UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA PROGRAMSKE REŠITVE ZA IZDAJO DIGITALNIH POTRDIL O OPRAVLJENEM IZOBRAŽEVANJU NA OSNOVI TEHNOLOGIJE VERIŽENJA BLOKOV

Ljubljana, maj 2023 ROK BENKO

IZJAVA O AVTORSTVU

Podpisani Rok Benko, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza programske rešitve za izdajo digitalnih potrdil o opravljenem izobraževanju na osnovi tehnologije veriženja blokov, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Mirom Gradišarjem

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 preko 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.

V Ljubljani, dne _____ Podpis študenta: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SEZNAM KRATIC

angl. – angleško
BTC – Bitcoin (kriptovaluta)
ETH – Ether (kriptovaluta)
EUR – Evro
HEOA – (angl. The Higher Education Opportunity Act); Zakon o možnostih visokošolskega izobraževanja
NFT – (angl. non-fungible token); nezamenljiv žeton
PoS – (angl. proof-of-stake); dokazilo o deležu
PoW – **(**angl. proof-of-work); dokazilo o delu
RS – Republika Slovenija
USD – Ameriški dolar
USDT – Tether (kriptovaluta)
UTXO – (angl. unspent transaction output); nepotrošeni transakcijski izhod
ZDA – Združene države Amerike

UVOD

Dandanes je uveljavljena praksa, da posamezniku, ki uspešno opravi določeno izobraževanje, pristojna izobraževalna institucija izda potrdilo o opravljenem izobraževanju (v nadaljevanju potrdilo). Npr., v Republiki Sloveniji (v nadaljevanju RS) izdajo javnih listin in potrdil Univerze v Ljubljani določa Pravilnik o izdaji javnih listin in potrdil Univerze v Ljubljani, Ur. l. RS, št. 180/20. Slednji natančno opredeljuje vrsto, obliko in vsebino javnih listin ter potrdil, ki jih izdaja Univerza v Ljubljani.

Na splošno so potrdila izdana v tiskani in/ali digitalni obliki. Tipičen primer tiskanega potrdila je diploma Univerze v Ljubljani. Diploma je natisnjena na posebnem, najmanj 180 gramskem papirju in mora vsebovati zaščitne elemente, vključno z nevidnimi, kot to določa Pravilnik o izdaji javnih listin in potrdil Univerze v Ljubljani. Tipičen primer digitalnega potrdila je certifikat za izobraževanje Bloomberg Market Concepts, ki ga je mogoče opraviti na terminalu Bloomberg v Centralni ekonomski knjižnici na Ekonomski fakulteti Univerze v Ljubljani. Certifikat je PDF datoteka, ki se samodejno ustvari po uspešno opravljenem izobraževanju in si ga posameznik lahko s terminala Bloomberg prenese na svoj osebni računalnik.

Ko govorimo o potrdilih, bodisi tiskanih bodisi digitalnih, obstaja problematika ponarejanja potrdil, ki bo naslovljena v magistrskem delu. Izobraževalni sistem v razvitem svetu temelji na akreditacijskem sistemu. Verodostojno pridobljeno potrdilo s strani akreditirane izobraževalne institucije posamezniku omogoča, da v družbi dokaže, da je usvojil določeno znanje, pridobi poklic in prevzame določeno vlogo. V kolikor posameznik predloži potrdilo ne da bi izpolnil vse zahtevane pogoje za pridobitev le-tega, gre za ponaredek. Ponarejanje potrdil je postala prava industrija, ki povzroča nezanemarljivo škodo celotni družbi (Sayed, 2019).

V Združenih državah Amerike (v nadaljevanju ZDA) se ocenjuje, da je 6 % dodiplomskih diplom (angl. bachelor's degree) in kar 35 % višješolskih diplom (angl. associate degree) ponarejenih (Sayed, 2019). Kljub temu, da v RS Zakon o visokem šolstvu (ZVis), Ur. l. RS, št. 32/12, določa, da se visokošolski zavodi financirajo iz proračuna RS, je problematika ponarejanja potrdil prisotna tudi v RS.

V RS v okviru spletnega portala eVŠ sicer obstaja Evidenca študentov in diplomantov (v nadaljevanju evidenca), ki jo zagotavlja Ministrstvo za izobraževanje, znanost in šport, v kateri lahko zainteresirana javnost preveri verodostojnost potrdila posameznika, vendar ima evidenca dve težavi (Ministrstvo za izobraževanje, znanost in šport, 2019). Prvič, v evidenco se vnašajo le podatki o izobraževanju v okviru visokošolskih zavodov RS. Drugič, evidenca je dostopna le s kvalificiranim digitalnim potrdilom (Ministrstvo za javno upravo, brez datuma).

Rešitev za problematiko ponarejanja potrdil ponuja tehnologija veriženja blokov (angl. blockchain), natančneje digitalno potrdilo v obliki nezamenljivega žetona (angl. non-fungible token, v nadaljevanju NFT).

Namena magistrskega dela sta:

- ozavestiti družbo o praktični uporabni vrednosti NFT-jev in
- prispevati k razvoju rešitve digitalnih potrdil v obliki NFT-jev.

Cilji magistrskega dela so:

- pregledati literaturo o tehnologiji veriženja blokov in NFT-jih,
- opredeliti najpogostejše načine ponarejanja potrdil in
- analizirati programsko rešitev izdaje digitalnih potrdil v obliki NFT-jev.

V magistrskem delu želimo odgovoriti na raziskovalno vprašanje, kako zasnovati sistem izdajanja digitalnih potrdil na osnovi tehnologije veriženja blokov, natančneje digitalnih potrdil v obliki NFT-jev, da se prepreči oz. minimizira možnost ponarejanja potrdil.

Vsebinski del magistrskega dela je razdeljen na dva sklopa. V prvem sklopu, ki je teoretični, predstavimo tehnologijo veriženja blokov in izbrano problematiko ponarejanja potrdil, kar nam pomaga pri odgovarjanju na raziskovalno vprašanje. Tematiko predstavimo po principu od splošnega k specifičnemu. Metode, ki jih uporabljamo v prvem sklopu magistrskega dela, so deskripcija (tj. opisovanje posameznih pojmov), kompilacija (tj. povzemanje drugih avtorjev), komparacija (tj. primerjava) in analiza (tj. razčlenjevanje celote na posamezne dele). V drugem sklopu, ki je praktični, predstavimo praktično implementacijo ugotovitev iz prvega dela. Apliciramo tehnologijo veriženja blokov, natančneje NFT-je, na področje izdajanja digitalnih potrdil, s čimer odgovorimo na raziskovalno vprašanje. Metoda, ki jo uporabljamo v drugem sklopu magistrskega dela, je kvalitativna.

Rešitev digitalnih potrdil v obliki NFT-jev je še povsem v povojih. Prve izdaje digitalnih potrdil v obliki NFT-jev segajo le nekaj mesecev nazaj od trenutka pisanja magistrskega dela, natančneje v konec leta 2021 oz. začetek leta 2022. Posledično je strokovna literatura o tej tematiki ekstremno skopa, prav tako se dobra praksa na tem področju šele oblikuje. Z magistrskim delom poskušamo prispevati k razvoju te rešitve.

1 BITCOIN TEHNOLOGIJA VERIŽENJA BLOKOV

Leta 2008, natančneje 31. oktobra 2008, Satoshi Nakamoto na več elektronskih naslovov oseb, ki se ukvarjajo s kriptografijo, pošlje elektronsko pošto, katere vsebina je prikazana na sliki 1. V njej napiše, da dela na novem medvrstniškem sistemu elektronskega denarja (angl. peer-to-peer electronic cash system) in zraven pripne belo knjigo z naslovom Bitcoin: A Peer-to-Peer Electronic Cash System (v nadaljevanju bela knjiga) (McSweeney, 2021). Leta

2009, natančneje 3. januarja 2009, Satoshi Nakamoto ustvari prvi Bitcoin blok (v nadaljevanju BTC blok) in s tem dejanjem nastane prvih 50 Bitcoinov (v nadaljevanju BTC) (Phillips, 2021). To, kar Satoshi Nakamoto v beli knjigi imenuje medvrstniški sistem elektronskega denarja, danes imenujemo tehnologija veriženja blokov.

Satoshi Nakamoto ni prvi, ki je želel ustvariti decentraliziran finančni sistem. Pred njim so probleme tradicionalnega finančnega sistema poskušali s kriptografijo reševati tudi drugi posamezniki. Bolj znani poskusi so projekt Hashcash (Adam Back leta 1997), projekt b-money (Wei Dai leta 1998) in projekt Bit gold (Nick Szabo leta 2005), vendar šele Satoshi Nakamoto ustvari povsem funkcionalno rešitev, ki postane popularna v družbi in sprejeta na svetovni ravni (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013).

Ko govorimo o Satoshiju Nakamotu, je treba omeniti, da gre za psevdonim. Lahko bi šlo za osebo ali za skupino oseb, čigar prava identiteta ostaja do današnjega dne neznana (Cointelegraph, brez datuma).

Slika 1: Vsebina elektronske pošte, ki jo 31. oktobra 2008 pošlje Satoshi Nakamoto

I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would
allow online payments to be sent directly from one party to another
without the burdens of going through a financial institution.
Digital signatures provide part of the solution, but the main
benefits are lost if a trusted party is still required to prevent
double-spending. We propose a solution to the double-spending
problem using a peer-to-peer network. The network timestamps
transactions by hashing them into an ongoing chain of hash-based
proof-of-work, forming a record that cannot be changed without
redoing the proof-of-work. The longest chain not only serves as
proof of the sequence of events witnessed, but proof that it came
from the largest pool of CPU power. As long as honest nodes control
the most CPU power on the network, they can generate the longest
chain and outpace any attackers. The network itself requires
minimal structure. Messages are broadcasted on a best effort basis,
and nodes can leave and rejoin the network at will, accepting the
longest proof-of-work chain as proof of what happened while they
were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to majordomo at metzdowd.com

Vir: Bitcoin.com (2008).

1.1 Okoliščine nastanka

Svet se danes skoraj ekskluzivno opira na tradicionalne finančne institucije, ki imajo vlogo zaupanja vredne tretje osebe (angl. trusted third party) pri procesiranju transakcij (Nakamoto, 2008). Da bi razumeli, zakaj tehnologija veriženja blokov sploh nastane, moramo razumeti družbeno-ekonomski kontekst takratnega časa.

Bela knjiga pride v javnost konec leta 2008. Gre za čas, ko globalna gospodarska kriza povzroči gospodarski šok svetovnih razsežnosti (The Blockchain Review, brez datuma). V enem segmentu družbe se začne širiti bes nad bankirji, nad tradicionalnimi finančnimi ustanovami, nad Wall Streetom, nad kapitalizmom. V ZDA pride do gibanja Occupy Wall Street, katerega posamezniki se opredeljujejo kot 99 %, medtem ko izražajo nezadovoljstvo nad preostalim 1 %, ki po njihovih besedah piše pravila nepravičnega svetovnega gospodarstva, ki malemu človeku onemogočajo prihodnost (Occupy Wall Street, brez datuma). Zdi se, da je tehnologija veriženja blokov, ki za svoje delovanje ne potrebuje tretje osebe, točno to, kar vsaj en segment družbe v tistem času želi. V tem pogledu je nastanek tehnologije veriženja blokov v bistvu posledica globalne gospodarske krize leta 2008.

Da je temu tako, priča tudi močno simbolično sporočilo, ki ga Satoshi Nakamoto pusti v prvem BTC bloku. Parameter baze denarja (angl. coinbase parameter) v prvem BTC bloku vsebuje naslednji zapis: »The Times 03/Jan/2009 Chancellor on brink of second bailout for banks«. Zapis se navezuje na naslovnico časnika The Times z dne 3. januar 2009, ki je prikazana na sliki 2. Satoshi Nakamoto s tem sporočilom izrazi kritiko do tradicionalnega finančnega sistema, ki ga v tistem času vlade po svetu rešujejo s paketi finančne pomoči (angl. bailout) bankam (Binance Academy, brez datuma a).

Slika 2: Naslovnica časnika The Times z dne 3. januar 2009


THE TIMES

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Vir: Yee (2021).

1.2 Pomanjkljivost tradicionalnega finančnega sistema

Tradicionalni finančni sistem deluje dovolj dobro za večino transakcij, vendar ima inherentno pomanjkljivost v tem, da je vsaka transakcija lahko reverzibilna. Povsem nereverzibilne transakcije v tradicionalnem finančnem sistemu niso mogoče, ker vedno obstaja možnost spora med plačnikom in prejemnikom. V kolikor pride do spora, morajo finančne institucije posredovati. Posledično pride do dveh posledic. Prvič, reverzibilnost transakcij v tradicionalnem finančnem sistemu povečuje potrebo po zaupanju v sistem. Drugič, stroški reševanja sporov se odražajo v višjih transakcijskih stroških vseh komitentov, saj finančne institucije stroške reševanja sporov vračunajo v ceno svojih storitev (Nakamoto, 2008).

Satoshi Nakamoto v beli knjigi napiše, da je model, ki temelji na zaupanju (angl. trust-based model) pomanjkljiv in da je model, ki temelji na kriptografiji (angl. cryptographic proof-based model) boljša rešitev. Nadaljuje, da družba potrebuje elektronski plačilni sistem, v katerem lahko plačnik in prejemnik opravita transakcijo direktno, brez tretje osebe (Nakamoto, 2008). V eni od svojih zgodnjih elektronskih pošt doda tudi, da moramo v tradicionalnem finančnem sistemu zaupati centralni banki, da ne bo razvrednotila fiat valute, pri čemer zgodovina po njegovem mnenju kaže drugače. Izpostavi, da poslovnim bankam zaupamo naša denarna sredstva, pri čemer poslovna banka obdrži le peščico teh sredstev v rezervah, s preostankom se po njegovem mnenju ustvarjajo kreditni baloni. Satoshi Nakamoto v tradicionalnem finančnem sistemu vidi veliko pomanjkljivosti, zato razvije tehnologijo veriženja blokov (Nakamoto, 2009).

Ko govorimo o zaupanju, je treba poudariti, da pravzaprav ne gre za to, da tehnologija veriženja blokov ne vsebuje komponente zaupanja. Tudi tehnologija veriženja blokov temelji na zaupanju, vendar na drugačen način kot tradicionalni finančni sistem. Obstajata vsaj dve možni razlagi. Prvič, lahko bi rekli, da tehnologija veriženja blokov temelji na decentraliziranem zaupanju (angl. decentralized trust-based model) (Atzori, 2015). Drugič, lahko bi rekli, da tehnologija veriženja blokov temelji na zaupanju do matematike (angl. trust-by-computation-based model) (Antonopoulos, 2014).

Centralizacija, na kateri temelji tradicionalni finančni sistem, ima nekaj pomanjkljivosti. Prvič, centralizirana avtoriteta pomeni obstoj enotne točke napake (angl. single point of failure). Drugič, centralizirana avtoriteta lahko preko regulatornega pritiska pomembno vpliva na delovanje deležnikov, pri čemer je centralizirana avtoriteta tista, ki definira, kaj je prav in kaj narobe. Tretjič, centralizirana avtoriteta lahko izkoristi privilegiran položaj v svoj prid na škodo širše družbe. Četrtič, centralizirana avtoriteta lahko izvaja tako imenovano finančno cenzuro, kar se je zgodilo v primeru Wikileaks, kjer so banke in ponudniki kreditnih kartic blokirali donacije, medtem ko so donacije v BTC lahko normalno prihajale kljub finančni blokadi tradicionalnih finančnih institucij (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013).

1.3 Problem dvojne potrošnje

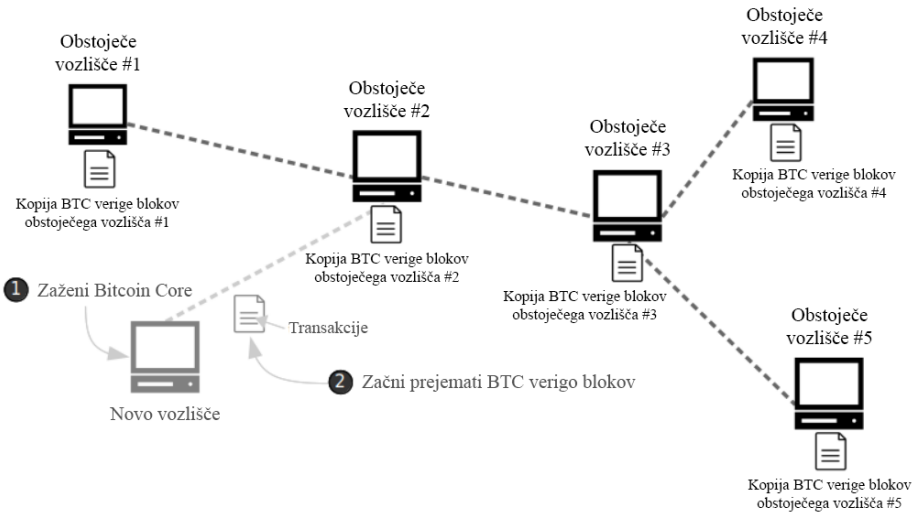
Danes tradicionalnim finančnim institucijam zaupamo vlogo tretje osebe pri procesiranju transakcij. Če Luka nakaže Maji 100 EUR, potem morajo tradicionalne finančne institucije zmanjšati stanje na transakcijskem računu Luki za 100 EUR in povečati stanje na transakcijskem računu Maji za 100 EUR. Tradicionalne finančne ustanove na ta način preprečujejo problem dvojne potrošnje (angl. double-spending problem). Luka ne more nakazati teh istih 100 EUR dvakrat ali večkrat. Če bi lahko, bi Luka pravzaprav ustvarjal nov denar, s čimer bi povzročil inflacijo. Problem dvojne potrošnje obstaja le pri elektronskih transakcijah, pri gotovinskih transakcijah ga ni. Če Luka izroči Maji 100 EUR v gotovini, potem Luka tega istega bankovca za 100 EUR ne more nikoli več znova uporabiti, ker je zdaj v Majinih rokah (The Blockchain Review, brez datuma).

1.4 Razpršena knjiga transakcij

Centraliziranih institucij, ki bi beležile transakcije, posledično spreminjale stanja in s tem preprečevale problem dvojne potrošnje, pri tehnologiji veriženja blokov ni. Da bi tehnologija veriženja blokov lahko preprečevala problem dvojne potrošnje, mora biti veriga blokov javno dostopna vsakomur. Namreč, v verigi blokov lahko opazimo zlonamerno (tj. manjkajočo, spremenjeno ali podvojeno) transakcijo le, če nam je znana celotna zgodovina transakcij, torej celotna veriga blokov (Nakamoto, 2008).

Tehnologija veriženja blokov zato deluje na osnovi razpršene knjige transakcij (angl. distributed ledger). Razpršena knjiga transakcij je pravzaprav celotna veriga blokov, od prvega do zadnjega trenutno znanega bloka, ki je javno dostopna vsakomur. Bistvo razpršene knjige transakcij je v tem, da ne obstaja le ena kopija verige blokov, temveč mnogo kopij. Vsak posameznik, ki na svoj računalnik naloži verigo blokov, od že obstoječih vozlišč (angl. nodes) v omrežju (angl. network) pravzaprav le kopira verigo blokov. Njegova kopija verige blokov je identična verigi blokov, ki jo imajo ostala vozlišča. S tem dejanjem se posameznik pridruži omrežju in tudi sam postane vozlišče, kot je prikazano na sliki 3. Torej je kopij verige blokov toliko, kolikor je vozlišč v omrežju (Feign, 2022).

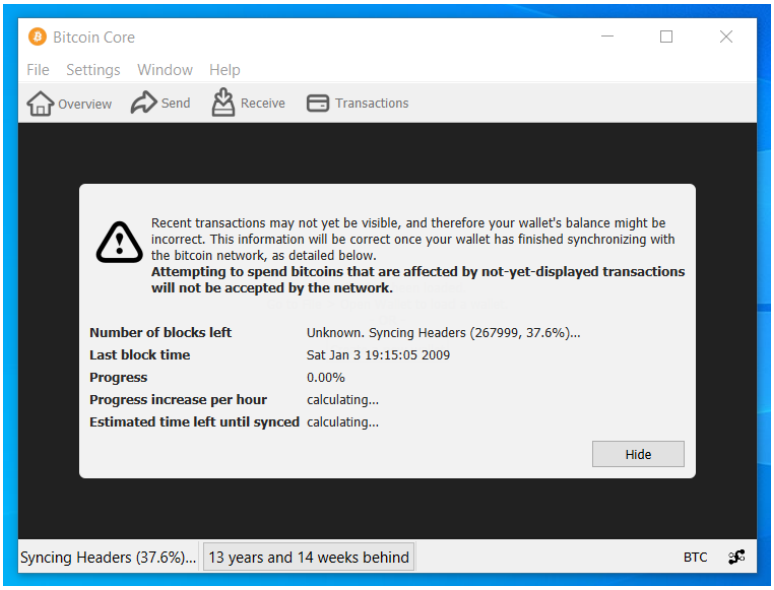
Slika 3: Obstoječa vozlišča v omrežju (s črno), ki se jim pridruži novo vozlišče (s sivo)



Prirejeno po Walker (brez datuma).

Procesu nalaganja kopije verige blokov na naš računalnik pravimo sinhronizacija verige blokov z omrežjem (angl. blockchain synchronization). Sinhronizacija verige blokov z omrežjem ni nič drugega kot to, da že obstoječa vozlišča v omrežju z nami delijo datoteke, ki tvorijo verigo blokov (Walker, brez datuma). BTC verigo blokov si lahko kdor koli zastonj naloži na svoj računalnik s pomočjo odprtokodne programske opreme Bitcoin Core. S tem dejanjem se pridružimo omrežju in postanemo vozlišče. Bitcoin Core na naš računalnik naloži celotno BTC verigo blokov, začenši s prvim BTC blokom iz leta 2009, kot je prikazano na sliki 4.

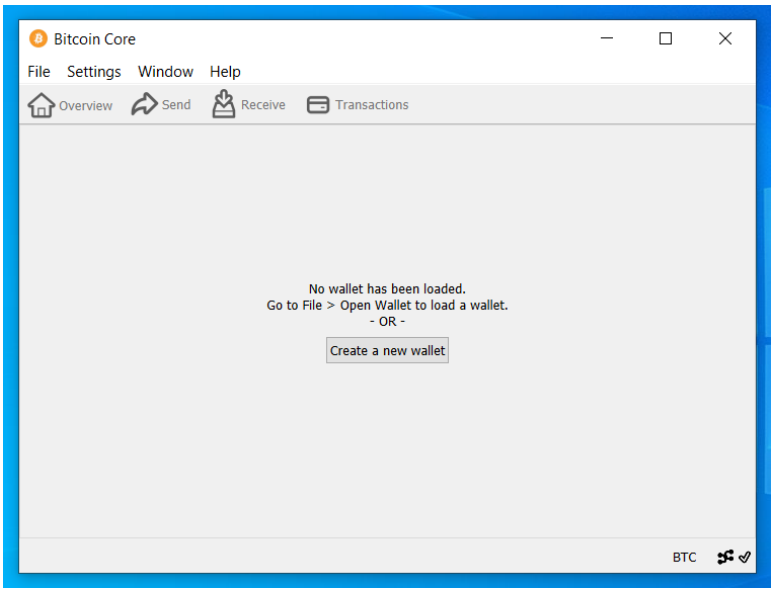
Slika 4: Začetek sinhronizacije BTC verige blokov z omrežjem na naš računalnik z uporabo programske opreme Bitcoin Core



Vir: lastno delo.

Sinhronizacija BTC verige blokov z omrežjem na naš računalnik traja kar nekaj časa, odvisno od zmogljivosti strojne opreme našega računalnika in hitrosti internetne povezave. Ko je BTC veriga blokov na našem računalniku uspešno sinhronizirana do zadnjega trenutno znanega BTC bloka, kot je prikazano na sliki 5, če računalnik ves čas deluje in je Bitcoin Core zagnan, potem se bo BTC veriga blokov na našem računalniku z omrežjem sinhronizirala sproti vsakič, ko bo v BTC verigo blokov dodan nov BTC blok. Če vmes zaustavimo Bitcoin Core, potem se bo sinhronizacija BTC verige blokov na našem računalniku naslednjič, ko zaženemo Bitcoin Core, nadaljevala tam, kjer se je nazadnje končala.

Slika 5: Konec sinhronizacije BTC verige blokov z omrežjem na našem računalniku z uporabo programske opreme Bitcoin Core



Vir: lastno delo.

