Kriptovalute

Sabljak, Dino

Sveučilište Jurja Dobrile u Puli
Fakultet Informatike u Puli

Dino Sabljak

KRIPTOVALUTE
CRYPTOCURRENCY

Završni rad

Pula, rujan 2021. godine

Sveučilište Jurja Dobrile u Puli
Fakultet Informatike u Puli

DINO SABLJAK

KRIPTOVALUTE
CRYPTOCURRENCY

Završni rad

JMBAG: 0303072661, redovni student

Studijski smjer: Sveučilišni preddiplomski studij Informatika

Predmet: Osnove IKT

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: doc. dr. sc. Snježana Babić

Pula, rujan 2021. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani/a Dino Sabljak, ovime izjavljujem da je ovaj seminarski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio seminarskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student/ica

Dino Sabljak

U Puli, rujan 2021. godine

IZJAVA

o korištenju autorskog djela

Ja, Dino Sabljak dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom „Kriptovalute“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

Potpis

U Puli, rujan 2021. godine

Sadržaj

1. UVOD

Kriptovalute su digitalne tj. virtualne valute osigurane kriptografijom što znači da ih je gotovo pa nemoguće krivotvoriti i temelje se na blockchain tehnologiji. Jednostavnija definicija je da je kriptovaluta oblik plaćanja koji se razmjenjuje za robu i usluge. Mijenjate pravu valutu za kriptovalutu, koju možete koristiti za kupnju i prodaju preko interneta. Kriptovaluta radi na peer to peer sustavu, što znači da banka i vlada nisu uključeni u transakcije između jedne i druge osobe.

Cilj ovoga rada je objasniti opći pojam, karakteristike te prednosti i rizike upotrebe kriptovaluta i njenih tehnologija. Završni rad je organiziran na sljedeći način.

Drugo poglavlje ovoga rada opisuje opći pojam kriptovaluta i njihov nastanak. Treće poglavlje bavi se vrstama kriptovaluta. Prvi odjeljak ovog poglavlja opisuje bitcoin kriptovalutu, njen nastanak, brzine transakcije i kretanje cijene tijekom godina. Drugi odjeljak opisuje ethereum kriptovalutu koja upotrebljava više funkcionalnosti blockchain tehnologije, i objašnjava se upotrebljavanje pametnih ugovora (eng. *Smart contracts).* Treći odjeljak ovog poglavlja opisuje stellar kriptovalutu. Objašnjava se stellar platforma i jedinice stellar kriptovalute pod imenom lumen. Također spominje se postupak putnog plaćanja.

Četvrto poglavlje bazira se na blockchain tehnologiji i informatičkim aspektima upotrebljavanja navedene tehnologije. Prvi odjeljak opisuje opći pojam rudarenja kriptovaluta, a drugi odjeljak objašnjava postupak rudarenja. Treći odjeljak prikazuje softvere i hardvere potrebne za rudarenje. Također, može se vidjeti prikaz rudarenja preko osobnog računala autora ovog završnog rada.

Peto poglavlje objašnjava novčanike za pohranjivanje kriptovaluta. U prvom odjeljku objašnjava se papirnati novčanik i postupak kreiranja istog. Drugi odjeljak opisuje hardverske novčanike i njihovu sigurnost. Navedeni su i neki od najkorištenijih hardverskih novčanika. Treći odjeljak opisuje softverske novčanike, njihov način rada i sigurnost. Prikazane su tri vrste softverskih novčanika i prikazan je postupak kreiranja

jednog od tih vrsta.

Šesto poglavlje opisuje transakcije i postupak transakcija. Pojašnjene su funkcije privatnog i javnog ključa, i kriptografskog potpisa. Sedmo poglavlje opisuje prednosti blockchain tehnologije i sigurnost kriptovaluta. Također objašnjavaju se rizici i nedostatci kriptovaluta.

2. OPĆI POJAM I NASTANAK KRIPTOVALUTA

Od početka interneta puno ljudi je zamišljalo internet valutu, točnije rečeno digitalni novac. Kriptograf David Chaum prvi je teoretizirao kriptovalutu kada je izumio šifrirani računalni algoritam koji je omogućio sigurnu, nepromjenjivu razmjenu između dvije strane. Chaum je kasnije osnovao DigiCash, jedno od prvih poduzeća koje je proizvodilo novčane jedinice na temelju svog algoritma. Važno je napomenuti da je samo tvrtka DigiCash mogla proizvesti valutu, što je razlika od bitcoina i drugih kriptovaluta gdje svatko može rudariti valutu. Nakon što je naišao na pravne probleme i odbio partnerstvo s Microsoftom, tvrtka je bankrotirala krajem 1990-ih. (Satoshi, 2017)

Sredinom devedesetih došle su prve ispravne digitalne valute, jedna od prvih bila je e-gold (e-zlato) osnovano 1996. i podržano zlatom. Bilo je jedinstveno u usporedbi s tradicionalnim načinima plaćanja i čisto digitalne prirode, a transakcije su bile potpuno nepovratne. E-gold valute postale su popularne i imale su više od 5 milijuna korisnika. Iako je spomenuta valuta počela dobronamjerno, brzo su postale utočište za kriminalce te je e-gold valuta bila zatvorena sa strane Američke vlasti. Nadalje najveći proboj u transakcijama dogodio se 1998. kada su Elon Musk, Peter Thiel i drugi osnovali PayPal. PayPal je još i danas vrlo popularan iako se suočava s velikim konkurencijama poput Apple pay-a i drugih. Dok su s PayPal-om olakšavali internet transakcije nedostajalo je puno karakteristika kriptovalute. PayPal je bio digitalni prijenos fiat-a ili valute, dok je kriptovaluta za razliku od toga, i sama vrijednost. Također kriptovalute su s druge strane decentralizirane, što znači da nema posrednika između dvije transakcije. No još uvijek e-gold i PayPal bili su važni prethodnici bitcoina jer se pokazala sposobnost korištenja kibernetičkog prostora[1] za prijenos sredstava. (Satoshi, 2017)

[1] kibernetički prostor, virtualni prostor stvoren s pomoću globalno umreženih računala

3. VRSTE KRIPTOVALUTA

Od 2021. godine postoji više od 10.000 različitih vrsta kriptovaluta (Sofi, 2021). U nastavku objašnjene tri vrste kriptovalute kao jedne od najviše korištenih valuta.

3.1. Bitcoin (BTC)

Bitcoin je izumila osoba ili grupa poznata pod pseudonimom Satoshi Nakamoto oko 2008. Nitko ne zna identitet ove osobe ili grupe, a koliko je poznato, nestali su i za njih se godinama nije čulo. 11. veljače 2009. Satoshi je na internetskom forumu za ljude koji se bave kriptografskom tehnologijom i zabrinuti za privatnost pojedinaca, otkrio prvi prototip bitcoina. (Pritzker, 2021)

Svatko ima kompletno transparentan pristup svim transakcijama koje se nalaze u javnoj knjizi. Pošto vlade i banke ne podržavaju bitcoin, ono nije zakonsko sredstvo plaćanja u većini dijelova svijeta. Unatoč tome bitcoin je vrlo popularna valuta i pomoću njega su pokrenute mnoge druge kriptovalute koje se nazivaju altcoins. (Investopedia, 2021)

Bitcoin radi kao isključivo elektronička valuta za razmjenu, što znači da se plaćanja šalju izravno od jedne osoba do druge. Računala u cijelom svijetu koriste matematičke funkcije za neovisnu provjeru svih bitcoin transakcija koje se zatim dodaju na javni stalni popis transakcija koji se naziva blockchain. Blockchain je pohranjen na svim tim računalima i radi kao siguran univerzalni zapis o tome tko što posjeduje. U ranoj povijesti bitcoina odrađivalo se vrlo malo transakcija, a kako je popularnost rasla došlo je sve više korisnika i samim time sve više transakcija. (Pritzker, 2021)

Kako bi sačuvali brze, jeftine i pouzdane transakcije bitcoin je podijeljen u dvije valute. Kreiran je bitcoin cash (BCH) koji može odraditi preko 100 transakcija u sekundi dok originalni bitcoin može odraditi do 7 transakcija. Pošto bitcoin cash odrađuje preko 100 transakcija, samim time nagrade su pouzdano manje (Gemini, 2021).

Glavna prednost bitcoina jest autonomija. Ono omogućuje korisnicima veću kontrolu nad vlastitim novcem, korisnik te valute tako može kontrolirati kako troši svoj novac bez da ima posla s nekim drugim oblikom posredničkog tijela. Nadalje kupnja bitcoina je sasvim anonimna osim ako korisnik ne poželi objaviti svoje transakcije. Kupnje koje korisnik izvrši nikada ne uključuju njegov osobni identitet, jer anonimna adresa koja se generira prilikom svake kupnje mijenja se sa svakom novom transakcijom. Sustav plaćanja pomoću bitcoina je isključivo peer-to-peer što znači a korisnik može slati i primati transakcije bez ikakvog odobrenja treće strane. Jedna od zanimljivijih prednosti je to što korisnici bitcoina imaju pristup svojim novcima bilo gdje na internetu, što znači da korisnici nikada ne moraju odlaziti u banku po novac da bi kupili neki proizvod. (Investopedia, 2021)

Slika 1: Primjer trgovine/lokala koji prihvaća bitcoin kao valutu kupnje

Izvor: (Flickr, 2014)

U nastavku je prikazana povijest cijena bitcoina u razdoblju od početka do 2021. godine. „Danas je vrlo lako kupiti bitcoin preko niza mobilnih aplikacija i servisa, poput

najpopularnijih *Coinbasea* i *Revoluta*. No prije takve investicije potrebno je dobro razmisliti. Cijena bitcoina snažno fluktuira, kao što je navedeno, te jedna objava Elona Muska na Twitteru može mu podignuti ili spustiti cijenu za više tisuća dolara u sekundi.“ (Tportal, 2021)

Međutim bitcoin je imao jednu od nestabilnijih povijesti trgovanja. Prvo povećanje cijene kriptovalute dogodilo se 2010. godine kada je bitcoin skočio s 0,0008 USD na 0,08 USD. Promjene cijena bitcoina u isto vrijeme privlače ulagače i raspršuju negativne stavove. (Bytwork, 2021)

Tablica 1: Vrijednost bitcoina (1 BTC) kroz godine - (Američki dolar) USD do 2021. godine

2009. godina	0.0001 USD
2010. godina	> 0.01 USD
2011. godina	1,00 USD
2012. godina	7,00 USD
2013. godina	350,00 – 1.242 USD
2014. godina	340,00 – 530,00 USD
2015. godina	200,00 – 504,00 USD
2016. godina	450,00 – 780,00 USD
siječanj 2017. godine	1.150 USD
prosinac 2017. godine	12.000 – 18.000 USD
2018. godina	3.778 – 6.300 USD
2019. godina	3.339 – 12.637 USD
2020. godina	3.800 – 18,000 USD

Izvor: (Bytwork, 2021)

Iz podataka prikazanih u *tablici 1* vidljivo je kako 2009. godine bitcoin je vrijedio gotovo ništa, korisnici su uglavnom bili obožavatelji kriptografije koji su slali bitcoin jedni drugima u svrhu zabave. Zatim 2010. godine Laszlo Hanyecz napravio je prvu pravu transakciju s kojom je kupio dvije pizze za 10.000 BTC. Nakon par mjeseci u srpnju 2010. godine cijena bitcoina unutar pet dana raste za 1000% sa 0,008 na 0,08 USD. Na početku 2011. cijena bitcoina se izjednačuje sa 1 Američkim dolarom (1 BTC

