KRIPTOVALUTE XRP I MONERO

Tomljanović, Tea

VELEUČILIŠTE U RIJECI

Tea Tomljanović

KRIPTOVALUTE XRP I MONERO

(specijalistički završni rad)

Rijeka, 2018.

VELEUČILIŠTE U RIJECI
Poslovni odjel
Specijalistički diplomski stručni studij Informacijske tehnologije u poslovnim sustavima

KRIPTOVALUTE XRP I MONERO

(specijalistički završni rad)

MENTOR

Mr.sc. Jasminka Tomljanović, viši predavač

STUDENT

Tea Tomljanović
MBS 2422000111/16

Rijeka, srpanj 2018.

VELEUČILIŠTE U RIJECI
Poslovni odjel

Rijeka, 13.03.2018.

ZADATAK
za specijalistički završni rad

Pristupnici TEI TOMLJANOVIĆ matični broj 2422000111/16 studentici Specijalističkog diplomskog stručnog studija Informacijske tehnologije u poslovnim sustavima izdaje se zadatak za specijalistički završni rad – tema specijalističkog završnog rada pod nazivom:

KRIPTOVALUTE XRP I MONERO

Sadržaj zadatka:

Objasniti pojmove kriptovaluta XRP i MONERO i njihove prednosti, nedostatke i razlike. Definirati XRP digitalne novčanike i MONERO digitalne novčanike, te objasniti njihovo korištenje. Napraviti usporedbu tih dviju kriptovaluta. U praktičnom dijelu zadatka prikazati rudarenje MONERO kriptovalute.

Rad obraditi skladno odredbama Pravilnika o završnom radu Veleučilišta u Rijeci.

Zadano: 13. 03. 2018.

Predati do: 15. 07. 2018.

Mentor

(mr. sc. Jasminka Tomljanović, viši predavač)

Pročelnica odjela

(mr. sc. Marino Golob, viši predavač)

Zadatak primio dana: 13.03.2018.

(Tea Tomljanović)

Dostavlja se:
- **mentoru**
- **pristupniku**

I Z J A V A

Izjavljujem da sam specijalistički završni rad pod naslovom „Kriptovalute XRP i Monero“ izradila samostalno pod nadzorom i uz stručnu pomoć mentorice mr. sc. Tomljanović Jasminke.

Tea Tomljanović

(potpis studenta)

Sažetak

U ovom radu objašnjena je tema o kriptovalutama i digitalnom novcu. Preciznije su objašnjene kriptovalute XRP i Monero. Opisane su njihove glavne prednosti i nedostaci, ali i razlike. Spomenuti su takozvani XRP i Monero digitalni novčanici te je objašnjeno njihovo korištenje. Prikazane su trgovine za razmjenu kriptovaluta kao što su Binance, Kraken i Changelly. Kao praktični dio prikazano je rudarenje kriptovalute Monero. Svi podaci napisani u radu su najnovije informacije, međutim svijet kriptovaluta se brzo mijenja, promjene se odvijaju u minutama.

Ključne riječi: kriptovaluta, Ripple, XRP, Monero, rudarenje.

SADRŽAJ:

1. UVOD 1
2. KRIPTOVALUTE 2
   2.1 Povijest kriptovaluta 2
   2.2 Korištenje kriptovaluta 3
   2.3 Ulaganje u kriptovalute 3
3. „RUDARENJE“ KRIPTOVALUTA 4
4. RIPPLE 6
   4.1 XRP (općenito) 6
   4.2 XRP (sigurnost) 8
   4.3 XRP konsenzus 9
   4.4 XRP validacija (potvrđivanje) 11
   4.5 Ključni koraci transakcija 13
5. RIPPLE NOVČANICI 14
   5.1 Adresa novčanika 14
   5.2 Tajni ključ 15
   5.3 Vrste novčanika 16
      5.3.1. Hosted novčanici: 16
      5.3.2. Exarpy 16
      5.3.3. *Hardware* novčanici 17
      5.3.4. Ledger Nano S 17
      5.3.5. *Software* novčanici 17
      5.3.6. Rippex 17
      5.3.7. Takozvana hladna pohrana 18
6. ZAŠTO KUPOVATI XRP - BUDUĆNOST XRP-A 19
7. MONERO 21
   7.1 Monero *“Ring signatures”* 22
   7.2 Monero *“Stealth addresses”* 22
   7.3 Prikaz normalne i Monero transakcije 23
   7.4 Upotrebljivost 24
8. MONERO NOVČANICI 25
   8.1 Monero internet novčanici 25
      8.1.1. MyMonero 25
   8.2 Monero desktop novčanici 26
   8.3 Monero GUI novčanik 26

8.4 Monero papirnati novčanici 27
8.5 Mobilni novčanik Monerujo 28
8.6 *Hardware* Monero novčanik 29
8.7 Bitne stavke novčanika 29
9. MJESTA ZA RAZMJENU KRIPTOVALUTA 31
9.1 Binance 32
9.2 Changelly 33
9.3 Kraken 35
10. RIPPLE vs MONERO 37
10.1 Monero 37
10.2 Ripple 38
10.3 Grafička prikaz (statistika) 38
11. POREZI NA KRIPTOVALUTE U HRVATSKOJ 40
12. RUDARENJE MONERA 41
12.1 Rudarenje Monera GPU 41
12.2 Rudarenje Monera CPU 46
13. ZAKLJUČAK 48
POPIS I OBJAŠNJENJE KORIŠTENIH KRATICA I INFORMATIČKIH POJMOVA 49
POPIS LITERATURE 50
POPIS SLIKA 51

1. UVOD

U današnjem svijetu gdje je sve brzo promjenjivo dolazi do potreba za bržom i jednostavnijom transakcijom novca kao i potrebe za sigurnijim načinom slanja novca s jednog kraja svijeta na drugi. Da bi se ušlo u svijet kriptovaluta potrebno je osnovno poznavanje nekih pojmova koji su objašnjeni u radu kao što su: digitalni novac, digitalni novčanici, kriptovalute i slično. Cilj ovog rada je što bolje predstaviti pojam kriptovaluta, kao i usporediti i objasniti dvije kriptovalute, XRP i XMR. U ovom trenutku postoji na tisuće kriptovaluta, od kojih nisu sve korisne i dobronamjerne. Svrha rada je što bolje upoznavanje s kriptovalutama i isticanje njihove prave vrijednosti, ali i upozoravanje na moguće probleme.

Rad je podijeljen u nekoliko poglavlja. Prvi dio rada odnosi se na upoznavanje općih pojmova, kao na primjer što su to kriptovalute, povijest kriptovaluta, ulaganje u kriptovalute i slično. Drugi dio rada opisuje Ripple protokol i XRP kriptovalutu. Pojašnjene su funkcionalnosti XRP kriptovalute, prednosti , nedostaci te novčanici koji se koriste za sigurno spremanje ove valute. Treći dio rada opisuje drugu kriptovalutu, a to je Monero (XMR). Istaknute su glavne značajke XMR-a, kao i novčanici koji se koriste za sigurno skladištenje ove kriptovalute. Četvrti dio rada odnosi se na usporedbu ranije opisanih kriptovaluta, isticanje njihovih zajedničkih odnosno različitih funkcija. Peti dio rada objašnjava oporezivanje profita stečenog trgovinom kriptovaluta u Hrvatskoj. Zadnji dio rada usredotočen je na praktični primjer rudarenja Monero (XMR) kriptovalute.

2. KRIPTOVALUTE

Kriptovalute su digitalne ili virtualne valute, dizajnirane da bi koristile kao medij razmjene. Kriptovalute se uglavnom koriste za osiguravanje i provjeru transakcija, za kontrolu stvaranja novih jedinica određene kriptovalute i slično. Detaljnije rečeno kriptovalute su ograničeni unosi u bazu podataka koju nitko ne može mijenjati, odnosno može se mijenjati samo ako su ispunjeni određeni uvjeti. Kriptovalute funkcioniraju na temelju kriptografskih algoritama. Danas postoji na tisuće kriptovaluta, dok je jedna od 5 najpoznatijih XRP, valuta koja je objašnjena nešto kasnije u radu. Također kao jedna od novijih, ali i popularnih kriptovaluta je Monero, također spomenuta i objašnjena u radu. Svaka od valuta ima svoje algoritme na temelju kojih radi, također nemaju sve kriptovalute istu svrhu postojanja.

2.1 Povijest kriptovaluta

Bilo je mnogo pokušaja stvaranja digitalnih valuta u vrijeme velikog tehničkog razvoja 90-tih godina prošlog stoljeća, međutim svi su propali. Neki od najvećih razloga zašto su propali bile su prijevare, financijski problemi, pa čak i velike napetosti između zaposlenika unutar tvrtki i njihovih nadređenih. Svi pokušaji izrade kriptovaluta temeljili su se na pristupu *„Trusted Third Party“* , što bi značilo da su tvrtke iza njih morale potvrditi i odobriti svaku transakciju. Zbog samog neuspjeha tih kompanija dolazi i do propasti svih pokušaja za izradom digitalnog gotovinskog sustava. (Cohen, 2017.)

Anonimni programer pod nazivom Satoshi Nakamoto 2009. godine uveo je Bitcoin te su ga proglasili elektroničkim bankovnim sustavom. Za razliku od prijašnjih pokušaja ova kriptovaluta je decentralizirana, što bi značilo da nema uključenih poslužitelja i nema središnje tijelo nadzora. Koncept je blizak *peer-to-peer* mrežama za dijeljenje datoteka. Jedan od najvećih problema koje je ova mreža morala riješit bila je dvostruka potrošnja, to jest trošenje istog iznosa dva puta. Klasično rješenje bila bi povjerljiva treća strana, središnji poslužitelj, koji je vodio evidenciju o bilanci i transakciji. Za razliku od toga ova nova kriptovaluta značila bi da svaki korisnik mora za sebe obavljati taj posao. (Cohen, 2017.)

2.2 Korištenje kriptovaluta

U prošlosti, pronalazak nekoga tko će prihvatiti kriptovalutu u zamjenu za neku robu, bilo je iznimno teško, čak i nemoguće. Međutim, zadnjih par godina situacija je postala drugačija. Postoji mnogo trgovaca koji prihvaćaju neku vrstu kriptovalute kao oblik plaćanja za uslugu ili neku robu. Došlo je do te razine da se sa nekim kriptovalutama mogu plaćati hoteli, letovi, kupovati nakit, pa čak i plaćati fakulteti. Postoje i takozvane darovne kartice koje je moguće zamijeniti za neku od kriptovaluta, jedna od stranica koja to omogućuje je „Gift Off“, ona također prihvaća 20 različitih kriptovaluta kao sredstvo plaćanja.

Za razliku od mrežne trgovina vanmrežne trgovine u kojima je moguće kupovati kriptovalutama su u manjini. Nešto popularnije kupovanje kriptovalutama je u Americi gdje je moguće taxi plaćati u obliku kriptovaluta. Također u Japanu postoji ugostiteljski objekti, drogerije, maloprodajna mjesta diljem zemlje koji prihvaćaju plaćanje u obliku kriptovalute.