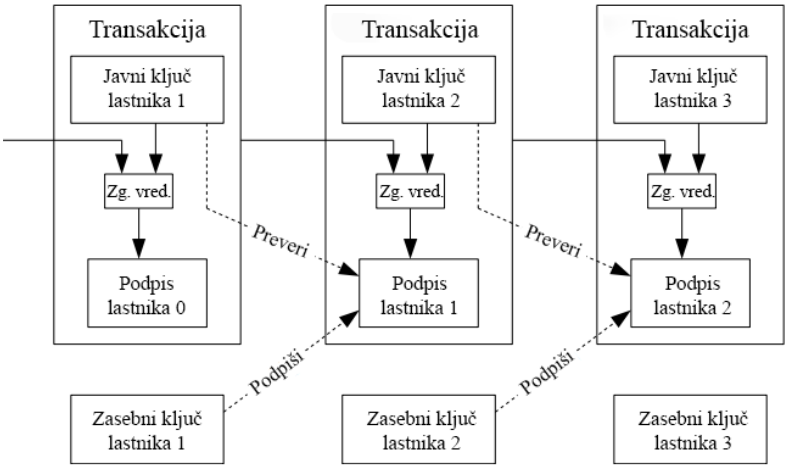
1.5 Transakcije

Razpršena knjiga transakcij kljub vsemu zgoraj napisanemu ni dovolj za preprečevanje problema dvojne potrošnje. Čeprav je veriga blokov javno dostopna vsakomur, je vanjo lahko dodana zlonamerna transakcija. Npr., Maja lahko v razpršeno knjigo transakcij doda zlonamerno transakcijo »Luka nakaže Maji 1 BTC«, s katero se Luka seveda ne strinja.

Tehnologija veriženja blokov ta problem preprečuje z digitalnim podpisom (angl. digital signature) pod vsako transakcijo. Satoshi Nakamoto opredeli BTC kot verigo digitalnih podpisov, kot je prikazano na sliki 6. Trenutni lastnik BTC-ja ga lahko nakaže novemu lastniku tako, da trenutni lastnik s svojim privatnim ključem digitalno podpiše zgoščeno vrednost (angl. hash) predhodne transakcije in javni ključ novega lastnika, kar doda na konec BTC-ja. Novi lastnik preveri digitalni podpis predhodnega lastnika tako, da s poznavanjem javnega ključa prehodnega lastnika dešifrira digitalni podpis predhodnega lastnika in

ugotovi, ali je veljaven ali neveljaven. Digitalni podpis je veljaven, če novi lastnik ob dešifriranju digitalnega podpisa predhodnega lastnika dobi identično zgoščeno vrednost, ki je bila generirana pred digitalnim podpisom predhodnega lastnika (Nakamoto, 2008).

Slika 6: BTC kot veriga digitalnih podpisov



Prirejeno po Nakamoto (2008).

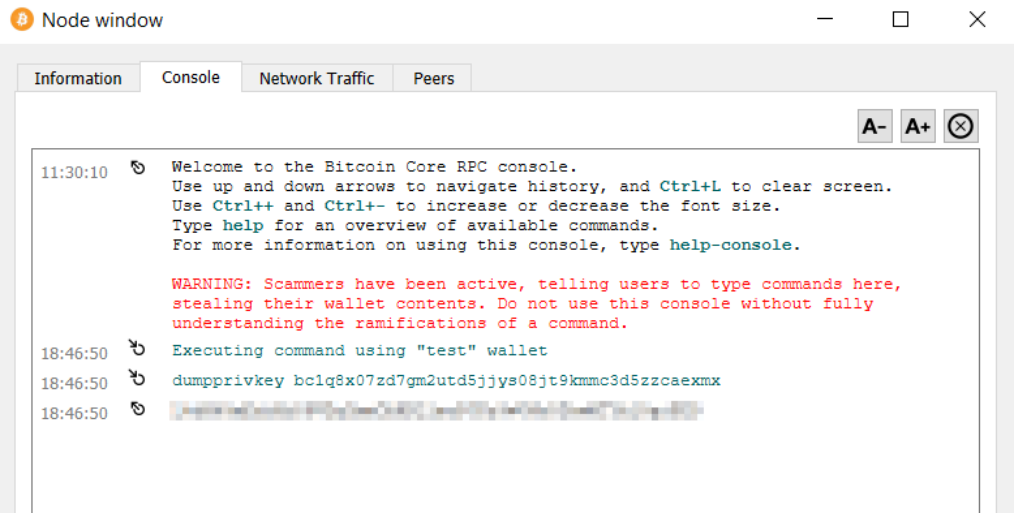
Luka se mora torej pod transakcijo »Luka nakaže Maji 1 BTC« digitalno podpisati. S tem izkaže svojo voljo, da se s transakcijo strinja. Posledično Maja v razpršeno knjigo transakcij ne more dodati nobene zlonamerne transakcije, s katero se Luka ne bi strinjal in je ne bi digitalno podpisal.

Digitalni podpis tudi onemogoča, da bi Maja lahko digitalno podpisala transakcijo »Luka nakaže Maji 1 BTC« v imenu Luke. Vsaka oseba ima za digitalno podpisovanje par ključev, in sicer privatni ključ ter javni ključ, kot je prikazano na sliki 7 in sliki 8. Luka in Maja imata vsak svoj par ključev, pri čemer privatnega ključa ne delita z nikomer (Meyer, 2020a). Bistvo kriptografije je v tem, da lahko Luka in Maja drug drugemu razkrijeta svoj javni ključ, vendar iz javnega ključa nikakor ne moreta ugotoviti privatnega ključa drug drugega. Z upoštevanjem tega dejstva lahko Luka in Maja izvršujeta transakcije ne da razkrijeta svoj privatni ključ. Noben od njiju ne sme svojega privatnega ključa nikoli razkriti, kajti samo s poznavanjem privatnega ključa lahko posameznik dostopa do svojih BTC-jev. S poznavanjem privatnega ključa se pravzaprav dokazuje lastništvo BTC-jev (Walker, brez datuma).

Slika 7: Javni ključ na primeru Bitcoin Core denarnice

Vir: lastno delo.

Slika 8: Privatni ključ (zamegljeno) na primeru Bitcoin Core denarnice



Vir: lastno delo.

Digitalno podpisovanje je funkcija transakcije in privatnega ključa, kot je razvidno iz enačbe (1). To pomeni, da vsaka transakcija zahteva nov digitalni podpis, ker je digitalni podpis funkcija tudi transakcije, ne le privatnega ključa. Če je Luka kdaj v preteklosti Maji nakazal 1 BTC in transakcijo digitalno podpisal, Maja te digitalno podpisane transakcije »Luka nakaže Maji 1 BTC« ne more kopirati in je s starim digitalnim podpisom znova večkrat dodati v razpršeno knjigo transakcij, ker bo digitalni podpis na vseh kopiranih transakcijah

neveljaven. Digitalni podpis bo veljaven le na prvotno digitalno podpisani transakciji »Luka nakaže Maji 1 BTC« (3Blue1Brown, 2017).

$$Podpiši(transakcija, privatni\ ključ) = digitalni\ podpis \quad (1)$$

Preverjanje digitalnega podpisa je funkcija transakcije, digitalnega podpisa in javnega ključa, kot je razvidno iz enačbe (2) (3Blue1Brown, 2017).

$$Preveri(transakcija, digitalni\ podpis, javni\ ključ) = veljaven/neveljaven \quad (2)$$

Najti veljaven digitalni podpis pod določeno transakcijo le s poznavanjem javnega ključa brez poznavanja privatnega ključa je sicer teoretično možno, vendar v praksi zelo malo verjetno. Maja bi sicer lahko poskušala z ugibanjem naključnih digitalnih podpisov najti točno tisti digitalni podpis pod transakcijo »Luka nakaže Maji 1 BTC«, ki bi dal ob dešifriranju digitalnega podpisa z javnim ključem Luke identično zgoščeno vrednost, ki je bila generirana pred digitalnim podpisom. Posledično bi digitalni podpis Luke bil veljaven, čeprav je transakcijo pravzaprav podpisala Maja v imenu Luke.

Kljub temu se Maji tega ne splača početi. Namreč, BTC veriga blokov uporablja zgoščevalno funkcijo SHA-256. Če je podpis 256 biten, to pomeni, da obstaja 2^{256} možnih digitalnih podpisov pod določeno transakcijo. Gre za tako veliko število možnosti, da se Maji niti ne splača ugibati. Torej, če je digitalni podpis pod določeno transakcijo ob preverjanju veljaven, potem lahko z veliko verjetnostjo rečemo, da jo je dejansko podpisala oseba s poznavanjem svojega privatnega ključa in ni šlo za ugibanje naključnih digitalnih podpisov tretje osebe (3Blue1Brown, 2017).

1.6 Časovni žig

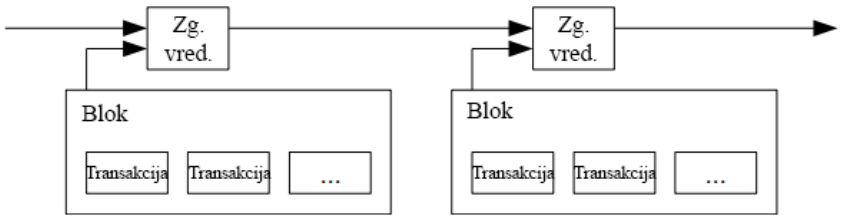
Digitalni podpisi pod transakcijami kljub vsemu zgoraj napisanemu še vedno niso dovolj za preprečevanje problema dvojne potrošnje. Luka lahko Maji pošlje 1 BTC in transakcijo tudi digitalno podpiše, vendar Maja nikakor ne more vedeti, ali Luka ni tega istega BTC-ja že pred tem poslal nekomu drugemu. Luka bi lahko ta isti BTC najprej poslal Nini in potem še Maji. Čeprav Luka obe transakciji digitalno podpiše, niti Nina niti Maja nikakor ne moreta vedeti, kakšen je vrstni red transakcij. Posledično ne moreta ugotoviti, ali je Luka ta isti BTC potrošil le enkrat ali večkrat.

Tehnologija veriženja blokov ta problem rešuje s časovnim žigom (angl. timestamp) pod vsakim blokom. Zaradi odsotnosti tretjih oseb pri tehnologiji veriženja blokov v omrežju ne obstaja nobena institucija, ki bi enolično določala zgodovino transakcij. Poleg tega, da je veriga blokov javno dostopna vsakomur in da so transakcije digitalno podpisane, se morajo osebe v omrežju tudi strinjati z enolično zgodovino transakcij, če želijo, da bi tehnologija veriženja blokov preprečevala problem dvojne potrošnje. Strinjanje z enolično zgodovino transakcij pomeni, da je v omrežju povsem jasno, kakšen je zgodovinski vrstni red transakcij.

Posledično je problem dvojne potrošnje preprečen, časovni žig pod vsakim blokom je tisto, kar enolično določa zgodovinski vrstni red blokov, torej zgodovinski vrstni red transakcij (Nakamoto, 2008).

Ko govorimo o časovnem žigu, je treba omeniti, da ni pomembno, kdaj je blok nastal časovno, zato se pod blok ne zapisuje datum in ura, kot bi morda sklepali. Pomembno je, kakšen je vrstni red blokov. Satoshi Nakamoto opredeli BTC verigo blokov kot verigo časovnih žigov, kot je prikazano na sliki 9. Najprej se v posamezen blok zberejo transakcije, potem se z zgoščevalno funkcijo SHA-256 izračuna zgoščena vrednost trenutnega bloka. Zgoščena vrednost novega bloka je z zgoščevalno funkcijo SHA-256 izračunana iz zgoščene vrednosti predhodnega bloka in zgoščene vrednosti novega bloka. Na tak način se tvori veriga blokov, pri čemer je vrstni red blokov povsem jasen (Meyer, 2020b).

Slika 9: BTC veriga blokov kot veriga časovnih žigov



Prirejeno po Nakamoto (2008).

Ker je veriga blokov javno dostopna vsakomur, so posledično tudi časovni žigi pod vsemi bloki javno dostopni vsakomur. Vsaka oseba v omrežju lahko samostojno potrdi ali ovrže vrstni red blokov, torej vrstni red transakcij. To naredi tako, da preveri, ali je zgoščena vrednost bloka B lahko izračunana iz zgoščene vrednosti bloka A. Če je lahko, potem so transakcije v bloku A bile izvršene pred transakcijami v bloku B. Nadalje preveri, ali je zgoščena vrednost bloka C lahko izračunana iz zgoščene vrednosti bloka B. Če je lahko, potem so bile transakcije v bloku B izvršene pred transakcijami v bloku C. Vrstni red blokov lahko s preverjanjem na tak način potrdimo ali ovržemo (Meyer, 2020b).

V kolikor bi katero koli vozlišče v omrežju spremenilo katero koli transakcijo v katerem koli bloku v verigi blokov, bi se zgoščena vrednost tistega bloka spremenila. Posledično bi se spremenile tudi zgoščene vrednosti vseh naslednjih blokov, ker je zgoščena vrednost posameznega bloka odvisna tudi od zgoščene vrednosti njegovega predhodnega bloka. Gre za rekurzivno izračunavanje zgoščenih vrednosti, ki tvori rekurzivno povezane bloke (Meyer, 2020b).

Namreč, zgoščevalna funkcija za dan vhod vedno generira identičen izhod, torej identično zgoščeno vrednost. Če se vhod spremeni za en bit, bo zgoščevalna funkcija generirala povsem različen izhod. Npr., če damo v zgoščevalno funkcijo SHA-256 kot vhod besedo »Bitcoin«, bomo dobili drugačen izhod, kot če damo kot vhod besedo »bitcoin«. Vendar bo

izhod za »Bitcoin« vedno identičen in izhod za »bitcoin« bo vedno identičen, kot je prikazano v tabeli 1 (Brownworth, 2016).

Tabela 1: Primerjava vhoda »Bitcoin« in »bitcoin« v zgoščevalno funkcijo SHA-256

Vhod	Izhod oz. zgoščena vrednost
Bitcoin	*b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4*
bitcoin	*6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b*

Vir: lastno delo.

Z uporabo časovnega žiga pod vsakim blokom se Luka, Maja in Nina strinjajo z enoličnim kronološkim vrstnim redom transakcij. Zdaj nihče od njih istega BTC-ja ne more potrošiti dvakrat ali večkrat, ker je enoličen kronološki vrstni red transakcij jasen in bi omrežje tako transakcijo, s katero bi bil isti BTC potrošen drugič, opazilo in zavrnilo. S tem je problem dvojne potrošnje preprečen.

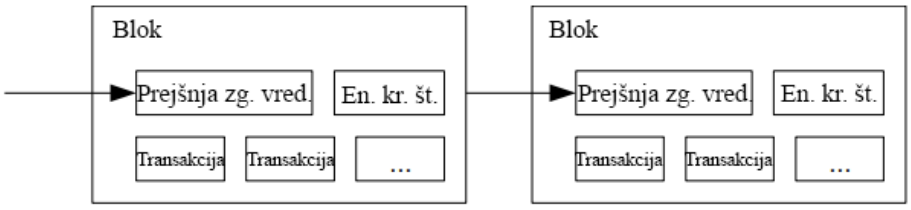
1.7 Dokazilo o delu

Tudi časovni žigi pod bloki kljub vsemu zgoraj napisanemu še vedno niso dovolj za preprečevanje problema dvojne potrošnje. Maja lahko v enem od predhodnih blokov spremeni transakcijo »Maja nakaže Nini 100 BTC« v »Maja nakaže Nini 1 BTC«. Gre za zlonamerno transakcijo. Maji tega dejanja nič ne preprečuje. Vse, kar mora narediti je, da ponovno izračuna zgoščeno vrednost bloka, v katerem je spremenila transakcijo in posledično ponovno izračuna zgoščene vrednosti tudi vseh naslednjih blokov. Potem mora spremenjeno verigo blokov naznaniti še omrežju. Luka in Nina sicer spremembe v verigi blokov vidita, ker je veriga blokov javno dostopna vsakomur, vendar se s spremenjeno verigo blokov, ki vsebuje lažno transakcijo, ne strinjata. Težava je v tem, da lahko tudi Luka in Nina naredita enako. Spremenita verigo blokov v svojo korist, izračunata zgoščene vrednosti in spremenjeno verigo blokov naznanita omrežju. Luka, Maja in Nina lahko neprestano spreminjajo verigo blokov in tekmujejo med seboj, čigava veriga blokov bo obveljala.

Tehnologija veriženja blokov ta problem rešuje z dokazilom o delu (angl. proof-of-work, v nadaljevanju PoW). Gre za proces, pri katerem vozlišča v omrežju iščejo, katero enkratno kriptografsko število (angl. nonce) morajo dodati k danim transakcijam v posameznem bloku, da bo zgoščena vrednost tega bloka, ki jo dobijo z zgoščevalno funkcijo SHA-256, vsebovala najmanj toliko začetnih ničel (angl. leading zeroes), kot jih vnaprej določi tehnologija veriženja blokov, kot je prikazano na sliki 10. Prvo vozlišče v omrežju, ki najde enkratno kriptografsko število, uspešno izračuna zgoščeno vrednost novega bloka, za kar

dobi nagrado v obliki BTC. Nov blok doda v verigo blokov in ga naznani omrežju. Iskanje enkratnega kriptografskega števila je časovno zelo potratna računska operacija. Ko najde enkratno kriptografsko število, vozlišče dokaže, da je v iskanje vložilo ogromno dela, zato Satoshi Nakamoto ta postopek imenuje PoW (Nakamoto, 2008).

Slika 10: Iskanje enkratnega kriptografskega števila



Prirejeno po Nakamoto (2008).

To, kar Satoshi Nakamoto v beli knjigi imenuje dokazilo o delu, danes imenujemo rudarjenje (angl. mining). Vozliščem v omrežju zato pravimo tudi rudarji. Iskanje enkratnega kriptografskega števila vsa vozlišča v omrežju odvrača od zlonamernih dejanj. Nobenemu vozlišču se ne splača spreminjati preteklih transakcij, ker bi moralo vložiti ogromno dela, da bi ponovno izračunalo zgoščene vrednosti blokov in s tem nadaljevalo zlonamerno verigo blokov, pri čemer bi zgoščene vrednosti morale vsebovati najmanj toliko začetnih ničel, kot bi jih vnaprej določila tehnologija veriženja blokov. Vozlišča enkratno kriptografsko število iščejo s strojno opremo. Čeprav bi morda sklepali, da je za strojno opremo to lahka naloga, temu ni tako. Proces je zahteven. Strojna oprema išče enkratno kriptografsko število neprestano, dokler ne najde tistega enkratnega kriptografskega števila, ki z zgoščevalno funkcijo SHA-256 generira zgoščeno vrednost novega bloka, ki vsebuje najmanj toliko začetnih ničel, kot jih vnaprej določi tehnologija veriženja blokov. Rudarjenje je pravzaprav reševanje računske uganke, ki jo je stežka rešiti, vendar zlahka preveriti (The Blockchain Review, brez datuma).

Zahtevano število začetnih ničel za nov blok je različno, vendar identično za vsa vozlišča in je znano vsem vozliščem v omrežju. Zahtevano število začetnih ničel je odvisno od tega, koliko vozlišč v omrežju trenutno rudari (Nakamoto, 2008). Če je interes za rudarjenje velik, potem je zahtevano večje število začetnih ničel, kar pomeni, da je težje najti enkratno kriptografsko število in uspešno izračunati zgoščeno vrednost novega bloka. Če je interes za rudarjenje majhen, potem je zahtevano manjše število začetnih ničel, kar pomeni, da je lažje najti enkratno kriptografsko število in uspešno izračunati zgoščeno vrednost novega bloka. Temu pravimo stopnja težavnosti (angl. difficulty rate). Stopnja težavnosti določa zahtevano število začetnih ničel in se posodobi na vsakih 2016 blokov. Cilj tehnologije veriženja blokov je, da je nov blok v verigo blokov dodan na približno 10 minut (Walker, 2015).

Sicer obstaja teoretična možnost, da vozlišče spremeni verigo blokov in zlonamerno verigo blokov tudi nadaljuje, kar imenujemo 51 % napad (angl. 51 % attack), vendar v praksi zelo malo verjetno. Namreč, za izvedbo 51 % napada potrebujemo večino strojne računske moči

(angl. mining hash rate) v omrežju, kar pomeni, da je potreben velik finančni vložek v strojno opremo, ki bo generirala ob visokih cenah energentov, ki smo jim priča v času pisanja magistrskega dela, ekstremno visok račun za električno energijo. Tehnologija veriženja blokov je zasnovana tako, da vozlišča v omrežju kot veljavno verigo blokov vedno sprejmejo najdaljšo verigo blokov. Če oseba v omrežju namerava spremeniti verigo blokov, mora imeti vsaj 51 % strojne računske moči, da lahko sama nadaljuje zlonamerno verigo blokov, ki bo najdaljša veriga blokov, da bo v omrežju sprejeta kot veljavna (Walker, 2019).

Torej je računanje zgoščenih vrednosti blokov vse prej kot hitro, enostavno in poceni. Gre za časovno, energetsko in finančno zelo potraten proces. Luki, Maji in Nini se ne splača spreminjati preteklih transakcij, ker bi vsak, ki bi spremenil transakcijo, moral ponovno izračunati zgoščene vrednosti spremenjenega bloka in vseh naslednjih blokov, če bi želel nadaljevati zlonamerno verigo blokov, pri čemer bi zgoščeno vrednost uspešno izračunal šele, ko bi za vsak posamezen blok našel tako enkratno kriptografsko število, da bi zgoščena vrednost posameznega bloka, ki bi jo dobil z zgoščevalno funkcijo SHA-256, vsebovala najmanj toliko začetnih ničel, kot bi jih vnaprej določila tehnologija veriženja blokov. Nadalje, da bi uspešno nadaljeval zlonamerno verigo blokov, bi moral imeti 51 % strojne računske moči.

1.8 Omrežje

Kot smo do zdaj spoznali, omrežje deluje po naslednjem principu (Nakamoto, 2008):

1. Nove transakcije so naznanjene vozliščem v omrežju.
2. Vsako vozlišče zbere nove transakcije v nov blok.
3. Vsako vozlišče išče enkratno kriptografsko število za nov blok.
4. Ko eno izmed vozlišč najde enkratno kriptografsko število za nov blok, uspešno izračuna zgoščeno vrednost novega bloka, za kar dobi nagrado v obliki BTC. Nov blok doda v verigo blokov in ga naznani omrežju.
5. Ostala vozlišča sprejmejo blok kot veljaven le, če so vse transakcije v njem veljavne.
6. Vozlišča izrazijo sprejetje novega bloka v verigo blokov s tem, da začnejo iskati enkratno kriptografsko število za naslednji blok, pri čemer uporabijo zgoščeno vrednost ravnokar sprejetega bloka kot enega izmed vhodnih podatkov v zgoščevalno funkcijo SHA-256 za računanje zgoščene vrednosti naslednjega bloka.

Kot rečeno, vozlišča v omrežju vedno kot veljavno verigo blokov sprejmejo najdaljšo verigo blokov, ki jo potem nadaljujejo. Če dve vozlišči naznanita v omrežje dva različna nova bloka istočasno, potem lahko ostala vozlišča prejmejo bodisi en blok bodisi drug blok. Gre za primer, ko dve vozlišči istočasno najdeta enkratno kriptografsko število in sta omrežju istočasno naznanjena dva nova bloka (Meyer, 2022c). V tem primeru posamezno vozlišče nadaljuje verigo blokov na podlagi tistega bloka, ki ga je prejelo, vendar shrani tudi drugo vejo verige blokov v primeru, da tista druga veja verige blokov postane najdaljša veriga blokov. V trenutku, ko je v verigo blokov dodan naslednji blok, postane jasno, katera od teh

dveh vej je najdaljša. Vsa vozlišča, ki so nadaljevala tisto verigo blokov, ki je zdaj postala krajša veriga blokov, prenehajo z nadaljevanjem te verige blokov in preklopijo na najdaljšo verigo blokov (Nakamoto, 2008).

Pri točki 1 je treba poudariti, da ni nujno, da so nove transakcije naznanjene prav vsem vozliščem v omrežju, da bi bile dodane v nov blok. Dovolj je, da so nove transakcije naznanjene večini vozlišč (Nakamoto, 2008). Omrežje namreč ni popolno, ker se vozlišča obnašajo različno, zato se lahko zgodi, da nove transakcije ne pridejo do vseh vozlišč (Meyer, 2022c).