= 1 USD), nakon toga slijedilo je prvo znatno povećanje cijene na čak 31,00 USD, što bi značilo i nagli pad na 2 USD u prosincu 2011. godine. Zatim cijena je rasla kroz cijelu godinu da bi 2012. se popela na 13 USD, nakon toga cijena je rasla preko 100 USD, da bih u prosincu 2013. godine dospjela čak preko 1000 USD. Između perioda od 2014. do 2016. godine cijena je varirala od 340 USD pa do 800 USD da bih 2017. godine prvi put prešla 2000 USD. Te godine cijena je samo rasla, uz to distribuirao se je bitcoin cash. Tada je cijena dostigla 6000 USD. Nadalje kroz godinu najveća cijena je bila 18000 USD, ali na kraju 2017. godine pala je na 13800 USD. Razdoblje od početka 2018. godine do početka 2019. godine bilo je razdoblje u kojemu je cijena bitcoina bila malo ispod 4000 USD, da bih se kroz 2019. godinu opet popela iznad 10000 USD. Zatim "petak 13-ti" 2020. godine. COVID-19 je proglašen pandemijom i sva tri glavna američka burzovna indeksa su pala. Samim time cijena bitcoina je pala ispod 4000 USD. Do kraja godine cijena se je popela do rekordnih 18000 USD. (Bytwork, 2021)

U nastavku je prikazano kretanje bitcoin cijene u 2021. godini. 2021. godina jest godina u kojoj je bitcoin postigao novu rekordnu cijenu. Razni analitičari govore kako bi mogao dostići cijenu višu od 200.000 dolara. Milijarder Tim Draper 2021. godine za CNBC je izjavio kako predviđa da će bitcoin do početka 2023. godine dosegnuti 250.000 dolara. (CNBC, 2021) „Ili ću biti u pravu ili jako pogriješiti (ali) prilično sam siguran da to ide u tom smjeru.“ (Draper, CNBC, 2021)

Tablica 2: Vrijednost bitcoina (1 BTC) u 2021. godini - (Američki dolar) USD

3. siječnja 2021.	34.800 USD
7. siječnja 2021.	40.000 USD
8. siječnja 2021.	41.973 USD
11. siječnja 2021.	33.400 USD
1. veljače 2021.	33.500 USD
13. ožujka 2021.	60.021 USD
1. lipnja 2021.	37.256 USD

Izvor: (Bytwork, 2021)

Iz podataka prikazanih u *tablici 2* vidljiv je kako uspon koji je bitcoin postigao krajem 2020. godine, zadržava se i 2021. kada u siječnju dostiže novu rekordnu cijenu od 34.800 USD. Uspon se još uvijek zadržava, pa 7. i 8. siječnja cijena raste na 42.000 USD. Nadalje kroz siječanj, cijena se polako spušta za 26% završavajući na 33.400 USD. U veljači, Elon Musk je izjavio da je njegova tvrtka proizvodnje automobila kupila bitcoin u vrijednosti od 1.5 milijardi dolara i da će se u budućnosti bitcoin prihvatiti kao valuta plaćanja. Također COVID-19 pandemija je imala veliku ulogu u rastu bitcoina, jer je sve više ljudi počelo kupovati preko interneta, samim time micati se od fizičkih kovanica ili novčanica. Zbog svih događanja koji su se desila, u ožujku 2021. bitcoin je dostigao novu rekordnu vrijednost od 60.000 USD. Naravno nakon velikog rasta, dolazi i do velikog pada cijene. 13. svibnja 2021. Elon Musk objavljuje tweet na kojemu objašnjava kako Tesla više neće primati bitcoin kao vrstu plaćanja. (Forbes, 2021)

„Tesla je obustavio kupnju vozila putem bitcoina. Zabrinuti smo zbog brzog povećanja upotrebe fosilnih goriva za rudarstvo i transakcije bitcoina, posebno ugljena, koji ima najgore emisije od svih goriva. Kriptovaluta je dobra ideja na mnogim razinama i vjerujemo da ima obećavajuću budućnost, ali to ne može imati velike troškove za okoliš. Tesla neće prodavati nikakav bitcoin i namjeravamo ga koristiti za transakcije čim rudarstvo prijeđe na održiviju energiju. Također gledamo i druge kriptovalute koje koriste <1% energije/transakcije bitcoina.“ (Twitter, 2021)

Nakon te objave bitcoin je počeo naglo padati, poslije toga objavio je još nekoliko objava koje su utjecale na kretanje bitcoina (slika 2). 19. svibnja 2021. cijena je pala na 30.000 USD.

Slika 2: Utjecaj Elona Muska na kretnju cijena bitcoina

Izvor: (https://allinonecrypto.app/blog/analysis/bitcoin/the-elon-musk-bitcoin-saga-continues-btc-rallies-10/)

Nekoliko mjeseci kasnije predsjednik Salvadora najavio je svoje planove kojima bih prihvatio bitcoin kao zakonsku valutu plaćanja, time bih Salvador postala prva država na svijetu koja bih to učinila. (Bytwork, 2021) U lipnju 2021. nakon naglog pada cijene u prethodnom mjesecu, bitcoin se vrača na 37.000 USD i dan danas drži eksponencijalni rast cijene. (Bytwork, 2021)

3.2. Ethereum (ETH)

Ethereum je mreža otvorene decentralizirane računalne platforme koja funkcionira isto kao i bitcoin jer je izgrađena na blockchain tehnologiji. Ethereum je uspio izvući više funkcionalnosti blockchain tehnologije (za razliku od bitcoina). Dopušta programerima da pokreću programe poznatima pod *smart contracts* koji mogu učitati decentraliziranu aplikacije koje su poznate pod imenom "dApps". Ethereum radi pomoću računalne snage. Znači da korisnici pomoću računala pokreću specifičan program ili čvor. Ethereum ovisi o administratorima čvorova (nodes) koji upravljaju razmjenama na ethereum mreži. Oni prikupljaju troškove ili naknadu za

pokretanje hardvera i softvera potrebnih za rad. Naknade nazivamo troškovima plina (eng. Gas fees) jer održavaju rad mreže i isplaćuju se u ether-u (ETH). Ether je digitalna valuta ethereum-a. Svrhe ethera su pohranjivanje vrijednosti, podmirivanje transakcija i olakšavanje mrežnih operacija. (Grayscale Investments, 2020)

Smart contracts ili pametni ugovori su kodovi koji korisnicima omogućavaju i olakšavaju razmjenu vrijednosti. To su mali programi koji su pohranjeni na ethereum blockchain-u i mogu se izvršiti samo kada su ispunjeni određeni uvjeti. Transakcije koje su učitane i izvršene u blockchain-u na dalje se ne mogu mijenjati. Pomoću njih korisnik može slati i primati ether. (Grayscale Investments, 2020)

Prema Coin Metricsu, ether je 10. svibnja 2021. godine postigao rekordnu cijenu koja se je digla preko 25.000 HRK (slika 3).

Slika 3: Kretanje cijene ethera u 2021. godini

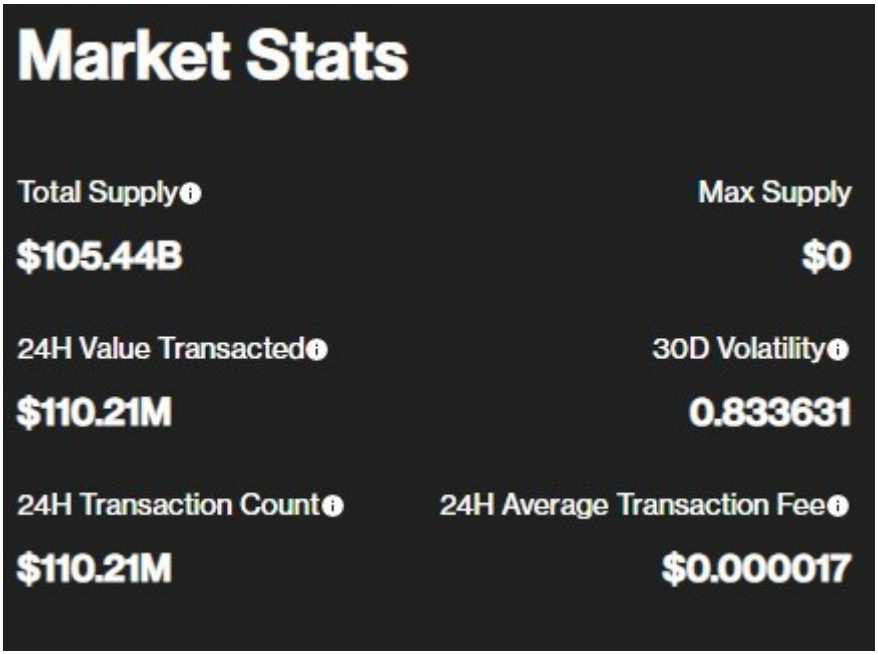
Izvor: (https://www.tradingview.com/chart/)

Slika 4: Cijene ethera od početka do 2021. godine

Izvor: (https://www.tradingview.com/chart/)

3.3. Stellar (XLM)

Stellar je kriptovaluta uz koju možete stvarati, slati i trgovati digitalno svim valutama poput dolara, pesosa, bitcoina i gotovo bilo koje druge vrste. Izgrađen je kako bi omogućio svim financijskim sustavima u svijetu da komuniciraju putem jedne mreže. Stellar je uglavnom platforma koja povezuje bankovne sustave plaćanja i ljude koji žele brzo i pouzdano prebacivanje novca i to bez ikakvih dodatnih troškova. Stellar koristi lumene kao jedinicu digitalne valute. Jedan lumen je jedinica digitalne valute isto kao i bitcoin. Stellar za razliku od drugih kriptovaluta ima ugrađenu inflaciju kao dio svoje mreže. To znači da se svake godine stvaraju novi lumeni. Prema coindesk.com trenutno na svijetu cirkulira 105.44 milijardi lumena (slika 5). S time da pomoću inflacije od 1% se svake godine kreira više od 150 milijuna novih lumena. (Stellar, 2021)



Slika 5: Prikaz zalihe stellar lumena 2021. godine

Izvor: (https://www.coindesk.com/price/stellar/)

Jedna od važnijih stvari u pitanju kriptovaluta i blockchain-a je mogućnost brzih transakcija. Što se više transakcija može obraditi u sekundi to je veća prednost prema konkurenciji. Stellar ima uobičajeno vrijeme potvrde transakcije od tri do pet sekundi, dok s ethereum-om može potrajati i do 15 minuta, a s bitcoinom i do 60 minuta. Što se tiče transakcija po sekundi, tim stellar mreže tvrdi da je moguće proizvesti više od 5000 transakcija u sekundi, za razliku od bitcoina koji obavlja maksimalno do 7 transakcija, a ethereum oko 30 transakcija po sekundi. (Medium, 2018)

U nastavku je objašnjeno putno plaćanje pomoću stellara. Stellar omogućuje korisniku da pošalje jednu valutu drugom korisniku. Također i da jedan korisnik pošalje jedan token jedne valute, a primatelj primi token u drugoj valuti, bez ikakvih gubitaka ili rizika.

Postupak putnog plaćanja (Stellar, 2021):

1. Pošiljatelj u Americi ima tokene u dolarima i daje signal mreži da želi poslati tokene pesosa primatelju.
2. Zatim mreža putem decentralizirane razmjene pronalazi najbolju cijenu za

pošiljatelja.

