DIGITALNO INOVACIJSKO STIČIŠČE SLOVENIJE
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO
EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST
Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega sklada za regionalni razvoj.

Blokovne verige, kriptovalute in nezamenljivi kriptožetoni

Gregor Burger, Digitalno inovacijsko stičišče Slovenija

Povzetek — Blokovne verige, kriptovalute in nezamenljivi kriptožetoni so tehnolgija, ki je v kratkem času zavzela svet in povzročila številne premike na področju digitalnega lastništva. Čeprav so navedene tehnologije pogosto omenjene v medijih, se o njih veliko govori, a še vedno ostajajo številne nejasnosti in napačna prepričanja o samem delovanju kriptotehnologij. V objavi najprej prestavljamo zgodovinski pregled področja, sledi prestavitev delovanja blokovnih verig. Pri tem izpostavljamo delovanje Bitcoin in Ethereum blokovnih verig in razčlenitev različnih tipov blokovnih verig. Objavo zaključujemo z opisom namena in delovanja nezamenljivih kriptožetonov.

Ključne besede — blokovne verige, kriptovalute, nezamenljivi žetoni, bitconin, ethereum

Abstract — Blockchains, cryptocurrencies and non-fungible tokens are a technology that has taken the world by storm in a short space of time and caused many shifts in digital ownership. Although these technologies are often mentioned in the media, there are still many uncertainties or misconceptions about how crypto-technologies work. In this publication, we first give a historical overview of the field, followed by a review of how blockchains work. In doing so, we highlight how Bitcoin and Ethereum blockchains work and provide a breakdown of the different types of blockchains. We conclude the post with a description of the purpose and functioning of non-exchangeable crypto tokens.

Keywords — Block chain, Crypto curency, Non-Fungible Tokens , Bitcoin, Ethereum

1. UVOD

Blokovne verige, kriptovalute in nezamenljivi kriptožetoni (angl. Non-fungible tokens, NFT) so v zadnjih letih doživeli veliko popularnost in medijsko prepoznavnost. Njihove tehnologije in rešitve dozorevajo ter postajajo del našega vsakdana. V tem času smo bili priče izjemnim oscilacijam vrednosti kriptovalut in nezamenljivih kriptožetonov, ko so se medsebojno izmenjevale rekordne vrednosti in globoki padci vrednosti do točke brez prave finančne vrednosti žetonov.

Začetki konceptov blokovnih verig segajo v leto 1991, ko sta Stuart Haber in Wakefield Scott Stornetta na kriptografski konferenci predstavila idejo, kako kriptografsko zaščititi verigo dokumentov oz. blokov [1]. Tektonski premik na področju blokovnih verig se je zgodil šele v letu 2008. Takrat je Satoshi Nakamoto, njegova prava identiteta je še vedno naznanka, predstavil objavo z originalnim naslovom: »Bitcoin: A Peer to Peer Electronic Cash System«. V njej opisuje model in način za plačevanje z uporabo blokovnih verig brez potrebnih finančnih inštitucij [2]. S tem se je rodil Bitcoin. Prva uspešna transakcija z žetonom Bitcoin je bila izvedena v letu 2009. Še leto kasneje je bil opravljen prvi nakup z Bitcoinom, ko je programer Laszlo Hanycez za 10.000 BTC (Bitcoinov) kupil dve Papa John's pici. V letu 2011 je žeton Bitcoina prvič dosegel vrednost 1 USD, prve organizacije pa so pričele sprejemati Bitcoine kot način donacij. Sledila je skokovita rast vrednosti žetonov Bitcoin, saj je njegova tržna vrednost že v letu 2013 presegla vrednost ene milijarde ameriških dolarjev. Leto 2013 pa je bilo prelomno še v enem pogledu. Vitalik Buterin je v svoji objavi »Ethereum Project« [3] izpostavil dodatne funkcionalnosti blokovnih verig, npr. pametne pogodbe (angl. Smart contracts). To prepoznamo kot začetek decentralizirane, oprto kodne blokovne verige s podporo za pametne pogodbe Ethereum. Prvi nezamenljivi kriptožeton pa je bil izdelan (angl. Minted) v letu 2014. V sledečih letih je sledila skokovita finančna rast in sprejemanje oz. prepoznavanje blokovnih verig ter kriptovalut kot legitimnih načinov plačevanja, izvajanja finančnih transakcij ter potrjevanja pametnih pogodb. Vrednost 1000 USD za žeton je Bitcoin prvič presegel leta 2017. Finančne priložnosti so v panogo blokovnih verig in kriptovalut privabile tudi velika podjetja in države. Podjetje Facebook – danes Meta – je v letu 2018 napovedalo aktivnosti na področju kriptovalut, pojavljala so se celo namigovanja o ustvaritvi lastne kiptovalute. Leto kasneje je celo Kitajska napovedala zanimanje za blokovne verige in najavila izdajo svoje kriptovalute. Leto 2020 ni bilo prelomno le zaradi pandemije virusa Covid-19. Bahami so postali prva država na svetu, ki je uvedla digitalno valuto centralne banke, imenovano "peščeni dolar" (angl. Sand Dollar), blokovne verige pa so bile uporabljene za varno hranjenje medicinskih podatkov in podatkov bolnikov virusa Covid-19. Salvador je storil še korak naprej in v letu 2021 postal prva država, ki je sprejela Bitcoin kot zakonito plačilno sredstvo. Kot nov tehnološki trend se je pojavil Web