Pri točki 4 je treba poudariti, da ni nujno, da je nov blok naznanjen prav vsem vozliščem v omrežju. Lahko se zgodi, da katero od vozlišč ne prejme novega bloka takoj, ko je bil dodan v verigo blokov. Vozlišče lahko ugotovi, da je zgrešilo vmesni blok, vendar šele, ko prejme naslednji blok. V tem primeru bo vozlišče zgrešen blok od ostalih vozlišč prekopiralo naknadno (Nakamoto, 2008). V praksi je tako, da ni nujno, da je vozlišče vedno dosegljivo omrežju. Vozlišče se lahko kadar koli ugasne. Ko se znova prižge, vozlišče ugotovi, da je zgrešilo vmesne bloke in jih prekopira od ostalih vozlišč (Meyer, 2022c).

Torej delovanje omrežja ni pogojeno z delovanjem vseh vozlišč v omrežju, temveč mora delovati večina vozlišč.

1.9 Spodbude

Posameznik, ki se odloči, da se bo pridružil omrežju in vzpostavil svoje vozlišče, bo v to moral vlagati svoj čas, energijo in denar. V kolikor posameznik nima interesa rudariti, ampak samo naložiti verigo blokov na svoj računalnik, je vložek neprimerljivo manjši. Gre za tako imenovano polno vozlišče (angl. full node) (Bitstamp, 2021). V kolikor posameznik ima interes rudariti, je vložek neprimerljivo večji. Gre za tako imenovano rudarsko vozlišče (angl. mining node) (Bitstamp, 2021). Polno vozlišče je torej vozlišče, ki hrani celotno verigo blokov in na disku zavzame veliko prostora. Rudarsko vozlišče je polno vozlišče, pri čemer se poleg hranjenja celotne verige blokov išče še enkratno kriptografsko število in s tem dodaja nove bloke v verigo blokov (Cryptopedia, 2021).

V primeru rudarskega vozlišča gre za konkretno investicijo. Višina investicije je sicer odvisna od ambicij posameznika. Najprej je treba kupiti strojno opremo, s katero se bo rudarilo. Strojna oprema za svoje delovanje porablja električno energijo, kar se bo izrazito poznalo na računu za električno energijo. Potrebno je seveda tehnično znanje in poznavanje strojne opreme, da se lahko sploh začne rudariti in da se opremo vzdržuje v primeru okvar, ki se bodo tekom rudarjenja zagotovo dogajale. Vložiti je potrebno ogromno resursov, da bo vse potekalo kot je treba. Postavimo si lahko vprašanje, zakaj bi se posameznik sploh odločil za rudarjenje, če gre za ogromen vložek resursov. Tehnologija veriženja blokov v ta namen pozna spodbude za rudarje.

Bitcoin tehnologija veriženja blokov (v nadaljevanju BTC tehnologija veriženja blokov) pozna dve vrsti spodbud (Nakamoto, 2008):

- spodbuda v obliki BTC-jev (angl. block reward) in
- spodbuda v obliki transakcijske provizije (angl. transaction fee).

Obe vrsti spodbud dobi tisto vozlišče, ki najde enkratno kriptografsko število in s tem doda nov blok v verigo blokov.

Spodbude obstajajo iz treh razlogov. Prvič, da vozlišča vzdržujejo omrežje. Spodbude pritegnejo posameznike, da vzpostavijo svoja vozlišča in začnejo rudariti. Brez spodbud se iz zgoraj opisanih razlogov ne bi nikomur splačalo rudariti, ker bi šlo zgolj za neracionalno porabo resursov. Drugič, da v obtok prihajajo novi BTC-ji. Tehnologija veriženja blokov ne pozna centralizirane institucije, ki bi izdajala BTC-je, zato morajo priti v obtok na drug način. Vsakič, ko eno izmed vozlišč najde enkratno kriptografsko število in s tem doda nov blok v verigo blokov, dobi za nagrado BTC-je. V tistem hipu pravzaprav v obtok pridejo novi BTC-ji. Tretjič, da vozlišča nimajo razloga za izvajanje zlonamernih dejanj. V trenutku, ko posameznik ali skupina posameznikov pridobi večino strojne računske moči, izbira med izkoriščanjem strojne računske moči za izvajanje zlonamernih dejanj ali izkoriščanjem strojne računske moči za pridobivanje BTC-jev kot nagrad. Spodbuda v obliki BTC-jev vozlišča spodbuja k temu, da sodelujejo v omrežju na pošten način. Bolj se jim splača strojno računsko moč izkoriščati za rudarjenje in s tem pridobivanje BTC-jev, kot za izvajanje zlonamernih dejanj. Gre za to, da se vozliščem ne splača spodkopavati sistema, katerega del so sami (Nakamoto, 2008).

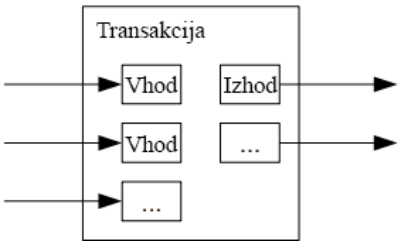
Spodbuda v obliki transakcijske provizije obstaja zato, ker ima BTC veriga blokov vnaprej fiksno določeno največjo možno ponudbo Bitcoinov, in sicer 21 milijonov BTC (Binance Academy, brez datuma b). To pomeni, da ko bo vseh 21 milijonov BTC v obtoku, ob novem dodanem bloku v verigo blokov vozlišče več ne bo dobilo novih BTC-jev kot nagrado, temveč bo njegova nagrada sestavljena le še izključno iz transakcijskih provizij (Nakamoto, 2008). Pomen transakcijskih provizij se povečuje skozi čas, četudi še ni vseh BTC-jev v obtoku. Namreč, začetna nagrada za nov dodan blok v verigo blokov je bila 50 BTC. Nagrada se razpolovi (angl. halving) vsakih 210.000 blokov, kar je približno vsake 4 leta, če upoštevamo, da se nov blok v verigo blokov doda v povprečju na vsakih 10 minut. Nagrada se torej periodično razpolavlja (50 BTC, 25 BTC, 12,5 BTC, 6,25 BTC itd.). Z vsako razpolovitvijo dobi transakcijska provizija nekoliko večji pomen, ker je nagrada v obliki BTC manjša (Meyer, 2020d).

1.10 Združitev in razdelitev vrednosti

Tehnologija veriženja blokov sicer omogoča, da se vsak BTC pri transakciji obravnava ločeno, vendar bi to bilo nesmiselno. BTC-ji se pri transakcijah lahko združijo ali razdelijo.

Tehnologija veriženja blokov zato pri transakcijah pozna vhode (angl. inputs) in izhode (angl. outputs), kot je prikazano na sliki 11 (Nakamoto, 2008).

Slika 11: Vhodi in izhodi transakcije



Prirejeno po Nakamoto (2008).

Danes to karakteristiko delovanja tehnologije veriženja blokov poznamo pod besedno zvezo nepotrošeni transakcijski izhod (angl. unspent transaction output, v nadaljevanju UTXO). Gre za zmožnost, da lahko BTC-je pri transakcijah združimo ali razdelimo po potrebi. Pri fiat valutah to ni mogoče. Npr., ni mogoče 5 kovancev za 1 EUR cent združiti v 1 kovanec za 5 EUR centov (Meyer, 2022).

Vzemimo za primer naslednjo transakcijo:

- vhodi: 5 BTC + 2,23 BTC + 2,1 BTC in
- izhodi: 8,5 BTC + 0,83 BTC.

Vhodi so tisti BTC-ji, ki so pri transakciji uničeni (angl. burned), medtem ko so izhodi tisti BTC-ji, ki so pri transakciji ustvarjeni (angl. created). Pri uničenju je treba poudariti, da ne gre za to, da se število BTC-jev v obtoku zmanjša. BTC-ji se samo združijo ali razdelijo, vsota vhodov in izhodov je nespremenjena (tj. 9,33 BTC v zgornjem primeru). Vsaka transakcija torej nekaj UTXO uniči in nekaj UTXO ustvari (Meyer, 2022).

Bistvo izvajanja transakcij pri tehnologiji veriženja blokov po načelu vhodov in izhodov najlažje opišemo na naslednjem primeru. Npr., imamo 1 BTC in hočemo nekomu poslati 0,1 BTC. V tem primeru ne bomo poslali samo 0,1 BTC, ampak bomo poslali 1 BTC, pri čemer se bo 0,9 BTC vrnilo v našo denarnico (Meyer, 2022).

Transakcija bi zgledala takole:

- vhodi: 1 BTC in
- izhodi: 0,1 BTC + 0,9 BTC.

Pri izhodih ni formalne razlike med nakazilom prejemniku in razliko, ki se vrne pošiljatelju. Ko pogledamo zgornji primer, bi 0,9 BTC lahko predstavljalo bodisi nakazilo prejemniku bodisi razliko, ki se vrne pošiljatelju. Šele, ko pogledamo naslove denarnic (v nadaljevanju

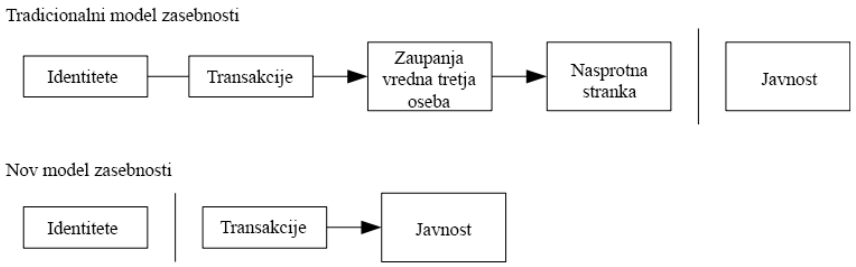
naslov) sodelujočih v transakciji, lahko ugotovimo, kaj je nakazilo prejemniku in kaj razlika, ki se vrne pošiljatelju (Meyer, 2022).

V praksi programska oprema, npr. Bitcoin Core, shranjuje UTXO v svojo lokalno bazo podatkov. Preprečevanje dvojne potrošnje se zagotavlja tako, da morajo biti pred potrditvijo vsake transakcije vsi njeni vhodi nepotrošeni, torej morajo biti pred potrditvijo vsake transakcije vsi njeni vhodi v lokalni UTXO bazi podatkov. Če jih ni, to pomeni, da so vhodi že bili potrošeni v preteklosti in gre za poskus dvojne potrošnje (Meyer, 2022).

1.11 Zasebnost

Tradicionalni finančni sistem zasebnost zagotavlja tako, da omeji dostop do informacij le na obe stranki v postopku in zaupanja vredno tretjo osebo. Pri tehnologiji veriženja blokov so sicer vse transakcije javno dostopne vsakomur, vendar je zasebnost vseh oseb v omrežju še vedno zagotovljena, in sicer z anonimnostjo javnih ključev. Javnost lahko vidi, ko nekdo pošlje nekomu določeno količino BTC, vendar ne ve, kdo je lastnik enega javnega ključa in kdo lastnik drugega javnega ključa. Gre za razliko med tradicionalnim modelom zasebnosti in novim modelom zasebnosti, ki ga uporablja tehnologija veriženja blokov, kot je prikazano na sliki 12 (Nakamoto, 2008).

Slika 12: Tradicionalni model zasebnosti in nov model zasebnosti



Prirejeno po Nakamoto (2008).

Vseeno obstaja tveganje, da se javno razve, kdo je lastnik posameznega javnega ključa. Iz tega razloga je smiselno za vsako transakcijo ustvariti nov par ključev. V kolikor se javno razve, kdo je lastnik posameznega javnega ključa, se v tem primeru ne more tega lastnika povezati z ostalimi transakcijami (Nakamoto, 2008).

2 »POBARVANI KOVANCI«

Leta 2013 Yoni Assia, Vitalik Buterin, M Liorhakilior, Meni Rosenfeld in Rotem Lev javno objavijo belo knjigo z naslovom Colored coins whitepaper. Avtorji bele knjige se sprašujejo, ali ima BTC tehnologija veriženja blokov še kakšno drugo aplikativno vrednost. Sprašujejo se, ali se lahko kriptografsko PoW kot temelj za vzdrževanje razpršene knjige transakcij uporabi še za kaj drugega, kot za BTC. Zaključijo, da se lahko tehnologija veriženja blokov

uporabi za vse, kar izpolnjuje dva pogoja. Prvič, gre za digitalno premoženje (angl. digital asset). Drugič, gre za tekmovalno dobrino (angl. rivalrous good), kar pomeni, da je njen lastnik lahko istočasno le en posameznik. Težava je v tem, da BTC tehnologija veriženja blokov tega potenciala ni predvidela in ne omogoča uporabe BTC tehnologije veriženja blokov za nič drugega kot za izvrševanje transakcij BTC. Avtorji zaključijo, da je potrebna nadgradnja BTC tehnologije veriženja blokov (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013).

Poudariti je potrebno, da je bela knjiga pravzaprav povzetek idej, ki so se v javnosti začele pojavljati že leto pred njenim nastankom. Smatra se, da Yoni Assia prvi predstavi idejo pobarvanih kovancev, ko leta 2012 na svojem blogu napiše članek z naslovom Bitcoin 2.X (aka Colored Bitcoin) – initial specs. Za tem istega leta Meni Rosenfeld objavi dokument z naslovom Overview of Colored Coins. Oba pozneje sodelujeta kot soavtorja pri izdaji bele knjige (Steinwold, 2019).

2.1 Potencial Bitcoin tehnologije veriženja blokov

Nadgradnja BTC tehnologije veriženja blokov, ki jo predstavijo avtorji bele knjige, je sestavljena iz dveh slojev. Prvi sloj predstavlja sistem transakcij, ki temelji na kriptografiji. Drugi sloj predstavlja sistem izdajanja raznoraznih unikatnih instrumentov, ki jih avtorji imenujejo »pobarvani kovanci« (angl. colored coins) (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013).

Prvi sloj ni nič novega, saj BTC tehnologija veriženja blokov za svoje delovanje uporablja identičen sistem. Drugi sloj je fundamentalna inovacija, ki jo avtorji predstavijo v beli knjigi (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013). Sicer Yoni Assia leta 2012 na svojem blogu piše le o možnosti izdajanja različnih kriptovalut na osnovi BTC tehnologije veriženja blokov, vendar je leta 2013 ideja v beli knjigi razširjena na možnost izdajanja raznoraznih unikatnih instrumentov, ne le na izdajanje različnih kriptovalut (Assia, 2012).

Avtorji predpostavijo, da če lahko z nadgradnjo BTC tehnologije veriženja blokov izdajamo unikatne instrumente, potem obstaja mnogo primerov uporabe v praksi (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013):

- izdajanje delnic (angl. share issuance),
- izdajanje lokalne valute (angl. community currency),
- izdajanje korporativne valute (angl. corporate currency),
- izdajanje depozitne valute (angl. deposit currency),
- obstoj pametne lastnine (angl. smart property),
- obstoj digitalnih zbirateljskih predmetov (angl. digital collectibles),
- ponujanje dostopa in naročniških storitev (angl. access and subscription services) itd.

2.2 Ideja »pobarvanih kovancev«

Avtorji bele knjige predstavijo idejo »pobarvanega kovanca« kot BTC, ki mu izdajatelj doda eno »barvo«, pri čemer izdajatelj postavi obveznosti in pravice do lastnikov »pobarvanih kovancev« določene »barve«. Obstajajo torej »nepobarvani kovanci« (tj. BTC) in »pobarvani kovanci« (tj. BTC z dodano določeno »barvo«). »Barva« je mišljena le metaforično. V praksi ne gre za dobesedno barvanje kovancev, ker BTC tako ali tako ne obstaja v fizični obliki, temveč je »barva« določena s simbolom in unikatno zgoščeno vrednostjo (Rosenfeld, 2012).

Izdajatelj »pobarvanega kovanca« ga lahko pošlje prejemniku in slednji ga lahko pošlje naprej, pri čemer mora biti zagotovljeno dvoje. Prvič, »pobarvan kovanec« ob pošiljanju ne sme izgubiti »barve«. Ne sme se zgoditi, da bi pošiljatelj poslal »pobarvan kovanec«, prejemnik pa bi dobil »nepobarvan kovanec«. Drugič, »nepobarvan kovanec« ob pošiljanju ne sme pridobiti »barve«. Ne sme se zgoditi, da bi lahko posameznik postal lastnik »pobarvanega kovanca« na noben drug način, kot da je kovanec že bil »pobarvan«, ko ga je prejel. Pravzaprav gre za to, da nihče ne sme biti sposoben naknadno »pobarvati« kovanca, razen izdajatelj v trenutku izdaje (Rosenfeld, 2012).

2.3 Izdajanje »pobarvanih kovancev«

»Pobarvan kovanec« nastane v prvotni transakciji (angl. genesis transaction). Izdajatelj določeno količino svojega BTC-ja da na stran in ga uporabi v prvotni transakciji »pobarvanega kovanca«. To je trenutek, ko BTC postane »pobarvan kovanec«. Vrednost »pobarvanega kovanca« izhaja iz vrednosti BTC-ja, ki je bil uporabljen za njegov nastanek, pri čemer menjalno razmerje med BTC in »pobarvanim kovancem« ni nujno 1:1. Določeno je poljubno, in sicer v trenutku izdaje »pobarvanega kovanca« (Assia, 2012).

2.3.1 Vhodi

Kar se tiče vhodov prvotne transakcije, obstajata dva primera. Prvič, »pobarvan kovanec« je lahko »barve«, ki je ni mogoče ponovno izdati (angl. non-reissuable colors). V tem primeru vhod ni pomemben, ker izdajatelj po izdaji tako ali tako nima več nobenega vpliva, ker »pobarvanega kovanca« ne more več ponovno izdati. Drugič, »pobarvan kovanec« je lahko »barve«, ki jo je mogoče ponovno izdati (angl. reissuable colors). V tem primeru mora izdajatelj izbrati en naslov, ki bo namenjen izdajanju »pobarvanih kovancev« določene »barve« in nastaviti vhod 0 tako, da prihaja iz tega naslova. Pozneje, v kolikor se izdajatelj odloči za ponovno izdajo »pobarvanih kovancev« določene »barve«, še enkrat izvede prvotno transakcijo z istim naslovom na vhodu 0. Posamezen naslov je lahko uporabljen za izdajanje le enega »pobarvanega kovanca« določene »barve«, ki ga je mogoče ponovno izdati in če je posamezen naslov uporabljen za izdajanje »pobarvanega kovanca« določene »barve«, ki ga je mogoče ponovno izdati, ga ni več mogoče uporabiti za izdajo katerega koli

»pobarvanega kovanca« določene »barve«, ki ga ni mogoče ponovno izdati (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013).

Naslov, torej par ključev, ki je namenjen izdajanju »pobarvanih kovancev« določene »barve«, ki jih je možno ponovno izdati, mora biti varen. V kolikor napadalec pridobi dostop do tega naslova, ima neomejeno možnost ponovnega izdajanja »pobarvanih kovancev« te »barve«. Za varnost se lahko poskrbi z več podpisnim (angl. multi-signature) sistemom potrjevanja transakcij. Pri več podpisnem sistemu 2-od-3 (angl. 2-of-3), obstajajo 3 pari ključev, pri čemer morata biti ob podpisu transakcije uporabljena vsaj 2 para ključev. Še bolj varen je več podpisni sistem 3-od-5 (angl. 3-of-5). Ne glede na število parov ključev, ki so potrebni za podpis transakcije, morajo biti privatni ključi shranjeni v hladni denarnici (angl. cold wallet). Naslov, ki je namenjen izdajanju »pobarvanih kovancev« določene »barve«, ki jih ni možno ponovno izdati, ni nujno, da je varen, ker je ponovna izdaja tako ali tako onemogočena. V primeru, da izdajatelj nekaj »pobarvanih kovancev« določene »barve«, ki jih ni mogoče ponovno izdati, zadrži sam, mora upoštevati identična varnostna pravila kot pri »pobarvanih kovancih«, ki jih je mogoče ponovno izdati (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013).

2.3.2 Izhodi

Kar se tiče izhodov prvotne transakcije, posamezen »pobarvan kovanec« določene »barve« ob izdaji vsebuje skupino izhodov, ki jih lahko razdelimo v tri skupine. Prvič, izhodi prejemnikov, ki bodo prejeli »pobarvan kovanec« določene »barve«. Drugič, OP_RETURN izhod, ki lahko vsebuje 40 bitov metapodatkov o »pobarvanih kovancih« določene »barve«. Namesto, da bi se protokol »pobarvanega kovanca« določene »barve« vezal na vhode in izhode transakcij, se protokol zapiše v OP_RETURN izhod. V OP_RETURN izhod se v bitih torej zapišejo »barva«, verzija protokola, politika ponovnega izdajanja in ostali neobvezni podatki. Tretjič, en ali več izhodov, ki pošljejo razliko »pobarvanih kovancev« določene »barve« nazaj k izdajatelju (Assia, Buterin, Liorhakilior, Rosenfeld & Rotem, 2013).

2.4 Distribucija »pobarvanih kovancev«

V prvi fazi ima vse »pobarvane kovance« določene »barve« v lasti izdajatelj. V drugi fazi imajo vse »pobarvane kovance« določene »barve« v lasti prejemniki. Prehod iz prve faze v drugo fazo imenujemo distribucija. Po koncu distribucije izdajatelj nima več centralizirane vloge in na »pobarvane kovance« ne more vplivati na noben način, saj so v rokah prejemnikov, ki lahko z njimi počnejo kar koli želijo. Za konec distribucije se šteje trenutek, ko izdajatelj pošlje še zadnji »pobarvani kovanec« določene »barve« prejemniku in nima v lasti več nobenega »pobarvanega kovanca« te »barve« (Assia, 2012).

2.5 Preverjanje »pobarvanih kovancev«

Ker je zgodovina vseh transakcij pri tehnologiji veriženja blokov zabeležena večno in ker »pobarvani kovanci« temeljijo na njej, lahko za vsak posamezen BTC kadar koli preverimo, ali je »pobarvan« ali »nepobarvan«. To naredimo tako, da gremo po verigi transakcij nazaj. Če je posamezen BTC v kateri koli prejšnji transakciji bil uporabljen v prvotni transakciji »pobarvanega kovanca« katere koli »barve«, potem gre za »pobarvan kovanec«. Če posamezen BTC ni v nobeni prejšnji transakciji bil uporabljen v prvotni transakciji »pobarvanega kovanca« katere koli »barve«, potem gre za »nepobarvan kovanec«, torej za navaden BTC (Assia, 2012).

Kot smo že ugotovili, sta fundamentalni enoti pri BTC transakciji vhod in izhod. Izdajatelj »pobarvanega kovanca« torej označi en ali več BTC izhodov kot pripadajočih določeni »barvi« in vsak izhod katerega koli posameznika v prihodnosti, ki nas po verigi transakcij pripelje nazaj do teh izhodov, ki jih je izdajatelj označil kot pripadajoče določeni »barvi«, pripada tej »barvi«. Preverjanje, ali je posamezen izhod »pobarvan« ali »nepobarvan« pomeni, da rekurzivno preverimo vhode tega izhoda. Če nas vhodi pripeljejo do prvotne transakcije »pobarvanega kovanca« katere koli »barve«, potem je ta izhod »pobarvan«. Če nas vhodi ne pripeljejo do nobene prvotne transakcije »pobarvanega kovanca« katere koli »barve«, potem je ta izhod »nepobarvan« (Rosenfeld, 2012).

2.6 Redkost »pobarvanih kovancev«

Dejstvo, da »pobarvani kovanci« temeljijo na osnovi BTC tehnologije veriženja blokov in da obstaja način za identifikacijo »pobarvanih kovancev«, pomeni dvoje. Prvič, ker je »pobarvan kovanec« le BTC z dodano določeno »barvo«, se lahko za pošiljanje »pobarvanih kovancev« uporablja BTC omrežje. Drugič, ker je vsak »pobarvan kovanec« BTC in hkrati ni vsak BTC »pobarvan kovanec«, gre pri »pobarvanih kovancih« za redke kovance (angl. rare coins), čigar vrednosti so različne od vrednosti BTC, upoštevajoč njihovo menjalno razmerje, odvisno od ponudbe in povpraševanja po »pobarvanih kovancih« določene »barve« (Assia, 2012).

3 ETHEREUM TEHNOLOGIJA VERIŽENJA BLOKOV

Leta 2014 Vitalik Buterin javno objavi belo knjigo z naslovom Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. V njej napiše, da je tako kot BTC, če ne celo bolj, pomembna sama tehnologija veriženja blokov, na kateri BTC temelji. Kot alternativne možnosti uporabe tehnologije veriženja blokov omeni finančne instrumente, NFT-je, pametne pogodbe in decentralizirane avtonomne organizacije (Buterin, 2014).