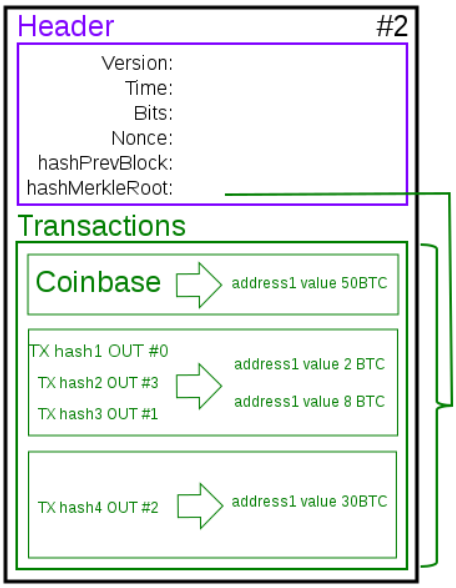
3. Mreža zaključava iznos i cijenu.
4. Pošiljatelj potvrđuje transakciju i tokeni dolara napuštaju njegov račun.
5. Transakcija se zatim izvršava i primatelj dobiva tokene pesosa.

4. BLOCKCHAIN TEHNOLOGIJA

Korisnici blockchain mreže mogu podnositi transakcije na mrežu putem različitih softverskih platformi. Ove se transakcije šalju na određeni poslužitelj ili čvorove unutar blockchain zajednice. Transakcije se zatim šire na druge čvorove u mreži. Međutim, ovaj proces ne stavlja transakcije u blockchain. Za većinu blockchain implementacija, transakcija na čekanju dodaje se u blockchain red prije nego što se doda u mrežu. Transakcije se dodaju u blockchain kada izdavački čvor objavi blok. Blockchain jest lanac više malih blokova koji sadrže informacije. Kako raste broj transakcija, tako raste i blockchain. To je tehnika koja je napravljena da se spreme digitalni dokumenti tako da je poslije nemoguće manipulirati s njima. Blokovi bilježe i potvrđuju vrijeme i slijed transakcija, koje se zatim prijavljuju u blockchain, unutar diskretne mreže uređene pravilima o kojima se dogovore sudionici mreže. Svaki blok se sastoji od zaglavlja bloka i podataka o bloku (slika 6) (Yaga, Mell, Roby i Scarfone, 2018).

Zaglavlje bloka sastoji se od:

- Broja bloka
- Hash vrijednosti prethodnog bloka
- Hash prikaz podataka bloka (npr. Merkle tree)
- Vremenske oznake
- Veličine bloka
- Vrijednosti *nonce* (pojašnjeno u odjeljku 4.2.)



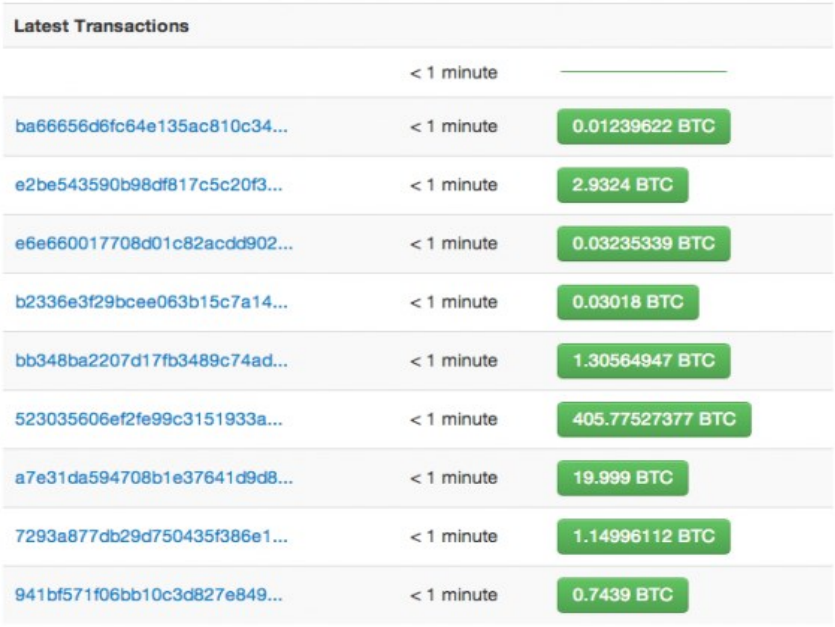
Slika 6: Struktura bloka u blockchain mreži

Izvor: (https://commons.wikimedia.org/wiki/File:Bitcoin_block_structure.svg)

Blockchain tehnologija osigurava sigurnost svih transakcija kriptovaluta. Za to se koristi koncept "ključa" (pojašnjeno u odjeljku 7. *Transakcije*). Dakle svaki korisnik dobiva svoju jedinstvenu identifikaciju pomoću skupa šifriranih ključeva. Postoje privatni i javni ključ. Korisnikov javni ključ služi za pronalazak korisnika na mreži, a privatni ključ služi kao autorizacija svih transakcija koje su povezane sa javnim ključem. Javni ključ se koristi kao adresa digitalnog novčanika, a privatni ključ se koristi da bi se digitalno novac podizao, poslao ili kupio. Ako netko sazna tuđi privatni ključ, tada bi mogao pristupiti svim digitalnim valutama i zloupotrijebiti ih. Prije bitcoina naviknulo se centralizirane usluge, to znači da postoji jedan entitet koji pohranjuje sve podatke i da bih dobili sve te podatke mora se komunicirati samo s pojedinim entitetom. Primjer toga je bankovni sustav. Banka kao entitet pohranjuje novac i jedini način da bih platili nekome ili podigli svotu novca je prolazak kroz bankovni sustav. Dok u decentraliziranom sustavu informacije ne pohranjuje samo jedan entitet, nego sva računala u toj mreži pohranjuju i posjeduju informacije. Ideja bitcoina je bila da ne postoji treća strana između vas i korisnika s kojim se razmjenjuju informacije. Upravlja se vlastitim valutama i može ih se slati bilo kome u bilo kojem trenutku bez smetnje trećih strana (Stephen i Alex, 2018).

Zbog decentralizirane prirode bitcoina, svim transakcijama može svjedočiti svatko s osobnim čvorom ili pomoću pretraživanja blockchaina. Svaki blok ažurira se vlastitom kopijom lanca, koja se potvrđuje i dodaje. Dakle, ako korisnik želi vidjeti povijest transakcija, neće vidjeti ime i prezime te osobe, već će vidjeti javnu adresu te osobe.

Dakle stvarni identitet osobe je sakriven, ali se i dalje mogu vidjeti sve transakcije koje su izvršene preko javne adrese (slika 7) (Investopedia, 2021).



Slika 7: Primjer transakcije Bitcoina

Izvor: (https://www.coindesk.com/markets/2013/12/20/blockchaininfo-the-worlds-most-popular-bitcoin-website-and-wallet/)

Blockchain je nepromjenjiv, što znači da nakon što je nešto uneseno u blockchain, to se nadalje ne može promijeniti. To se postiže uz pomoć kriptografske hash funkcije.

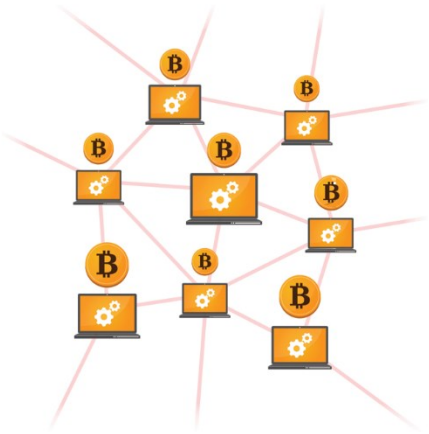
„Hashing je transformacija informacija bilo koje duljine i veličine do određenih parametara, koji su definirani hash funkcijom. Za funkcije nije važno koliko je informacija izvorno uneseno. Nakon što se obavlja hash funkcija, bez obzira na početnu količinu informacija, samo fiksni niz znakova koji se naziva hash. Na primjer, u bitcoinu, hash se sastoji od 64 znaka ili 256 bita, a svi digitalni kovanice, brojevi

transakcija, ključevi i novčanici u kripto valutnim sustavima imaju ovu vrstu raspršenog niza.“ (Chwilowek, 2021)

4.1. Rudarenje valuta

Rudarenje kriptovaluta je postupak kojim se transakcije dodaju u javnu knjigu blockchain-a. Bitcoin je najpopularnija kriptovaluta koja se može rudariti, ali također ne mogu se sve kriptovalute rudariti. Da bi se kriptovalute rudarile potrebno je računalo i poseban program za rudarenje. Za rudarenje pomoću tih programa potrebno je računalo s visokim specifikacijama.

Kako je rudarenje postajalo sve popularnije, pristigao je i algoritam tolerancije grešaka. bitcoin-ov Proof-of-Work. Dakle, na bitcoin mreži (slika 8) imamo čvorove koji su poznatiji kao "rudari". Mrežni čvor je točka povezivanja koja može primati, stvarati, pohranjivati i slati podatke pomoću mreže. Jednostavnije rečeno, svako računalo je zaseban čvor. Sva računala su povezana međusobno i mogu isto tako primati, stvoriti, pohraniti i slati podatke. Algoritam tolerancije grešaka nam dolazi od pretpostavke da se nikome na spomenutoj mreži ne može vjerovati. Zbog toga bitcoinov Proof-of-Work osigurava mrežnu suglasnost tj. sigurnost rada čak i ako čvorovi nisu usklađeni. Odnosno, ako postoji čvor koji ne radi. (Simplilearn, 2021)



Slika 8: Bitcoin mreža

Izvor: (https://www.facebook.com/BITPANDA/photos/who-controls-the-bitcoin-networknobody-owns-the-bitcoin-network-much-like-no-one/1430006697013858/)

4.2. Postupak rudarenja

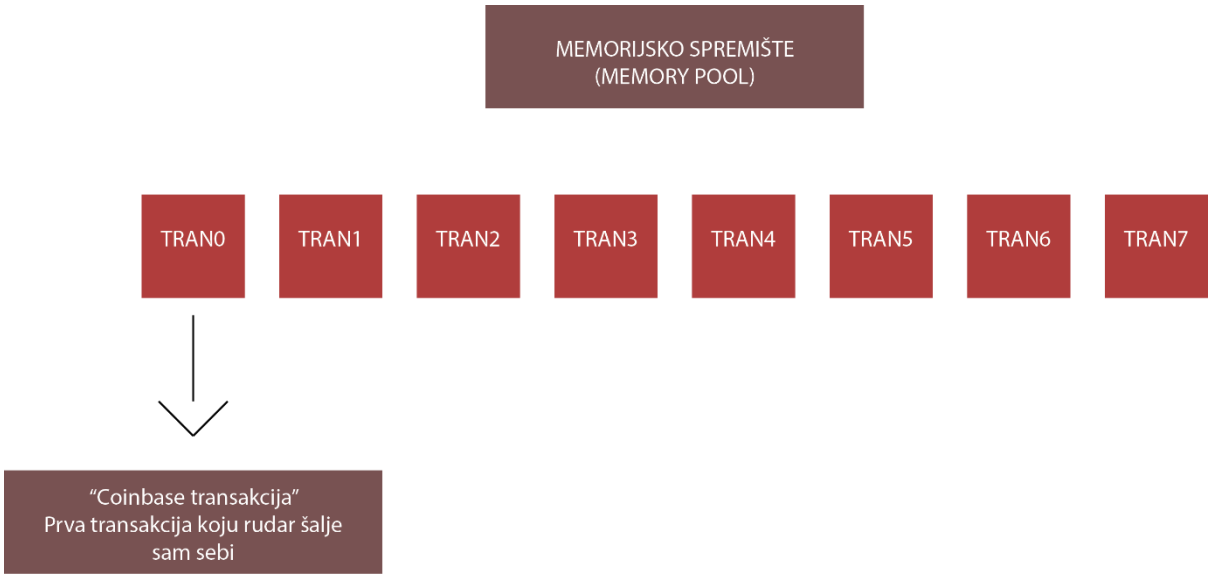
Rudarenje bitcoina bazira se na aktivnostima korisnika putem odgovarajućih softvera i hardvera. Rudarstvo izvode korisnici mreže, također ono zahtjeva takozvani Proof-of-Work. To zahtjeva poveliki broj proračuna koje se izvršava preko računala korisnika u cilju da se riješe kriptografske zagonetke (*eng. hash puzzle*). Rudar je čvor u mreži koji prikuplja transakcije i organizira ih u blokove. Kada god je transakcija izvršena, svi mrežni čvorovi primaju i provjeravaju valjanost te iste transakcije. Nakon toga rudarski čvorovi prikupljaju transakcije iz memorijskog spremišta (*eng. memory pool)* (slika 10) i stvaraju blok kandidata (*eng. candidate block*)[2].