3.0 in metaverse, katerih delovanje temelji tudi na tehnologijah blokovnih verig. Prvič pa je bilo mogoče za Bitcoine kupiti tudi električni avtomobil Tesla. Leto 2022 je prineslo temne oblake nad preteklo finančno uspešno panogo. Kriptovalute so zaradi gospodarske inflacije in naraščajočih obrestnih mer izgubile 2 bilijona ameriških dolarjev tržne vrednosti. Vedno glasnejši postajajo pozivi po pravni ureditvi področja in vgradnji varoval za imetnike stabilnih kovancev (angl. Stablecoin). Svoje nestrinjanje in nezadovoljstvo z uporabo NFT-jev v popularnih video igrah so jasno izrazili tudi igralci video iger. Med drugim je MS Minecraft v svoji igri prepovedal uporabo tehnologij blokovnih verig in NFT-jev.

2. TEHNOLOGIJE BLOKOVNIH VERIG

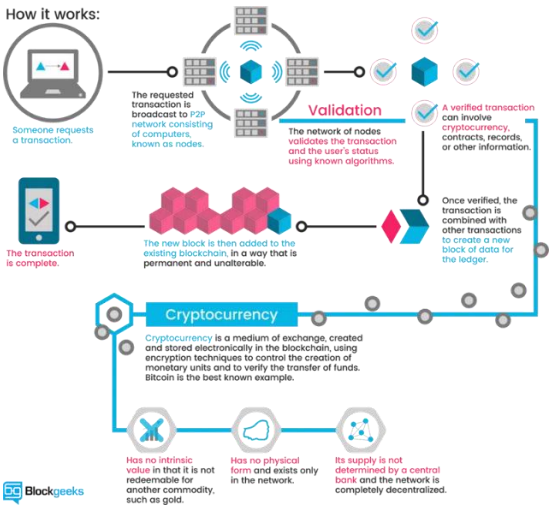
Tehnologije blokovnih verig oz. veriženja blokov predstavljajo distribuirane podatkovne baze oz. glavne knjige (angl. Ledger), ki so deljene med vozlišči računalniškega omrežja. Podrobnejši pregled in njihovo delovanje predstavlja sledeče poglavje [4], [5], [5].

Tako kot podatkovne baze tudi blokovne verige shranjujejo podatke v digitalni obliki in igrajo ključno vlogo pri implementaciji kriptovalut. Shranjujejo namreč decentralizirane podatke ter zagotavljajo varnost in zaupanje tretjih strani. Blokovne verige shranjujejo podatke v grupe, znane tudi kot bloke. Bloki imajo omejitev kapacitete količine shranjenih podatkov. Ob zapolnitvi bloka z informacijami se ta zapre in poveže s preteklimi bloki, kar tvori tako imenovano verigo podatkov, ki ji tudi pravimo blokovna veriga or. veriga blokov. Prihajajoči podatki pa medtem pričnejo polniti naslednji blok. Podatkovna struktura blokovne verige onemogoča spreminjanje časovnice nastanka podatkov, ki so nastali in bili implementirani v decentraliziranem načinu delovanja. V blokovnih verigah je mogoče shraniti različne podatke, ne le podatke o transakcijah, pač pa tudi kontakte, podatke za identifikacijo ali podatke o produktih.