2.3 Ulaganje u kriptovalute

Vjeruje se da je ulaganje u kriptovalute trenutno najatraktivnija investicijska prilika na tržištu. Postoje na tisuće priča ljudi diljem svijeta koji su zaradili ulažući u neku od kriptovaluta. Potrebno je napomenuti da su sva ulaganja u kriptovalute rizična. Njihova tržišna vrijednost se stalno mijenja. Potrebno je poznavanje tržišta i kriptovalute koja se kupuje.

Sama kupovina kriptovaluta je vrlo jednostavna. Postoji nekoliko platformi preko kojih se mogu kupiti kriptovalute. Nakon same kupovine kriptovalute potrebno ju je zaštititi na pravodoban način. Većina kriptovaluta nudi i takozvane digitalne novčanike, ali i izvan mrežne novčanike koji su nešto sigurnija opcija. Ovo su najsigurniji načini pohranjivanja kriptovaluta te daju potpunu kontrolu nad njima. Ukoliko kupac želi izvući svoj zarađen iznos postoji mogućnost da će biti primoran platiti porez na dobit. Pa se tako na primjer u Njemačkoj oporezuje tek dobit veća od 600 Eura, dok su državljani Danske osloboljeni plaćana dobiti na kriptovalute. (Cohen, 2017.)

3. „RUDARENJE“ KRIPTOVALUTA

Rudarenje podataka ili na engleskom *„Data mining“* je jedna vrsta sortiranja, organiziranja i/ili grupiranja ogromnog broja nesređenih podataka te nakon toga izvlačenje potrebnih informacija iz tih podataka. Rudarenjem se može poboljšati poslovanje nekog poduzeća, doći do neki novih i zanimljivih informacija koje uvelike mogu promijeniti postojeće stanje na bolje i ukazati na moguće pogreške u poslovanju.

U svijetu kriptovaluta rudarenje ima nešto drugačiju značenje. Kod tradicionalnih novčanih sustava, vlade jednostavno izdaju više novca kada je to potrebno, međutim kod kriptovaluta to ne ide tako. Kriptovalutni novac nije izdan već je otkriven, što bi značilo da računala diljem svijeta „rudare“ neku kriptovalutu.

Izraz „rudarenje“ je takozvani naziv za korištenje računalne snage za obradu transakcija kriptovaluta te se tako dobiva neka vrijednost u ovom slučaju jedna jedinica neke kriptovalute. Za svaku uspješno izvršenu dionicu ili završene izračune koji se rade preko algoritama rudari budu nagrađeni. Snaga računala koje bi moglo odrađivati rudarenje kriptovalute ovisi i razlikuje se od valute do valute, odnosno od algoritma do algoritma.

Na početku kriptovaluta bilo je moguće „rudariti“ sa osobnim računalom, što trenutno više nije slučaj. Kako sve više ljudi sudjeluje u rudarenje povećava se i potreba za jačim i boljim GPU-om, pa u većini slučajeva i do nekoliko GPU-ova koji rade zajedno pomoću specijaliziranih čvorova koji su posebno dizajnirani za rudarenje. Procjenjuje se da je potrebno oko 1100 Eura potrošiti samo na *hardware*, dok su tu još stalni, dnevni troškovi električne energije i tako dalje. Prije kupovine i ulaženja u ovaj svijet potrebno se informirati. Svaki nepromišljeni pokušaj rudarenje neke kriptovalute mogao bi donesti velike troškove umjesto moguće zarade.

Može se reći da su rudari (osobe koje rudare kriptovalute) jedan od najvažnijih dijelova bilo koje mreže kriptovalute, osim toga rudarstvo u ovom smislu postaje i investicija. Rudari kao takvi doprinose računalnoj moći rješavanjem kompliciranih kriptografskih zagonetki, što je neophodno za potvrde transakcija i zapisivanje istih. Jedna od zanimljivih stvari u

rudarstvu je da težina zagonetki/algoritama stalno raste, to jest raste u ovisnosti na broj ljudi koji sudjeluje u rudarenju. Dalje, što je neka kriptovaluta popularnija, više ljudi pokušava rudariti te samo rudarenje postaje sve teže i teže. Na samom početku kriptovaluta, mnogi ljudi su uspjeli zaraditi velike količine novaca rudarenjem valuta i to koristeći stolno računalo ili čak laptop. U današnje vrijeme, samo nekoliko godina nakon prve kriptovalute, postići profit rudarenjem je postalo zahtjevno. Svako rudarenje neke kriptovalute zahtjeva dodatan napor, ulaganje u opremu, ali i visoke troškove struje. Dakako još uvijek postoje neke od valuta koje je moguće rudariti i zaraditi pomoću kućnog računala. Pa tako zarada može varirati od 50 centi do 10 dolara po danu. Što se više računalne snage uspije akumulirati, to je veća šansa za rješavanjem kriptografskih zagonetki.

Kao što je već rečeno, kako kriptovalute privlače sve više i više interesa, rudarstvo postaje sve teže, a s time su i nagrade za rudarenje sve manje. Jedan od primjera je i Bitcoin, za uspješno rudarenje Bitcoina dobivalo se 50 BTC-a dok je sada ta nagrada pala na 12,5 BTC-a. Proporcionalno s tim vrijednost svakog Bitcoina eksponencionalno raste.

Svi ovi čimbenici čine rudarstvo iznimno konkurentnim tržištem, koje nagrađuje one koji su ga rano otkrili i uložili u njega.

4. RIPPLE

Ripple je sustav koji funkcionira u realnom vremenu, odnosno RTGS *„Real-time gross settlement system“* koji je nastao od strane istoimene tvrtke Ripple. Postoji i Ripple protokol koji se koristi za transakcije. Izgrađen je na distribuiranom internetskom protokolu otvorenog koda, kriptovaluti skraćeno nazvanom XRP. Objavljena je 2012. godine, jedna od njihovih vodilja bila je osigurati sigurne, odmah dostupne, globalne financijske transakcije bilo kojeg obujma i oblika. (Cohen, 2017.)

Ripple je poznatiji po svom digitalnom platnom protokolu nego kao kriptovaluta. On djeluje na otvorenoj decentraliziranoj platformi koja omogućuje besprijekoran prijenos novca u bilo kojem obliku, dolarima, jenima, bitcoinima i slično.

4.1 XRP (općenito)

Kako je već spomenutu u tekstu prije, XRP je kriptovaluta koja koristi Ripple-ov protokol koji omogućuje bržu, jednostavniju, sigurniju transakciju bilo kojeg oblika novce, valute, s jednom kraja svijeta na drugi kraj svijeta.

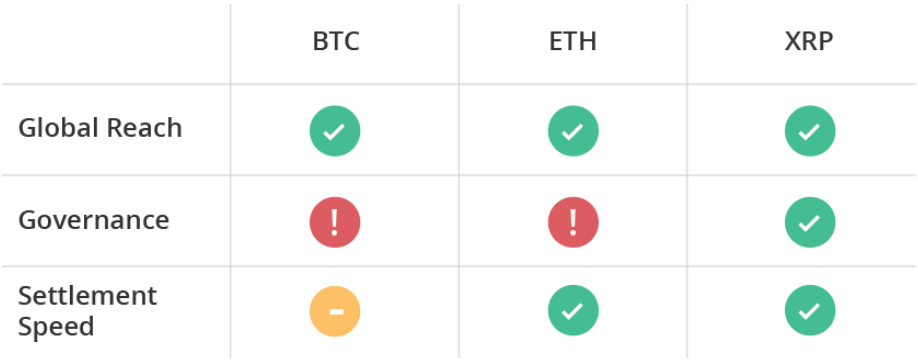
Praktični primjer čemu služi XRP bio bi : da bi se razumjelo kako sustav funkcionira potrebno je zamisliti dvije strane koje žele napraviti transakciju novca te to odrađuju putem neke treće strane kao poslužitelja. Ivan mora poslati 100 $ Maji koja živi na drugom kraju svijeta. On daje svojem lokalnom agentu Dinu , novac i lozinku kako bi Maja mogla na kraju dobiti sredstva. Nadalje Dino kontaktira Majinog agenta i obavještava ga o transakciji i lozinki. Ako Maja da svom agentu dobru lozinku dobiti će sredstva odnosno 100 $. Također je potrebno razumjeti koji novci idu sa kojeg računa i tko će na kraju kome dugovati novac te kako će se to izbalansirati. (Cohen, 2017.)

Iako je mreža Ripple-a nešto složenija od ovog primjera, primjer pokazuje osnovu funkcioniranja Ripple sustava. Iz gornjeg primjera može se vidjeti da je potrebno povjerenje za pokretanje transakcija, povjerenje između svih sudionika transakcije. Ripple koristi medij poznat kao veza u lancu povjerenje između dvije strane koje žele izvršiti transakciju. *Gateway*

djeluje kao kreditni posrednik koji prima i šalje valute na javne adrese preko Ripple mreže. Bilo tko kao pojedinac ili kao poslovna osoba može registrirati i otvoriti „prolaz“ koji omogućuje da ta osoba ili posao djeluje ili djeluju kao posrednici za razmjenu valuta, održavanje likvidnosti i transakcije plaćanja na mreži.

XRP kao digitalna valuta djeluje kao most u odnosu na druge valute. Razlikuje se od nekih valuta, baš zbog svoje specifične namjene pa tako na primjer može koristiti za brzu razmjenu i transakciju između jedna u drugu valutu. Ukoliko se transakcija vrši u dolarima, a korisnik koji prima transakciju želi taj iznos u nekom drugom obliku različitom od dolara, i to je moguće napraviti.

Slika 4.11 - Prikaz razlike između BTC, ETH i XRP



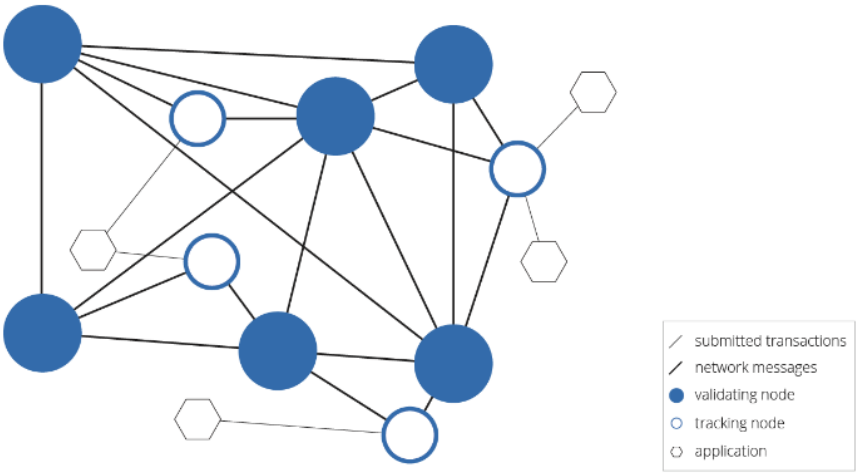
Izvor : https://ripple.com/insights/xrp-compares-btc-eth/ (21.4.2018.)

