-of-ethereums-2014-premine/
44. Simplilearn. (2023). *What is Solidity Programming: Data Types, Smart Contracts, and EVM?* Pridobljeno 13. junija 2023 iz https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-solidity-programming
45. Singh, S. (2023). *Why Do People Hate NFTs? Full List of Reasons.* Pridobljeno 11. junija 2023 iz https://moneymint.com/why-do-people-hate-nfts/
46. Soliditylang. (brez datuma). *Solidity*. Pridobljeno 24. oktobra 2022 iz https://docs.soliditylang.org/en/v0.8.17/
47. Tasatanattakool, P. & Techapanupreeda, C. (2018, January). Blockchain: Challenges and applications. V *2018 International Conference on Information Networking (ICOIN)* (str. 473–475).
48. Williams, M. (2022). *Ethereum's History: From Whitepaper to Hardforks and the ETH Merge.* Pridobljeno 29. aprila 2023 iz https://cryptopotato.com/ethereums-history-from-whitepaper-to-hardforks-and-the-eth-merge/
49. Young, J. (2016). *Ethereum Announces the Launch of Homestead.* Pridobljeno 29. aprila 2023 iz https://cointelegraph.com/news/ethereum-announces-the-launch-of-homestead
50. Zhang, S. & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT express*, *6*(2), 93–97.

PRILOGE

Priloga 1: Nastavljanje OpenZeppelinove predloge za podžeton ERC-20

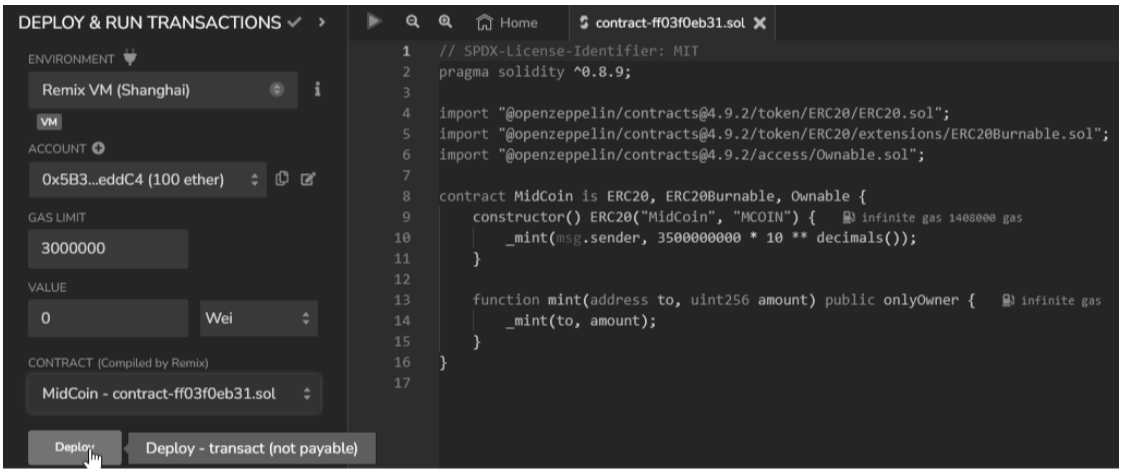
Slika 1: Nastavljanje OpenZeppelinove predloge



Vir: lastno delo.