Blokovne verige delujejo na decentraliziran način, bloki se nahajajo v različnih vozliščih omrežja na oddaljenih lokacijah. V primeru poizkusa poneverbe podatkov na bloku v enem vozlišču decentralizirana zasnova blokovnih verig omogoča preverjanja podatkov v drugih vozliščih, kar onemogoča nepooblaščeno spreminjanje podatkov. Zasnova sistema tako omogoča jasen in pregleden način spremljanja zaporedja izvedbe dogodkov. Validacija vnosa podatkov v nov blok blokovne verige za svojo izvedbo potrebuje soglasje večine preostalih omrežnih vozlišč omrežja. Blokovne verige imajo vgrajene mehanizme konsenza, kot sta dokaz dela (angl. Proof of Work) ali dokaz deleža (Proof of Stake), ki preprečujeta izvedbo nepravilnih ali zlonamernih transakcij.

Delovanje blokovnih verig je transparentno, njihovo delovanje in transakcije je mogoče vedno preveriti, transakcijam pa je mogoče tudi slediti. Kar pa ne velja za uporabnike blokovnih verig, saj so te pogosto kriptirane in le lastnik blokovne verige ima možnost dekriptirati njihovo vsebino in identificirati uporabnike. Tako uporabniki blokovnih verig ostanejo anonimni, še vedno pa se ohrani javnost opravljenih transakcij.

Kako blokovne verige dosežejo decentralizirano varnost in zaupanje? Bloki v blokovnih verigah se shranjujejo linearno in kronološko, novi bloki se vedno dodajo na konec blokovne verige. Ko je blok enkrat dodan blokovni verigi, je izjemno težko spremeniti njegovo vsebino brez večinskega konsenza omrežja. Vsak blok vsebuje tako imenovani Hash ključ. To je fiksno dolga binarna vrednost, ki se uporablja za predstavitev velikega dela podatkov v sistemu zgoščevanja, vsebuje pa, v primeru blokovnih verig, tudi del podatkov iz predhodnega bloka. Za spremembo vsebine bloka bi napadalec moral prevzeti vsaj 51 % nadzora nad omrežjem. Kar je zaradi velikosti omrežja izjemno velik zalogaj.



Slika 1: Delovanje blokovnih verig [4]

2.1. Različni tipi blokovnih verig

Javne blokovne verige so odprte blokovne, decentralizirane verige, ki so dostopne vsem za izvedbo zahteve za validacijo oz. izvedbo transakcije. Rudarji (angl. Miners), ki izvajajo transakcije, prejmejo za izvedbo določeno plačilo.

Zasebne blokovne verige niso javno dostopne in imajo omejitve pri dostopu. Za dostop je običajno treba pridobiti dovoljenje administratorja, posledično so takšne blokovne verige centralizirane.

Hibridne blokovne verige ali konzorciji so kombinacija javnih in privatnih blokovnih verig ter vsebujejo funkcionalnosti decentraliziranih in centraliziranih blokovnih verig.

Vzporedne oz. stranske blokovne verige (angl. Sidechains) so blokovne verige, ki delujejo vzporedno z glavnimi blokovnimi verigami. Uporabnikom omogočajo premikanje digitalnih dobrin med obema blokovnima verigama, kar povečuje skalabilnost in učinkovitost.

2.2. Bitcoin

Bitcoin protokol je bil ustvarjen na osnovi blokovnih verig in opisuje digitalno valuto, temelječo na per-to-per tehnologiji brez zaupanja vrednih tretjih strani. Bitcoin uporablja blokovno verigo le za transparentno beleženje transakcij plačil v glavni knjigi (angl. Ledger).

Bitcoin transakcije je mogoče izvajati vse dni v letu. Za vsako izvedbo transakcije je treba plačati tarifo, ki jo določijo rudarji transakcij. Vrednost transakcije se lahko giblje med 0 in 50 $, a imajo uporabniki blokovne verige možnost določiti zgornjo mejo višine plačila izvedbe transakcije. Izvedba transakcije traja v povprečju od 15 minut do več kot eno uro, odvisno od zasedenosti omrežja. Uporab Bitcoin-ov omogoča anonimnost, saj je njihovo uporabo izjemno težko pripisati določenemu uporabniku.