Prvi korak rudarenja bloka je pojedinačno raspršivanje (*eng. hashing*) svake transakcije preuzete iz memorijskog spremišta, ali prije početka procesa rudar dodaje transakciju u kojoj sami sebi šalju nagradu za rudarenje (nagrada bloka). Ova se transakcija naziva coinbase transakcija, to je prva transakcija (slika 10) koja se bilježi u novom bloku. Nakon što se transakcija hash-ira, formira se hash tree (*eng. Merkle tree*) (slika 13). Ono se formira razdvajanjem različitih hash blokova u parove i zatim ih se opet hash-ira (slika 12). Taj dio se ponavlja sve dok se ne dospije do vrha stabla koji se naziva hash root (*eng. Merkle root*). Taj vrh stabla odnosno hash root je zapravo jedan "hash" koji predstavlja sve ostale prethodne hasheve koji su korišteni da bi se došlo do vrha. Nakon svega toga vrh stabla (root hash), zajedno s hash-om prethodnog bloka i nasumice generiranim brojem koji se naziva nonce[3] stavlja se u zaglavlje bloka (*eng. block's header*). Rezultat toga je hash bloka. Da bi se mogao smatrati valjanim, izlaz (hash bloka) mora biti manji od određene ciljne vrijednosti koja je određena protokolom. (Simplilearn, 2021)

[2] Blok kandidata je blok koji rudarski čvor (rudar) pokušava minirati kako bi primio nagradu za blok.
[3] Nonce se odnosi na broj ili vrijednost koja se može koristiti samo jednom.

Slika 9: Memorijsko spremište

Izvor: Obrada autora

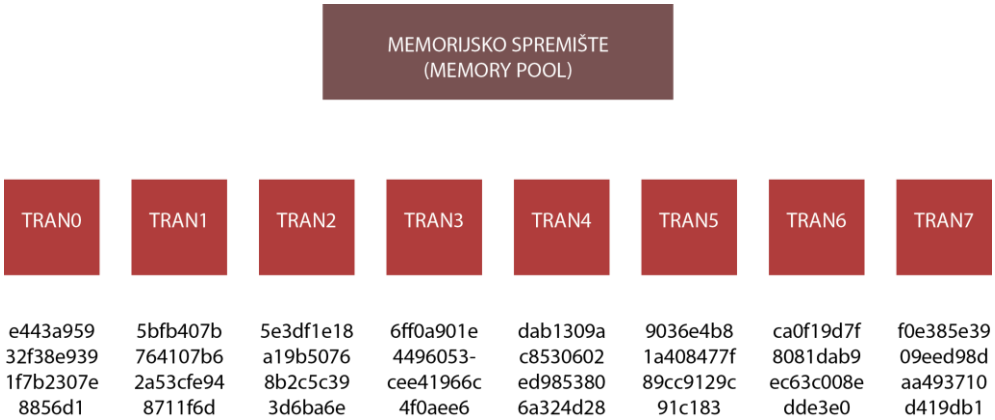


Slika 10: Prva transakcija

Izvor: Obrada autora

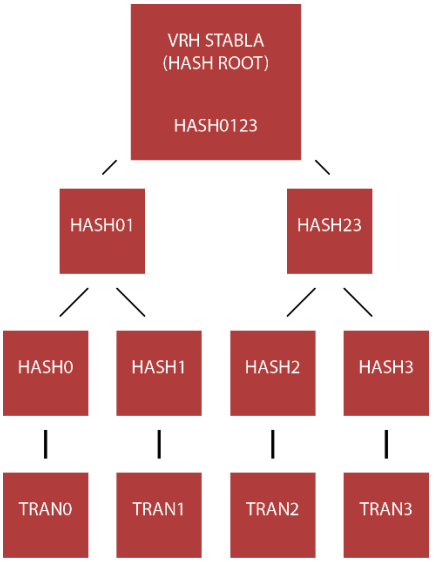
Slika 11: Metoda "hashiranja"

Izvor: Obrada autora



Slika 12: Hashirani blokovi unutar memorijskog spremišta

Izvor: Obrada autora



Slika 13: Merkle tree

Izvor: Obrada autora

4.3. Softver i hardver za rudarenje

Početkom bitcoina korisnici su mogli rudariti blokove s običnim računalom, ali kako su bitcoin i ostale kriptovalute napredovale, to više nije moguće. Ako bih netko želio rudariti kriptovalute u današnjem vremenu, potrebna mu je velika računalna snaga. Ako bih korisnik želio rudariti, potrebno mu je početno ulaganje u skupocjenu opremu. Ta oprema se može sastojati od nekoliko različitih hardvera, a najpopularniji su (Investopedia, 2021):

- ASIC (*eng. Application Specific Integrated Circuit)*
- Grafičke kartice (*eng. GPU)*

ASICs se koriste za rudarenje određenih kriptovaluta na temelju velike izlazne snage računala, ali isto tako konzumiraju puno električne energije.

Najbolji ASICs uređaj na tržištu 2021. godine jest „Whatsminer M32-70“ (slika 14). Uređaj se može pronaći po cijeni od 6200 USD, konzumira 3360W i može proizvesti 70 TH izračuna u sekundi (Techradar, 2021).

Slika 14: Whatsminer M32-70

Izvor: (https://www.techradar.com/best/asic-devices)

Grafičke kartice se koriste kako bih imali što veću računalnu snagu, što više grafičkih kartica korisnik ima, to mu je veća računalna snaga. Kako je rudarenje na vrhu popularnosti, konkurencija je velika. Zbog toga rudari se okreću najboljim i najjačim grafičkim karticama, koje se inače spajaju skupa u takozvanu rudarsku platformu (*eng. Mining rig)* (slika 15).

Slika 15: Rudarska platforma (*eng. Mining rig)*

Izvor: (https://freedomnode.com/blog/how-to-build-a-mining-rig-step-by-step-guide/#h-what-to-consider-when)

Rudarska platforma je skup moćnih komponenata koje su spojene tako da proizvode što više računalne snage za rudarenje kriptovalutama, što u cijelosti znači i mogućnost obavljanja što više izračuna u sekundi. Pri izgradnji rudarske platforme potrebno je uzeti u obzir nekoliko stvari (Freedomnode, 2018):

- Koliko izračuna u sekundi može izvesti (*eng. Hashrate).*
- Koliko električne energije će platforma koristiti.
- Proučiti i istražiti cijene i raspoloživost opreme koja je potrebna za izradu.

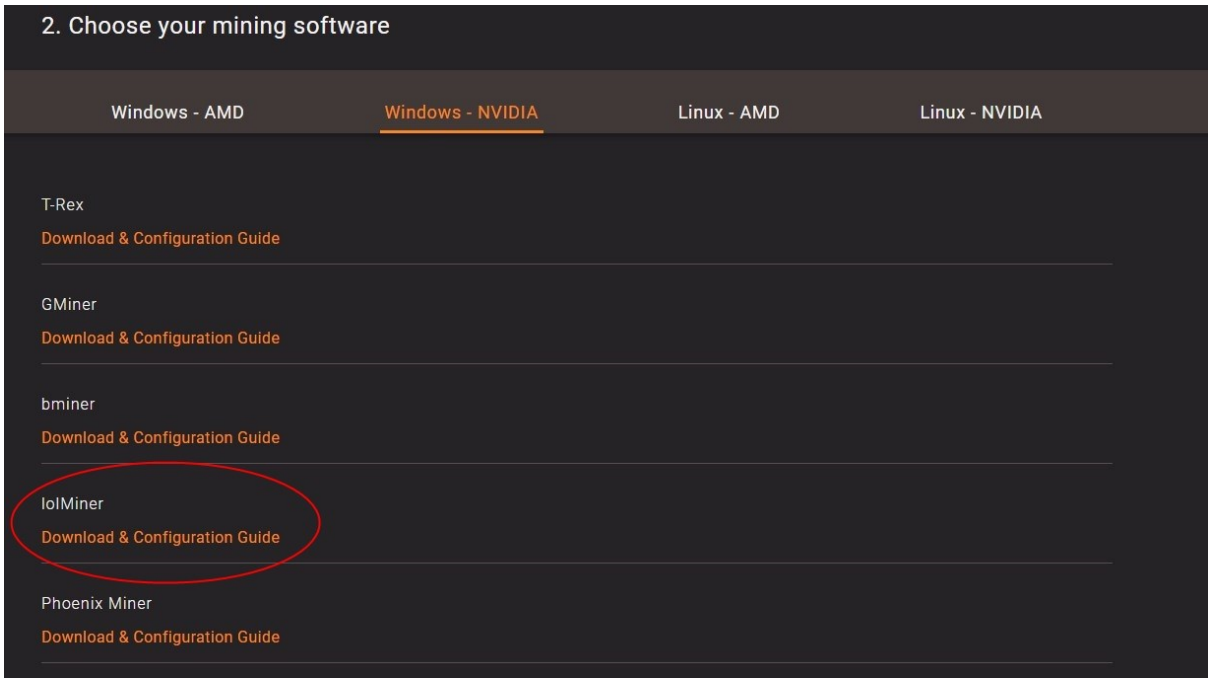
- Imati na umu troškove koje dovodi platforma. Troškovi održavanja i rashladnog sustava.