3.1 Pametne pogodbe

BTC tehnologija veriženja blokov kot taka, brez nadgradnje, omogoča obstoj nekakšne šibke različice pametnih pogodb. Pametna pogodba je pogodba, ki je izražena v programskem jeziku in določa, kateri pogoji morajo biti izpolnjeni, da se transakcija med dvema strankama izvede. Torej, UTXO se lahko lastijo ne le s parom ključev, temveč tudi s skripto programske kode, torej s pametno pogodbo (Buterin, 2014).

Preprost primer pametne pogodbe na podlagi BTC tehnologije veriženja blokov je več podpisni sistem potrjevanja transakcij. V tem primeru se v skripti določi pogoj, da je transakcija uspešno izvedena le, če se za podpis uporabita najmanj dva od treh parov ključev, v kolikor se npr. uporabi sistem 2-od-3 (Buterin, 2014).

Vitalik Buterin (2014) v beli knjigi izpostavi, da ima BTC tehnologija veriženja blokov nekaj omejitev, ki onemogočajo obstoj kompleksnejših pametnih pogodb:

- Turingova nepopolnost (angl. Turing incompleteness), saj BTC tehnologija npr. ne podpira uporabe zank pri programiranju pametnih pogodb,
- nedeljivost UTXO (angl. value blindness), saj BTC tehnologija veriženja blokov ne omogoča, da bi oseba A, ki ima v lasti 1 BTC in bi rada osebi B poslala le 0,1 BTC, lahko poslala le 0,1 BTC, ampak mora poslati 1 BTC in razliko 0,9 BTC prejme kot razliko nazaj v svojo denarnico (vhod: 1 BTC, izhod 1: 0,1 BTC v denarnico osebe B, izhod 2: 0,9 BTC v denarnico osebe A),
- pomanjkanje stanja (angl. lack of state), saj BTC tehnologija veriženja blokov pozna samo dve stanji (tj. izhod je lahko potrošen ali nepotrošen) in
- nepoznavanje verige blokov (angl. blockchain blindness), saj BTC tehnologija veriženja blokov ne omogoča, da bi UTXO lahko poznali podatke verige blokov (enkratno kriptografsko število, časovni žig, zgoščena vrednost prejšnjega bloka itd.).

Zgoraj našteta dejstva onemogočajo obstoj kompleksnejših (npr. večstopenjskih) pametnih pogodb na podlagi BTC tehnologije veriženja blokov.

3.2 Možnosti izboljšave Bitcoin tehnologije veriženja blokov

Vitalik Buterin (2014) vidi tri možnosti, ki bi odpravile zgoraj opisane omejitve BTC tehnologije veriženja blokov in omogočile obstoj kompleksnejših pametnih pogodb:

- razvoj nove tehnologije veriženja blokov,
- razvoj skript, ki bi temeljile na BTC tehnologiji veriženja blokov ali
- razvoj meta protokola, ki bi temeljil na BTC tehnologiji veriženja blokov.

Izbere prvo možnost in tako nastane nova tehnologija veriženja blokov, in sicer Ethereum tehnologija veriženja blokov (v nadaljevanju ETH tehnologija veriženja blokov). Ustvarjalci

razvijejo ETH tehnologijo veriženja blokov kot alternativni protokol za programiranje pametnih pogodb in decentraliziranih aplikacij, pri čemer je poudarek na hitrem razvojnem času, varnosti in učinkoviti interakciji med različnimi aplikacijami. S tem obstoj kompleksnejših pametnih pogodb ni več nemogoč (Buterin, 2014).

ETH tehnologija veriženja blokov ima preko svojega edinstvenega fundamentalnega nivoja (angl. layer) vgrajen Turing popoln programski jezik, ki omogoča programiranje pametnih pogodb in decentraliziranih aplikacij, pri čemer se poljubno določi, pod katerimi pogoji se bo transakcija izvršila (Bistarelli, Mazzante, Micheletti, Mostarda & Tiezzi, 2019). Ravno Turingova popolnost (angl. Turing completeness), deljivost UTXO (angl. value awareness), poznavanje stanja (angl. state) in poznavanje verige blokov (angl. blockchain awareness) je tisto, kar ločuje ETH od BTC tehnologije veriženja blokov in omogoča obstoj kompleksnejših pametnih pogodb na podlagi ETH tehnologije veriženja blokov (Buterin, 2014).

Obstajajo tri vrste aplikacij, ki se jih lahko gradi na podlagi ETH tehnologije veriženja blokov. Prvič, finančne aplikacije, pri katerih izstopa monetarna vloga (podvalute, izvedeni finančni instrumenti, pogodbe o varovanju pred tveganji, varčevalne denarnice, oporoke itd.). Drugič, polfinančne aplikacije, pri katerih je poleg monetarne vloge izražena tudi nemonetarna vloga (npr. nagrade za rešitve računalniških problemov). Tretjič, nefinančne aplikacije, pri katerih izstopa nemonetarna vloga (npr. decentralizirano upravljanje in glasovanje) (Buterin, 2014).

3.3 Računi

Pri ETH tehnologiji veriženja blokov stanje (angl. state) sestavljajo računi (angl. accounts), ki vsebujejo naslednje (Buterin, 2014):

- enkratno kriptografsko število (angl. nonce),
- trenutno stanje Ether (v nadaljevanju ETH) na računu (angl. account's current Ether balance),
- pogodbeno programsko kodo računa (angl. account's contract code), če obstaja in
- shrambo računa (angl. account's storage), ki je privzeto prazna.

ETH je pri ETH tehnologiji veriženja blokov uporabljen za plačevanje transakcijske provizije (angl. transaction fee), tako kot je za plačevanje transakcijske provizije pri BTC tehnologiji veriženja blokov uporabljen BTC (Buterin, 2014).

V glavnem obstajata dve vrsti računov. Prvič, računi v zunanji lasti (angl. externally owned accounts), ki jih nadzorujejo zasebni ključi. Drugič, pogodbeni računi (angl. contract accounts), ki jih nadzoruje njihova programska koda (Vujičić, Jagodić & Ranđić, 2018). Računi v zunanji lasti nimajo programske kode, zato lahko z računa v zunanji lasti sporočila pošiljamo le tako, da ustvarimo transakcijo in jo podpišemo z zasebnim ključem. Pogodbeni

računi imajo programsko kodo, zato se vsakič, ko pogodbeni račun dobi sporočilo, njegova programska koda izvede, pri čemer se bere in piše v shrambo, kar omogoča pošiljanje drugih sporočil in ustvarjanje pametnih pogodb (Buterin, 2014).

Poudariti je potrebno, da pogodbenih računov ne smemo razumeti kot nekaj, kar mora nujno biti izpolnjeno, temveč kot nekakšne avtonomne agente, ki živijo v ETH verigi blokov in vedno izvedejo isto programsko kodo, ko dobijo sporočilo. Pogodbeni računi, torej pametne pogodbe, imajo direktno kontrolo nad samim seboj (Buterin, 2014).

3.4 Transakcije

Pri ETH tehnologiji veriženja blokov transakcija (angl. transaction) pomeni podatkovni paket (angl. data package), podpisan z zasebnim ključem, v katerem je shranjeno sporočilo, ki je bilo poslano z računa v zunanji lasti. Transakcija vsebuje naslednje (Buterin, 2014):

- prejemnika sporočila,
- podpis, ki identificira pošiljatelja,
- znesek ETH, ki ga pošiljatelj pošlje prejemniku,
- neobvezno podatkovno polje,
- vrednost STARTGAS, ki predstavlja maksimalno število računskih korakov, ki jih lahko izvedba transakcije opravi in
- vrednost GASPRICE, ki predstavlja transakcijsko provizijo, ki jo pošiljatelj plača za vsak računski korak.

Prve tri točke so nujne za pošiljanje katere koli kriptovalute, ne samo za pošiljanje ETH. Neobvezno podatkovno polje privzeto nima tako pomembne funkcije. Zadnji dve točki sta kritični za preprečevanje pomotnih ali zlonamernih zank v programski kodi in preprečevanje izvajanja druge nepotrebne programske kode (Buterin, 2014).

Transakcijska provizija se imenuje gorivo (angl. gas), s katerim se plača za izvedbo računskih korakov. Bolj kompleksni računski koraki ali računski koraki, ki zahtevajo zapis večje količine podatkov v stanje, zahtevajo plačilo večje transakcijske provizije, torej več goriva (Zarir, Oliva, Jiang & Hassan, 2021). Ideja je, da vsak posameznik, ki od ETH tehnologije veriženja blokov zahteva več, naj tudi plača več provizije (Buterin, 2014).

3.5 Sporočila

Pri ETH tehnologiji veriženja blokov je sporočilo (angl. message) podobno kot transakcija, le da sporočilo generira pametna pogodba, torej je poslano s pogodbenega računa. Sporočilo vsebuje naslednje (Buterin, 2014):

- pošiljatelja sporočila,
- prejemnika sporočila,

- znesek ETH,
- neobvezno podatkovno polje in
- vrednost STARTGAS, ki predstavlja maksimalno število računskih korakov, ki jih lahko izvedba transakcije opravi.

Sporočilo se generira, ko pametna pogodba izvede CALL programsko kodo, ki generira in izvede sporočilo. Sporočilo se pošlje prejemniku, ki izvede svojo programsko kodo. Na tak način pametne pogodbe komunicirajo med seboj tako, kot lahko komunicirajo med seboj zunanji posamezniki (Buterin, 2014).

3.6 Dokazilo o deležu

Leta 2022 ETH tehnologija veriženja blokov zamenja PoW za dokazilo o deležu (angl. proof-of-stake, v nadaljevanju PoS) kot način potrjevanja blokov (angl. consensus mechanism). Od tega trenutka naprej se ETH tehnologija veriženja blokov in BTC tehnologija veriženja blokov bistveno razlikujeta. Torej, ETH tehnologija veriženja blokov od leta 2022 naprej za potrjevanje blokov uporablja PoS, medtem ko BTC tehnologija veriženja blokov od začetka do danes še vedno uporablja PoW. PoS ima v primerjavi PoW naslednje prednosti (Ethereum, 2022a):

- manjšo porabo električne energije za vzdrževanje omrežja,
- nižjo vstopno oviro, ker ni potrebe po dragi in konkurenčni strojni opremi,
- zmanjšana stopnja centralizacije,
- večja stopnja participacije zaradi manjše porabe električne energije in
- visoke finančne sankcije za nepoštene rudarje.

Pri PoW rudarji v procesu potrjevanja blokov dokažejo, da tvegajo kapital preko potrošene električne energije, medtem ko pri PoS rudarji v procesu potrjevanja blokov dokažejo, da tvegajo kapital v obliki ETH. Namreč, vsak rudar, ki želi potrjevati ETH bloke, mora kot depozit dati 32 ETH v depozitno pogodbo in zagnati programsko opremo, ki omogoča potrjevanje blokov. Rudar na tak način veže svoj kapital, ki služi kot zavarovanje (angl. collateral), kar pomeni, da se mu ne splača obnašati nepošteno. V kolikor bi se rudar obnašal nepošteno, se lahko njegovo zavarovanje uniči, kar pomeni, da izgubi svoj kapital (Ethereum, 2022a).

Pri PoW je hitrost dodajanja novih blokov v verigo blokov uravnavana preko zahtevnosti rudarjenja, medtem ko je pri PoS hitrost dodajanja novih blokov fiksna. Čas pri PoS je razdeljen na reže (angl. slots), ki štejejo 12 sekund in epohe (angl. epochs), ki štejejo 32 rež. V vsaki reži je naključno izbran en rudar, ki je predlagatelj bloka. Ta rudar je odgovoren za ustvarjanje novega bloka in njegovo pošiljanje ostalim vozliščem v omrežje. Prav tako je v vsaki reži naključno izbran odbor potrjevalcev (angl. committee of validators), ki glasujejo za veljavnost novega bloka. Rudarji za sodelovanje pri potrjevanju blokov prejmejo nagrado

v obliki ETH. Njihov vložek (angl. staked balance) se poveča z vsako pridobljeno nagrado (Ethereum, 2022a).

Posameznik, ki se odloči, da bo postal rudar, mora zagotoviti stabilno sodelovanje pri potrjevanju blokov, kar pomeni, da mora skrbeti za strojno in programsko opremo. Gre za obvezo, torej za dolžnost in ne za pravico. Rudar ne dobi nagrade v obliki ETH, če ne sodeluje, ko je naključno izbran. V kolikor se rudar obnaša nepošteno, se lahko njegovo zavarovanje uniči. Obstajata dve vrsti obnašanja, ki se smatrata kot nepošteno. Prvič, kadar rudar v isti reži predlaga več kot 1 blok. Drugič, kadar rudar o novem bloku da nasprotujoče si glasove (Ethereum, 2022a).

Finančna kazen je odvisna od tega, koliko ostalih rudarjev se je v približno enakem času obnašalo nepošteno, kar imenujemo korelacijska kazen (angl. correlation penalty). Finančna kazen je lahko majhna (npr. uničenje 1 % zavarovanja, v kolikor je bil kaznovan samo 1 rudar), ali velika (npr. uničenje 100 % zavarovanja, v kolikor gre za množično kaznovanje). V skrajnem primeru se nepoštenega rudarja lahko izključi iz omrežja. Obdobje prisilnega izstopa se začne s takojšnjo kaznijo do 0,5 ETH 1. dan, korelacijsko finančno kaznijo 18. dan in izključitvijo iz omrežja 36. dan. Nenamerno ali namerno neodziven rudar (npr. v primeru sabotaže) vsak dan prejme manjšo finančno kazen, ker je prisoten v omrežju, vendar ne oddaja glasov, torej ne sodeluje. Posledično bi usklajen napad bil izredno drag za napadalca. Sicer je 51 % napad pri PoS še vedno teoretično možen, vendar v praksi zelo malo verjeten. Namreč, napadalec bi moral biti lastnik 51 % vseh zavarovanj, kar bi v procesu glasovanja zlorabil tako, da bi njegova odcepljena veriga blokov dobila največ glasov. Omrežje sprejme kot veljavno verigo blokov tisto, ki prejme največ glasov, kar pomeni, da bi napadalec lahko svojo odcepljeno verigo blokov naredil kot veljavno. V tem primeru lahko omrežje sproži protinapad, v katerem se pošteni rudarji zmenijo, da ignorirajo napadalčevo nepošteno odcepljeno verigo blokov. Prav tako lahko napadalcu uničijo njegovo zavarovanje v celoti in ga izključijo iz omrežja. Torej se napadalcu ne splača poskušati izvesti napada (Ethereum, 2022a).

4 NEZAMENLJIVI ŽETONI

NFT je potrdilo o lastništvu digitalnega premoženja, ki temelji na tehnologiji veriženja blokov, najpogosteje na ETH tehnologiji veriženja blokov. Z ETF-ji se trguje na tako imenovanih NFT tržnicah, npr. OpenSea. NFT-ji se pogosto kupujejo in prodajajo v kriptovalutah in ne v fiat valutah, npr. v ETH. Lastništvo posameznega NFT-ja je zabeleženo s pametno pogodbo (angl. smart contract). Javnost se je za trg NFT-jev začela masovno zanimati šele leta 2021, ko sta število kupoprodajnih poslov in cena NFT-jev, tako kot trg kriptovalut, poletela v nebo, čeprav začetek NFT-jev sega že v leto 2012 (Nadini in drugi, 2021).

Bistvo NFT-jev izhaja že iz njihovega imena. Vsaka stvar je bodisi zamenljiva (angl. fungible) bodisi nezamenljiva (angl. non-fungible). Slednje lahko razložimo na primeru kovanca fiat valute in umetniškega dela. Kovanec za 1 EUR je zamenljiv, ker nima unikatnih lastnosti. Vrednost mu ne določajo unikatne lastnosti, ampak njegova nominalna vrednost. Če dve osebi zamenjata kovanec za 1 EUR, nobena od njiju ni niti na boljšem niti na slabšem. Umetniško delo je nezamenljivo, ker ima unikatne lastnosti. Vrednost mu določajo njegove unikatne lastnosti. Tako kot umetniško delo so tudi NFT-ji nezamenljivi (Ethereum, 2022b).

4.1 Primerjava današnjega spleta in spleta nezamenljivih žetonov

Današnji splet in NFT splet imata pomembne razlike, kot je prikazano v tabeli 2 (Ethereum, 2022b).

Tabela 2: Primerjava današnjega spleta in NFT spleta

Današnji splet	**NFT splet**
Kopija dokumenta je enaka originalu.	Kopiranje NFT-ja ni mogoče.
Podatki o lastništvu digitalnega premoženja so shranjeni na strežnikih, ki jih nadzirajo institucije, torej moramo institucijam zaupati na besedo.	Podatki o lastništvu digitalnega premoženja so javno shranjeni v verigi blokov, torej lastništvo lahko javno vsakdo preveri.
Institucije za nudenje produktov in storitev morajo zgraditi in zagotavljati nemoteno delovanje lastne infrastrukture.	Institucije za nudenje produktov in storitev uporabljajo ETH tehnologijo veriženja blokov.
Nudenje produktov in storitev ni kompatibilno z drugimi platformami, ker ima vsaka institucija lastno infrastrukturo.	Nudenje produktov in storitev je kompatibilno z drugimi platformami, ker vse institucije uporabljajo ETH tehnologijo veriženja blokov.
Ustvarjalci vsebin se zanašajo na platforme, ki so podvržene regulatornim restrikcijam, zato ni nujno, da jim je dostopen celoten globalen trg.	Ustvarjalci vsebin se zanašajo na platforme, ki niso podvržene regulatornim restrikcijam, zato jim je dostopen celoten globalen trg.
Platforme pri prodaji digitalnih vsebin pogosto zaračunajo zajetne provizije, zato ustvarjalci vsebin nimajo toliko ekonomske svobode.	Platforme pri prodaji digitalnih vsebin sicer računajo provizije, vendar lahko ustvarjalci vsebin ohranijo lastniško pravico in dobijo honorar ob vsaki nadaljnji preprodaji njihovih digitalnih vsebin (angl. royalties).

Vir: Ethereum (2022b).

4.2 Standardi nezamenljivih žetonov

ETH tehnologija veriženja blokov pozna več standardov, med najpomembnejši so (Ethereum, 2022c):

– ERC-20,

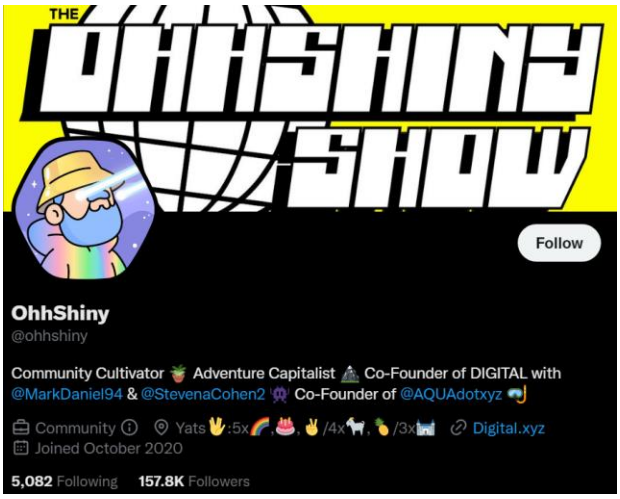
– ERC-721,
– ERC-777,
– ERC-1155 in
– ERC-4626.

Najpomembnejša standarda sta ERC-20 in ERC-721. Za zamenljive žetone (tj. kriptovalute) se uporablja ERC-20, za nezamenljive žetone (tj. NFT-je) se uporablja ERC-721. Standard ERC-777 je nadgradnja ERC-20 in se uporablja za razvoj dodatnih funkcionalnosti za NFT-je, kot je npr. izboljšana anonimnost in funkcija izhoda v sili, v kolikor posameznik izgubi privatni ključ. Standard ERC-1155 se uporablja za zniževanje transakcijskih stroškov tako zamenljivih žetonov (npr. kriptovaluta BNB) kot nezamenljivih žetonov (npr. NFT kolekcija CryptoPunks) (Ethereum, 2022c).

4.3 Kategorije nezamenljivih žetonov

Profilni NFT-ji (angl. profile pictures NFTs – PFP NFTs) je kategorija, kjer se posamezen NFT lahko uporabi kot profilno sliko na družbenih omrežjih in je javnosti verjetno najbolj znana kategorija. Na tak način lastnik javnosti pokaže, da je lastnik posameznega NFT-ja. Družbeno omrežje Twitter v okviru plačljive storitve Twitter Blue od januarja 2022 naprej ponuja možnost preveritve lastništva posameznega NFT-ja. Namreč, načeloma lahko kdor koli zajame sliko zaslona posameznega NFT-ja in jo nastavi kot profilno sliko na svojem Twitter profilu, vendar se samo dejanskemu lastniku okrog profilne slike pojavi šest-kotni lik, kot je prikazano na sliki 13. Za namen preverjanja lastništva mora posameznik svoj Twitter profil povezati s svojo denarnico. Ker ima dostop do denarnice le njen lastnik, lahko le lastnik dokaže lastništvo posameznega NFT-ja. Če vidimo šest-kotni lik okrog profilne slike na Twitter profilu, to pomeni, da je posameznik dejansko lastnik tega NFT-ja, kar je dokazal tako, da je povezal svojo denarnico s svojim Twitter profilom (George, 2022).

Slika 13: Profilni NFT uporabnika @ohhshiny na Twitterju



Vir: OhhShiny (brez datuma).

Primer profilnih NFT-jev je NFT kolekcija CryptoPunks, ki je prikazana na sliki 14. Kolekcijo leta 2017 izda podjetje Larva Labs. Gre za 10.000 avatarjev, ki so unikatni in temeljijo na ETH tehnologiji veriženja blokov, natančneje na standardu ERC-721. Posamezen avatar je lahko last le enega posameznika, pri čemer je lastništvo zabeleženo v ETH verigi blokov. Na začetku je lahko vsak posameznik z denarnico brezplačno zaprosil za avatarja, vendar je hitro bilo podarjenih vseh 10.000 avatarjev. Njihovo število je do danes ostalo fiksno, zato jih je danes možno kupiti le še na sekundarnem trgu, kjer dosegajo vrtoglave vrednost. Najdražji kupoprodajni posel kadar koli je bil sklenjen 12. februarja 2022, in sicer CryptoPunk #5822 je bil prodan za 8.000 ETH oz. 23,7 milijonov USD. V času pisanja magistrskega dela je najcenejši CrpytoPunk #4117 na voljo za 65,1 ETH oz. 103.408,74 USD (Larva Labs, a).

Slika 14: NFT kolekcija CryptoPunks

Vir: Larva Labs (brez datuma a).

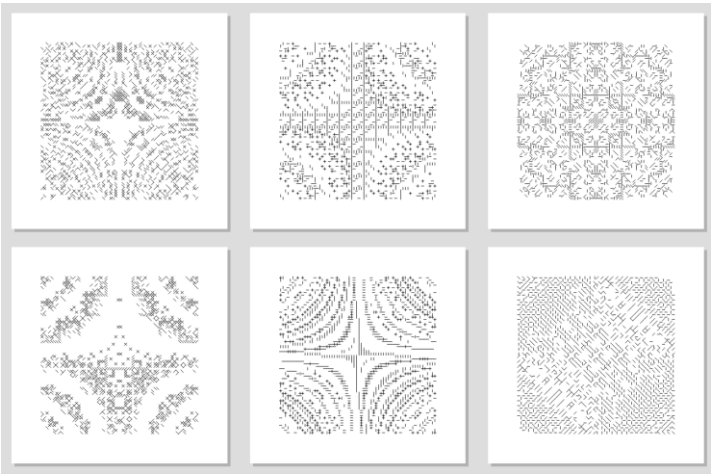
Naslednji primer profilnih NFT-jev je NFT kolekcija Bored Ape Yacht Club, ki je prikazana na sliki 15. Kolekcijo leta 2021 izda podjetje Yuga Labs. Kolekcija se v marsičem zgleduje po kolekciji CryptoPunks, le da gre za počlovečene opice, torej drug motiv. Novost v primerjavi s kolekcijo CryptoPunks je to, da lastništvo NFT-ja iz kolekcije Bored Ape Yacht Club prinaša dodatne ugodnosti. Recimo, v preteklosti so lastniki NFT-ja iz kolekcije Bored Ape Yacht Club dobili zastonj NFT iz kolekcije Bored Ape Kennel Club. Lastništvo NFT-ja iz kolekcije Bored Ape Yacht Club zagotavlja ekskluzivno članstvo v zaprti skupnosti, od koder izvira tudi beseda »Club« v imenu (George, 2022).

Slika 15: NFT kolekcija Bored Ape Yacht Club

Vir: Yuga Labs (brez datuma).