2.3. Ethereum

Ethereum je druga največja decentralizirana, odprtokodna blokovna veriga s funkcionalnostmi pametnih pogodb. Večja blokovna veriga je le Bitcoin. V letošnji jeseni je Ethereum prešel iz dokaza dela (angl. proof-of-work - PoW) na dokaz deleža (angl. proof-of-stake - PoS) [7] način delovanja. Dokaz dela je energetsko zelo potraten proces, ki zahteva veliko porabo električne energije. Pri načinu delovanja v dokazu dela so potrjevanje izvajale velike farme rudarjev, katerih oprema je temeljila na številnih grafičnih karticah višjega razreda. Sistem deluje na principu kriptografije in matematičnih enačb, kjer ena stran dokaže drugim, da je bilo izvedeno določeno število računalniških operacij. Medtem ko je dokaz deleža mehanizem konsenza temelječ na deležu oz. številu kovancev, ki jih nekdo poseduje, in je približno 1000 krat energetsko manj potraten. Večje število kripto kovancev kot oseba poseduje, večjo moč ima, s tem pa tudi večjo verjetnost, da bo izbrana za potrjevanje transakcije.

2.4. Prednosti in uporaba blokovnih verig

Med prednosti uporabe blokovnih verig najbolj pogosto prištevamo njeno decentralizirano zasnovo. Veriga deluje brez centralnega telesa upravljanja in sledi algoritmom konsenza. Uporabniki izvajajo interakcije direktno med seboj s popolnim lastništvom nad svojimi viri. Med prednosti prištevamo povečano varnost in zasebnost, ki prav tako izhaja iz decentralizirane zasnove blokovnih verig. Čeprav so transakcije javne, uporabniki še vedno ohranijo svojo zasebnost in anonimnost. Dodano med prednosti uvrščamo znižane stroške delovanja v primerjavi s tradicionalnimi finančnimi institucijami. Blokovne verige omogočajo raznolike možnosti prenosa sredstev med mednarodnimi entitetami.

Med pogostimi načini uporabe blokovnih verig zasledimo bančne in finančne storitve, izvedbo volitev, podatke dobavne verige, zdravstvene podatke, podatke o nepremičninah, pametne pogodbe itd.

3. NAZEMNLJIVI KRIPTOŽETONI

Področje nezamenljivi kriptožetonov doživlja v zadnjem letu velike padce vrednosti NFT žetonov. Vrh vrednosti je panoga dosegla v mesecu avgustu 2021, ko je povprečna vrednost vsakega prodanega nezamenljivega kriptožetona znašala v preko 1000 ameriških dolarjev, v mesecu septembru 2022 pa povprečna cena nezamenljivega kriptožetona ni presegla 80 ameriških dolarjev. Propadi in razvrednotenje številnih nezamenljivih kriptožetonov so pustili globoke sledi na trgu.

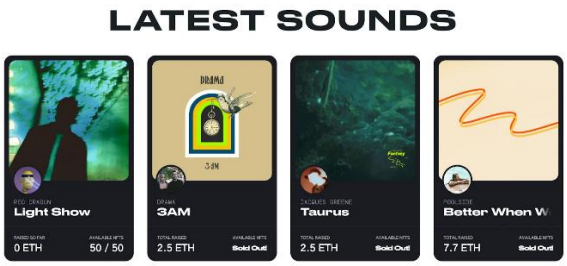
Nezamenljivi kriptožetoni so unikatni kriptožetoni in predstavljajo nezamenljiv set metapodatkov, ki so shranjeni na blokovni verigi. Za razliko od nezamenljivih kriptožetonov so kovanci oz. žetoni tipa Bitcoin zamenljivi žetoni. NFT žetone je mogoče unikatno identificirati, zato je tudi pomembno razlikovati med vizualno podobnimi žetoni, a različnimi metapodatki.