Slika iznad teksta prikazuje neke od razlika između BTC (Bitcoin), ETH (Ethereum) i XRP kriptovaluta. Dakako ovo nisu jedine razlike između ovih kriptovaluta, ali su zanimljive razlike. Pa se tako može primijetiti da sve od valuta imaju veliki globalni doseg odnosno globalno su dostupne. Također se može zaključiti da je brzina transakcije različita od valute do valute. Pa tako BTC-u treba sat vremena za neku transakciju, dok ETH-u nekoliko minuta, a XRP-u par sekundi, što dokazuje njegovu moć i samu potrebu za njegovim korištenjem u transakcijama neovisno da li se radi o transakcijama istih valuta ili o transakcijama iz jedne valute u drugu. (Cohen, 2017.)

4.2 XRP (sigurnost)

Peer -to- peer XRP *Ledger* mreža sastoji se od mnogo distribuiranih poslužitelja, koji se nazivaju čvorovima, oni prihvaćaju i obrađuju transakcije. Klijentske aplikacije potpisuju i šalju transakcije na čvorove, koji prenose ove kandidirane transakcije po mreži. Primjeri klijentskih aplikacija uključuju mobitele i *web* novčanike, pristupnice za financijske institucije i elektroničke trgovinske platforme.

Slika 2 – Prikaz sudionika u XRP Ladger protokolu



Izvor : https://ripple.com/build/xrp-ledger-consensus-process/ (22.4.2018.)

Čvorovi koji primaju, prenose i obrađuju transakcije mogu biti ili čvorovi za praćenje ili čvorovi za validiranje. Primarne funkcije čvorova praćenja uključuju distribuciju transakcija od klijenta i odgovaranje na upite o *Ledgeru*[1]. Validacijski čvorovi obavljaju iste funkcije kao čvorovi za praćenje te dodatno pridonose unapređenju *Ledger* sekvenci. Prilikom prihvaćanja transakcija koje se šalju putem korisnikove aplikacije, svaki čvor za praćenje koristi zadnji validirani *Ledger* kao početnu točku. Prihvaćene transakcije su mogući kandidati. Čvorovi prenose svoje odabrane transakcije svojim klijentima, omogućujući tako odabranim transakcijama propagiranje u cijeloj mreži. U idealnom slučaju, svaka odabrana transakcija bila bi poznata svim čvorovima, dopuštajući svima da razmotre isti skup transakcija koje se događaju na posljednji validirani *Ledge*r. Transakcije trebaju vrijeme za propagiranje, međutim čvorovi ne rade s istim skupom odabranih transakcija u svakom trenutku. Kako bi se

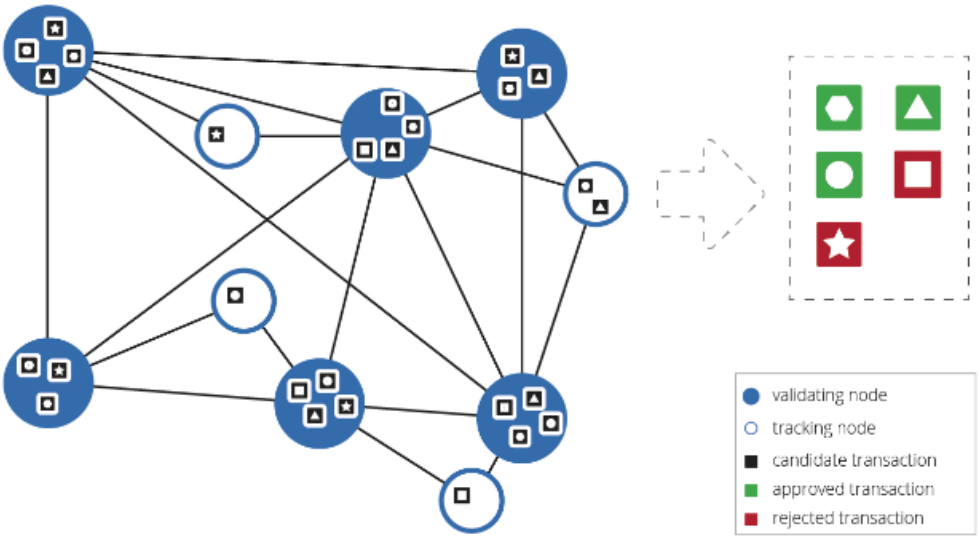
[1] Kriptografska knjiga koju pokreće mreža poslužitelja

to opravdalo, XRP *Ledger* koristi proces koji se zove konsenzus kako bi se osiguralo da se iste transakcije obrađuju i potvrđuju te da su *Ledgeri* dosljedni unutar XRP *Ledger peer-to-peer* mreže. (Cohen, 2017.)

4.3 XRP konsenzus

Čvorovi na mreži dijele informacije o odabranim transakcijama. Kroz proces konsenzusa, validiranje čvorova prihvaća se na specifičan podskup odabranih transakcija koje će biti razmotrene za sljedeći *Ledger*. Konsenzus je iterativni proces u kojem čvorovi prenose prijedloge ili skupine odabranih transakcija. Čvorovi komuniciraju i ažuriraju prijedloge sve dok se pet najutjecajnijih članova ne složi oko istog skupa odabranih transakcija. Tijekom konsenzusa , svaki čvor procjenjuje prijedloge određenog seta istovrsnih članova mreže, imenovanih odabranim validatorima. Odabrani validatori predstavljaju podskup mreže koji je, gledano općenito, pouzdan u smislu da se ne može prevariti čvor koji ocjenjuje prijedloge. Ova definicija povjerenja ne zahtjeva pouzdanost svakog pojedinog odabranog validatora. Validatori su odabrani na temelju očekivanja da neće omogućiti niti moći imati koordinirani pokušaj krivotvorenja podataka poslanih na mrežu. (Cohen, 2017.)

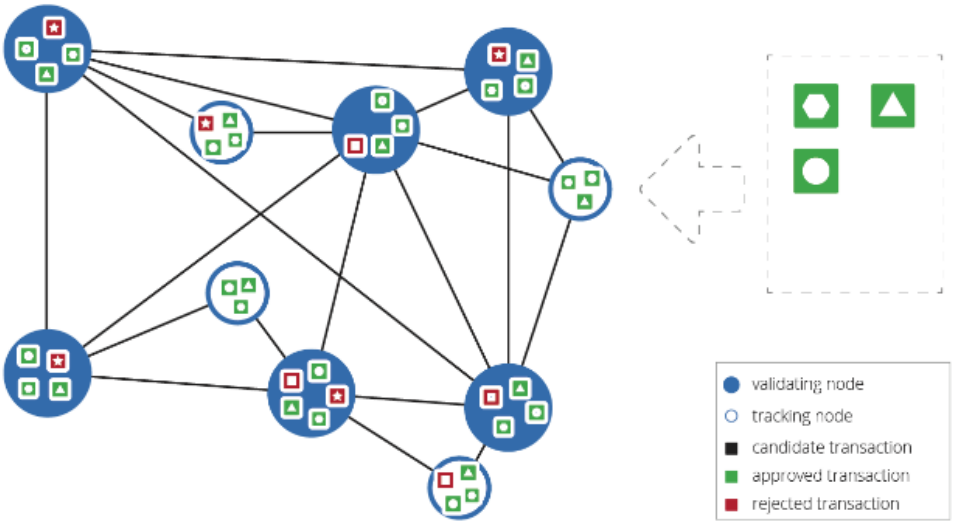
Slika 3- Prikazuje validatore koji predlažu transakcijski skup



Izvor: https://ripple.com/build/xrp-ledger-consensus-process/ (22.4.2018.)

Na početku konsenzusa čvorovi rade s različitim skupovima transakcija. Zaokruživanje prijedloga određuje koje se transakcije primjenjuju na glavni *Ledger*, a koje moraju čekati kasniji krug konsenzusa. Odabrane transakcije koje nisu uključene u dogovoreni prijedlog ostaju predložene transakcije. Može ih se ponovo razmotriti u sljedećem krugu konsenzusa.

Slika 4– Prikaz kako se čvorovi slažu u skupu transakcija



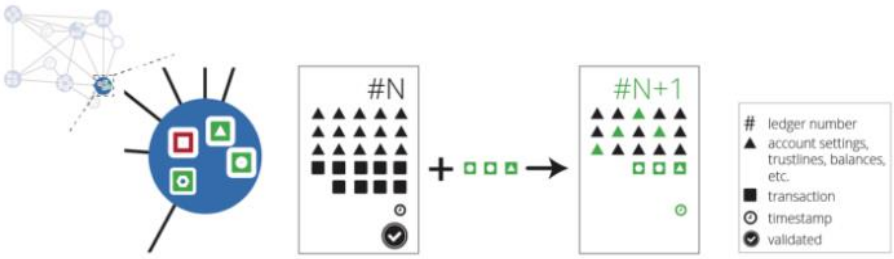
Izvor: https://ripple.com/build/xrp-ledger-consensus-process/ (22.4.2018.)

Uglavnom, transakcije koje ne prođu u prvom krugu konsenzusa uspijevaju proći u sljedećem. Međutim u nekim okolnostima transakcija ne bi mogla proći konsenzus neko određeno vrijeme. Jedna od takvih okolnosti je kada mreža povećava osnovnu naknadu na vrijednost veću od same transakcije. Transakcija bi mogla biti uspješna kada bi se naknada smanjila u jednom trenutku. Transakcijsko polje *„LastLedgerSequence“* je mehanizam koji omogućuje nestanak takve transakcije, ako se ne izvrši u nekom razumnom roku. Aplikacije bi trebale sadržavati *„LastLedgerSequence“* parametar za svaku transakciju. To bi osiguralo da transakcija ili uspije ili ne uspije prije specificiranog broja slijeda *Ledgera*. Čime bi se ograničilo vrijeme koje aplikacija mora čekati prije dobivanja konačnog rezultata transakcije. (Cohen, 2017.)

4.4 XRP validacija (potvrđivanje)

Kada završi jedan krug konsenzusa, svaki čvor izračunava novi *Ledger* tako što primjenjuje odabrane transakcije u transakcijski konsenzusa, koji je postavljen na zadnji ovjereni *Ledger*. Dakle, svaki čvor za praćenje primjenjuje dogovorene transakcije na posljednjem ovjerenom *Ledgeru*. Validirani čvorovi šalju svoje rezultate na cijelu mrežu.

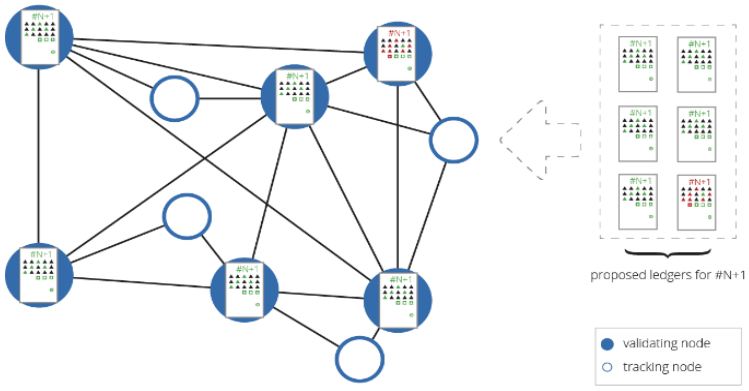
Slika 5- Prikazuje mrežni čvor koji izračunava valjanost Ledgera



Izvor: https://ripple.com/build/xrp-ledger-consensus-process/ (23.4.2018.)