Umetniški NFT-ji (angl. art NFTs) so kategorija, kjer posamezen NFT predstavlja umetniško delo. Gre za umetniška dela razno raznih zvrsti, med katerimi je npr. generativna umetnost (angl. generative art). Generativna umetnost je računalniško ustvarjanje digitalnih slik, kjer se s pomočjo algoritmov kreirajo slike, ki imajo znotraj kolekcije nekatere skupne značilnosti (barve, oblike, vzorce, motive itd.). Kljub temu, da imajo slike znotraj kolekcije skupne značilnosti, je vsaka slika unikat. Umetnik v računalniškem programu vnaprej določi pravila, pri čemer algoritem kreira slike tako, da pravila uporabi naključno (Marcobello, 2022). Primer umetniških NFT-jev je NFT kolekcija Autoglyphs, ki je prikazana na sliki 16. Kolekcijo leta 2019 izda podjetje Larva Labs. Slike so bile ustvarjene v programskem jeziku Solidity, ki je jezik za programiranje Ethereum pametnih pogodb. Koda znotraj pametne pogodbe je samostojno kreirala naključna umetniška dela (Larva Labs, brez datuma b).

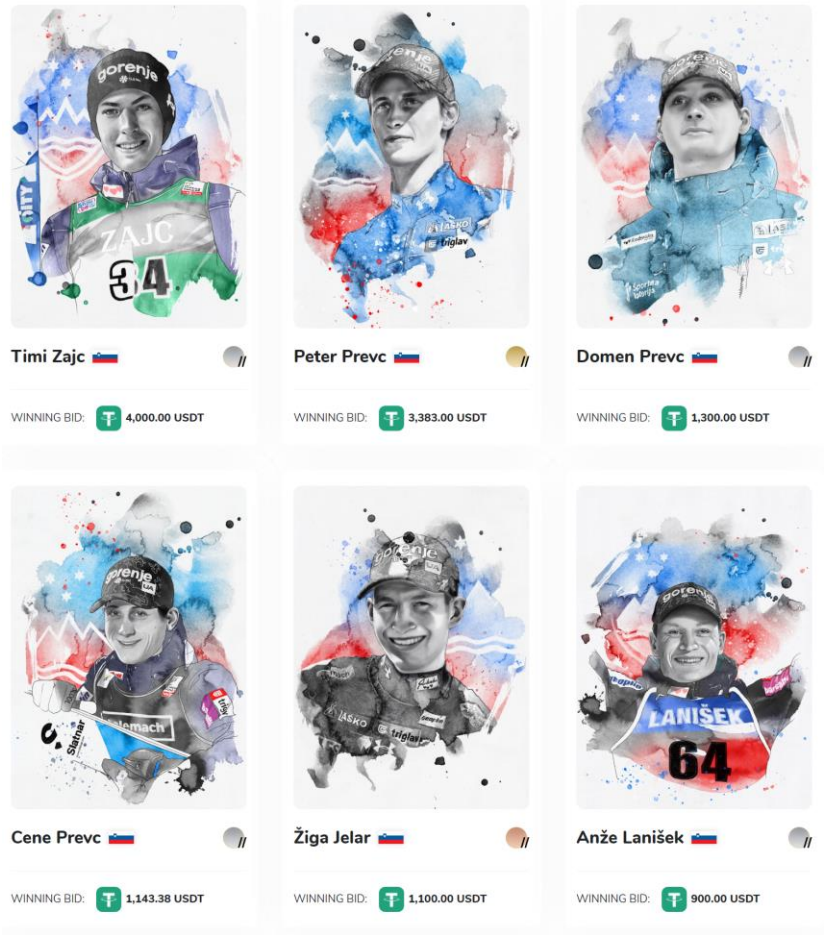
Slika 16: NFT kolekcija Autoglyphs



Vir: Larva Labs (brez datuma b).

Zbirateljski NFT-ji (angl. collectibles NFTs) so kategorija, kjer NFT-ji sestavljajo posamezno kolekcijo. Primer je NFT kolekcija Planica NFT – Planica 2022, ki je prikazana na sliki 17, natančneje je na njej prikazana slovenska reprezentanca znotraj te kolekcije. Kolekcijo leta 2022 izda organizator planiških smučarskih skokov v času, ko se dogodek v živo odvija v Planici. Organizator pravi, da gre za pionirski projekt, saj so se prvič v zgodovini združili NFT-ji s katerim koli zimskim športom. Kolekcija je bila prodana za 37.060,62 USDT. Šlo je za dražbo, pri čemer je posameznik lahko oddal ponudbo za enega ali več NFT-jev znotraj kolekcije. Najvišji ponudnik je postal lastnik posameznega NFT-ja, s katerimi se danes trguje na sekundarnem trgu. Ilustracije smučarskih skakalcev je narisal slovenski ilustrator Mitja Bokun (Planica, brez datuma).

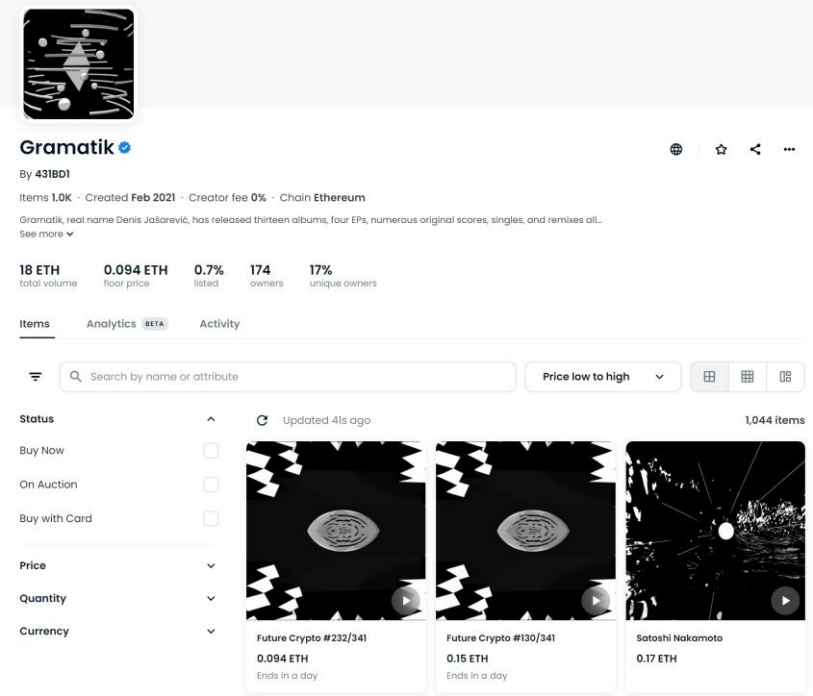
Slika 17: Slovenska reprezentanca znotraj NFT kolekcije Planica NFT – Planica 2022



Vir: Planica (brez datuma).

Glasbeni NFT-ji (angl. music NFTs) so kategorija, kjer posamezen NFT predstavlja glasbeno delo. Primer je zgodba slovenskega glasbenika Gramatika, ki leta 2021 v 5-minutni dražbi svojih dveh še neizdanih pesmih zasluži 1,3 milijona EUR in si s tem pokrije izpad dohodka, ki ga kot glasbenik utrpi leta 2020 zaradi protikoronskih ukrepov. Gramatik svoje izdelke še danes prodaja na NFT tržnici OpenSea, kot je prikazano na sliki 18 (TSmedia, medijske vsebine in storitve, 2021).

Slika 18: Uporabniški profil Gramatika na NFT tržnici OpenSea



Vir: OpenSea (brez datuma).

Spominski NFT-ji (angl. souvenir NFTs) so kategorija, kjer posameznik dobi ali kupi spominek v obliki NFT-ja. Primer je slovenska predstavitev na EXPO DUBAI leta 2020. Slovenija kot prva država na svetu izda NFT kolekcijo, in sicer EXPO DUBAI 2020. Kolekcijo sestavlja 14 različnih NFT-jev v obliki 3D fotografij, ki predstavljajo Slovenijo (npr. Kranjska čebela, ki je prikazana na sliki 19). Vsakdo lahko za spominek na spletni strani zaprosi zastonj. Namen izdaje kolekcije je promocija Slovenije, ki poudari njene naravne znamenitosti in hkrati pokaže sledenje tehnološkim trendom (Tehnološki park Ljubljana, 2021).

Slika 19: NFT z motivom Kranjske čebele znotraj NFT kolekcije EXPO DUBAI 2020

Vir: ifeelsLOVEnia NFT (brez datuma).

NFT-ji z dodatno uporabno vrednostjo (angl. utility NFTs) so kategorija, kjer posameznik poleg lastništva NFT-ja dobi še »nekaj več«. Primer je slovenski projekt Ballies, ki je prikazan na sliki 20. Gre za NFT platformo, ki združuje NFT-je in strast do športa. Cilj projekta je približati znane športnike njihovim oboževalcem. Ustvarjalci projekta sklepajo pogodbe z znanimi športniki, kot je npr. Dino Rađa, ki postanejo njihovi ambasadorji. V kolikor si lastnik NFT-ja in kupiš vstopnico za košarkarsko tekmo, dobiš npr. 15 min druženja po tekmi z znanim košarkarjem, s katerim so ustvarjalci projekta sklenili pogodbo (Tehnološki park Ljubljana, 2022).

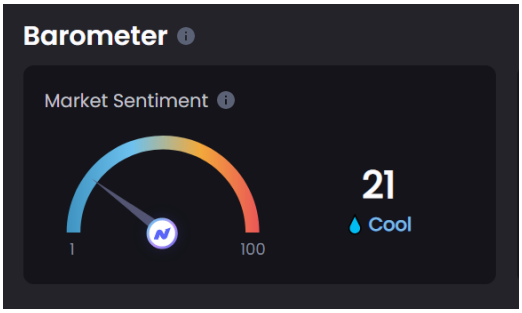
Slika 20: NFT znotraj NFT kolekcije Ballies

Vir: Ballies (brez datuma).

4.4 Analiza trenutnega stanja trga nezamenljivih žetonov

V času pisanja magistrskega dela so globalni finančni trgi v medvedjem trendu (angl. bear market), kar velja tudi za trg kriptovalut in posledično tudi za trg NFT-jev. Sentiment na trgu NFT-jev je dne 30. oktobra 2022 negativen, kot je prikazano na sliki 21. Sentiment je izračunan na podlagi nihajnosti cene, obsega trgovanja, sentimenta na družbenih omrežjih in Google Trends (NFTGo, brez datuma).

Slika 21: Sentiment na trgu NFT-jev dne 30. oktober 2022



Vir: NFTGo (brez datuma).

Tržna kapitalizacija trga NFT-jev je v zadnjih nekaj mesecih padla in dne 15. oktobra 2022 znaša 22,46 milijard USD, medtem ko je obseg trgovanja drastično padel na samo 169 milijonov USD v obdobju 3 tednov, kot je prikazano na sliki 29 v prilogi 1. Tržna kapitalizacija je izračunana kot vsota tržnih kapitalizacij vseh NFT kolekcij, ki so zabeležene na spletni strani NFTGo, pri čemer so domnevni pralni posli (angl. wash trades) izvzeti. Obseg trgovanja je izračunan kot vsota obsega trgovanja vseh NFT kolekcij, ki so zabeležene na spletni strani NFTGo znotraj določenega časovnega obdobja, pri čemer so domnevni pralni posli izvzeti (NFTGo, brez datuma).

Število denarnic, ki držijo NFT-je (angl. holders), se zadnjih nekaj let vztrajno povečuje, tudi v času trenutnega medvedjega trga. Število denarnic, ki trgujejo z NFT-ji (angl. traders), se je povečevalo v zadnjem bikovskem trgu (angl. bull market), vendar je vidno izrazito zmanjševanje, ko je januarja 2022 nastopil medvedji trg. Število denarnic, ki kupujejo (angl. buyers), je v zadnjem bikovskem trgu prevladovalo nad denarnicami, ki prodajajo (angl. sellers), vendar je v trenutnem medvedjem trgu situacija ravno obratna, kot je prikazano na sliki 30 v prilogi 1. Število denarnic, ki držijo NFT-je, je definirano kot število unikatnih denarnic, ki držijo NFT-je vseh NFT kolekcij, ki so zabeležene na spletni strani NFTGo. Število denarnic, ki trgujejo z NFT-ji, je definirano kot število unikatnih denarnic, ki so kupile ali prodale vsaj en NFT izmed vseh NFT kolekcij, ki so zabeležene na spletni strani NFTGo znotraj določenega časovnega obdobja, pri čemer so domnevni pralni posli izvzeti. Število denarnic, ki kupuje NFT-je, je definirano kot število unikatnih denarnic, ki so kupile vsaj en NFT izmed vseh NFT kolekcij, ki so zabeležene na spletni strani NFTGo znotraj določenega časovnega obdobja, pri čemer so domnevni pralni posli izvzeti. Število denarnic, ki prodajajo NFT-je, je definirano kot število unikatnih denarnic, ki so prodale vsaj en NFT izmed vseh NFT kolekcij, ki so zabeležene na spletni strani NFTGo znotraj določenega časovnega obdobja, pri čemer so domnevni pralni posli izvzeti (NFTGo, brez datuma).

Največjo tržno kapitalizacijo glede na NFT kategorijo imajo profilni NFT-ji, katerih tržna kapitalizacija dne 30. oktobra 2022 znaša 13,01 milijard USD. Drugo največjo tržno kapitalizacijo imajo zbirateljski NFT-ji, katerih tržna kapitalizacija dne 30. oktobra 2022 znaša 3,18 milijard USD. Tretjo največjo tržno kapitalizacijo imajo NFT-ji z dodatno uporabno vrednostjo, katerih tržna kapitalizacija dne 30. oktobra 2022 znaša 1,98 milijard USD, kot je prikazano na sliki 31 v prilogi 1 (NFTGo, brez datuma).

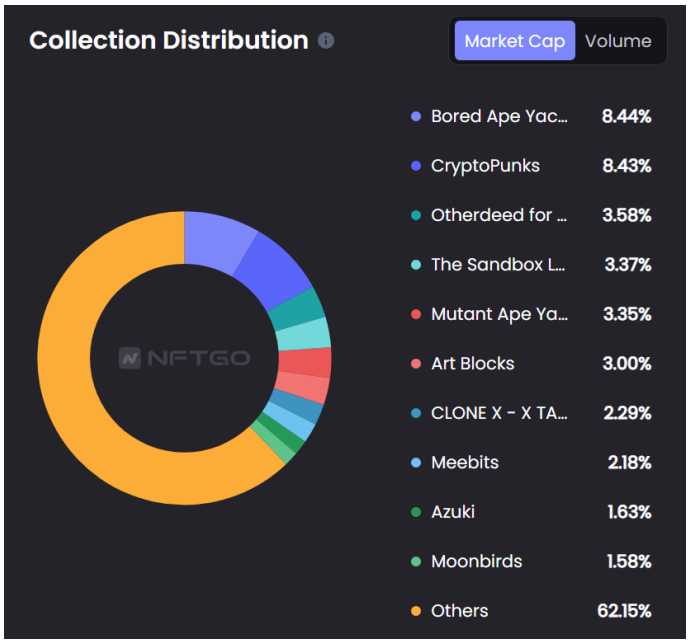
Največji obseg trgovanja glede na NFT kategorijo imajo profilni NFT-ji, katerih obseg trgovanja do dne 30. oktobra 2022 znaša 22,09 milijard USD. Drugi največji obseg trgovanja imajo zbirateljski NFT-ji, katerih obseg trgovanja do dne 30. oktobra 2022 znaša 4,86 milijard USD. Tretji največji obseg trgovanja imajo NFT-ji z dodatno uporabno vrednostjo, katerih obseg trgovanja do dne 30. oktobra 2022 znaša 3,38 milijard USD, kot je prikazano na sliki 32 v prilogi 1 (NFTGo, brez datuma).

Največjo likvidnost glede na NFT kategorijo imajo NFT-ji z dodatno uporabno vrednostjo, katerih povprečna likvidnost do dne 30. oktobra 2022 znaša 538,98 %. Drugo največjo

likvidnost imajo profilni NFT-ji, katerih povprečna likvidnost do dne 30. oktobra 2022 znaša 154,56 %. Tretjo največjo likvidnost imajo športni NFT-ji (angl. sport NFTs), katerih povprečna likvidnost do dne 30. oktobra 2022 znaša 129,84 %, kot je prikazano na sliki 33 v prilogi 1 (NFTGo, brez datuma).

Če pogledamo relativno, je največja NFT kolekcija glede na tržno kapitalizacijo dne 30. oktobra 2022 kolekcija Bored Ape Yacht Club, ki predstavlja 8,44 % tržne kapitalizacije vseh NFT kolekcij. Druga največja NFT kolekcija glede na tržno kapitalizacijo dne 30. oktobra 2022 je kolekcija CryptoPunks, ki predstavlja 8,43 % tržne kapitalizacije vseh NFT kolekcij. Tretja največja NFT kolekcija glede na tržno kapitalizacijo dne 30. oktobra 2022 je kolekcija Otherdeed for Otherside, ki predstavlja 3,58 % tržne kapitalizacije vseh NFT kolekcij, kot je prikazano na sliki 22 (NFTGo, brez datuma).

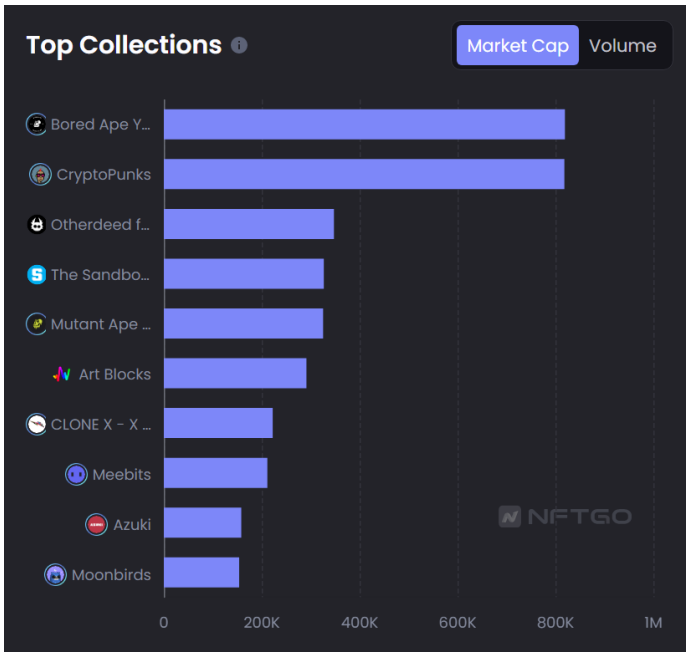
Slika 22: NFT kolekcije glede na tržno kapitalizacijo dne 30. oktober 2022 [v %]



Vir: NFTGo (brez datuma).

Če pogledamo absolutno, dne 30. oktobra 2022 tržna kapitalizacija kolekcije Bored Ape Yacht Club znaša 819.341,68 ETH, tržna kapitalizacija kolekcije CryptoPunks znaša 818.232,69 ETH in tržna kapitalizacija kolekcije Otherdeed for Otherside znaša 347.518,56 ETH, kot je prikazano na sliki 23 (NFTGo, brez datuma).

Slika 23: NFT kolekcije glede na tržno kapitalizacijo dne 30. oktober 2022 [v ETH]



Vir: NFTGo (brez datuma).

5 PROBLEMATIKA PONAREJANJA POTRDIL

Potrdilo je dokument, s katerim posameznik dokaže, da je usvojil določeno znanje. Posamezniku potrdilo omogoča, da pridobi poklic in s tem v družbi prevzame določeno vlogo. V kolikor posameznik predloži potrdilo, ne da bi izpolnil vse zahtevane pogoje za pridobitev le-tega, gre za ponaredek. Ponarejanje potrdil povzroča nezanemarljivo škodo celotni družbi, predvsem zato, ker načenja načelo zaupanja, na katerem sistem potrdil, kot ga poznamo danes, temelji (Sayed, 2019).

5.1 Začetki ponarejanja

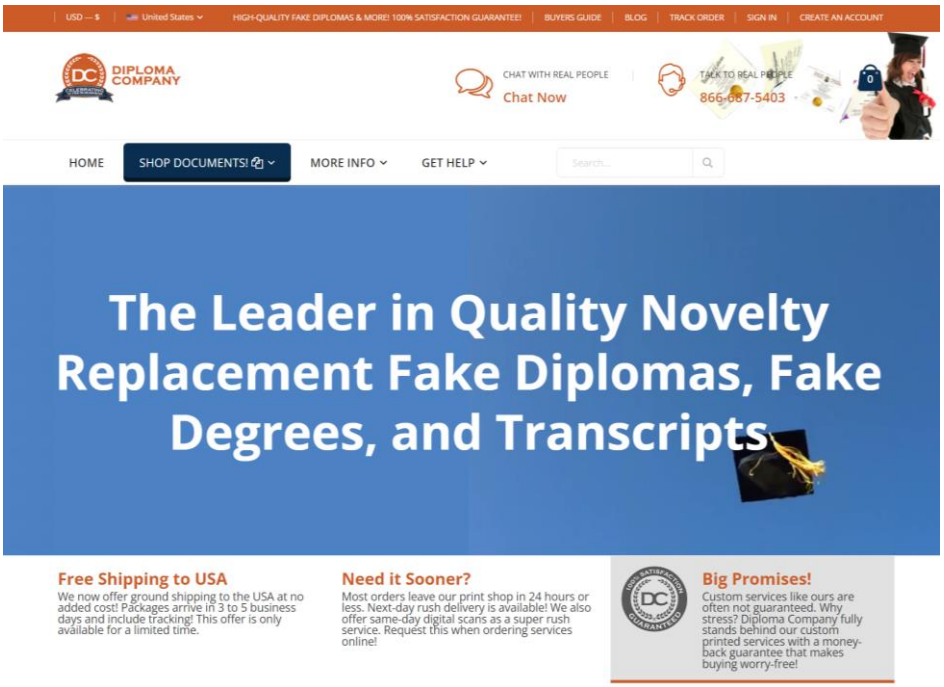
Robert de Sorbonne leta 1257 ustanovi Collège de Sorbonne, ki šteje kot ena izmed prvih pomembnih izobraževalnih ustanov takratne srednjeveške pariške univerze. V 14. stoletju se kot najboljša knjižnica v Evropi smatra ravno knjižnica Univerze v Parizu, v katero imajo vstop le doktoranti. Univerza v Oxfordu in Univerza v Cambridgeu v tistem času nimata tako dobrih knjižnic kot je pariška univerzitetna knjižnica, čeprav prav tako ponujata doktorski študij. Ljudje hitro ugotovijo, da bi jim ponaredek doktorata z Univerze v Oxfordu ali Cambridgeu omogočil vstop v knjižnico Univerze v Parizu. Posledično se začnejo v družbi pojavljati ponarejeni doktorati z Univerze v Oxfordu in Cambridgeu. To obdobje se nekako smatra kot začetek masovnega ponarejanja potrdil (Ezell, 2019).

5.2 Industrija ponarejanja

Ponarejanje potrdil je danes globalna, več milijardna industrija, ki iz leta v leto raste. Ne obstaja institucija, ki bi uradno beležila število podjetij, ki se trenutno ukvarjajo s ponarejanjem potrdil, vendar ocene strokovnjakov kažejo na trenutno vsaj 5.000 aktivnih tovarn diplom (angl. diploma mills) in 1.500 akreditacijskih tovarn (angl. accreditation mills). Trg ponarejanja potrdil je tako velik, da obstajajo celo spletne strani, ki ocenjujejo tovarne diplom po kakovosti njihovih storitev (Ezell, 2019).

Že leta 1986 John Bear v svojem članku razpravlja o tem, kako tehnologija omogoča ponarejanje potrdil in takrat je bilo govora o uporabi seznamov elektronske pošte (angl. mailing list), prilagojenih pismih (angl. personalized letters) in vse večji dostopnosti zmogljivih tiskalnikov (Bear, 1986). Svetovni splet v zadnjih dveh desetletjih omogoča obstoj tovarn diplom kot virtualnih šol. Spletne strani tovarn diplom so moderne, s slikami mogočnih stavb »njihovih« izobraževalnih institucij in polne smejočih obrazov »njihovih« študentov. Tovarna diplom je danes tipično le spletna trgovina, ki prodaja ponarejena potrdila, kot je prikazan primer na sliki 24 (Ezell, 2019).

Slika 24: Primer tovarne diplom



Vir: DiplomaCompany (brez datuma).