Primarno uporabljena blokovna veriga za NFT-je je Ethereum, na področju resnih iger pa se uporabljajo tudi nišne blokovne verige, kot so Flow in Ronin. Metapodatki NFT žetonov se nahajajo v pametnih pogodbah, shranjenih na blokovnih verigah. Pogosto zmotno prepričanje pri NFT žetonih je, da je slika, ki je bila uporabljena za izdelavo NFT

žetona, shranjena v blokovni verigi, kar drži le za nekaj nišnih rešitev. Bolj pogosta je rešitev, ko je grafična slika shranjena na zunanji platformi, metapodatki pa so shranjeni na blokovni verigi. Razlog za ločeno shranjevanje slike in metapodatkov je v visoki ceni shranjevanja slik v blokovni verigi zaradi same velikosti slikovne datoteke. NFT-ji so pogosto ustvarjeni iz grafičnih umetnin, GIF datotek, video posnetkov, zbirateljskih vsebin, virtualnih avatarjev, glasbe itd.

NFT žetoni rešujejo problem digitalnega lastništva na svetovnem spletu. Predstavljali naj bi potrdilo o lastništvu v digitalni ekonomiji. Kar bo omogočilo kreatorjem vsebin lažje in bolj učinkovito vrednotiti svoje delo in pridobiti pravično nadomestilo zanj.

Za lastništvo NFT žetona mora kupec imeti kripto denarnico (angl. Crypto wallet), ki je naprava oz. program na uporabnikovem računalniku, v katero je mogoče shraniti ali prenesti digitalne dobrine. Poznamo programske (znane tudi kot hot wallet) in stojne denarnice (znane tudi kot cold wallet). V naslednjem koraku mora kupec imeti v svoji kripto denarnici ustrezno količino izbrane kriptovalute za nakup NFT žetona. Nato je treba poiskati tržnico FNT žetonov, na kateri bo izveden nakup. Ustvarjanju NFT-jev se angleško reče minting. V bistvu je to proces, pri katerem se povežejo specifični metapodatki s pripadajočim objektom (slika, GIF, glasba itd.). Povezani metapodatki in pripadajoči objekt predstavljajo NTF žeton, katerega lastništvo pripišemo kupcu.



Slika 2: NFT žetoni [8]

4. ZAKLJUČEK

Področje blokovnih verig, kriptovalut in nezamenljivih kriptožetonov je nestabilno področje s številnimi nihanji vrednosti žetonov. Trenutno gospodarsko stanje z visoko inflacijo in vedno višjo obrestno mero jemlje zalet celotni panogi kriptovalut in kriptožetonov. Se pa z zorenjem področja oblikujejo zreli in stabilni poslovni modeli ter produkti, manj pa je možnosti za hitri zaslužek, ki je pogost pri pojavu zelo novih tehnologij. V objavi smo predstavili osnovne pojme in delovanje področja.

LITERATURA

[1] Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg, 1990. (prvi dostop: 7. 5. 2022)

[2] Satoshi, Nakamoto. »Bitcoin: A Peer to Peer Electronic Cash System« ,2008, https://bitcoin.org/bitcoin.pdf (prvi dostop: 7. 5. 2022)

[3] Vitalik, Buterin. Ethereum Project. 2013. https://ethereum.org/en/whitepaper/ (prvi dostop: 7. 5. 2022)

[4] Blockchain For Beginners: What Is Blockchain Technology? A Step-by-Step Guide: https://blockgeeks.com/guides/what-is-blockchain-technology/ (prvi dostop: 7. 5. 2022)

[5] Everything you need to know about blockchain technology: https://www.euroscientist.com/everything-you-need-to-know-about-blockchain-technology/ (prvi dostop: 7. 5. 2022)

[6] What is Blockchain Technology? How Does Blockchain Work? [Updated]: https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology (prvi dostop: 7. 5. 2022)

[7] Ethereum's "Merge" is about to put every ether miner out of work https://arstechnica.com/tech-policy/2022/08/the-merge-the-biggest-change-in-ethereum-history-explained/ (prvi dostop: 7. 5. 2022)

[8] What is NFT and How Does NFT Work? The Ultimate Guide https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-nft (prvi dostop: 7. 5. 2022)

[9] NFTs Explained: A Must-Read Guide to Everything Non-Fungible https://nftnow.com/guides/what-is-nft-meaning/ (prvi dostop: 7. 5. 2022)

[10] What Is An NFT? Non-Fungible Tokens Explained https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/#:~:text=An%20NFT%20is%20a%20digital,underlying%20software%20as%20many%20cryptos (prvi dostop: 7. 5. 2022)