Validirai čvorovi izračunavaju novu verziju *Ledgera* i prenose te podatke na mrežu, svako slanje potpisanog *hash-a* od *Ledgera* je temeljeno na izračunu odabranih transakcija predloženih tijekom konsenzusa. Ti potpisani hasho-vi, koji se nazivaju validacijom, omogućuju svakom čvoru da uspoređuje *Ledger* koji je izračunat s ostalima *Ledger-ima*. Dakle čvorovi uspoređuju svoje izračunate *Ledgere* s *hash-ovima* dobivenih od odabranih validatora. Ako nisu u skladu, čvor mora ponovo raditi izračun ili dohvatit ispravan *Ledger*.

Slika 6- Prikaz provjere Ledger-a (kada glavni izračuna isti rezultat)

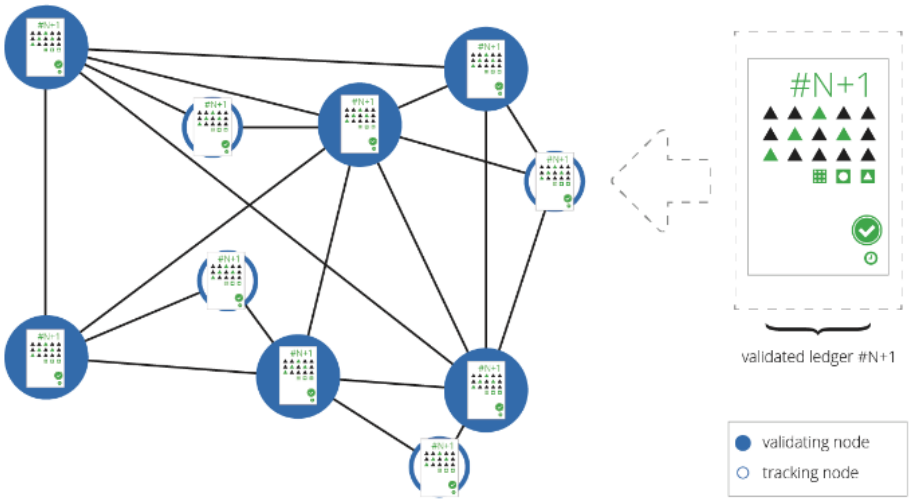


Izvor: https://ripple.com/build/xrp-ledger-consensus-process/ (23.4.2018.)

Čvorovi mreže prepoznaju *Ledger* instancu kao validiranu kada je glavni od njih potpisan i kada emitira isti validacijski *hash*. nadalje, transakcije se primjenjuju na ažurirani i validirani *Ledger* s rednim brojem N + 1. U slučajevima kada je čvor u manjini, nakon što je izračunao *Ledger* koji se razlikuje od ostalih, čvor ga ignorira. Ako mreža ne postigne supermajoriti ugovor o provjeri valjanosti, to znači da je volumen transakcije bio previsok ili je latencija mreže prevelika za proces. U tom slučaju čvorovi ponavljaju proces konsenzusa. Što je duži period vremena prošao od konsenzusa, postaje sve vjerojatnije da većina čvorova ima isti skup odabranih transakcija, zbog toga što svaki krug konsenzusa smanjuje neslaganja. XRP *Ledger* dinamički prilagođava troškove transkacije i vrijeme čekanja konsenzusa kao odgovor na ove uvjete. (Cohen, 2017.)

Nakon što čvorovi postignu sporazum o validaciji, počinju raditi s novim validiranim Ledgerom N+1. Proces konsenzusa i validacije se ponavlja. Uzimaju se u obzir odabrane transakcije koje nisu bile uključene u posljednji krug zajedno s novim transakcijama koje su u međuvremenu dostavljene.

Slika 7- Prikaz kada mreže prepoznaje novi validirani Ledger



Izvor: https://ripple.com/build/xrp-ledger-consensus-process/ (23.4.2018.)

4.5 Ključni koraci transakcija

Transakcije poslane XRP *Ledgeru* ne obrađuju se u trenu. Određeni vremenski period, svaka transakcija ostaje samo odabrana/kandidirana. Životni ciklus pojedine transakcije sastoji se od nekoliko koraka. Koraci su sljedeći:

- Transakciju stvara i potpisuje vlasnik računa
- Transakcija je poslana na mrežu
    - Loše oblikovane transakcije mogu biti odmah obijene
    - Dobro oblikovane transakcije mogu biti odobrene, pa naknadno odbijene
    - Dobro oblikovana transakcija može biti odbijena, pa naknadno odobrena
- Tijekom konsenzusa transakcija je uključena u knjigu
    - Rezultat uspješno zaokruženog konsenzusa je validirani *Ledger*
    - Ako krug konsenzusa a ne uspije, proces konsenzusa ponavlja
- Validirani Ledger uključuje transakciju i njezin učinak na stanje Ledgera

Aplikacije bi se trebale oslanjati samo na informacije validiranih *Ledgera*, a ne na privremenim rezultatima odabranih transakcija. rezultati transakcije postaju nepromjenjivi samo kada je ta transakcija uključena u validirani *Ledger*, ili kada transakcija uključuje *"LastLedgerSeguence"* te se ne pojavljuje u niti jednom validiranom *Ledgeru* s tim rednim brojem ili nižim od njega. (Cohen, 2017.)

Najbolja praksa za rukovanje aplikacijama koje potvrđuju transakcije trebala bi:

- Upotrijebiti *"LastLedgerSequence"* parametar kako bi se osiguralo da transakcija bude validirana ili neuspješna na deterministički i brz način.
- Provjeriti rezultate transakcija u validiranim *Ledger-ima*:
    - dok se *Ledger* koji sadrži transakciju ne potvrdi, ili dok ne prođe *"LastLedgerSequence*, rezultati su privremeni
    - transakcije s rezultatom – tesSUCCESS, "validated":true - su nepromjenjivo uspjele
    - transakcije s drugim kodovima i "validated":true su nepromjenjivo propale

5. RIPPLE NOVČANICI

Može se reći da je XRP novčanik isto što i svaku drugi novčanik u kojem se čuvaju papirnate novčanice, samo što postoji više načina i oblika spremanja i pohranjivanja kriptovaluta. Za pravilno korištenje ove vrste novčanika potrebno je poznavanje osnovnih pojmova kao što su: adresa novčanika i tajni ključ. Ove dvije linije koda, koje se generiraju slučajnim odabirom je sve što je potrebno kako bi se mogao koristiti XRP novčanik i kako bi se mogle izvršiti transakcije. Ripple novčanik može se generirati na različite načine.

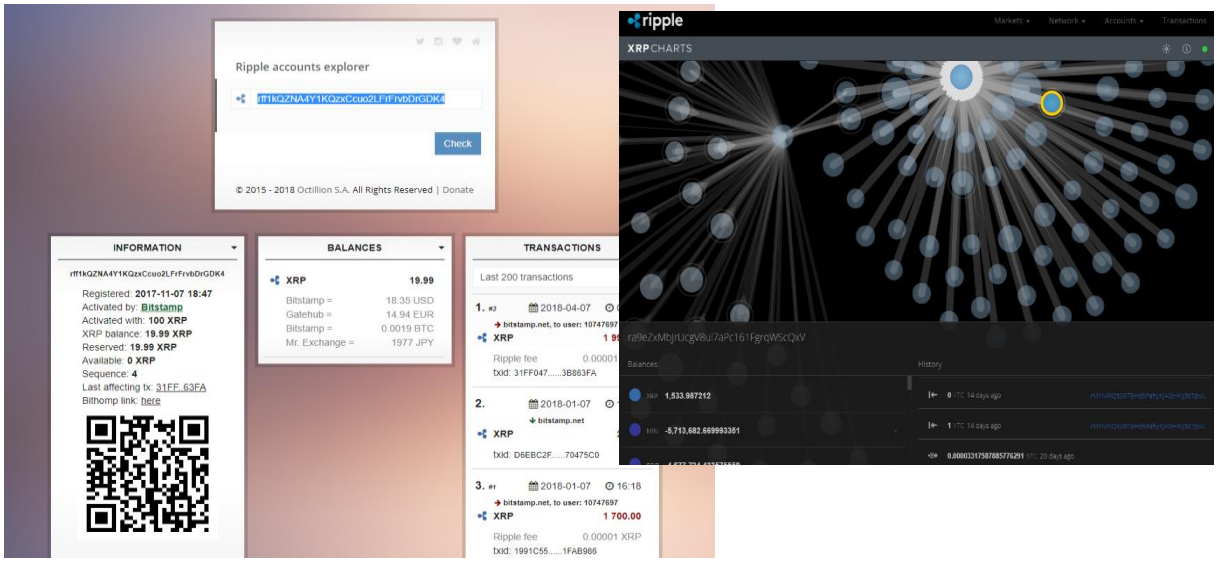
Prije upotrebe samog Ripple novčanika, mora se dogoditi aktivacija. Aktivacija se događa kada se 20 XRP-a pohrani na adresu novčanika te će tih 20 XRP-a biti pohranjeno u novčanik kao neka vrsta pričuve. Pričuva se stvara kako bi se zaustavili hakeri i mogući zlonamjerni napadi. Nadalje, trebalo bi se izbjegavati stvaranje više novčanika te umjesto toga uvoziti postojeće novčanike ako se isprobavaju nove aplikacije i slično.

5.1 Adresa novčanika

Novčanik adresa je jedinstveni indentifikator na XRP *Ledgeru*. XRP *Ledger* nikada ne prestaje pratiti sadržaj tih adresa. Kada se izvrši transakcija, *Ledger* jednostavno smanjuje sredstva iz jedne adrese i povećava sredstva na adresi primatelja. Kao što se može vidjeti na slici ispod teksta adresa novčanika je javna i može se dijeliti na mreži, što ne bi trebalo predstavljati problem. Međutim izloženost na mreži i osiguravanje privatnosti uvijek bi trebala biti na prvom mjestu pa se tako ne preporuča dijeljenje adrese sa svima.

Slika lijevo prikazuje takozvani Ripple *Explorer* napravljen od treće strane kroz koji je moguće vidjeti sve transakcije i podatke na nekoj određenoj adresi novčanika. Slika desno prikazuje originalni Ripple *Explorer* koji također prikazuje mrežu te je moguće pretraživati unutar mreže sve novčanike, upisivanjem adrese direktno ili traženjem ručno. Prikazuje se povijest transakcija i slično.