5.3 Tovarne diplom

Ameriški zakon, natančneje Zakon o možnostih visokošolskega izobraževanja (angl. The Higher Education Opportunity Act, v nadaljevanju HEOA), iz leta 2008 definira tovarno diplom kot institucijo (Ezell, 2019):

A. *(i) ki posamezniku proti plačilu ponuja potrdilo, s katerim se lahko posameznik v družbi predstavlja kot nekdo, ki je izpolnil vse zahtevane pogoje za pridobitev le-tega; in (ii) od posameznika ne zahteva nič ali malo vloženega truda, ki bi ga sicer posameznik moral vložiti za pridobitev le-tega; in*
B. *ki nima pridobljene akreditacije s strani kredibilne akreditacijske agencije ali organizacije (ki so definirane v zakonu).*

Novinarji domnevajo, da je trenutno največja tovarna diplom na svetu podjetje Axact (Ezell, 2019). Gre za pakistansko podjetje, ki naj bi obvladovalo mrežo spletnih strani, ki prodajajo ponarejena potrdila. Podjetje se sicer na svoji spletni strani predstavlja kot eno od globalno vodilnih podjetij v panogi informacijske tehnologije. The New York Times leta 2015 začne preiskavo in ugotovi, da Axact obvladuje vsaj 370 tovarn diplom. Poudari, da podjetje sicer res prodaja tudi programsko opremo, vendar je njihova osnovna dejavnost prodajanje ponarejenih potrdil (Walsh, 2015). Axact se na preiskavo odzove in pravi: »Družba Axact to zgodbo obsoja kot neutemeljeno, obrekovalno, temelječo na lažnih obtožbah, plod domišljije in objavljeno brez upoštevanja stališča družbe Axact« (The New York Times Company, 2015).

5.4 Statistika ponarejanja

Podatki iz ZDA kažejo, da je ponarejenih 6 % dodiplomskih potrdil (angl. bachelor's degree) in kar 35 % višješolskih potrdil (angl. associate degree). Večina posameznikov s ponarejenimi potrdili je izobraževalni program sicer dejansko obiskovalo, vendar le del obveznosti uspešno opravilo, kljub temu pa lažno trdijo, da so izobraževalni program uspešno opravili v celoti in pridobili potrdilo. Avtorji študije vzgibe za ponarejanje najdejo v dveh dejstvih. Prvič, ker trg dela ceni potrdila, kar se kaže v plačilnem razkoraku, saj imajo bolj izobraženi v ZDA večje osebne prihodke za opravljanje primerljivega dela, torej obstaja izobraževalna premija. Drugič, ker je študij v ZDA plačljiv, z razliko od RS, in s tem posledično nedostopen nekaterim posameznikom, ki se zatečejo k ponarejanju, ker si študija ne morejo privoščiti (Attewell & Domina, 2011).

V RS je ponarejanja sicer manj, vendar se slednje dogaja tudi pri nas. Za javne medije slovenska policija leta 2019 potrdi, da so v obdobju 5-ih let, od leta 2014 do leta 2019, obravnavali 17 primerov ponarejanja potrdil (tj. spričeval, diplomskih del, magistrskih del, doktorskih disertacij), za kar je v RS zagrožena zaporna kazen do 3 let. Kar se tiče Univerze v Ljubljani, na Naravoslovnotehniški fakulteti, Pravni fakulteti, Fakulteti za družbene vede in Ekonomski fakulteti potrdijo, da so v obdobju 10-ih let, od leta 2009 do leta 2019, odkrili posamezne primere ponarejanja potrdil.

5.5 Načini ponarejanja

Obstaja več načinov ponarejanja, nekateri so preprostejši, nekateri so zahtevnejši. Ponarejanje lahko v razdelimo v dve skupini, in sicer ponarejanje brez plačila in ponarejanje proti plačilu. V prvi skupini pri ponarejanju ne obstaja monetarna komponenta, medtem ko v drugi skupini monetarna komponenta obstaja. Razdelitev je sicer relativna, saj posameznik lahko posamezen način ponarejanja izvede bodisi brez plačila (tj. ga izvede sam) bodisi s plačilom (tj. ga zanj izvede tretja oseba). Načine ponarejanja bi lahko razdelili tudi v skupine tudi drugače, npr. glede na to, kdo je ponarejevalec (učenec, učitelj, tovarna diplom, heker itd.).

Pri tem je treba poudariti, da pri ponarejanju ne gre vedno dobesedno za ponarejanje kot tako, temveč lahko gre tudi za vzbujanje občutka velikega akademskega dosežka, ki to dejansko ni. Vzemimo za primer naslednji dve situaciji. Prvič, posameznik podkupi zaposlenega v akreditirani izobraževalni instituciji, ki zagotovi originalen žig za potrdilo. Drugič, posameznik potrdilo kupi pri tovarni diplom. V prvem primeru gre za očitno ponarejanje (tj. potrdilo ima originalen žig, čeprav posameznik ni izpolnil vseh zahtevanih pogojev za pridobitev le-tega), medtem ko v drugem primeru ne gre za očitno ponarejanje (tj. posameznik je dejansko »izpolnil« vse zahtevane pogoje za pridobitev potrdila, ker pravzaprav ne obstaja noben pogoj za pridobitev potrdila, le plačilo je potrebno). V drugem primeru potrdilo sicer ni ponarejeno, vendar nima nobene vrednosti, ker ga je izdala neakreditirana izobraževalna institucija. Gre le za vzbujanje občutka velikega akademskega dosežka, ki to dejansko ni. Kljub temu tovarne diplom smatramo kot ponarejanje potrdil, če sledimo definiciji tovarne diplom po HEOA.

Prepisovanje oz. plagiatorstvo spodaj ni našteto niti v skupini ponarejanja brez plačila niti v skupini ponarejanja proti plačilu, čeprav seveda gre za ponarejanje. Razloga, zakaj prepisovanje spodaj ni našteto, sta dva. Prvič, za ugotavljanje plagiatorstva danes obstaja programska oprema, ki preveri ujemanje posameznega zaključnega dela, torej za to obstaja rešitev. Drugič, tehnologija veriženja blokov ne more reševati problema prepisovanja, ker nima vpliva na sam proces pisanja, temveč lahko rešuje problem ponarejanja, ker ima vpliv na to, kaj se dogaja s potrdilom po izdaji.

5.5.1 Ponarejanja brez plačila

Načini ponarejanja brez plačila so naslednji (Sayed, 2019):

- posameznik na družbenem omrežju LinkedIn objavi certifikat ali trdi, da je dokončal izobraževalni program, pri čemer dejansko certifikata nikoli ni pridobil ali izobraževalnega programa nikoli ni uspešno zaključil,
- posameznik v svoj življenjepis doda certifikat ali trdi, da je dokončal izobraževalni program, pri čemer dejansko certifikata nikoli ni pridobil ali izobraževalnega programa nikoli ni uspešno zaključil,

- posameznik pri zaposlovanju v tujini namerno zavajajoče prevede originalno potrdilo, s čimer želi vzbuditi občutek večjega in/ali drugačnega akademskega dosežka, kot to dejansko je,
- posameznik ponaredi le predpogoj za pridobitev potrdila in ne potrdilo samo (npr. navede lažne podatke o delovnih izkušnjah) in/ali
- posameznik vdre v podatkovno bazo izobraževalne institucije in spremeni podatke (npr. ocene), s čimer postane upravičen do izdaje potrdila.

5.5.2 Ponarejanje proti plačilu

Načini ponarejanja proti plačilu so naslednji (Sayed, 2019):

- posameznik potrdilo kupi pri tovarni diplom ali
- posameznik podkupi zaposlenega v akreditirani izobraževalni instituciji, pri čemer:
  - zaposlen zagotovi originalen žig za potrdilo,
  - zaposlen zagotovi pozitivno oceno brez vloženega truda, ki bi ga sicer posameznik moral vložiti,
  - zaposlen sodeluje s tovarno diplom in zagotovi, da so podatki o potrdilu zabeleženi v podatkovni bazi izobraževalne institucije in/ali,
  - zaposlen spremeni podatke (npr. ocene) v podatkovni bazi izobraževalne institucije, s čimer posameznik postane upravičen do izdaje potrdila.

5.6 Primeri ponarejanja iz Slovenije in tujine

Spodaj opisani primeri iz prakse kažejo, da posamezniki s ponarejenimi potrdili nezanemarljivo vplivajo na celotno družbo. V najhujših primerih lahko pride tudi do smrtnih žrtev, ki so neposredno ali posredno posledica ponarejanja (Ezell, 2019).

5.6.1 Primer Gerald Morton Shirtcliff

William Anthony Fisher je londonski gradbeni inženir z akademsko izobrazbo. Službo dobi kot vodja gradnje sedemnadstropne stavbe v kraju Christchurch na Novi Zelandiji. Gradbišče obišče le približno enkrat na mesec. Leta 2011 se zgodi potres, ki poruši stavbo in ubije 115 ljudi, med njimi tudi otroke, ki so bili takrat v varstvu v pritličju stavbe. Preiskava pokaže, da je šlo za ponarejanje potrdila. Gerald Morton Shirtcliff je ukradel identiteto svojega znanca (tj. William Anthony Fisher) in se predstavljal z njegovo inženirsko diplomo z Univerze v Sheffieldu (Nine Entertainment, 2012).

5.6.2 Primer Anders Breivik

Anders Breivik je norveški ekstremist, ki julija 2011 detonira eksplozivno napravo v kombiju v bližini pisarne predsednika vlade v Oslu, pri čemer ubije 8 ljudi. Za tem se odpravi na otok Utøya, kjer poteka poletni tabor mladinske politične organizacije in v strelskem pohodu ubije 69 udeležencev in jih 319 rani (Buruma, 2015). Anders Breivik naj bi svoja ekstremistična dejanja financiral med drugim tudi s prodajanjem ponarejenih potrdil. Po oceni naj bi s tem zaslužil približno 630.000,00 USD (Ezell, 2019).

5.6.3 Primer Petra Sever Žveglič

Petra Sever Žveglič je zdravnica, ki dela v Splošni bolnišnici Izola. Od leta 2015 do leta 2016 kot medicinska sestra, pozneje kot zdravnica. Leta 2017 zamenja službo kot zdravnica v Splošni bolnišnici Trbovlje. Leta 2019 v javnost pride afera, saj takrat 29-letna Petra Sever Žveglič pravzaprav ni imela nobene izobrazbe, primerne za opravljanje tako poklica medicinske sestre kot poklica zdravnice. V Splošni bolnišnici Izola je bila najprej kot medicinska sestra zaposlena na podlagi fotokopije ponarejene medicinske diplome, pozneje pa kot zdravnica na podlagi fotokopije ponarejene zdravniške diplome (Slovenska tiskovna agencija, 2019a). Tožilstvo jo obsodi na pogojno kazen pet mesecev zapora s preizkusno dobo treh let (Slovenska tiskovna agencija, 2019b).

5.7 Posledice ponarejanja

Zgoraj opisani primeri iz prakse kažejo, da posledice ponarejanja nosi celotna družba, ne le posameznik, ki poseduje ponarejeno potrdilo. Posledice ponarejanja so v družbi lahko naslednje:

- posameznik s ponarejenim potrdilom v družbi pridobi slabo ime,
- izobraževalni sistem utrpi upad vpisa,
- delodajalci postanejo sumničavi do vseh kandidatov v zaposlitvenih postopkih,
- delodajalec utrpi upad prihodkov,
- stranke so zavedene ob nakupu izdelkov ali storitev pri posamezniku s ponarejenim potrdilom in/ali
- davkoplačevalci so oškodovani, v kolikor je bil posameznik s ponarejenim potrdilom zaposlen v javni upravi.

5.8 Ugotavljanje ponaredkov

Težavnost ugotavljanja ponaredkov je odvisna od načina ponarejanja. V kolikor gre za sum ponarejanja potrdila pri neakreditirani izobraževalni instituciji (npr. nakup potrdila pri tovarni diplom), je ugotavljanje, ali je potrdilo ponarejeno, enostavnejše. V kolikor gre za sum ponarejanja potrdila pri akreditirani izobraževalni instituciji (npr. vdor v podatkovno

bazo izobraževalne institucije), je ugotavljanje, ali je potrdilo ponarejeno, kompleksnejše (Sayed, 2019).

Namreč, posameznik težje pride do ponarejenega potrdila akreditirane izobraževalne institucije, ker je v proces izdajanja potrdila vključenih več deležnikov (učenec, učitelji, zaledne pisarne, informacijski sistem itd.), kar pomeni, da obstaja več potencialno kritičnih točk, kjer lahko posamezniku pri ponarejanju spodleti. Posledično je tudi ugotavljanje ponaredkov kompleksnejše, ker obstaja več točk, ki jih je potrebno preveriti, da bi lahko prišli do zaključka, ali je potrdilo ponarejeno. Preverjanje dejanj posameznega deležnika, ki ima vpliv na proces izdajanja potrdila, je zahtevno ne le za zunanje deležnike (npr. delodajalce), temveč tudi za notranje deležnike (npr. izobraževalno institucijo). Posebej zahtevno je takrat, če so v procesu ponarejanja sodelovali zaposleni v izobraževalni instituciji, ki v preiskavi nočejo sodelovati, preiskavo zavirajo, prirejajo ali uničujejo dokaze (Sayed, 2019).

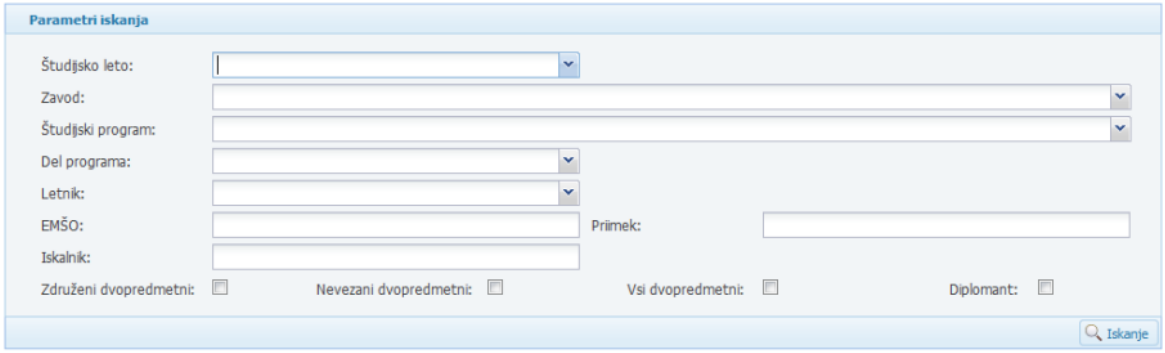
Na nacionalni ravni v okviru spletnega portala eVŠ obstaja evidenca, ki jo zagotavlja Ministrstvo za izobraževanje, znanost in šport Republike Slovenije. Vstop v aplikacijo je mogoč le registriranim uporabnikom, ki za dostop potrebujejo veljavno digitalno potrdilo in odobren dostop. Za odobritev dostopa mora posameznik poslati vlogo za dostop na ministrstvo in prijaviti svoje digitalno potrdilo v varnostno shemo (Ministrstvo za izobraževanje, znanost in šport, 2019).

Evidenco sestavljajo (Ministrstvo za izobraževanje, znanost in šport, 2019):

- Evidenca študentov in diplomantov na študiju v RS, v kateri se vodijo naslednji podatki:
  - vpis, izpis, diplomiranje slovenskih in tujih študentov, ki študirajo v RS in
  - podatki o mednarodni izmenjavi študentov,
- Evidenca tujih študentov na izmenjavi v RS, v kateri se vodijo podatki o tujih študentih, ki so na izmenjavi v RS in
- Spletni servis za kreiranje EMŠO za tuje študente.

Zainteresirana javnost lahko z iskalnikom, ki je prikazan na sliki 25, v evidenci poizveduje o diplomantih posameznega študijskega leta, pri čemer lahko doda več filtrov (zavod, študijski program, letnik, EMŠO itd.) in na tak način preveri verodostojnost potrdila posameznika. Poimenski izpis diplomantov je mogoč, če je odkljukan filter »Diplomant«. Rezultate iskanja je mogoče izvoziti v Excel (Ministrstvo za izobraževanje, znanost in šport, 2019).

Slika 25: Iskalnik v evidenci



Vir: Ministrstvo za izobraževanje, znanost in šport (2019).

Evidenca ima dve težavi. Prvič, v evidenco se vnašajo le podatki o izobraževanju v okviru visokošolskih zavodov RS. Svet je globalen, kar pomeni, da različna izobraževanja, ki niso opravljena v okviru visokošolskih zavodov RS, niso vnesena v evidenco. Drugič, evidenca je dostopna samo s kvalificiranim digitalnim potrdilom, pri čemer kvalificirano digitalno potrdilo SIGEN-CA lahko pridobijo državljani RS, starejši od 15 let, in tujci, ki imajo v RS dodeljeni matično in davčno številko (Ministrstvo za javno upravo, brez datuma). Tujci, ki želijo v evidenci preveriti verodostojnost potrdila posameznika, morajo najprej pridobiti matično in davčno številko v RS, kar pomeni, da verodostojnost potrdila posameznika bistveno težje preverijo v primerjavi z državljani RS. Taka evidenca ne omogoča, da bi potrdila bila preverljiva s strani kogar koli, kjer koli in kadar koli, kot Konstantinidis in drugi (2018) ugotavljajo, da bi potrdila morala biti preverljiva.

5.9 Problem zaupanja

Kot smo ugotovili, sistem potrdil, kot ga poznamo danes, temelji na zaupanju. Na zaupanju v ljudi in v informacijski sistem, podobno kot na zaupanju temelji tradicionalni finančni sistem, ker fiat valute niso podprte z zlatom. Težava zaupanja je, da v družbi vedno obstaja manjšina, ki ima interes to zaupanje podreti, pri čemer posledice nosi celotna družba, ker se zaradi manjšine naenkrat ne zaupa niti večini. Ko delojemalec predloži potrdilo delodajalcu, če delodajalec sprejme potrdilo brez preverjanja verodostojnosti, potem to pomeni, da delodajalec zaupa delojemalcu, da potrdilo ni ponarejeno. Ker se delodajalec in delojemalec ne poznata, obstaja velika verjetnost, da med njima ni zaupanja, zato bo delodajalec o potrdilu poizvedoval pri izobraževalni instituciji, pri čemer mora delodajalec spet zaupati na besedo, tokrat izobraževalni instituciji. Vidimo lahko, da sistem na vsakem koraku temelji na zaupanju, kar pomeni, da vedno obstaja problem zaupanja in posledično dvom v verodostojnost akcij vseh vpletenih deležnikov (Sayed, 2019).

6 NEZAMENLJIVI ŽETONI KOT DIGITALNA POTRDILA

Rešitev za problematiko ponarejanja potrdil ponuja tehnologija veriženja blokov, natančneje NFT-ji. Kot rečeno, tudi tehnologija veriženja blokov vsebuje komponento zaupanja, vendar na drugačen način. Tehnologija veriženja blokov je sistem, ki po vnaprej določenih pravilih sam kontrolira akcije vseh vpletenih deležnikov (Sayed, 2019).

Kot osnovo za analizo rešitve NFT-jev kot digitalnih potrdil bomo vzeli rešitev izobraževalne institucije d.MBA, ki jo bomo v nadaljevanju dodatno teoretično nadgradili.

6.1 Primer rešitve d.MBA

d.MBA je izobraževalna institucija, namenjena oblikovalcem, ki jo leta 2017 ustanovi Slovenec Alen Faljić (d.MBA, brez datuma). Svojim študentom med drugim izdaja tudi digitalna potrdila v obliki NFT-jev. Ideja za izdajanje digitalnih potrdil v obliki NFT-jev izhaja iz opažanja, da potrdila pri študentih pogosto gredo hitro v pozabo, poleg tega so tudi predmet ponarejanja. Izpostavljajo, da so se v preteklosti že srečevali z uporabniki na družbenem omrežju LinkedIn, ki so lažno trdili, da so uspešno končali njihov študijski program. Posledično so morali take uporabnike redno prijavljati. Pri d.MBA izpostavljajo, da so na tem projektu porabili več časa, kot bi bilo smiselno iz podjetniškega vidika, z namenom, da najdejo čim boljšo rešitev in hkrati, da projekt ne postane preveč kompleksen za implementacijo (d.MBA, 2022). Iz tega razloga je rešitev d.MBA dobra osnova za našo nadaljnjo teoretično nadgradnjo, ker je vanjo bilo vloženega že veliko truda.

Cilja d.MBA z izdajanjem digitalnih potrdil v obliki NFT-jev sta naslednja (Faljić, 2022):

- potrdilo naj postane umetniški izdelek, ki ga študent s ponosom obesi na steno (angl. wall-worthy) in
- potrdilo naj postane neizpodbitno dokazilo o opravljenem izobraževanju (angl. proof-of-completion).

Študent ob zaključku študijskega programa dobi naslednje 3 stvari (d.MBA, 2022):

- PDF datoteko umetnine z imenom študenta, ki je namenjena za tiskanje in obešanje na steno,
- JPG datoteko umetnine z imenom študenta, ki je namenjena objavi na družbenih omrežjih in
- NFT brez imena študenta, ki je dodan v verigo blokov.

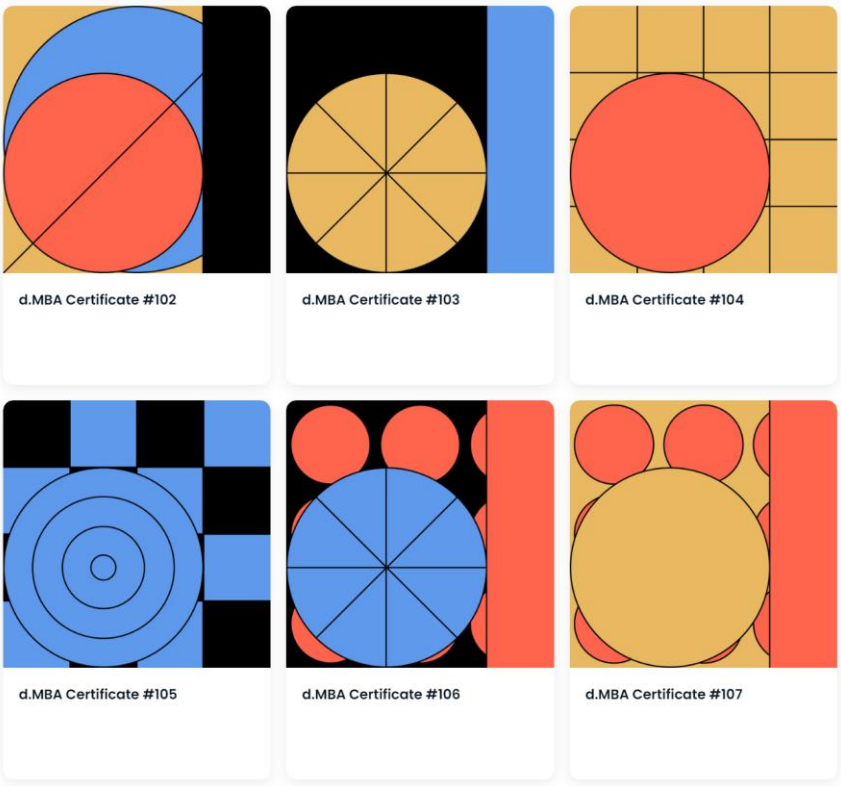
Če rešitev d.MBA predstavimo zelo abstraktno in se vrnemo na idejo »pobarvanih kovancev«, ki smo jo predstavili v enem od prejšnjih poglavij, bi lahko rekli, da posamezno digitalno potrdilo v obliki NFT-ja predstavlja »pobarvan kovanec«. Namreč, ideja »pobarvanih kovancev« temelji na razmisleku o potencialni možnosti izdajanja raznoraznih

unikatnih instrumentov na podlagi BTC tehnologije veriženja blokov. V tem pogledu je posamezno digitalno potrdilo v obliki NFT-ja primer takega unikatnega instrumenta. Če rešitev d.MBA predstavimo zelo konkretno, gre za digitalna potrdila v obliki NFT-jev na podlagi Polygon tehnologije veriženja blokov (v nadaljevanju MATIC tehnologija veriženja blokov) (d.MBA, 2022). MATIC tehnologija veriženja blokov je Ethereum stranska veriga blokov (angl. sidechain, v nadaljevanju ETH stranska veriga blokov), pri čemer smo v enem od prejšnjih poglavij spoznali, da se ETH tehnologija veriženja blokov razvije kot odgovor na razmislek o potencialu BTC tehnologije veriženja. Namreč, ETH tehnologija veriženja blokov dejansko začne omogočati izdajanje raznoraznih unikatnih instrumentov, o čemer so razpravljali avtorji ideje »pobarvanih kovancev«. Kakorkoli pogledamo rešitev d.MBA, bodisi abstraktno bodisi konkretno, nas rešitev vodi nazaj do prvotne ideje, torej do ideje »pobarvanih kovancev«.