Za izgradnju rudarske platforme potrebne su sljedeće glavne komponente. One se sastoje od matične ploče, grafičke kartice i napajanja. (Freedomnode, 2018)

Prema Windowscentral (2021), najbolje grafičke kartice na tržištu za rudarenje kriptovaluta su:

1. NVIDIA GeForce RTX 3060 Ti
2. NVIDIA GeForce RTX 2070
3. AMD Radeon RX 5700 XT
4. NVIDIA GeForce RTX 3090
5. AMD Radeon RX 580
6. NVIDIA GeForce GTX 1660 SUPER

Slijedi opis postupka rudarenja preko osobnog računala autora ovog završnog rada. Da bi rudario, korisnik može pronaći rudarski bazen[4] (*eng. Mining pool)*. Primjer jednog je ethermine. Prva stvar koju korisnik mora imati jest adresu svog novčanika (više vidjeti u poglavlju *6. Novčanici*). Nakon što je adresa novčanika uparena sa sustavom ethermine slijedi odabir softvera koji odgovara grafičkoj kartici korisnika (slika 16). Za primjer koristi se grafička kartica proizvođača NVIDIA i rudarski softver pod nazivom *lolMiner.*



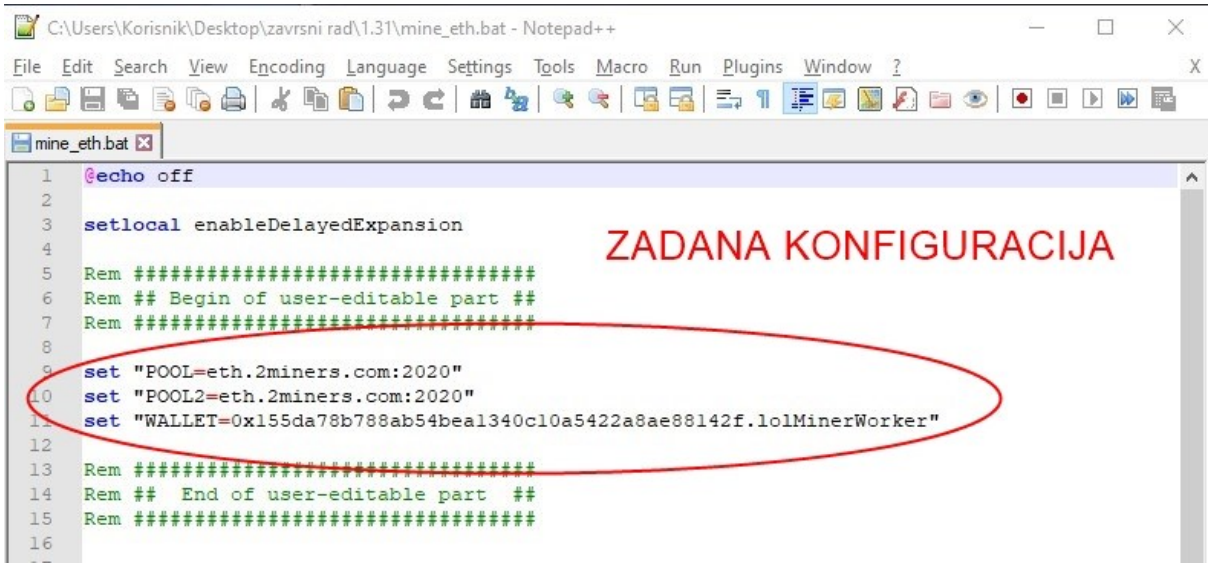
Slika 16: Odabir softvera za rudarenje na ethermine.org

Izvor: Obrada autora

Nakon odabira softvera prigodnog za grafičku karticu koja se koristi, softver se može vrlo jednostavno preuzeti sa Github repozitorija. Prije samog početka rudarenja mora se doraditi već prije konfigurirana datoteka unutar preuzetog softvera. Za primjer je korištena datoteka *mine_eth.bat* koja služi za rudarenje ethereuma. Prilikom otvaranja datoteke *mine_eth.bat* postavljene su već postojane konfiguracije servera *pool-a* i adrese novčanika (slika 17). Zatim pomoću uputa danih na *ethereum.org* postavlja se točan server *pool-a* (ovisno o lokaciji korisnika) i vlastita adresa novčanika

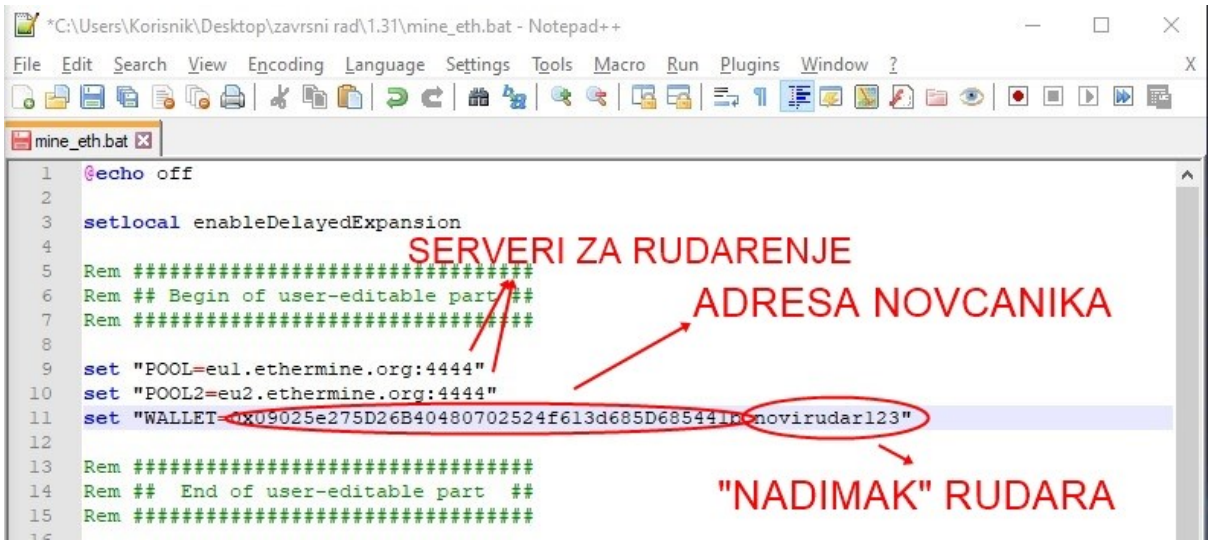
[4] Rudarski bazen je zajednička skupina rudara kriptovaluta koji kombiniraju svoje računske resurse preko mreže kako bi povećali vjerojatnost pronalaska bloka ili na drugi način uspješno rudarenje kriptovalute (Investopedia, 2021).

skupa sa dodanim nazivom rudara (slika 18).



Slika 17: Zadana konfiguracija unutar datoteke mine_eth.bat

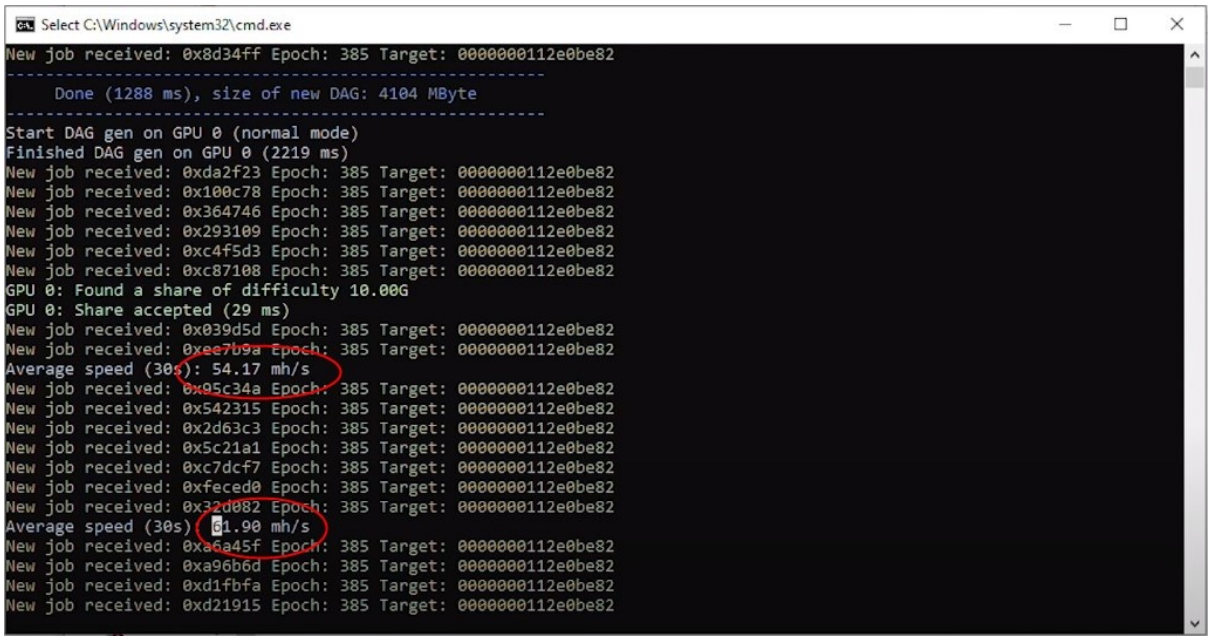
Izvor: obrada autora



Slika 18: Vlastita konfiguracija datoteke mine_eth.bat

Izvor: obrada autora

Nakon pokretanja datoteke *mine_eth.bat* korisnik/rudar pokreče postupak rudarenja. Pokrenuta datoteka pokreče ujedno i grafičku karticu koja radi na maksimalnoj brzini kako bi što prije obradila podatke. Zatim svakih nekoliko sekundi korisniku na uvid dolazi brzina kojom rudari (slika 19).



Slika 19: Prikaz brzine rudarenja

Izvor: Obrada autora

5. NOVČANICI

Izvorni softver za bitcoin koji je objavio Satoshi došao je sa softverskim novčanikom. Ovaj bi novčanik generirao vaš par privatnih/javnih ključeva (javni ključ koristi se za kreiranje korisnikove bitcoin adrese, a korisnikov privatni ključ omogućuje potpisivanje transakcija za trošenje novčića s te adrese). (Pritzker, 2021)

U nastavku se opisuju opći pojmovi i vrste novčanika za spremanje kriptovaluta. Novčanici se koriste za interakciju s blockchain mrežom. Hardverski, softverski i papirnati. Kripto novčanici zapravo ne pohranjuju valutu već generiraju informacije za primanje i slanje novca pomoću blockchain transakcija. Postoje privatni i javni ključevi, pomoću njih se generira alfanumerički podatak kojeg zovemo adresom novčanika. S adresom određujemo mjesto na koje se može prebacivati novac u blockchain mrežu. Privatni ključ je većinom podijeljen s vama, osim ako ne koristite novčanik koji je dio aplikacije ili softvera, tada nemate pristup svom javnom ključu i izloženiji ste napadima i krađi podataka treće strane. Novčanici se dijele na tople i hladne novčanike. Topli novčanici ili softverski novčanici (detaljnije vidjeti u odjeljku 5.3. *Softverski novčanici*) su povezani s internetom što znači da su manje sigurni i predstavljaju veći rizik. Laki su za korištenje i jednostavno ih je za postaviti. Preuzme li se mobilna ili desktop aplikacija za rad s kriptovalutama. Čim je račun kreiran, kreira se i topli novčanik. Prilikom kreiranja računa odmah se kreira i novčanik koji se može koristiti na toj aplikaciji i preko njega slati i primati transakcije. Pošto je novčanik dio aplikacije, vlasnik nema pristup svome javnom ključu, nego se o tome brinu kreatori aplikacije. Samim time korisnik je izloženiji hakerskim napadima i krađi podataka s treće strane. Topli novčanici namijenjeni su korisnicima koji svakodnevno trguju malim transakcijama. Pri svemu rečenom, spremanje velike količine kriptovaluta na topli novčanik nije preporučeno. Hladni novčanici pohranjuju sve informacije izvan mreže i ne zahtijevaju internetski vezu. Oni se smatraju najsigurnijim za pohranu kriptovaluta. Hladni novčanici povezuju se internetskom vezom samo kada je potrebno učiniti transakciju. U hladne novčanike spadaju hardverski i papirnati novčanici. Najpopularniji od ta dva su hardverski jer se lako koriste i uz njih dolazi korisnička podrška koju pruža proizvođač tog novčanika. Ako se kriptovalute pohranjuju na hardverski novčanik, kriptovalute se šalju s toplog novčanika (aplikacije) pomoću javne

adrese. Ako se šalju s hladnoga na topli postupak je isti. Prilikom slanja valute s hardverskog novčanika na potpuno drugu adresu, prvo se povezuje vlastiti novčanik s internetom pomoću softvera načinjenog za taj uređaj, a zatim se potpisuje transakcija privatnim ključem (slika 20) (Youtube, 2021).