Slika 8- Prikaz Adrese novčanika



Izvor: Autor

5.2 Tajni ključ

Tajni ključ bi se mogao opisati kao lozinka i potpis u nekom drugom obliku zaštite podataka. Prilikom prijenosa sredstava s Ripple novčanika, XRP *Ledger* zahtjeva dokaz o vlasništvu prije nego dopusti da se sredstva u novčaniku smanje, odnosno prije nego nastane sam prebačaj sredstava. Tajni ključ se ne može promijeniti ili prilagoditi, dobiva se nasumičnim odabirom.

Ako netko dođe do nečijeg tajnog ključa i adrese, sredstva koja su u novčaniku mogu biti trajno ispražnjena. Zato je potrebno tajni ključ čuvati na sigurnom mjestu. Podrazumijeva se da ne bude spremljen na banalna mjesta i pod banalnim nazivom koji bi mogao aludirati da se radi o tajnom ključu. Nije preporučljivo skladištenje ključa u tekstualne datoteke na računalu. Neki od preporučenih načina čuvanja lozinke su spremanje u wordu, ali spremljenu pod šifrom. Također je moguće napraviti enkripciju na USB te tako dodatno zaštititi sadržaj.

5.3 Vrste novčanika

Za odabir novčanika potrebno je poznavanje vlastitih potreba poznavanje sigurnost. Sigurnost nikada ne može biti sto postotna, ali može dosegnuti visoku raznu ukoliko se uloži znanja i truda. Ripple je usmjeren na velike organizacije koje šalju velike količine transakcija. Cilj mu je sigurnost i trajanje transakcija u sekundama. Ripple također ima svoj prilagođeni *"Ripple Transaction Protocol",* ovaj protokol ne podupire storniranje transakcija. Potrebno je napomenuti da ne mogu svi novčanici čuvati Ripple valutu, baš zato što Ripple želi osigurati sigurnost svojim korisnicima. Pa tako postoje četiri glavne vrste novčanika koje se razlikuju oblikom i zaštitom. (Nel, 2018.)

5.3.1. Hosted novčanici:

Ova vrsta novčanika se smatra najlošije zaštićenom vrstom. Ako se mora koristiti depozitna oznaka kako bi se sredstva položila u novčanik onda se radi o Hosted novčaniku. Hosted novčanik je kao račun u banci, sva fizička sredstva nalaze se u istom pool-u unutar novčanika. Samo se prati koliki udio propada kome. Kao što je već rečeno ovaj novčanik se smatra najriskantnijim novčanikom za čuvanje sredstava jer sredstva nisu po kontrolom vlasnika sredstava već treće strane. (Nel, 2018.)

5.3.2. Exarpy

Ovo je novčanik koji je baziran na internetu. Ovaj novčanik ne sprema fizički sredstva, nego pruža usluge aplikacije za obavljanje transakcija na Ripple mreži. Za svaku transakciju izvedenu preko ovog novčanika potrebno je platit 0,025 XRP-a. U to je uključena mrežna naknada za Ripple, te tako nema skrivenih troškova. Baš kao i bankovni račun, ovaj novčanik koristi pin od 16 brojeva. Korisnici moraju znati ovaj pin i negdje ga skladištiti inače neće biti u mogućnost pristupiti svom računu.

5.3.3. *Hardware* novčanici

Hardware novčanici su ustvari *hardware* uređaji za spremanje podataka pod enkripcijom. Adresa novčanika i tajni ključ kriptirani su u uređaju. Međutim potrebno je i programsko rješenje na računalu kako bi se uspostavila komunikacija sa *Ledgerom*, ali tajni ključ nije pohranjen na računalu. (Nel, 2018.)

5.3.4. Ledger Nano S

Ovo je jedan od najpopularniji *hardware* novčanika te je u pravom smislu novčanik s puno mogućnosti. Tvrtka koja ga proizvodi nalazi se u Francuskoj, od 2014. godine bavi se izradom hardverskih novčanika za kriptovalute. Osim Ripple valute ovaj hardverski novčanik može pohranjivati i neke druge jednako popularne valute. Posjeduje dodatnu razinu sigurnosti što ga dovodi u top izbor novčanika.

5.3.5. *Software* novčanici

Ovo je najčešći tip novčanika koji se koristi. To je ustvari program na nekom uređaju, mobilnom telefonu, tabletu i slično, koji sadrži adresu novčanika i tajni ključ. Ovaj program obavlja komunikaciju sa blockchain-om. (Nel, 2018.)

5.3.6. Rippex

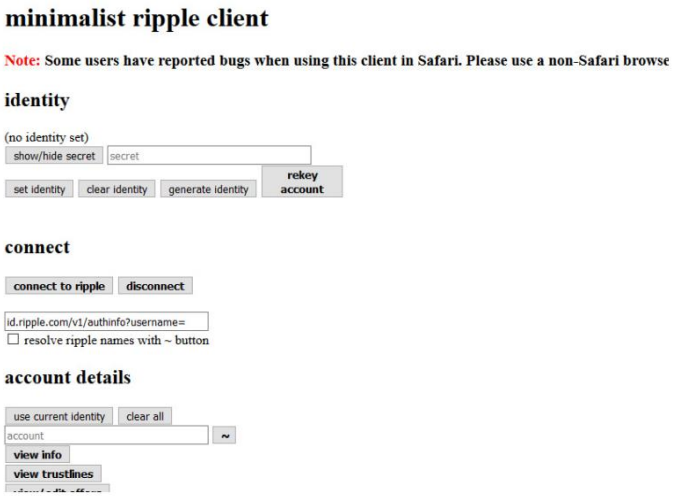
Ovo je novčanik koji se temelji na desktop novčaniku za čuvanje Ripple kriptovalute. On je ustvari eksperimentalni novčanik razvijen od strane Ripple-a. Podržava operativne sustave kao što su Widows, OSX i Linux. Izvorni kod dostupan je na GitHubu. Ukoliko je korisnik iskusan programer, moguće je sastavljanje vlastite verzije novčanika. Novčanik se nije aktivno razvijao i još uvije postoje greške u sustavu. (Nel, 2018.)

5.3.7. Takozvana hladna pohrana

Najpopularniji oblik ovog novčanika je papirnati oblik. Kao što je već napomenuto ranije u tekstu, sve što je potrebno imati za kontrolu novčanika su adresa novčanika i tajni ključ, dok se adresa novčanika može generirati iz tajnog ključa. Pa se tako može zaključiti da su ovi novčanici baš to, adresa i tajni ključ. Kako bi se osigurao sigurniji pristup, takvi novčanici se mogu generirati u izvan mrežnoj okolini.

Smatra se jednom od najsigurnijih načina pohrane kriptovaluta, poslije hardverskog novčanika. Činjenica da se ne povezuje na internet daje ovom novčaniku dodatnu zaštitu. Korisnici ovog novčanika također mogu izgenerirati identitet, odnosno aplikacija će za njih generirati javni i privatni ključ. Vrlo je važno napomenuti da korisnici moraju zapisivati sve dobivene podatke. Najbolji način za kreiranje novčanika za pohranu Ripple-a je korištenje "Minialist Ripple Client".

Slika 9- Prikaz "Minialist Ripple Client"



Izvor: https://blockonomi.com/best-ripple-wallets/#Web_Wallets (25.4.2018)

Može se zaključiti da se Ripple novčanici razlikuju od Bitcoin novčanika. *Hardware* i papirnati novčanici najsigurniji su za pohranu sredstava. Korisnik je dužan napraviti provjeru tih novčanika i tako sebi osigurati okolinu za pohranu sredstava. Stopostotna sigurnost ne postoji.

6. ZAŠTO KUPOVATI XRP - BUDUĆNOST XRP-A

Kako bi korisnik bio što bolje upoznat sa prednostima i nedostacima same kriptovalute potrebno je ispitivanje, analiziranje tržišta. Isto tako je potrebno znati da stanje kriptovaluta na tržištu ovise o vijestima i događajima u svijetu. Za Ripple bi se moglo reći da radi s najvećim financijskim institucijama širom svijeta. Ripple za cilj ima poticanje cjelokupnog financijskog sektora postizanjem instant transakcija. U nekoj skoroj budućnosti se predviđa da će se koristiti za rješavanje likvidnosti prekograničnih transakcija. Banke i davatelji transakcija mogu koristiti XRP za podmirivanje transakcija pomoću valuta kako bi se smanjili opći troškovi.

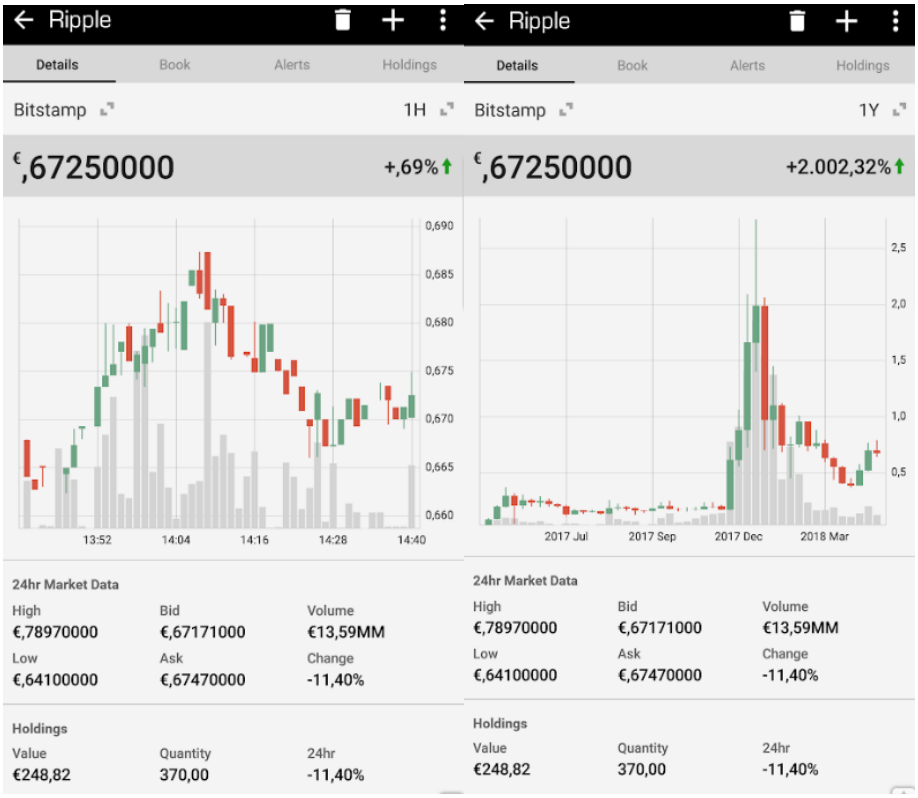
Ripple može obraditi 1500 transakcija u sekundi, što je za razliku od drugih kriptovaluta velika brojka. Usporedno na primjer s Bitcoinom koji može podnesti do 7 transakcija u sekundi, Ripple je daleko ispred. Ripple.ova tehnologija je dovoljno snažna da zamijeni međunarodne platne sustave kao što je VISA, istovremeno smanjujući troškove i omogućavajući trenutačne prijenose sredstava. Veliki broj banaka iz cijelog svijeta aktivno radi s Ripple-om, omogućavajući im tako Ripple tehnologiju preko njihove infrastrukture za plaćanje. To dakako čini Ripple pouzdanim i sigurnijim za ulaganje.