6.1.1 Izdajanje digitalnega potrdila v obliki nezamenljivega žetona

Digitalna potrdila v obliki NFT-jev so ustvarjena z generativno umetniško zvrstjo. Rezultat so estetsko dovršena, unikatna in zaupanja vredna digitalna potrdila v obliki NFT-jev. NFT-je je ustvarila slovenska oblikovalska agencija Ljudje. Ustvarjena je bila NFT kolekcija d.MBA Certificates, ki je prikazana na sliki 26, pri čemer je vsak posamezen NFT unikaten, vendar vizualno podoben ostalim NFT-jem znotraj kolekcije (d.MBA, 2022).

Slika 26: NFT kolekcija d.MBA Certificates na NFT tržnici OpenSea



Vir: OpenSea (2022).

Kolekcija temelji na barvah d.MBA (tj. modra, rdeča in rumena), d.MBA logotipu (tj. podoba grafičnega oblikovalca z dvignjeno roko) in mreži 4x4, kot je prikazano na sliki 27. V kolekciji je prvotno bilo ustvarjenih 1999 unikatnih NFT-jev, vendar so pri d.MBA izvzeli tiste, ki so predstavljali nenavadne kombinacije (npr. povsem črn NFT). Tako je v kolekciji bilo izdanih 1677 NFT-jev. V prihodnosti, ko bo vseh 1677 NFT-jev dodeljenih študentom, bodo pri d.MBA izdali novo kolekcijo, ki bo različna od prve (d.MBA, 2022).

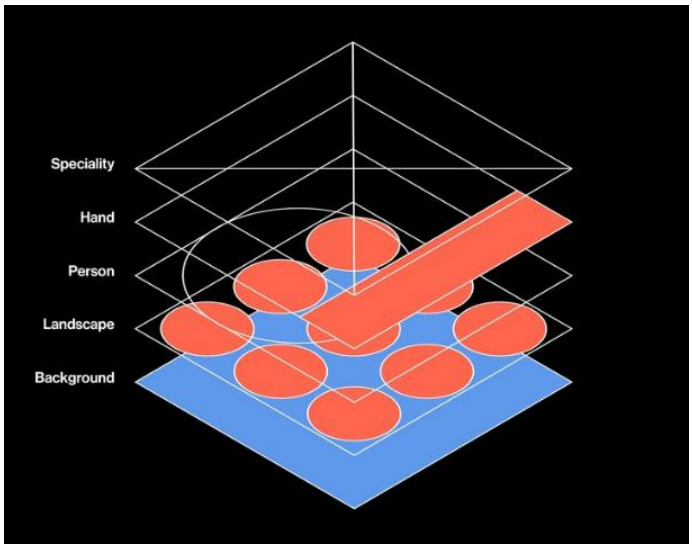
Slika 27: Koncept NFT kolekcije d.MBA Certificates

Vir: d.MBA (2022).

Koncept je nadalje razvit v 5 plasti, kot je prikazano na sliki 28, iz katerih je sestavljen vsak NFT znotraj kolekcije (d.MBA, 2022):

- prva plast predstavlja 5 možnih različnih barv ozadja,
- druga plast predstavlja element krajine,
- tretja in četrta plast predstavljata d.MBA logotip v različnih barvnih kombinacijah in
- peta plast, ki je posebna in dodana le določenemu odstotku NFT-jev.

Slika 28: Plasti posameznega NFT-ja iz NFT kolekcije d.MBA Certificates



Vir: d.MBA (2022).

Študentu je ob zaključku študijskega programa naključno dodeljen NFT iz kolekcije, ki še ni bil dodeljen nobenemu drugemu študentu. Študent zaprosi za digitalno potrdilo v obliki NFT-ja tako, da sporoči d.MBA svoj naslov. NFT študent dobi kot darilo zastonj, saj stroške transakcije pokrije d.MBA. Stroški transakcije so nizki, saj kolekcija temelji na MATIC tehnologiji veriženja blokov, ki omogoča nizke transakcijske stroške (d.MBA, 2022).

6.1.2 Preverjanje digitalnega potrdila v obliki nezamenljivega žetona

Kdor koli, ki lahko dokaže, da je v svojo denarnico prejel NFT iz kolekcije d.MBA Certificates direktno iz denarnice d.MBA, potrdi, da je uspešno končal študijski program (d.MBA, 2022).

Najbolj ključna v postopku preverjanja digitalnega potrdila v obliki NFT-ja sta dva pogoja:

1. denarnica d.MBA mora biti javno znana in
2. študent mora biti sposoben dokazati lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan.

Denarnica d.MBA je bila javno objavljena na spletni strani d.MBA. Imenuje se designmba.eth oz. 0x95F72EDA8B3fBc313c3C95991bBF8Bfc27fE09c6 (d.MBA, 2022).

Po razmisleku so se pri d.MBA odločili, da bodo NFT-ji iz kolekcije d.MBA Certificates prenosljivi, kar pomeni, da lahko prvotni lastnik NFT proda naprej. Razlog je v tem, da so NFT-ji iz kolekcije d.MBA Certificates pravzaprav umetniški izdelki, ki se jih lahko zbira. Torej, tisti, ki je trenutno lastnik NFT-ja iz kolekcije d.MBA Certificates ni nujno tudi končal študijski program, saj je lahko NFT od nekoga preprosto kupil na sekundarnem trgu. Študijski program je končal tisti, ki je NFT iz kolekcije d.MBA Certificates v svojo denarnico prejel direktno iz denarnice d.MBA (d.MBA, 2022).

6.1.3 Analiza rešitve d.MBA

Rešitev d.MBA bomo analizirali glede na načine ponarejanja, kot smo jih opredelili v prejšnjih poglavjih. Najprej bomo pogledali, kako rešitev d.MBA rešuje načine ponarejanja brez plačila, nato še načine ponarejanja proti plačilu.

Kot nam prikazuje tabela 3, rešitev d.MBA ne rešuje nobenega načina ponarejanja brez plačila. Razlog, zakaj je temu tako, je drugi pogoj v postopku preverjanja digitalnega potrdila v obliki NFT-ja, in sicer, da mora biti študent sposoben dokazati lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan. Če ne obstaja aplikacija, ki bi omogočala, da lahko posameznik zainteresirani javnosti dokaže lastništvo denarnice, potem digitalna potrdila v obliki NFT-ja ne rešujejo prav nič. Kot smo ugotovili, lastništvo denarnice posameznik dokaže s poznavanjem privatnega ključa, vendar privatnega ključa ne

sme deliti z nikomer. Edini način, da bi posameznik dokazal lastništvo denarnice bi bil, da z zainteresirano javnostjo deli privatni ključ, vendar tega ne sme storiti.

Tabela 3: Analiza rešitve d.MBA za načine ponarejanja brez plačila

Načini ponarejanja brez plačila	Ali rešitev d.MBA rešuje problem?
Lažna trditev na družbenem omrežju LinkedIn	Ne
Lažna trditev v življenjepisu	Ne
Zavajajoč prevod potrdila	Ne
Ponarejen predpogoj	Ne
Vdor v podatkovno bazo	Ne

Vir: lastno delo.

Kot nam prikazuje tabela 4, rešitev d.MBA prav tako ne rešuje nobenega načina ponarejanja proti plačilu. Razlog, zakaj je temu tako, je enak. Ne obstaja aplikacija, ki bi omogočala, da lahko posameznik zainteresirani javnosti dokaže lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan.

Tabela 4: Analiza rešitve d.MBA za načine ponarejanja proti plačilu

Načini ponarejanja proti plačilu	Ali rešitev d.MBA rešuje problem?
Nakup potrdila pri tovarni diplom	Ne
Podkupitev zaposlenega v akreditirani izobraževalni instituciji	Ne

Vir: lastno delo.

6.2 Nadgradnja rešitve d.MBA

Hitro bi lahko zaključili, da je rešitev d.MBA neaplikativna, vendar temu ni tako. Rešitev d.MBA bomo teoretično nadgradili. Namreč, v kolikor bi obstajala aplikacija, ki bi omogočala, da lahko posameznik zainteresirani javnosti dokaže lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan, rešitev d.MBA postane neprimerljivo bolj aplikativna.

Npr., družbeno omrežje LinkedIn bi lahko dodalo funkcijo preveritve lastništva NFT-jev, kot je to naredilo družbeno omrežje Twitter, kar smo že omenili v enem od prejšnjih poglavij. Postopek bi bil naslednji (Hill, 2022):

1. uporabnik na svojem LinkedIn profilu klikne »Dodaj certifikat«,
2. izbere možnost »Digitalni certifikat (NFT)«,

3. v kolikor nima povezane še nobene denarnice, klikne »Poveži mojo denarnico«,
4. izbere ponudnika denarnice (MetaMask, Coinbase Wallet, Rainbow, Ledger Live, Argent, Trust Wallet itd.),
5. LinkedIn se avtomatsko poveže z izbranim ponudnikom denarnice, prosi za dovoljenja (npr. za poznavanje javnega ključa denarnice) in generira prošnjo za verifikacijo denarnice,
6. uporabnik vnese privatni ključ denarnice in podpiše prošnjo za verifikacijo denarnice,
7. denarnica je povezana z LinkedIn profilom, zato lahko uporabnik izbira med NFT-ji, ki so v tej denarnici in
8. izbere digitalni certifikat ter klikne »Končaj«, s čimer doda NFT kot certifikat na svoj profil.

Tako bi družbeno omrežje LinkedIn služilo kot aplikacija, ki omogoča, da lahko posameznik zainteresirani javnosti dokaže lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan.

Kot nam prikazuje tabela 5, nadgrajena rešitev d.MBA rešuje večino načinov ponarejanja brez plačila. Posameznik na družbenem omrežju LinkedIn ne more objaviti lažnega (tj. ponarejenega) digitalnega certifikata v obliki NFT-ja, če ne pozna privatnega ključa denarnice. Posameznik tudi ne more v svoj življenjepis dodati lažnega (tj. ponarejenega) certifikata, ker lahko zainteresirana javnost zahteva, da na družbenem omrežju LinkedIn dokaže lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan. Sicer je v tem primeru na posamezniku, ali to stori ali ne, vendar v kolikor je potrdilo verodostojno, posameznik načeloma nima razloga, da tega ne bi storil in utišal nezaupanje ter vzpostavil zaupanje. Posameznik prav tako ne more zavajajoče prevesti originalnega potrdila, saj lahko zainteresirana javnost spet zahteva, da na družbenem omrežju LinkedIn dokaže lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan. Tako lahko zainteresirana javnost pride do originalnega (tj. neprevedenega) potrdila, s čimer lahko ugotovi, ali je bilo originalno potrdilo korektno prevedeno ali ne. Namreč, posameznik bi sicer lahko ponaredil NFT in denarnico uspešno povezal s svojim LinkedIn profilom, vendar ponarejen NFT nikakor v njegovo denarnico ne bi mogel priti iz denarnice d.MBA, saj d.MBA nikoli ne bi izdala ponarejenega NFT-ja, torej posamezniku nikoli ne bi poslala NFT-ja, ne da bi izpolnil vse zahtevane pogoje za pridobitev le-tega. Posameznik niti ne more ponarediti predpogoja za pridobitev potrdila, v kolikor tudi za predpogoj dobi digitalno potrdilo v obliki NFT-ja, ki je spet preverljivo na družbenem omrežju LinkedIn. Edino vdora v podatkovno bazo izobraževalne institucije nadgrajena rešitev d.MBA ne rešuje, ker posameznik lahko vdre v podatkovno bazo in spremeni podatke, s čimer postane upravičen do izdaje potrdila in s tem pride do verodostojnega digitalnega potrdila v obliki NFT-ja. Problem vdora v podatkovno bazo bi bil rešen le, če bi se ocene in vsi ostali podatki shranjevali v verigo blokov, pri čemer bi podatke v verigi blokov bilo nemogoče naknadno spreminjati, kot to ugotavljata Sharples in Domingue (Sharples & Domingue, 2016). Evropska komisija v svojem poročilu iz leta 2017 temu pritrjuje in celo pravi, da bo

tehnologija veriženja blokov na ta način pospešila konec potrdil, kot jih poznamo danes, saj se vsi relevantni podatki lahko shranijo v verigo blokov (European Commission, Joint Research Centre, 2017).

Tabela 5: Analiza nadgrajene rešitve d.MBA za načine ponarejanja brez plačila

Načini ponarejanja brez plačila	Ali nadgrajena rešitev d.MBA rešuje problem?
Lažna trditev na družbenem omrežju LinkedIn	Da
Lažna trditev v življenjepisu	Da
Zavajajoč prevod potrdila	Da
Ponarejen predpogoj	Da
Vdor v podatkovno bazo izobraževalne institucije	Ne

Vir: lastno delo.

Kot nam prikazuje tabela 6, nadgrajena rešitev d.MBA delno rešuje problem, ko posameznik potrdilo kupi pri tovarni diplom. Digitalna potrdila v obliki NFT-jev ne preprečujejo, da posameznik več ne bi mogel kupiti potrdila pri tovarni diplom. Kar digitalna potrdila v obliki NFT-jev prinašajo, je to, da je potrdila, ki so kupljena pri tovarni diplom, lažje odkriti. Kot smo ugotovili, pri tovarnah diplom gre za vzbujanje občutka velikega akademskega dosežka, ki to dejansko ni. Zainteresirana javnost lahko zahteva, da na družbenem omrežju LinkedIn posameznik dokaže lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan. Tako lahko zainteresirana javnost hitro ugotovi, ali je bil NFT poslan iz denarnice d.MBA ali iz denarnice tovarne diplom. Nadgrajena rešitev d.MBA lahko rešuje tudi problem, ko posameznik podkupi zaposlenega v akreditirani izobraževalni instituciji, odvisno od tega, ali se uporablja več podpisni sistem ali ne. Namreč, denarnico akreditirane izobraževalne institucije mora nadzirati, torej poznati privatni ključ denarnice, vsaj 1 zaposlen, ki ga posameznik lahko še vedno podkupi in pride do verodostojnega digitalnega potrdila v obliki NFT-ja, ne da bi izpolnil vse zahtevane pogoje za pridobitev le-tega. V kolikor se implementira več podpisni sistem 2-od-3, je nadgrajena rešitev d.MBA bistveno boljša, ker to pomeni, da bi moral posameznik podkupiti vsaj 2 od 3 zaposlenih, ker ima vsak od njih en privatni ključ, pri čemer morata biti za transakcijo uporabljena vsaj 2. Torej, nadgrajena rešitev d.MBA bistveno bolje preprečuje problem ponarejanja, v kolikor se uporablja več podpisni sistem.

Tabela 6: Analiza nadgrajene rešitve d.MBA za načine ponarejanja proti plačilu

Načini ponarejanja proti plačilu	Ali nadgrajena rešitev d.MBA rešuje problem?
Nakup potrdila pri tovarni diplom	Delno

se nadaljuje

Tabela 6: Analiza nadgrajene rešitve d.MBA za načine ponarejanja proti plačilu (nad.)

Načini ponarejanja proti plačilu	Ali nadgrajena rešitev d.MBA rešuje problem?
Podkupitev zaposlenega v akreditirani izobraževalni instituciji	Da, v kolikor se implementira več podpisni sistem

Vir: lastno delo.

SKLEP

Namena magistrskega dela sta dva. Prvič, ozavestiti družbo o praktični uporabni vrednosti NFT-jev, saj v zadnjem bikovskem trgu, ko so cene NFT-jev poletele v nebo, marsikdo v družbi ni videl nobene uporabne vrednosti v slikah počlovečenih opic, kot je npr. kolekcija Bored Ape Yacht Club. Drugič, prispevati k razvoju rešitve digitalnih potrdil v obliki NFT-jev, saj je ideja še povsem v povojih in dobra praksa še ni izoblikovana.

V prvem sklopu magistrskega dela, od 1. poglavja do 5. poglavja, pišemo o tehnologiji veriženja blokov in izbrani problematiki ponarejanja potrdil. V prvem poglavju opišemo BTC tehnologijo veriženja blokov, ki je osnova za nadaljnje razumevanje magistrskega dela, saj ves nadaljnji razvoj tega področja temelji na BTC tehnologiji veriženja blokov. V drugem poglavju nadaljujemo z idejo »pobarvanih kovancev«, ki je plod vprašanja, kakšne potenciale BTC tehnologija veriženja blokov omogoča. V tretjem poglavju predstavimo ETH tehnologijo veriženja blokov, ki se razvije iz ideje »pobarvanih kovancev«. ETH tehnologija veriženja blokov omogoča obstoj kompleksnejših pametnih pogodb in s tem omogoča možnost razvoja tega potenciala, o katerem govorijo avtorji ideje »pobarvanih kovancev«. V četrtem poglavju razdelamo NFT-je, ki temeljijo na ETH tehnologiji veriženja blokov in na katerih temelji rešitev, ki je opisana v drugem sklopu magistrskega dela. V petem poglavju poudarimo problematiko ponarejanja potrdil, ki zadeva celotno družbo.

V drugem sklopu magistrskega dela, v 6. poglavju, opišemo digitalna potrdila v obliki NFT-jev kot rešitev za izbrano problematiko ponarejanja potrdil. Za osnovo vzamemo rešitev d.MBA, ki sicer kot taka ne rešuje prav nobenega način ponarejanja, niti ponarejanja brez plačila niti ponarejanja proti plačilu. Težava je v tem, da mora biti študent sposoben dokazati lastništvo denarnice, v katero je NFT iz kolekcije d.MBA Certificates bil direktno poslan, kar rešitev d.MBA kot taka, ne omogoča. Rešitev d.MBA v nadaljevanju dodatno teoretično nadgradimo, tako da postane bistveno bolj aplikativna. Npr., v kolikor bi družbeno omrežje LinkedIn dodalo funkcijo preveritve lastništva NFT-jev, bi rešitev d.MBA rešila večino načinov ponarejanja brez plačila in delno rešila načine ponarejanja proti plačilu. Nadgrajena rešitev d.MBA tako minimizira možnost ponarejanja potrdil, pri čemer ni preveč kompleksna za implementacijo v praksi.

LITERATURA IN VIRI

1. 3Blue1Brown. (2017, 7. julij). *But how does bitcoin actualy work?* [YouTube]. Pridobljeno 13. aprila 2022 iz https://www.youtube.com/watch?v=bBC-nXj3Ng4&ab_channel=3Blue1Brown
2. Antonopoulos, A. (2014, 20. februar). Bitcoin security model: trust by computation. *Radar*. Pridobljeno 9. aprila 2022 iz http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html
3. Assia, Y. (2012, 27. marec). *Bitcoin 2.X (aka Colored Bitcoin) – initial specs.* Pridobljeno 28. avgusta 2022 iz https://yoniassia.com/coloredbitcoin/
4. Assia, Y., Buterin, V., Liorhakilior, M., Rosenfeld, M. & Rotem, L. (2013). *Colored Coins whitepaper*. Pridobljeno 20. avgusta 2022 iz https://www.etoro.com/wp-content/uploads/2022/03/Colored-Coins-white-paper-Digital-Assets.pdf
5. Attewell, P. & Domina, T. (2011, januar). Educational imposters and fake degrees. *Research in Social Stratification and Mobility, 29*(1), 57-69. https://doi.org/10.1016/j.rssm.2010.12.004
6. Atzori, M. (2015, 1. december). *Blockchain technology and decentralized governance: Is the state still necessary?.* Pridobljeno 9. aprila 2022 iz https://deliverypdf.ssrn.com/delivery.php?ID=088024100123020120119094017079030065121004001038027088066090117107020111065118068098119033023106033000111097100015127002090090106034037051088091093015011071010082127041026076024115096124085001127029095080106070107030107082012026081102093024097020024017&EXT=pdf&INDEX=TRUE
7. Ballies. (brez datuma). *Become the king of the metacourt*. Pridobljeno 31. oktobra 2022 iz https://ballies.gg/
8. Bear, J. (1986, april). The Diploma Mill and modern technology. *Education + Training, 28*(4), 122-123. https://doi.org/10.1108/eb017261
9. Binance Academy. (brez datuma a). *Genesis Block.* Pridobljeno 10. aprila 2022 iz https://academy.binance.com/en/glossary/genesis-block
10. Binance Academy. (brez datuma b). *Circulating Supply.* Pridobljeno 16. julija 2022 iz https://academy.binance.com/en/glossary/circulating-supply
11. Bistarelli, S., Mazzante, G., Micheletti, M., Mostarda, L. & Tiezzi, F. (2019). Analysis of Ethereum Smart Contracts and Opcodes. *Advanced Information Networking and Applications: Proceedings of the 33rd International Conference on Advanced Information Networking and Applications 33*, 546-558. https://doi.org/10.1007/978-3-030-15032-7_46
12. Bitcoin.com. (2008, 31. oktober). *Bitcoin P2P e-cash paper.* Pridobljeno 10. aprila 2022 iz https://www.bitcoin.com/satoshi-archive/emails/cryptography/1/
13. Bitstamp. (2021, 23. avgust). *What are blockchain nodes?.* Pridobljeno 17. julija 2022 iz https://blog.bitstamp.net/post/what-are-blockchain-nodes/

14. Brownworth, A. (2016, 5. november). *Blockchain 101 - A Visual Demo* [YouTube]. Pridobljeno 22. maja 2022 iz https://www.youtube.com/watch?v=_160oMzblY8&ab_channel=AndersBrownworth
15. Buruma, I. (2015, 26. februar). One of Us: The Story of Anders Breivik and the Massacre in Norway by Åsne Seierstad – review. *The Guardian.* Pridobljeno 13. novembra 2022 iz https://www.theguardian.com/books/2015/feb/26/one-of-us-the-story-of-anders-breivik-massacre-norway-asne-seierstad-review
16. Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.* Pridobljeno 25. septembra 2022 iz https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf
17. Cointelegraph. (brez datuma). *Who is the mysterious Bitcoin creator Satoshi Nakamoto?*. Pridobljeno 9. aprila 2022 iz https://cointelegraph.com/bitcoin-for-beginners/who-is-satoshi-nakamoto-the-creator-of-bitcoin
18. Cryptopedia. (2021, 21. oktober). *Merkle Trees and Merkle Roots Help Make Blockchains Possible.* Pridobljeno 17. julija 2022 iz https://www.gemini.com/cryptopedia/merkle-tree-blockchain-merkle-root
19. d.MBA. (2022). *School certificates for the digital age* [objava na blogu]. Pridobljeno 8. januarja 2023 iz https://d.mba/blog/school-certificates-for-the-digital-age
20. d.MBA. (brez datuma). *About us.* Pridobljeno 20. februarja 2023 iz https://d.mba/about
21. DiplomaCompany. (brez datuma). *The Leader in Quality Novelty Replacement Fake Diplomas, Fake Degrees, and Transcripts*. Pridobljeno 26. november 2022 iz https://www.diplomacompany.com/
22. Ethereum. (2022a, 10. oktober). *Poof-of-stake (POS).* Pridobljeno 23. oktobra 2022 iz https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
23. Ethereum. (2022b, 21. oktober). *Non-fungible tokens (NFT).* Pridobljeno 23. oktobra 2022 iz https://ethereum.org/en/nft/#what-are-nfts
24. Ethereum. (2022c, 15. avgust). *Token standards.* Pridobljeno 30. oktobra 2022 iz https://ethereum.org/en/developers/docs/standards/tokens/
25. European Commission, Joint Research Centre. Camilleri, A., Inamorato dos Santos, A. & Grech, A. (2017). *Blockchain in education*. Publications Office. https://data.europa.eu/doi/10.2760/60649
26. Ezell, A. (2019). *Diploma mills and counterfeit operations.* Pridobljeno 13. novembra 2022 iz https://www.aacrao.org/docs/default-source/webinar-documents/94-3-diploma-mills-and-counterfeit-operations.pdf?sfvrsn=ffabe7f9_2
27. Faljić, A. [@alenfaljic]. (2022, 16. februar). *How should school certificates of the future look like?* [Twitter]. Pridobljeno 8. januarja 2023 iz https://twitter.com/alenfaljic/status/1493996124730019847
28. Feign, A. (2022, 9. marec). What Is Blockchain Technology?. *CoinDesk*. Pridobljeno 23. aprila 2022 iz https://www.coindesk.com/learn/what-is-blockchain-technology/