Priloga 2: REMIX IDE – virtualizacija Shanghai testnega omrežja

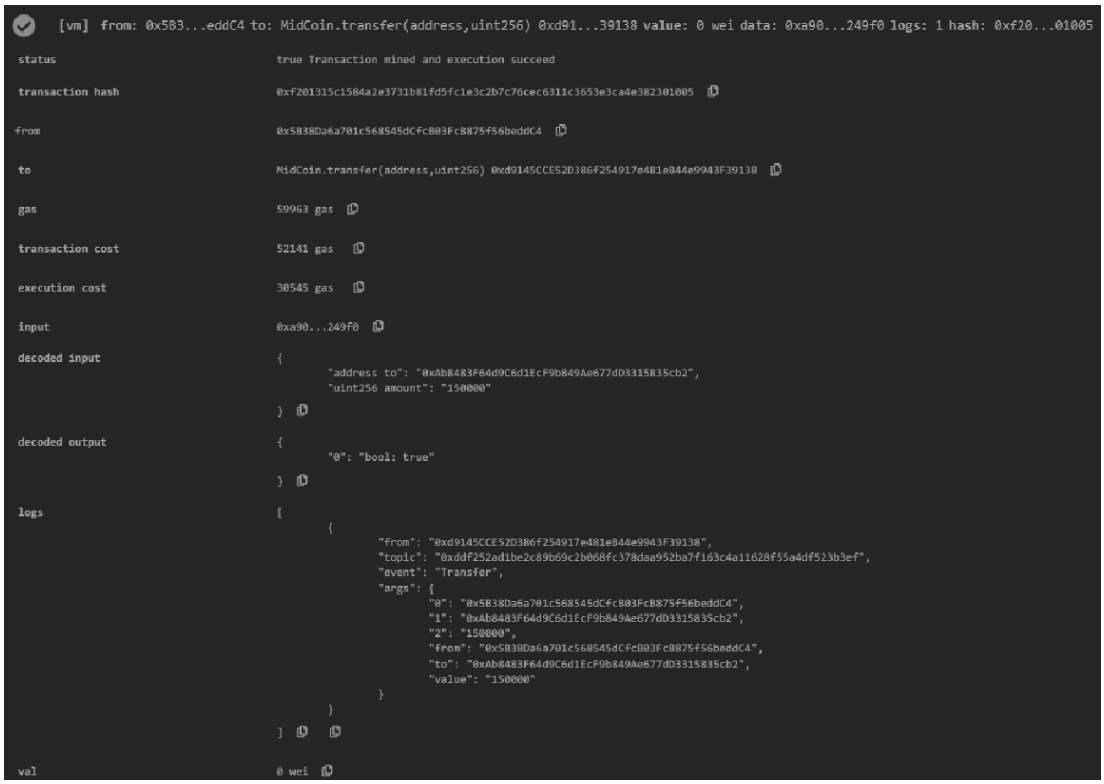
Slika 2: Virtualizacija Shanghai testnega omrežja v programski opremi REMIX IDE



Vir: lastno delo.

Priloga 3: REMIX IDE – transakcija podžetonov med računi, prenos 150.000 MidCoin žetonov

Slika 3: Transakcija 150.000 MidCoin podžetonov med računi na virtualiziranem Shanghai testnem omrežju



Vir: lastno delo.

Priloga 4: REMIX IDE – preverjanje stanja na naslovljenem računu po transakciji

Slika 4: Preverjanje stanja na naslovljenem računu po transakciji na virtualiziranem Shanghai testnem omrežju

Vir: lastno delo.

Priloga 5: Sepolia.etherscan.io – seznam opravljenih transakcij na testnem omrežju Sepolia

1. **Ustvarjanje pametne pogodbe za podžeton MidCoin:** https://sepolia.etherscan.io/tx/0xd67c3a5bf63d986a26d193aa23bab2749af6162c1386c50f11346e98ba70d40d
2. **Naslov računa, ki vsebuje pametno pogodbo za Midcoin:** https://sepolia.etherscan.io/address/0x3b71674b5bf1225e2cdff55fd1c49940ee012b3a
3. **Testni prenos podžetona Midcoin med dvema računoma:** https://sepolia.etherscan.io/tx/0x2b4437a09fc3691d3fff0dbbda191fca76b61f4987a67a55f5d2b1308f44de1a
4. **Uporaba funkcije »mint«, ustvarjanje novih podžetonov Midcoin:** https://sepolia.etherscan.io/tx/0xa9fad3c75353c5620e7faa965fd4ef9ee627c43db14a0a74bf727a40e4f12f6a