Vrijednost ove kriptovalutue u kratkom je vremenu narasla na neočekivane vrijednosti tijekom 2017. godine, te je početkom 2018. naglo pala. Međutim stanje na tržištu je variralo svake godine u isto vrijeme, pa se smatra da će cijena opet ići gore.

Gledajući najnovija dostignuća i povećanje interesa za XRP-u, do kraja 2018. godine, očekuje se da će cijena Ripple prijeći minimalnu barijeru od $ 7. Također je trgovanje XRP valutom jedno od najpopularnijih nakon Bitcoina i Etheriuma. Očekuje se da će obujam trgovanja rasti tijekom cijele 2018. godine, te će tako Ripple doći do očekivanih 7-10 $. Smatra se da će ukupna vrijednost, odnosno cijena narasti, ali dakako to neće biti iz mjeseca u mjesec tako. Mnogi korisnici kriptovaluta ne vole ideju da bi ijedna banka ili institucija mogla regulirati kriptovalute. Prema tome u određenim trenucima XRP će biti u znatnom padu, na što uvijek treba biti spreman kada se radi o kriptovalutama.

Slike ispod teksta prikazuju grafove koji predstavljaju padove i poraste kriptovalute. Prvi graf odnosi se na zadnjih sat vremena i variranje u cijeni u tih zadnjih sat vremena, dok drugi graf prikazuje zadnjih godinu dana i promjene nastale u zadnjih godinu dana. Iz priloženog se može vidjeti koliko je tržište stabilno, ali i nestabilno. Vrijednost valute prije godinu dana bila je znatno manja u odnosu na današnju vrijednost valute. Aplikacija kroz koju su prikazani grafovi je mobilna aplikacija "Blockfolio" koja na jednostavan način prikazuje najbitnije informacije o kriptovalutama. Također kroz aplikaciju se može iščitati koliko je vrijednost valute porasla ili pala u zadnjih godinu dana do zadnjih sat vremena. Kao što je već spomenuto u radu vrijednost Ripple-a je jako porasla, u brojkama bi to bilo 2002,32% u odnosu na zadnju godinu u ovo vrijeme.

Slika 10- Prikazuje grafove vrijednosti valute



Izvor: Autor

7. MONERO

Monero je kriptovaluta otvorenog koda, stvorena u travnju 2014.godine. Usmjerena je na privatnost i decentralizaciju. Podržana je od strane operativnih sustava kao što su : Windows, MacOS, Linux, Andorid, iOS i FreeBSD. Monero koristi javni *Ledger* za zapisivanje transakcija, dok se nove jedinice kreiraju takozvanim "rudarenjem" procesom. Kao glavni cilj može se reći da mu je unaprijediti postojeći dizajn kriptovaluta zatajivanjem pošiljatelja, primatelja i količine svake izvršene transakcije. Usredotočenost na privatnost privukla je osobe koje izbjegavaju provođenje zakona. (Buntinx, 2018.)

Za razliku od mnogih drugih kriptovaluta koje su dosta slične Bitcoinu, Monero se temelji na *"CriptoNight proof-of-work hash"* algoritmu, koji potječe iz *"CryptoNote"* protokola. Monero je zamjenjiv, odnosno svaka jedinica valute može biti zamijenjena drugom jedinicom. To čini Monero različitim od ostalih kriptovaluta kao što su Bitcoin, dakle adrese s novcem koje su prethodno povezane sa neželjenim radnjama mogu bit stavljene na crnu listu te njihov novac može biti odbijen od strane drugih korisnika. Također, *"Stealth address"*[2] generirane za svaku transakciju onemogućuju otkrivanje stvarne odredišne adrese, od strane bilo koga drugog osim od pošiljatelja i primatelja.

Slika 11- Prikaz grafa Monero kriptovalute

Izvor: Autor

[2] Automatske jednokratne adrese za svaki transakciju

7.1 Monero *"Ring signatures"*

U kriptografiji, *"Ring signature"* je vrsta digitalnog potpisa, koju može izvesti bilo koji član grupe korisnika, koji imaju ključ. Stoga, poruka potpisana *"Ring signature-om"* je potvrđena od strane nekoga iz određene grupe ljudi. Jedno od sigurnosnih svojstava *"Ring signature-a*" je svojstvo da bi trebalo biti potpuno nemoguće utvrditi čiji je ključ u grupi iskorišten za kreiranje potpisa. Na primjer, ova vrsta potpisa može se koristiti za potpis neke javne osobe, bez otkrivanja imena osobe koja ju je potpisala. Ova vrsta sigurnosnih postavki dobra je za aplikacije jer se anonimnost *"Ring signature-a"* ne može opozvati.

Potrebo je znati da *"Ring signature-a"* koristi kombinaciju korisnikovog ključa i javnih ključeva. Ovi ključevi dobivaju se preko Monero blockchain-a te brzo mogu stvoriti mnoštvo potpisa. Rezultat toga je da bilo tko, tko dolazi izvana nije u mogućnosti prepoznati pošiljatelja. Korištenjem ove kriptovalute za čuvanje privatnosti, dovodi do visokih rezultata. Upotreba ovog koncepta nije nova pojava na tržištu, ali je jedan od najboljih načina za održavanje sigurnosti na mreži. (Buntinx, 2018.)

7.2 Monero *"Stealth addresses"*

"Stealth addresses" važan su dio Monero inherentne privatnosti. One zahtijevaju od pošiljatelja stvaranje slučajnih jednokratnih adresa za svaku transakciju i to u ime primatelja. Primatelj može objaviti samo jednu adresu, dok sve dolazne uplate idu na unikatne adresa na blok mreži, gdje se ne mogu povezati niti s objavljenom adresom primatelja niti s adresama drugih transakcija. Samo pošiljatelj i primatelj mogu znati gdje je plaćanje poslano.

Nakon stvaranja Monero računa, kreira se privatni ključ, ključ za privatne troškove i javna adresa. Ključ potrošnje upotrebljava se za slanje uplata, ključ za prikaz koristi se za prikaz dolaznih transakcija namijenjenih korisnikovom računu te javna adresa služi za primanje uplata. Ključ za potrošnju i ključ za prikaz koriste se za izradu Monero adrese. Također je moguće postojanje novčanika samo za gledanje, koji koristi ključ za prikaz. Dijeljenjem ključa za prikaz moguće je odrediti tko može vidjeti korisnikovo stanje na računu. Monero je privatan, i polu-transparentan po izboru korisnika.

7.3 Prikaz normalne i Monero transakcije

Glavna tehnologija koja stoji iza Monera je ravnoteža koja omogućuje korisniku da kontrolira svoje ključeve i radi zaštićeno s dokazanim sigurnosnim mehanizmima, a u isto vrijeme omogućava fleksibilnost i razvoj na mreži. Zadane postavke za na primjer Bitcoinove transakcije potpuno su transparentne i pod pseudonimima, ako se ne poduzimaju koraci kako bi se očuvao identitet i transakcija. Što bi značilo da korisnikova IP adresa može biti povezana sa korisnikovim uređajem s dovoljno resursa kako bi se povezalo to dvoje. (Buntinx, 2018.)

Slika 12- Prikaz normalne transakcije

Izvor: https://coincentral.com/what-is-monero/ (5.2.2018.)

"Ring signature" su digitalni potpisi koje nekoliko potpisnika potpisuje jednu transakciju. Potpisivanje se odvija za pridruženim računima, ali nitko ne zna tko je prvi potpisao. Pošiljatelj generira jednokratni ključ, a primatelj je jedina strana koja može detektirati i potrošiti novac pronađen na temelju tog ključa. Ključne slike, kriptografski ključ, izvedeni su iz svakog slanja te tako sprječavaju dvostruku potrošnju. (Buntinx, 2018.)

Slika 13- Prikaz *"Ring Signature"* transakcija

Izvor: https://coincentral.com/what-is-monero/ (5.2.2018.)

7.4 Upotrebljivost

Potrebno je napomenuti da Monero na tržištu stoji podjednako kao i ostale poznatije kriptovalute. Monero se nalazi na raznim trgovinama za razmjenu i trgovanje kriptovalutama kao što su Kraken, Bitfinex i Poloniex te mnogi drugi. Za trgovanje valutama potrebno je posjetiti neke od ovih trgovina i kupiti željenu količinu kriptovalute te ga spremiti na sigurno mjesto kao što su novčanici za kriptovalute. Osim samog trgovanja ovom kriptovalutom moguće ju je i rudariti i tako proizvesti određeni broj Monero jedinica koje se lako mogu pretvoriti u novčane vrijednosti.

Vrijednost ove kriptovalute, kao i svih na tržištu, varira kroz vrijeme te na nju utječu različiti čimbenici. U zadnjih nekoliko mjeseci ovaj je valuta doživjela nagli porast vrijednosti, odnosno njena cijena je ekponencionalno narasla. Svaki ulog u kriptovalute dok su one u padu i na svojoj najnižoj točci isplatiti će se u budućnosti. Greška koju korisnici rade je kupovanje valuta kada počinju rasti i prodavanje istih kada su već znatno pale. Iako zvuči skoro nemoguće mnogi kupci su se uhvatili u ovu zamku.

Budući da Monero nudi visok stupanj privatnosti, svi njegovi kupci ne moraju se brinuti o tome. Razina privatnosti je visoka, a jedinice su jednostavne za trgovanje. Također je moguće mijenjati jedinice Monera za neke druge kriptovalute. Što daje dodatnu sigurnost. Ukoliko dođe do naglih promjena stanja na tržištu moguće je prebaciti jedinice na sigurniju valutu ili slično. Monero također ima zajednicu koja pruža veliku potporu svim korisnicima. Pomaže u rješavanju nedoumica i problema.

Kako se razvija sama tehnologija tako se i povećava rizik nad osobnim podacima, transakcijama i slično. Korisnici interneta postaju sve više svjesni važnosti privatnosti i sigurnosti, ali isto tako i činjenice koliko su nezaštićeni na internetu. Iz ovih jednostavnih razloga, Monero bi mogao postati jedna od glavnih kriptovaluta za sigurnost, u budućnosti. Kao što je već spomenut u tekstu Monero uspijeva sakriti vrijednost neke transakcije, što omogućava potpuno sakrivanje transakcije, odnosno nitko ne može znati da li je uopće transakcija postojala.

8. MONERO NOVČANICI

Skoro svaka kriptovaluta posjeduje svoj novčanik za skladištenje jedinica. Bez obzira na koji način se žele skladištiti određene jedinice neke kriptovalute (desktop, web) svi ti alati mogu se pronaći za sve valute koje žele konkurirati na tržištu i zaštititi svoje korisnike. Za Monero kriptovalutu postoji nekoliko različitih rješenja. Neka od njih su dobra dok druga baš i ne. Iako spada u jednu od najpopularnijih kriptovaluta Monero ne podržava dva glavna *hardware* novčanik poduzeća, a to su Trezor i Ledger.