Slika 20: Postupak povezivanja hardverskog novčanika na internetsku vezu

Izvor: (https://www.thecryptomerchant.com/blogs/resources/how-to-send-coins-from-an-exchange-to-a-hardware-wallet)

5.1. Papirnati novčanici

Papirnati novčanici (eng. *Paper wallets)* funkcioniraju slično poput hardverskih, ali kao što i sama riječ govori, papirnati novčanici su komad papira na kojemu je javna adresa novčanika i privatni ključ istoga. Ono što nedostaje papirnatim novčanicima jest što su nepraktični za svakodnevne transakcije. Da bi se kreirao papirnati novčanik koristi se bankomat za trgovanje kriptovalutama. Prije nego što se umetne gotovina, bankomat kreira javnu adresu i javni ključ. Zatim pritiskom na "Kreirajte novi novčanik"

bankomat kreira transakciju u papirnatom obliku (slika 21) (Athenabitcoin, 2018).

Slika 21: Prikaz papirnatog novčanika

Izvor: (https://www.athenabitcoin.com/news/2018/4/9/how-to-use-a-paper-wallet)

Neki od najpopularnijih softverskih novčanika su Coinbase Wallet, Gemini, BlockFi, Crypto.com i ZenGo. U slučaju hardverskih novčanika najbolji su Ledger Nano X, Trezor One, Trezor Model T, SafePal S1 i Ellipal Titan. (Benzinga, 2021)

5.2. Hardverski novčanici

Hardverski novčanici (eng. *Hardware wallets)* su često veličine i izgledom slični kao obični USB prijenosnik. U hardverskom novčaniku se ne pohranjuju same kriptovalute, nego samo privatni ključ. Ako se ikada desi da je hardverski novčanik ukraden, osoba ne može pristupiti korisnikovom privatnom ključu jer je novčanik zaštićen s PIN-om i dodatnih 24 nasumično generiranih riječi koje se generiraju kada

vlasnik novčanika prvi put upali uređaj. Te riječi je potrebno zapisati na papirić ili na neko sigurno mjesto. Naime, ako se novčanik izgubi ili je ukraden, vlasnik novčanika može vratiti svoje privatne ključeve samo ako kupi novi uređaj i u njega unese 24 riječi i pin s prijašnjeg uređaja. Na primjeru uređaja Ledger Nano X, ako je PIN krivo unesen tri puta, Ledger uništava sve podatke i resetira se na tvorničke postavke. (Hardware Wallets, 2021)

Slika 22: Hardverski novčanik Ledger Nano X

Izvor: (https://www.buybitcoinworldwide.com/wallets/ledger-nano-x/)

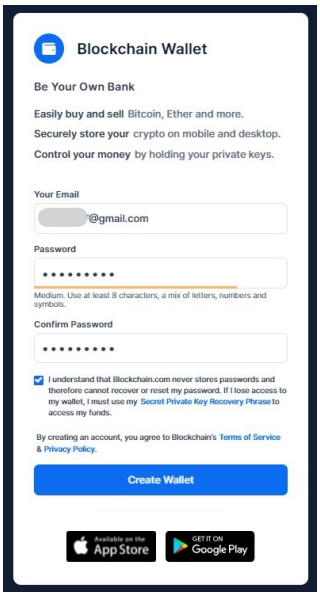
5.3. Softverski novčanici

Softverski novčanici (eng. *Software wallets)* spadaju u tople novčanike. Znači da koriste internetsku mrežu i pohranjeni su na vašem uređaju bilo to računalo ili mobilni uređaj. Softverske novčanike možemo podijeliti u tri skupine (Investopedia, 2021):

- Web novčanici
- Desktop novčanici
- Mobilni novčanici

Web novčanicima pristupa se pomoću Internet preglednika. Omogućeno je direktno pristupanje blockchainu bez preuzimanja programa ili aplikacija na uređaj.

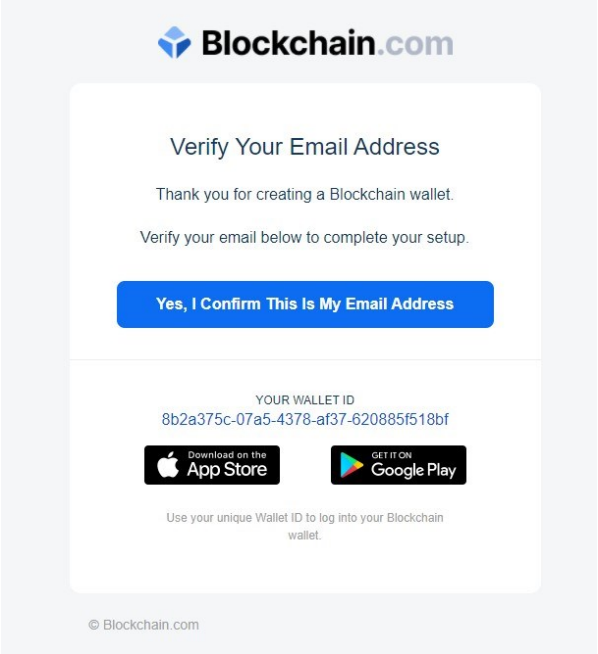
Kreiranje web novčanika vrlo je jednostavno. Kao primjer koristi se blockchain.com novčanik. Prvim klikom na web stranicu, dobije se upit koji pita korisnika želi li se prijaviti ili registrirati. Klikom na registraciju otvara se novi prozorčić u kojemu korisnik unosi svoj email, lozinku i zatim potvrdu lozinke (slika 23).



Slika 23: Registracija web novčanika

Izvor: Obrada autora

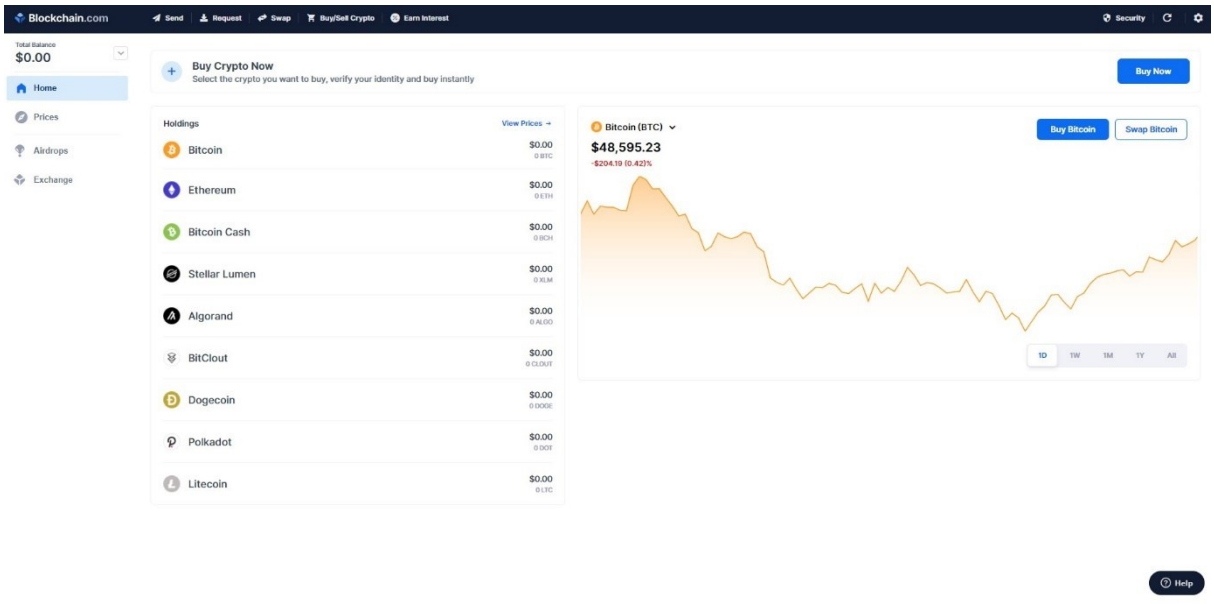
Nakon što korisnik upiše potrebne podatke, klikom na gumb za registraciju, otvara se novi prozorčić u kojemu korisnika pita za potvrdu svog email-a klikom na poveznicu koja je stigla na korisnikov upisani email (slika 24). Unutar email poruke koja je stigla, odmah se može vidjeti vlastita adresa novčanika.



Slika 24: Potvrda email-a prilikom registracije web novčanika

Izvor: Obrada autora

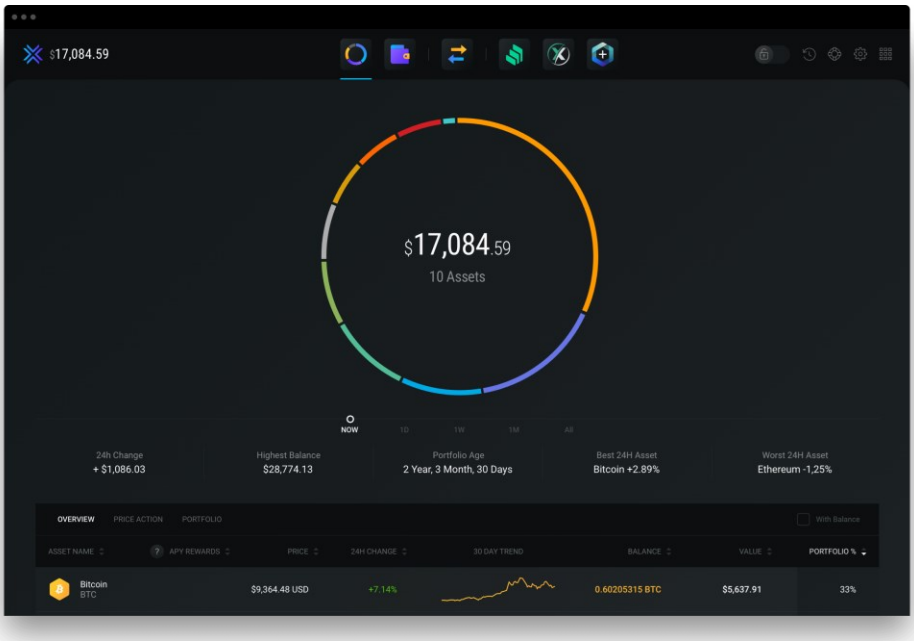
Kada je korisnik potvrdio svoj račun, prilikom prve prijave potrebna je autorizacija uređaja s kojeg se prijavljuje. To se odrađuje tako da nakon upisivanja lozinke, na email stiže poruka koju korisnik potvrđuje. Nakon toga je korisnik uspješno prijavljen i može koristiti svoj web novčanik (slika 25).