29. George, B. (2022, 23. avgust). What Are PFP NFTs?. *CoinDesk.* Pridobljeno 30. oktobra 2022 iz https://www.coindesk.com/learn/what-are-pfp-nfts/
30. Hill, S. (2022, 22. januar). *How to use a verified NFT as your profile photo on Twitter*. Pridobljeno 9. februarja 2023 iz https://www.inverse.com/input/guides/how-to-verify-set-nft-twitter-profile-photo
31. ifeelsLOVEnia NFT. (brez datuma). *Kranjska čebela*. Pridobljeno 31. oktobra 2022 iz https://ifeelnft.si/item/54c6a918fb557ef6b19801d42f4014d287c6bc90a8ba66096b
32. Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V. & Decker, S. (2018, julij). Blockchain for business applications: A systematic literature review. *Business Information Systems: 21st International Conference, BIS 2018, Berlin, Nemčija* (str. 384-399). http://doi-org-443.webvpn.fjmu.edu.cn/10.1007/978-3-319-93931-5_28
33. Larva Labs. (brez datuma a). *CryptoPunks.* Pridobljeno 30. oktobra 2022 iz https://www.larvalabs.com/cryptopunks
34. Larva Labs. (brez datuma b). *Autoglyphs.* Pridobljeno 31. oktobra 2022 iz https://www.larvalabs.com/autoglyphs
35. Marcobello, M. (2022, 25. oktober). What Are Generative Art NFTs?. *CoinDesk.* Pridobljeno 31. oktobra 2022 iz https://www.coindesk.com/learn/what-are-generative-art-nfts/
36. McSweeney, M. (2021, 31. oktober). *Bitcoin's white paper was published 13 years ago today.* Pridobljeno 9. aprila 2022 iz https://www.theblockcrypto.com/linked/122703/bitcoins-white-paper-was-published-13-years-ago-today
37. Meyer, R. (2020a, 30. marec). *The Bitcoin whitepaper, explained and commented – section 2: transactions.* Pridobljeno 24. aprila 2022 iz https://meyer-raph.medium.com/the-bitcoin-whitepaper-explained-and-commented-section-2-transactions-327651bb52fa
38. Meyer, R. (2020b, 4. april). *The Bitcoin whitepaper, explained and commented — section 3: timestamp server.* Pridobljeno 29. aprila 2022 iz https://meyer-raph.medium.com/the-bitcoin-whitepaper-explained-and-comment-section-3-timestamp-server-d5ceb84368a4
39. Meyer, R. (2020c, 24. april). *The Bitcoin whitepaper, explained and commented: part 5 — network.* Pridobljeno 12. junija 2022 iz https://meyer-raph.medium.com/the-bitcoin-whitepaper-explained-and-commented-part-5-network-a5c2dedca2a2
40. Meyer, R. (2020d, 30. april). *The Bitcoin whitepaper, explained and commented: section 6 — incentives.* Pridobljeno 16. julija 2022 iz https://meyer-raph.medium.com/the-bitcoin-whitepaper-explained-and-commented-section-6-incentives-da6835015db
41. Meyer, R. (2022, 8. april). *The Bitcoin whitepaper explained and commented: part 9 — Combining and Splitting Value.* Pridobljeno 23. julija 2022 iz https://meyer-raph.medium.com/the-bitcoin-whitepaper-explained-and-commented-part-9-combining-and-splitting-value-83f90f616ad2

42. Ministrstvo za izobraževanje, znanost in šport. (2019, 7. januar). *eVŠ evidenca študentov in diplomantov.* Pridobljeno 6. aprila 2022 iz http://eportal.mss.edus.si/portal/documents/215302/216221/Navodila_eV%C5%A0-E%C5%A0D_v.3.pdf/d07cfabd-3714-47b5-82fe-a593f0b9f8ea
43. Ministrstvo za javno upravo. (brez datuma). *Kvalificirano digitalno potrdilo.* Pridobljeno 7. aprila 2022 iz https://e-uprava.gov.si/podrocja/osebni-dokumenti-potrdila-selitev/osebni-dokumenti/digitalno-potrdilo-za-elektronsko-poslovanje.html
44. Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M. & Baronchelli, A. (2021). *Mapping the NFT revolution: market trends, trade networks, and visual features.* Pridobljeno 15. avgusta 2022 iz https://arxiv.org/pdf/2106.00647.pdf
45. Nakamoto, S. (2008, 31. oktober). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Pridobljeno 9. aprila 2022 iz https://bitcoin.org/bitcoin.pdf
46. Nakamoto, S. (2009, 11. februar). *Bitcoin open source implementation of P2P currency.* Pridobljeno 1. maja 2022 iz https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/#selection-9.0-9.50
47. NFTGo. (brez datuma). *Market Overview.* Pridobljeno 30. oktobra 2022 iz https://nftgo.io/analytics/market-overview
48. Nine Entertainment. (2012, 15. september). *How a fraudster engineered his past.* Pridobljeno 13. novembra 2022 iz https://www.smh.com.au/national/how-a-fraudster-engineered-his-past-20120914-25xpz.html
49. Occupy Wall Street. (brez datuma). *About.* Pridobljeno 23. aprila 2022 iz http://occupywallst.org/about/
50. OhhShiny. [@ohhshiny]. (brez datuma). [Profil]. Pridobljeno 30. oktobra 2022 iz https://twitter.com/ohhshiny
51. OpenSea. (2022, februar). *d.MBA Certificates.* Pridobljeno 8. januarja 2023 iz https://opensea.io/collection/dmba
52. OpenSea. (brez datuma). *Gramatik.* Pridobljeno 31. oktobra 2022 iz https://opensea.io/collection/gramatik?search[sortAscending]=true&search[sortBy]=UNIT_PRICE
53. Phillips, D. (2021, 10. februar). *The Bitcoin Genesis Block: How It All Started.* Pridobljeno 9. aprila 2022 iz https://decrypt.co/56934/the-bitcoin-genesis-block-how-it-all-started
54. Planica. (brez datuma). *Planica NFT kolekcija skakalcev 2022.* Pridobljeno 31. oktobra 2022 iz https://planicanft.com/
55. Rosenfeld, M. (2012, 4. december). *Overview of Colored Coins.* Pridobljeno 21. avgusta 2022 iz https://bitcoil.co.il/BitcoinX.pdf
56. Sayed, R. H. (2019). *Potential of blockchain technology to solve fake diploma problem.* Pridobljeno 6. aprila 2022 iz https://jyx.jyu.fi/bitstream/handle/123456789/64817/URN%3aNBN%3afi%3ajyu-201906253406.pdf?sequence=1&isAllowed=y

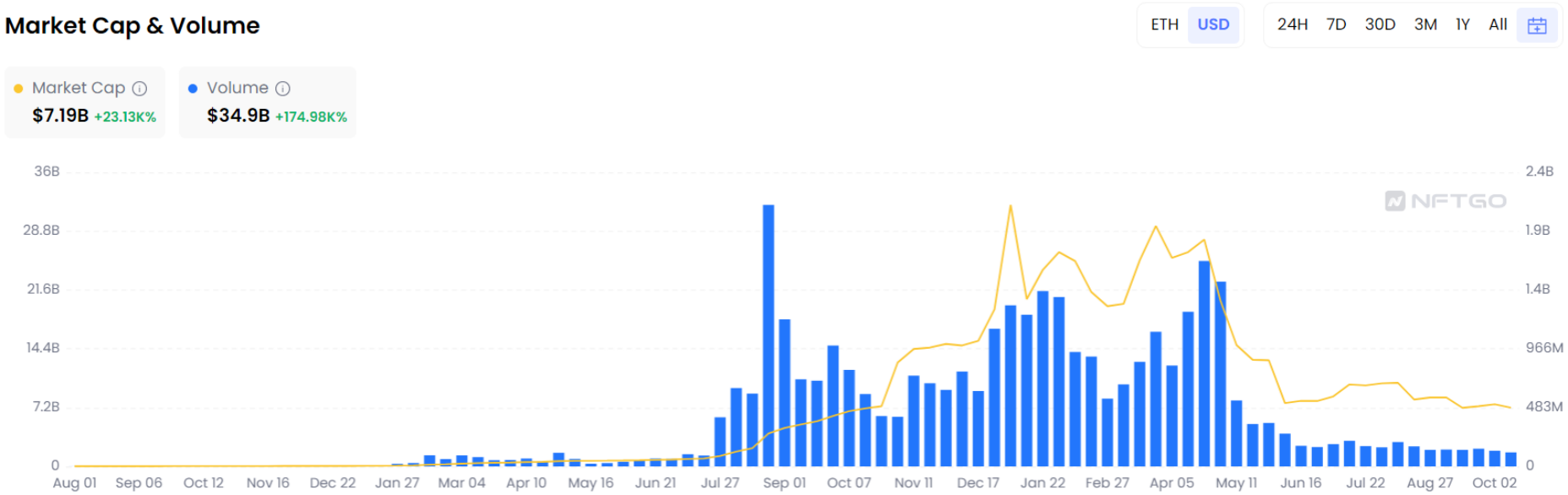
57. Sharples, M. & Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. *Lecture Notes in Computer Science*, 490-496. https://doi.org/10.1007/978-3-319-45153-4_48
58. Slovenska tiskovna agencija. (2019a, 22. februar). *Mediji: Sestra v Trboveljski bolnišnici in zdravnica v Izoli ena in ista oseba*. Pridobljeno 13. novembra 2022 iz https://www.sta.si/2608956/mediji-sestra-v-trboveljski-bolnisnici-in-zdravnica-v-izoli-ena-in-ista-oseba
59. Slovenska tiskovna agencija. (2019b, 27. maj). *Lažna zdravnica obsojena na pogojno kazen.* Pridobljeno 13. novembra 2022 iz https://www.sta.si/2641051/lazna-zdravnica-obsojena-na-pogojno-kazen
60. Steinwold, A. (2019, 7. oktober). *The History of Non–Fungible Tokens (NFTs).* Pridobljeno 21. avgusta 2022 iz https://medium.com/@Andrew.Steinwold/the-history-of-non-fungible-tokens-nfts-f362ca57ae10
61. Tehnološki park Ljubljana. (2021, 21. september). *Slovenija prva država na svetu izdala NFT žetone (Non-fungible tokens).* Pridobljeno 31. oktobra 2022 iz https://www.tp-lj.si/sl/novice/slovenija-prva-drzava-na-svetu-izdala-nft-zetone-non-fungible-tokens-2021-09-21
62. Tehnološki park Ljubljana. (2022, 7. oktober). *Podjetja, ki bodo v naslednjih letih zavračala uvajanje novih tehnologij, bodo precej zaostala za konkurenco.* Pridobljeno 31. oktobra 2022 iz https://www.tp-lj.si/sl/novice/podjetja-ki-bodo-v-naslednjih-letih-zavracala-uvajanje-novih-tehnologij-bodo-precej-zaostala-za-konkurenco-2022-10-07
63. The Blockchain Review. (brez datuma). *Bitcoin White Paper Made Simple.* Pridobljeno 9. aprila 2022 iz https://static1.squarespace.com/static/567bb4f069a91a95348fa0b2/t/5cd27c8bb208fcb3a45d2196/1557298317565/Intrepid+Ventures+Bitcoin+White+Paper+Made+Simple.pdf
64. The New York Times Company. (2015, 18. maj). *Text of Axact's Response to The New York Times*. Pridobljeno 15. februarja 2023 iz https://www.nytimes.com/2015/05/19/world/asia/text-of-axact-response-to-the-new-york-times.html
65. TSmedia, medijske vsebine in storitve, d. o. o. (2021, 27. februar). *Slovenski glasbenik v petih minutah zaslužil 1,3 milijona evrov?.* SiolNET. Pridobljeno 31. oktobra 2022 iz https://siol.net/digisvet/novice/slovenski-glasbenik-v-petih-minutah-zasluzil-13-milijona-evrov-546789
66. Vujičić, D., Jagodić, D. & Ranđić, S. (2018, marec). Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview. *2018 17th international symposium infoteh-jahorina,* 1-6. https://doi.org/10.1109/INFOTEH.2018.8345547
67. Walker, G. (2015, 26. marec). *Difficulty.* Pridobljeno 12. junija 2022 iz https://learnmeabitcoin.com/beginners/difficulty
68. Walker, G. (2019, 7. september). *51% Attack.* Pridobljeno 22. maja 2022 iz https://learnmeabitcoin.com/technical/51-attack

69. Walker, G. (brez datuma). *How does Bitcoin work?.* Pridobljeno 1. maja 2022 iz https://learnmeabitcoin.com/
70. Walsh, D. (2015, 17. maj). Fake Diplomas, Real Cash: Pakistani Company Axact Reaps Millions. *The New York Times.* Pridobljeno 15. februarja 2023 iz https://www.nytimes.com/2015/05/18/world/asia/fake-diplomas-real-cash-pakistani-company-axact-reaps-millions-columbiana-barkley.html
71. Yee, A. [@ahkyee]. (2021, 3. januar). *Happy Bitcoin Day* [Twitter]. Pridobljeno 10. aprila 2022 iz https://twitter.com/ahkyee/status/1345578096863285248?lang=en
72. Yuga Labs. (brez datuma). *Bored Ape Yacht Club.* Pridobljeno 30. oktobra 2022 iz https://boredapeyachtclub.com/#/gallery
73. Zarir, A. A., Oliva, G. A., Jiang, Z. M. & Hassan, A. E. (2021). Developing Cost-Effective Blockchain-Powered Applications: A Case Study of the Gas Usage of Smart Contract Transactions in the Ethereum Blockchain Platform. *ACM Transactions on Software Engineering and Methodology*, *30*(3), 1-38. https://doi.org/10.1145/3431726

PRILOGA

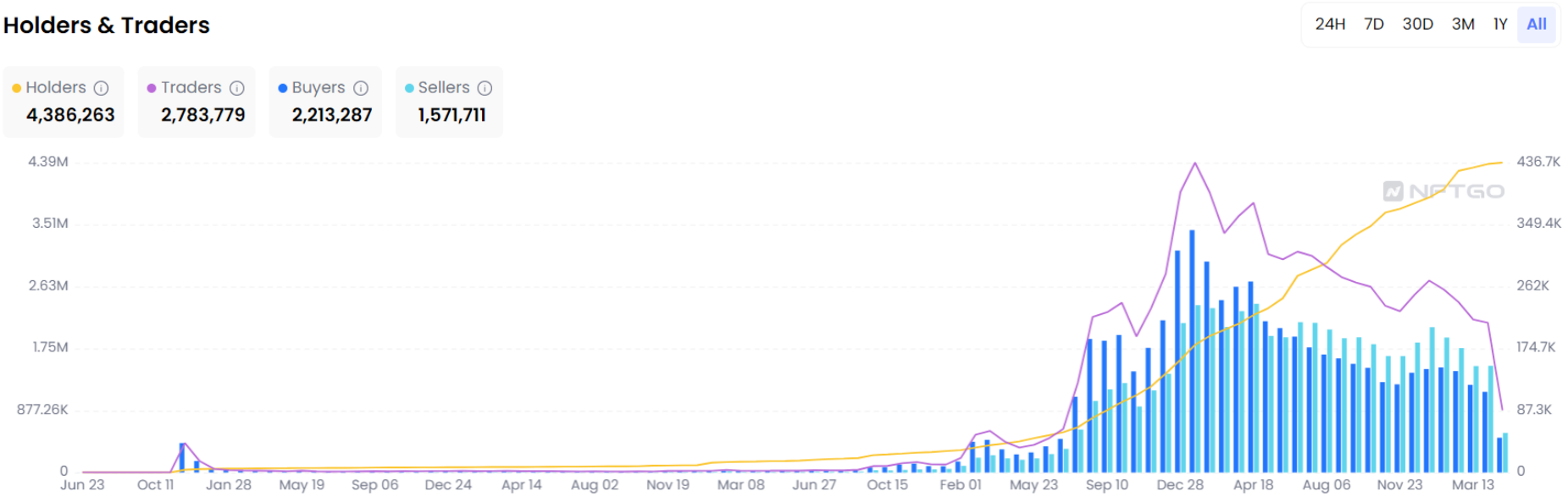
Priloga 1: Grafični prikaz analize trenutnega stanja trga nezamenljivih žetonov

Slika 29: Tržna kapitalizacija in obseg trgovanja z NFT-ji za obdobje od 1. avgust 2020 do 15. oktober 2022



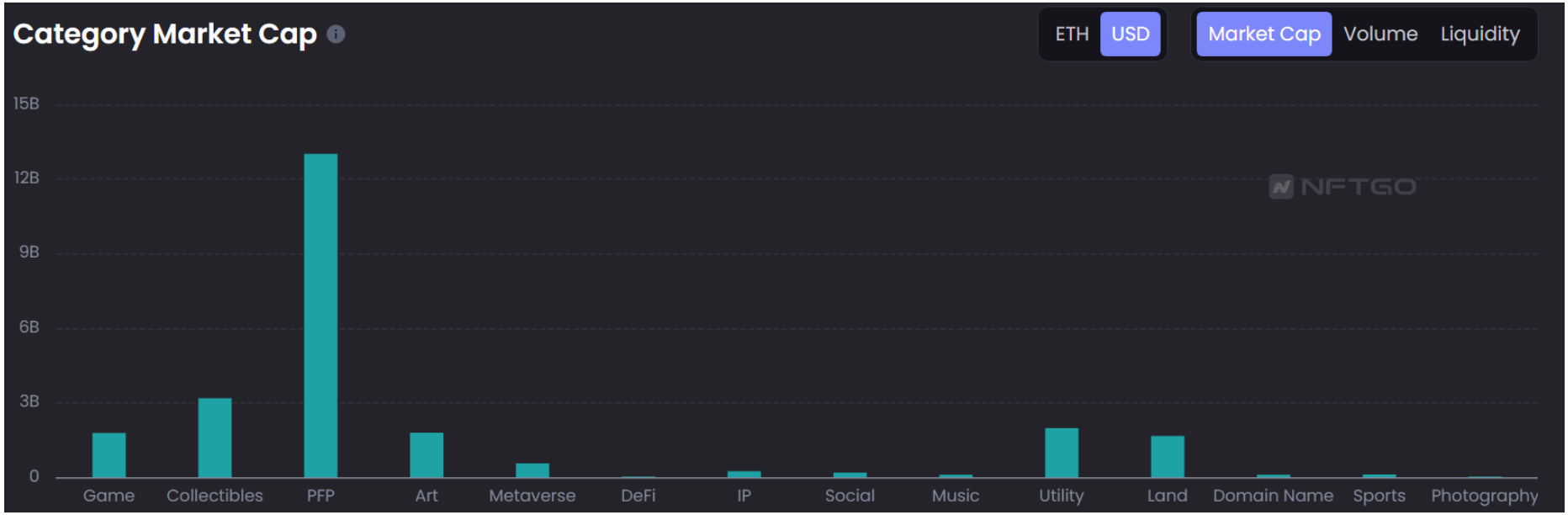
Vir: NFTGo (brez datuma).

Slika 30: Število denarnic, ki držijo, trgujejo, kupujejo in prodajajo NFT-je za obdobje od 23. junij 2017 do 27. april 2023



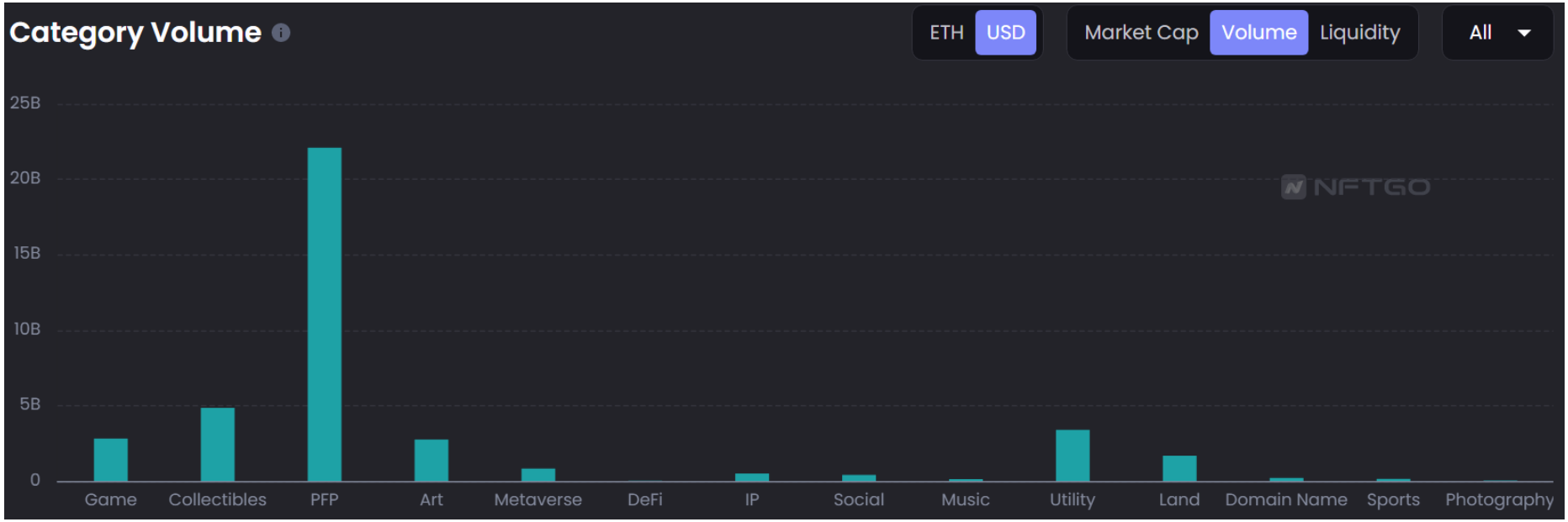
Vir: NFTGo (brez datuma).

Slika 31: Tržna kapitalizacija glede na NFT kategorijo dne 30. oktober 2022



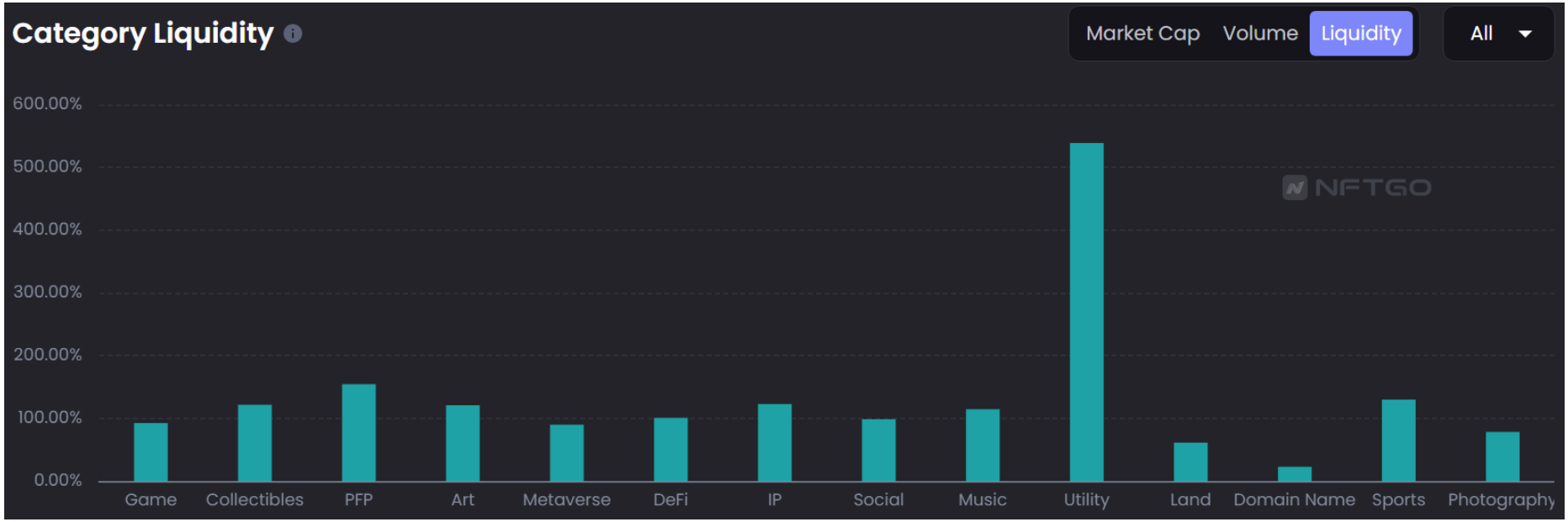
Vir: NFTGo (brez datuma).

Slika 32: Obseg trgovanja glede na NFT kategorijo dne 30. oktober 2022



Vir: NFTGo (brez datuma).

Slika 33: Likvidnost glede na NFT kategorijo dne 30. oktober 2022



Vir: NFTGo (brez datuma).