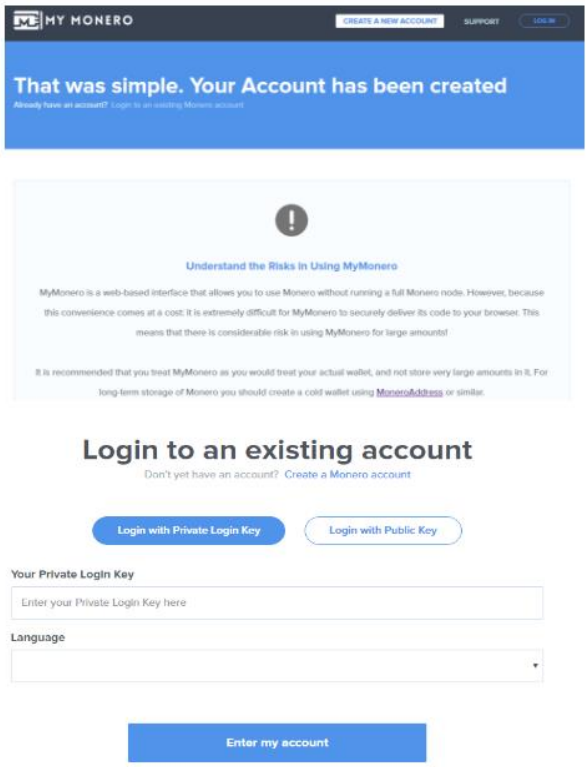
8.1 Monero internet novčanici

Iako internet - novčanici predstavljaju sigurnosni rizik pri skladištenju velikih količina valute, platforma MyMonero ugledna je u Monero zajednici. Njome upravlja Riccardo Spagni, jedan od vodećih razvojnih programera Monero od sada. Ključevi i podaci novčanika kriptirani su, a sama usluga nikada ne može izravno pristupiti svojim sredstvima. To je dobra opcija ukoliko je potrebno držati XMR na strani, u svrhu potrošnje. Međutim, pri pohranjivanju tisuća jedinica, novčanik za papir ili desktop može se pokazati kao bolja opcija.

8.1.1. MyMonero

MyMonero je najpopularniji internet novčanik za skladištenje Monero jedinica. Jednostavan je i praktičan te pruža jednako jednostavnu i praktičnu pohranu XRP-a. Ovim novčanikom upravljam Riccardo Spagni, glavni član Monero Core tima. MyMonero pruža sigurne Monero račune. Internet sučelje je intuitivno i vrlo jednostavno. Izrada računa traje nekoliko sekundi. Sigurnosni ključ se sastoji od 13 jedinica, koji je potrebno spremiti a sigurno mjesto. Ključ nije moguće pohraniti na poslužitelju. Iako pruža jednostavnu i brzu uslugu, glavni rizik je sigurnost. Nakon što korisnik izradi račun dobiva i upozorenje u obliku poruke, gdje se naglašava da je iznimno teško osigurati sigurno slanje koda u preglednik. Što bi značilo da postoji značajan rizik od napada. Također je napomenuto ukoliko se želi skladištiti Monero jedinice na duže vrijeme, potrebno je koristiti neke sigurnije novčanike, kao što su novčanici hladne pohrane.

Slika 14- Prikaz kreiranja računa na MyMonero



Izvor: Autor (03.5.2018)

8.2 Monero desktop novčanici

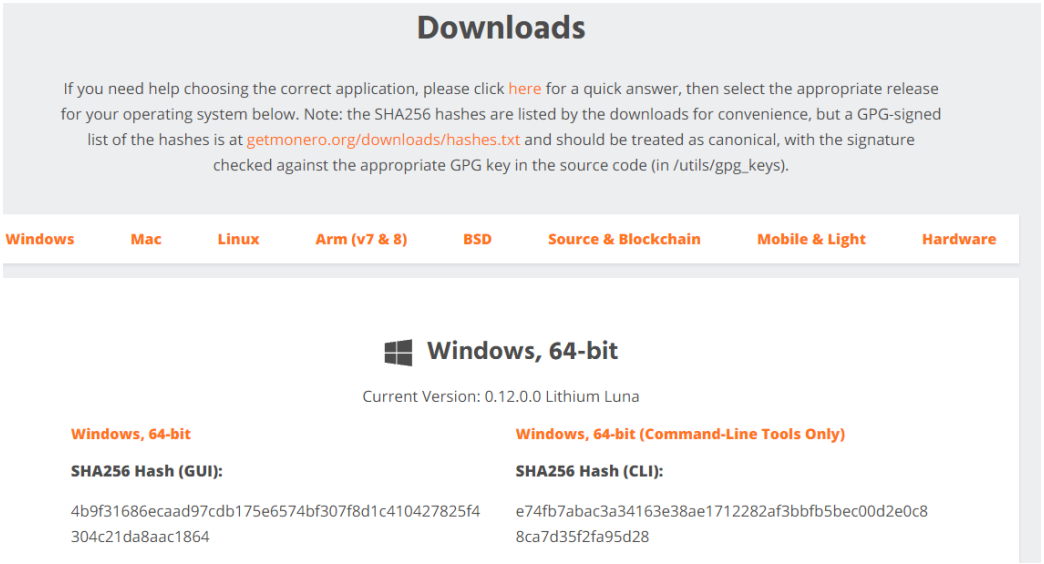
Za razliku od drugih novčanika, Monero GUI client je najbolji destop novčanik trenutno na tržištu. Također se koristi kao puni čvor za korisnike kojima je to potrebno i koji su spremni zaviriti malo dublje u taj svijet. Sinkroniziranje s Monero nešto se sporije odvija, ali bi se taj problem trebao riješiti u bližoj budućnosti, uvođenjem uporabe udaljenih čvorova. Ovo nije slučaj samo sa Monerom kriptovalutom, sličan ili isti problem imaju i ostale kriptovalute. Buduća razvojna istraživanja mogla bi ubrzati ovaj proces.

8.3 Monero GUI novčanik

Smatra se prvim desktop novčanikom koji je bio vrijedan razmatranja i proučavanja. Dostupan je za preuzimanje i moguće ga je koristiti na operacijskim sustavima kao što su Windows, Mac, Linux i niz drugih operacijskih sustava. Osmišljen je kako bi korisnici mogli lakše komunicirati sa svojim XMR-ima. Kao takozvani puni - čvor novčanik, postupak

preuzimanja i sinkronizacije korištenjem GUI novčanika traje neko vrijeme. Također se koristi velika količina prostora na tvrdom disku, kao i procesorske snage, pa ovaj novčanik možda nije pravi izbor za sve korisnike. Ovisno o potrebama samog korisnika potrebno je birati i novčanike. Nakon dovršetka sinkronizacije, novčanik je relativno jednostavan za upotrebu, svakoga tko ima imalo iskustva u svijetu kriptovaluta se može snaći. Potrebno je napomenuti da korištenje ovog novčanika može biti lako iskusnim korisnicima, dok onim drugim možda to neće biti. Preporuča se razmatranje drugih opcija i novčanika.

Slika 15- Prikaz stranice za preuzimanje potrebne vrste Monero GUI novčanika



Izvor: Autor

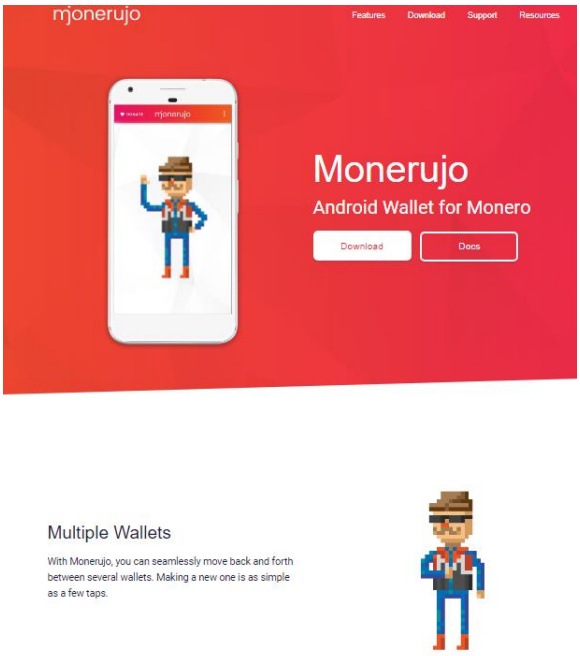
8.4 Monero papirnati novčanici

Iako se čini da su papirnati novčanici nešto manje popularni nego što je to bilo prije nekoliko godina, oni su još uvijek dobro rješenje za pohranu kriptovalutnih jedinica, na duži period. U slučaju Monera, rješenje odabira papirnatog novčanika moguće je naći na web stranici Monero Address. Štoviše, ovaj papirnati novčanik podržava engleski, japanski i španjolski jezik, što je rijetko za vidjeti. Također je moguće raditi izvan mreže, kako bi se postigla dodatna sigurnost.

8.5 Mobilni novčanik Monerujo

Radi praktičnosti upravljanja XMR-om u pokretu, moguće je koristiti mobilne aplikacije. Pa je tako jedna od najpopularnijih takozvana Monerujo aplikacija, novčanik. Ova aplikacija može se koristiti na Andorid uređajima. Upotrebljava udaljene čvorove za usklađivanje s blockchainom od Monera. Ovo je novčanik otvorenog koda te su svi privatni podaci pohranjeni na samom uređaju. Korisničko sučelje aplikacije intuitivno je i lako za proučiti i naučiti kako ga koristiti. Neke od ključnih značajki Monerujo aplikacije uključuju mogućnost upravljanja s više novčanika, kao i funkcionalnost skeniranja QR koda za slanje i primanje XMR plaćanja. Jedan od nedostataka je činjenica je ju nije moguće koristiti na drugim operacijski sustavima osim Andorida. Pa tako na primjer iPhone korisnici neće biti u mogućnosti pristupiti ovoj aplikaciji, novčaniku.

Slika 16- Prikaz Monerujo stranice za preuzianje aplikacije



Izvor: Autor

Nakon kupovine Monero kriptovalute, korisnik može doći u iskušenje da čuva svoje jedinice na trgovini preko koje trguje. Ovo može biti brzo i praktično rješenje ako se radi o manjoj količini jedinica ili ako korisnik ne namjerava dugo zadržavati svoje jedinice na poslužitelju. Ukoliko je situacija drugačija ovo nije dobra praksa za skladištenje jedinica

kriptovaluta općenito. Ove vrste novčanika ne osiguravaju vam sigurnost baš iz činjenice da sigurnosni ključ nije u potpunosti u vašem vlasništvu. Najbolja praksa bila bi premještanje jedinica XMR- a u privatne novčanike dobro zaštićene privatnim ključevima.