Slika 25: blockchain.com web novčanik

Izvor: Obrada autora

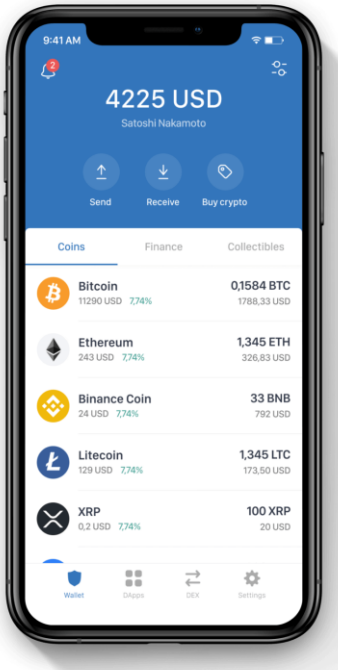
Za razliku od web novčanika, **desktop novčanici** se preuzimaju. Desktop novčanik je računalni program koji se preuzima i instalira na računalo korisnika. Također pomoću desktop novčanika imamo pristup ključevima. Oni se generiraju pri prvom pokretanju programa. Pošto korisnik ima pristup ključevima, važno je smisliti jedinstvenu lozinku.



Slika 26: Primjer desktop novčanika

Izvor: (https://www.exodus.com)

Mobilni novčanici rade na istom principu kao i desktop novčanici. Razlikuju se po tome što je mobilni novčanik dostupan samo kao aplikacija za mobilni uređaj. Jedna od prednosti mobilnog novčanika je da ga se može koristiti bilo gdje i bilo kada.



Slika 27: Primjer mobilnog novčanika

Izvor: (https://trustwallet.com)

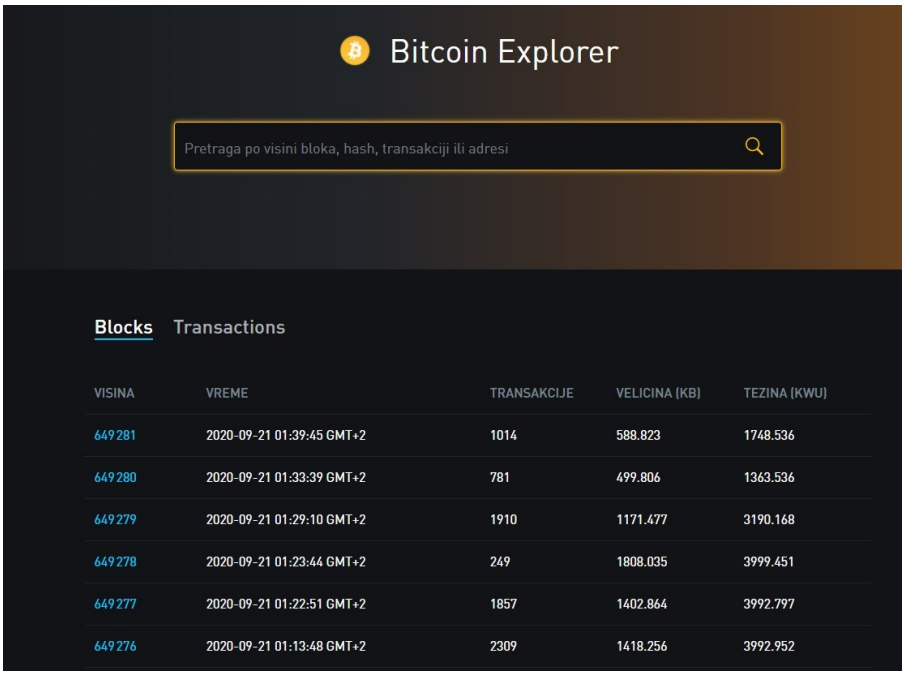
6. TRANSAKCIJE

Kako bi izvršili transakciju već određenog iznosa s jednog novčanika na drugi nam je javni ključ, privatni ključ i kriptografski potpis.

Adresa ili javni ključ jedinstvena je osobna adresa koja se dijeli u blockchainu. Javni ključ je kriptografski kod koji se generira algoritmima za šifriranje asimetričnog ključa i koristi se za pretvaranje poruke u nečitljiv format. Javni ključ sastoji od izuzetno dugog niza brojeva, on se komprimira i skraćuje kako bi se stvorila javna adresa. Ako vlasnik izgubi svoj javni ključ, moguće ga je ponovno stvoriti pomoću privatnog ključa. **Privatni ključ** je tajni ključ koji poznaje samo njegov vlasnik, a privatni i javni ključ upareni su tako da primatelj može upotrijebiti odgovarajući ključ za dešifriranje teksta šifre i čitanje izvorne poruke. Privatni ključevi generiraju se pomoću istih algoritama koji stvaraju javne ključeve za stvaranje jakih ključeva koji su matematički povezani. **Kriptografski potpis** koristi posebne algoritme nekog javnog ključa tako da osiguraju cjelovitost podataka. Kada se podaci potpisuju digitalnim potpisom može se lako provjeriti da podaci potječu od korisnikove strane i da nisu krivotvoreni ili promijenjeni nakon što je korisnik potpisao određenu stvar (Stephen i Alex, 2018).

Svakih 10 minuta stvara se novi blok i dodaje se u blockchain postupkom rudarstva. Tako se provjeravaju i pohranjuju sve nove transakcije. Tada se može sa sigurnošću reći da je transakcija potvrđena. Npr. kada se šalje jedna vrsta kriptovalute od strane jednog korisnika drugome, transakcija će ostati nepotvrđena sve dok se ne stvori sljedeći blok. Nakon stvaranja bloka ta transakcija će imati jednu potvrdu, tako nakon svakih 10 minuta mreža ponovo potvrđuje transakciju (Medium, 2017).

Neke usluge zahtijevaju samo jednu potvrdu ili su jednostavno potvrđene istog trenutka. Dok će mnoge druge tvrtke zahtijevati mnogo više, jer svaka potvrda transakcije smanjuje mogućnost storniranja te iste. Uobičajeno je da se traži 6 ili više potvrda, što može trajati i do 2 sata. Nakon što je transakcija izvršena, novčanik nudi mogućnost pregledavanja te iste tako da vam prikaže ID transakcije. Pomoću dobivenog ID-a može se provjeriti broj potvrda za tu transakciju. Kao primjer korištena je web stranica *blockchain.com* (slika 28).



Slika 28: Sučelje provjera blokova transakcija blockchain.info

Izvor: (https://www.blockchain.com/explorer)

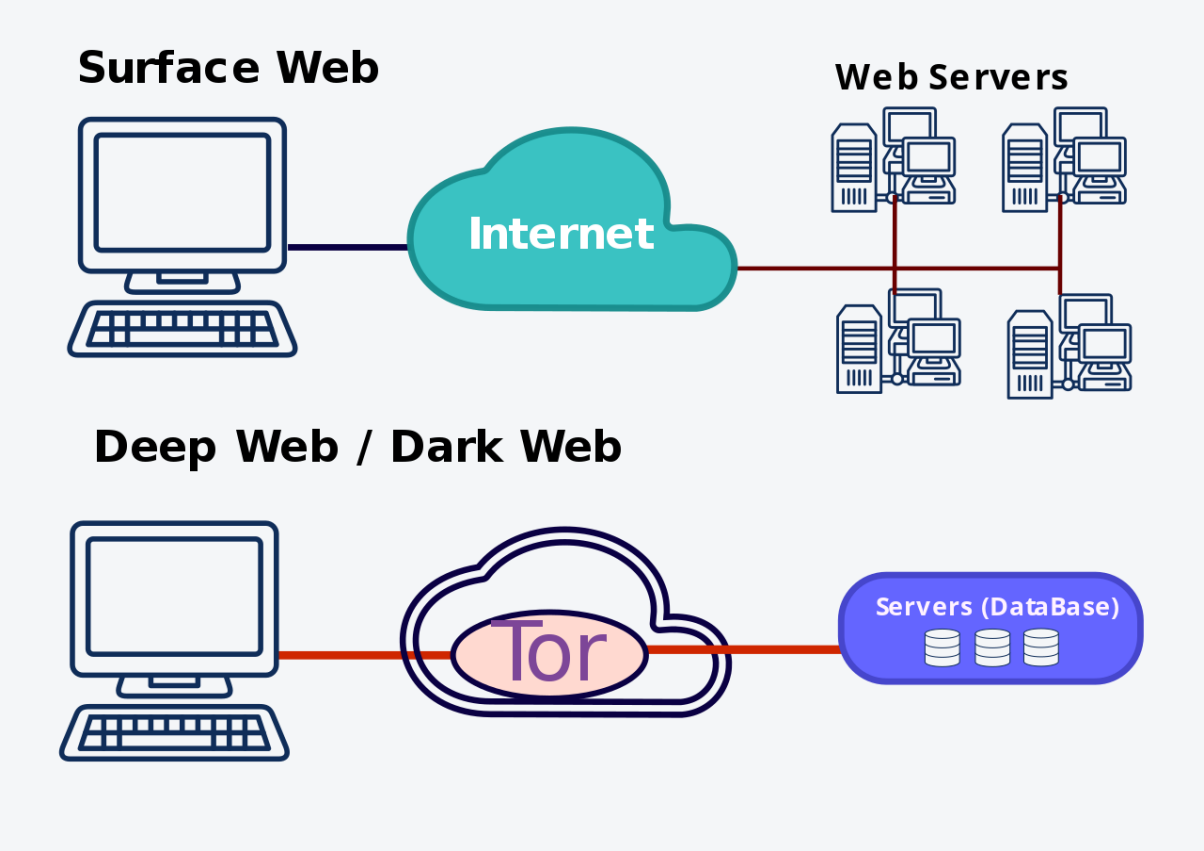
7. PREDNOSTI I RIZICI KRIPTOVALUTA

U nastavku ovoga rada opisat će se prednosti i rizici kriptovaluta. Kako je su kriptovalute zasnovane na temelju matematičkih algoritama i pošto u blockchain mreži ne postoje podaci o primateljima ili vlasnicima kriptovaluta, hakerima je vrlo teško postići ikakve rezultate. Nadalje već spomenuto, niski transakcijski troškovi su vrlo bitna prednost kriptovaluta. Niski troškovi omogućavaju kriptovalutama da se natječu s bankama ili nekim web platnim sustavima koji imaju visoke naknade. Također to znači da se pri transakciji od jedne osobe prema drugoj gotovo pa nema naknade. Uz to, transakcije su neograničene, što znači da jedna osoba može poslati neograničen iznos drugoj osobi. Transakcije su anonimne, što znači da se ne vidi ime i prezime pošiljatelja već samo njegova javna adresa, a u isto vrijeme transakcije su transparentne tj. bilo tko može vidjeti svaku transakciju koja se je dogodila. Tome je zaslužan blockchain koji pohranjuje svu povijest transakcija. Anonimnost je ključna značajka kriptovaluta, jer ne pohranjuje korisnikove privatne podatke poput imena, prezimena, mail adresa. Zbog toga nije moguće da se korisnikovi podaci ukradu ili koriste za prevaru. Još jedna bitna prednost jest nemogućnost otkazivanja transakcije. Za primjer se navodi PayPal platni sustav. Pri plaćanju PayPal-om, korisnik koji plača može nakon nekoliko dana povući transakciju, prilikom čega se sav novac vrača nazad korisniku. To se može interpretirati kao prevara. Na primjer osoba A plača usluge grafičkog dizajna osobi B, pri tome osoba B dostavlja završnu datoteku osobi A, pri čemu osoba A poduzima zahtjev za povrat novca. To nije moguće pri transakcijama kriptovalutama. Ako osoba A pošalje novac osobi B, transakcija je završena i nepovratna (Bunjaku, Gjorgieva-Trajkovska i Miteva-Kacarski, 2017).

Kao i u svakoj tehnologiji, postoje rizici i negativnosti. Jedan od rizika je nestabilnost. Vrijednost kriptovaluta se često mijenja, znači da u bilo kojem trenutku vrijednost može naglo skočiti ili u drugom slučaju naglo pasti. Ta informacija se mora imati na umu prilikom odluke ulaganja u kriptovalute. Prilikom naglog pada osoba A može zaraditi veliku svotu novca, dok osoba B može izgubiti istu količinu novca. U manu kriptovaluta spada i kriminalna aktivnost preko interneta. Kriminalci se bave prodajom oružja, droge i drugih ilegalnih stvari preko *dark web-a*[5] pri kojemu je

[5] Dark web dio je interneta čiji sadržaj nije dostupan putem konvencionalnih mrežnih pretraživača.

moguće pristupiti samo Tor preglednikom (slika 29), a kao valutu plaćanja koriste kriptovalute baš zbog prije navedene anonimnosti (Bunjaku, Gjorgieva-Trajkovska i Miteva-Kacarski, 2017).



Slika 29: Pristup *dark web-u* pomoču Tor preglednika

Izvor:
(https://hr.wikipedia.org/wiki/Duboki_web#/media/Datoteka:Deep_web_vs_surface_web.svg)

8. ZAKLJUČAK

Predmet ovog završnog rada je kriptovaluta. Kriptovaluta je internetsko "blago" koje svatko može imati, bilo to kupljeno preko mjenjačnica ili prikupljeno pomoću rudarenja. Razvojem tehnologije i interneta kriptovalute su postale važan dio svjetske ekonomije i konkurencija svim bankama i tržištima.

Svrha ovoga rada je istraživanje kriptovaluta i njihovog nastajanja te prikaz glavnih tehnologija koje sve to pokreću. Naglasak se stavlja na blockchain tehnologiju i bitcoin kao prvu i najveću kriptovalutu. Blockchain nudi zapis svih transakcija koje su se provele od početka do danas. Provedene transakcije zapisuju se u knjizi blockchaina, a ulaganja i samim time uloženi novac se čuva u kriptografskim novčanicima koji se dijele na papirnate, softverske i hardverske. Uz bitcoin postoje i druge vodeće kriptovalute, poput ethereuma i stellara. Zbog velikog porasta popularnosti i tehnologije, svaki dan se pojavljuje pojedina nova kriptovaluta, samim time i sve više korisnika i entuzijasta. Porastom kriptovaluta, raste i tehnologija oko njih. Na temelju toga, sve više se upotrebljava rudarenje računalom. Korisnici pomoću snage svoga računala mogu rudariti kriptovalute koje oni odaberu. Prikupljene kriptovalute spremaju se u navedene novčanike, ili se mijenjaju za pravi novac.

Na osnovu istražene literature i primjera dobre prakse u ovom završnom radu utvrđeno je kako kriptovalute omogućavaju korisnicima sigurne i jeftine transakcije u bilo koje vrijeme. One se smatraju sigurnijim u odnosu na obične elektroničke transakcije, a za to je zaslužna spomenuta blockchain tehnologija koja zbog svojih kompliciranih matematičkih zagonetaka nije laka meta cyber kriminalcima. Sve transakcije i privatne informacije vlasnika kriptovaluta su zaštićene matematički generiranim pseudonima. Kriptovalute nisu česta meta cyber kriminalcima, ali cyber kriminalci baš zbog anonimnosti prilikom transakcija koriste kriptovalute kao način plaćanja za njihove ilegalne aktivnosti preko interneta. Također jedna od mana kriptovaluta je preveliko ulaganje bez istraživanja pojedinog tržišta.

LITERATURA

Knjige:

Satoshi, S. (2017.) *Cryptocurrency: Ultimate Beginners Guide to Making Money with Cryptocurrency like Bitcoin, Ethereum and altcoins* [online] Dostupno na: https://pdfroom.com/books/cryptocurrency-ultimate-beginners-guide-to-making-money-with-cryptocurrency-like-bitcoin-ethereum-and-altcoins/e1j5KlqZdKr [pristupljeno 12.8.2021]

Pritzker, Y. (2021.) *Inventing Bitcoin* [online] Dostupno na: https://pdfroom.com/books/inventing-bitcoin/jndOKGP3dRq [pristupljeno: 5.8.2021]

Grayscale, B. B. (2020.) *An Introduction to Ethereum* [online] Dostupno na: https://pdfroom.com/books/an-introduction-to-ethereum/kZdowXqMdM8 [pristupljeno 12.8.2021]

Članci:

Stephen, R. i Alex A. (2018.) *A Review on BlockChain Security* [online] Dostupno na: https://iopscience.iop.org/article/10.1088/1757-899X/396/1/012030/pdf [pristupljeno 20.7.2021]

Yaga, D., Mell, P., Roby, N. i Scarfone, K. (2018.) *Blockchain Technology Overview* [online] Dostupno na: https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf [pristupljeno 21.7.2021]

Bunjaku, F., Gjorgieva-Trajkovska, O., Miteva-Kacarski, E. (2017.) *Criptocurrencies – Advantages and disadvantages* [online] Dostupno na: https://js.ugd.edu.mk/index.php/JE/article/view/1933 [pristupljeno 11.9.2021]

Poveznice:

Sofi, *Understanding The Different Types of Cryptocurrency*, (2021.) Dostupno na: https://www.sofi.com/learn/content/understanding-the-different-types-of-cryptocurrency [pristupljeno 12.8.2021]

Gemini, *Bitcoin Cash (BCH): There's More Than One Bitcoin?*, (2021.) Dostupno na: https://www.gemini.com/cryptopedia/what-is-bitcoin-cash [pristupljeno 5.8.2021]

Investopedia, *What Are the Advantages of Paying with Bitcoin?*, (2021.) Dostupno na: https://www.investopedia.com/ask/answers/100314/what-are-

advantages-paying-bitcoin.asp [pristupljeno: 10.8.2021]

Tportal, *Cijena bitcoina uzletjela je iznad 50.000 dolara. Što to uopće znači za ovu kriptovalutu i za što je sve možete koristiti?*, (2021.) Dostupno na: https://www.tportal.hr/biznis/clanak/cijena-bitcoina-uzletjela-je-iznad-50-000-dolara-sto-to-uopce-znaci-za-ovu-kripovalutu-i-za-sto-je-sve-mozete-koristiti-20210217 [pristupljeno 6.8.2021]

Bytwork, *Bitcoin price chart for the entire history from 2008 to 2021*, (2021.) Dostupno na: https://bytwork.com/en/articles/btc-chart-history [pristupljeno 10.8.2021]

Investopedia, *Bitcoin's Price History*, (2021.) Dostupno na: https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp [pristupljeno 10.8.2021]

Musk, E., Twitter, (2021.) Dostupno na: https://twitter.com/elonmusk/ [pristupljeno 12.8.2021]

Forbes, *Elon Musk's 'Promising' Tweet Boosts Bitcoin*, (2021.) Dostupno na: https://www.forbes.com/sites/carlieporterfield/2021/05/24/elon-musk-promising-tweet-boosts-bitcoin/?sh=5441ca426241 [pristupljeno 12.8.2021]

Stellar: an open network for money (2021) Dostupno na: https://www.stellar.org/?locale=en [pristupljeno 12.8.2021]

Medium, *Why We Chose Stellar*, (2018.) Dostupno na: https://medium.com/@blockeq/why-we-chose-stellar-e5b9966c63b7 [pristupljeno 18.8.2021]

Chwilowek, *Hash funkcija u kriptografiji,* (2019.) Dostupno na: https://hr.ranking-chwilowek.net/hash-funkcija-u-kriptografiji-opis-primjeri-145 [pristupljeno 20.7.2021]

Simplilearn, *Bitcoin Mining Explained*, (2021.) Dostupno na: https://www.simplilearn.com/bitcoin-mining-explained-article [pristupljeno 21.7.2021]

Medium, *The Mystery Behind Block Time,* (2017.) Dostupno na: https://medium.facilelogin.com/the-mystery-behind-block-time-63351e35603a [pristupljeno 21.7.2021]

Athenabitcoin, *How to use a paper wallet*, (2018.) Dostupno na: https://www.athenabitcoin.com/news/2018/4/9/how-to-use-a-paper-wallet [pristupljeno 20.7.2021]

Benzinga, *Best cryptocurrency wallets,* (2021.) Dostupno na: https://www.benzinga.com/money/best-crypto-wallet/ [pristupljeno 20.7.2021]

Hardware Wallets, *Ledger Nano X Review,* (2021.) Dostupno na: https://www.hardware-wallets.net/ledger-nano-x-review/ [pristupljeno 15.8.2021]

Investopedia, *Bitcoin Wallet*, (2021.) Dostupno na: https://www.investopedia.com/terms/b/bitcoin-wallet.asp [pristupljeno 15.8.2021]

Investopedia, *How Does Bitcoin Mining Work,* (2021.) Dostupno na: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/ [pristupljeno 28.8.2021]

Techradar, *Best ASIC devices for mining cryptocurrency in 2021,* (2021.) Dostupno na: https://www.techradar.com/best/asic-devices [pristupljeno 28.8.2021]

Freedomnode, *How to Build a Mining Rig? Step by Step Guide,* (2018.) Dostupno na: https://freedomnode.com/blog/how-to-build-a-mining-rig-step-by-step-guide/#h-what-to-consider-when [pristupljeno 28.8.2021]

Windowscentral, *Best mining GPU 2021,* (2021.) Dostupno na: https://www.windowscentral.com/best-gpus-crypto-mining [pristupljeno 28.8.2021]

CNBC, *Billionaire Tim Draper is still bullish that bitcoin will reach $250,000 by the end of 2022,* (2021.) Dostupno na: https://www.cnbc.com/2021/06/14/billionaire-tim-draper-still-predicts-bitcoin-will-reach-250000-.html https://www.cnbc.com/2021/06/14/billionaire-tim-draper-still-predicts-bitcoin-will-reach-250000-.html [pristupljeno 28.8.2021]

POPIS SLIKA

SAŽETAK

Cilj ovog rada je objasniti opći pojam kriptovaluta i povezanih tehnologija. S tim u vezi, opisan je pojam blockchain tehnologije kao temeljni dio kriptovaluta. Definirane su tri kriptovalute te su opisane mogućnosti i tehnologije navedenih kriptovaluta. Uz definiran pojam blockchain tehnologije opisani su postupci rudarenja i pohranjivanja kriptovaluta. U praktičnom djelu rada opisan je postupak rudarenja na odabranom primjeru. Objašnjen je pojam transakcija i navedene su prednosti i rizici kriptovaluta i tehnologije. Rezultati ovog završnog rada mogu biti od koristi svima onima koji se žele educirati u području kriptovaluta.

Ključne riječi: blockchain, kriptovalute, bitcoin, ethereum

SUMMARY

This paper aims to explain the general concept of cryptocurrencies and related technologies. In this regard, the concept of blockchain technology is described as a fundamental part of cryptocurrencies. Three cryptocurrencies have been defined and the possibilities and technologies of these cryptocurrencies have been described. In addition to the defined term blockchain technology, cryptocurrency mining and storage procedures are described. In the practical part of the paper, the mining procedure is described on a selected example. The concept of transactions is explained and the advantages and risks of cryptocurrencies and technology are stated. The results of this final paper can be useful to all those who want to be educated in the field of cryptocurrencies.

Keywords: blockchain, cryptocurrency, bitcoin, ethereum