8.6 *Hardware* Monero novčanik

Moneru je zasigurno potreban hardverski novčanik. Pogotovo u ovom trenutku kada njegova popularnost raste iz dana u dan. Iako još ne postoji hardverski novčanik koji podržava Monero jedinice, grupe razvojnih programera rade na tome. Ne zna se točno kada će ovaj novčanik biti dostupan, ali potražnja za istim je uvelike porasla. Također dolazi do integracije Monera za Ledger Nano S hardverski novčanik. Iako se na ovom radi već neko vrijeme, sam proces implementacije je dosta spor. Smatra se da će ova opcija biti omogućena kroz nekoliko tjedana, ali možda čak i mjeseci. Nema službenih informacija. Postoji mogućnost implementacije Monera u Trezor. Iako se smatra da se to neće ostvariti u bližoj budućnosti, ta opcija još uvijek postoji. Korisnici se nadaju da će uskoro bit jedna od ove tri opcije za hardversko skladištenje Monero jedinica dostupna na tržištu.

8.7 Bitne stavke novčanika

Neke od najbitnijih stvari koje je potrebno provjeriti da li novčanik ima/nema prije početka korištenja novčanika. Osim toga u toku traženje pravog novčanika za korisnika, bitno je poznavanje nekih stavki.

- Postoji mnoštvo novčanika koji podržavaju razmjenu XMR jedinica. Prije korištenja novčanika potrebno je utvrditi da je novčanik moguće koristiti za razmjenu XMR-a.
- Razumijevanje korisničkog sučelja novčanika od izuzetne je važnosti. Imajući to na umu, korisnik bi trebao potražiti novčanik koji je jednostavan za korištenje.
- Jedna od važnijih stavki je sigurnost. Prije početka korištenja novčanika, potrebno se informirati o sigurnosti istog. Kontrola nad privatnim ključevima, razina šifriranja, lakoća hakiranja novčanika ili krađe.
- Privatnost je također stavka koju novčanik treba ispuniti. Pojedini novčanici ne omogućavaju anonimnost, što se korisnicima ne mora svidjeti.

- Korisnička podrška koju osigurava pružatelj usluga od strane novčanika također je bitna za korisnike. Za sva pitanja i moguće nedoumice, se imaju kome obratiti.
- Da li je novčanik u razvoju ili si radi o samom pokušaju nastanka novčanika.
- Potrebno je pregledati recenzije koje se odnose na neki novčanik, i tako preko drugih korisnika otkriti da li novčanik zadovoljava vaše potrebe ili ne. Recenzije mogu pružiti bolju predodžbu o tome koliko je novčanik siguran, koliko je jak tip podrške, koliko je jednostavan za korištenje i slično.

Kako bi korisnik mogao sigurno pohraniti svoje jedinice neke kriptovalute potrebno je slijediti neke od savjeta:

- Napraviti interno istraživanje. Prije odabira novčanika, potrebno je napraviti detaljno istraživanje kako bi znali što određeni novčanik točno nudi u usporedbi sa onim što nama treba. Da li je novčanik ponuđen i izrađen od poznatih razvojnih stručnjaka ili je samo još jedan pokušaj izrade novčanika. Da li nudi sigurnosne značajke koje korisniku odgovaraju ili ne nudi dovoljnu privatnost i zaštitu.
- Potrebno je razmotriti izvan mrežnu pohranu podataka. Pohranjivanje privatnih ključeva izvan mreže smatra se najboljom sigurnosti. Također Ledger pokušava uvesti Monero u svoj novčanik Nano S, koji je hardverski novčanik. Za sada dok se to ne ostvari, svi korisnici koji žele takozvanu hladnu pohranu mogu skladištiti svoj podatke na papirnatim novčanicima.
- Prije instaliranja ili pristupa bilo kojem novčaniku, potrebno je provjeriti da li je antivirusni softver i softver za uklanjanje zlonamjernog softvera na uređaju ažuriran. Također je potrebno redovito ažurirati zaštitu, kako bi se sigurnost još više unapredila.
- Postavljanje jakih zaporki još je jedna od stavki koje korisnik mora imati na umu. Potrebno je odvojiti vrijeme za stvaranje snažne, složene lozinke. Privatne ključeve potrebno je pravovaljano skladištiti.

9. MJESTA ZA RAZMJENU KRIPTOVALUTA

Prvi korak u svijetu kriptovaluta je razmjena i kupovina istih. Postoje dvije vrste razmjene kriptovaluta. Prvi tip razmjene je ono što većina ljudi zove *fiat* razmjena. To je razmjena koja omogućuje izravni prijenos američkih dolara, eura i većine drugih valuta u zamjenu za neku kriptovalutnu jedinicu ili jedinice. Druga vrsta razmjene jesu razmjena kriptovaluta za kriptovalutu. Ovisno o tome koju od ove dvije opcije korisnik želi, morati će odrediti i trgovinu preko koje će vršiti razmjenu. Obadva načina razmjene imaju svoje prednosti i nedostatke. Prije određivanja načina razmjene i odabira trgovina potrebno je odgovorit na neka pitanja kao što su:

- Koliko je sigurno *web* mjesto preko kojeg se trguje?
- Koliko korisnički podaci zaštićeni?
- Da li je osigurano web sjedište u slučaju napada?
- Kakva je likvidnost?
- Kolike su naknade za razmjenu/transakciju?
- Koje su i koliko različitih opcija plaćanja postoji?
- Kakva je korisnička podrška vezana za razmjenu i transakcije?

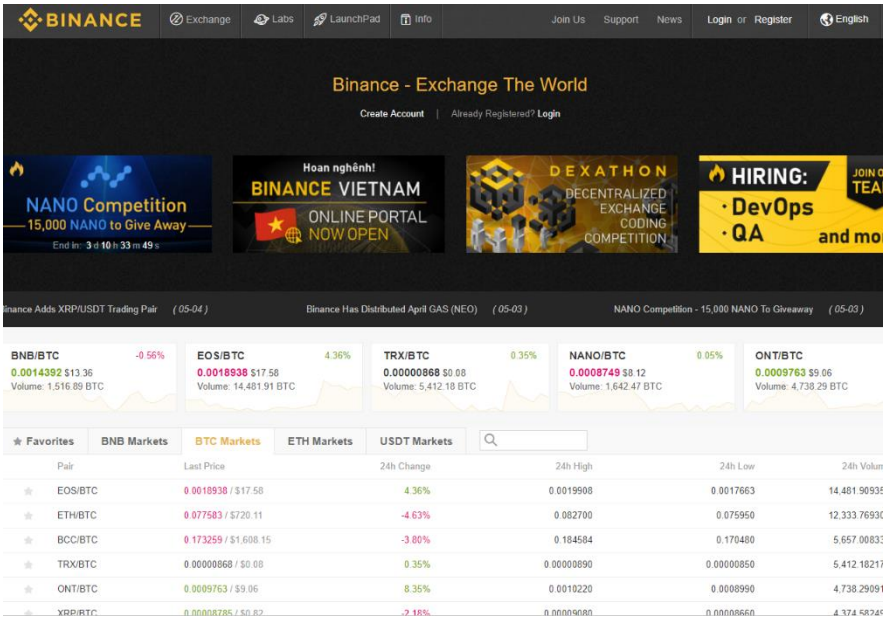
Kriptovalute sve više i više dobivaju pozornost velikih ulagača. Kriptovalute su se počele smatrati sigurnim mjestom za ulaganje, ali i u borbi protiv vladinih inflacijskih politika. Zbog toga neki korisnici svoje kriptovalutne jedinice osiguravaju kao mirovinske fondove, dok neki trguju jedinicama, kupujući po niskim cijenama i prodavajući po visokim. Za sve korisnike koji još uvijek razmišljaju o ulaganju u kriptovalute, još uvijek ulaganje može biti isplativo. Zbog velike potražnje korisnika za uslugama razmjene, mnoge trgovine su onemogućile nove korisnike. Neke od trgovina koje omogućuju nove korisnike su:

- Binance - ograničen broj korisnika se može dnevno registrirati
- Bitmax - jedna od većih trgovina kriptovalutama
- KuCoin - također jedna od većih trgovina, nudi i mobilnu aplikaciju za iOS i Android
- Gate.io - mnoge nove kriptovalute nalaze se na ovoj trgovini
- Changelly - odmah pretvara kriptovalutu u željeni oblik

9.1 Binance

Binance je i kriptovaluta i trgovina za razmjenu. Binance predstavlja simbolično riječi "Binarne financije", a kao mjesto za razmjenu valuta, ima za cilj potaknuti i poboljšati budućnost kriptovaluta i razmjena. Binance je centralizirana razmjena , nastala u Kini. Njezini zastupnici tvrde da je ova trgovina za razmjenu alternativa mnogim drugim centraliziranim trgovinama. Smatraju da su identificirali probleme ostalih trgovina za razmjenu i tako unaprijedili vlastitu te da će ju još unaprijediti. Korisnička podrška im je jedan od glavnih prioriteta. (Khatwani, 2018.)

Slika 17- Prikaz stranice Binance trgovine



Izvor: Autor

Problemi koje Binance pokušava riješiti i unaprijediti postojeće stanje su:

- Loša tehnička arhitektura
- Nesigurnost platforma
- Loša likvidnost na tržištu
- Loša služba za korisnike
- Loša internacionalna i jezična podrška

Binance je uveo neke nove značajke kako bi se ti problemi suzbili i smanjili. To su:

- Odgovarajući "motor" - sposoban je upravljati s 1400 000 narudžbi po sekundi, čineći ga takom jednim od najbržih trgovina za zamjenu.
- Pokrivenost uređaja - dostupni su na raznim operacijskim sustavima, kao što su Andorid, iOS, mobilni HTML5, Windows (računani).
- Višejezična podrška - obećali su da će lansirati Binance, odnosno korisničko sučelje koje će biti podržano engleskim, kineskim, japanskim i korejskim jezikom.
- Korisnička podrška - već su dodali korisničku podršku na japanskom, španjolskom, korejskom, engleskom i kineskom jeziku.

Struktura naknade koju je potrebno plaćati za korištenje Binance također je jedinstvena. Naknada za trgovanje preko njihovog poslužitelja iznosi 0,1%, što je dosta niska naknada u usporedbi sa drugim trgovinama za razmjenu. Naknada se može i smanjiti ukoliko se plaća BNB valutom tj. Binance valutom. Pomoću BNB-a moguće je plaćati sve naknade na stranici (tečajne naknade, naknade za povlačenje, naknade za listu, te sve ostale naknade). Kao što je već spomenuto, koristeći njihovu valutu za plaćanje dobiva se određeni popust.

Slika 18- Prikazuje popuste BNB

	1st year	2nd year	3rd year	4th year	5th year
Discount Rate	50%	25%	12.5%	6.75%	no discount

Izvor: Autor

9.2 Changelly

Ova trgovina predstavlja jedan od najlakših načina trgovanja različitim kriptovalutama. Changelly je proizvod rudarskog bazena, MinerGate, koje je poznat po dobrim proizvodima iz kripto svijeta. Jedna od novosti vezana za ovu trgovinu je činjenica da nije potrebna registracija i provjera prije same razmjene. Prijava se vrši preko e-mail adrese koja predstavlja ID te razmjena može početi. Trenutno podržava više od 35 kriptovaluta, uz koje podržava i fiat valute USD/EUR i tako dalje. Također se smatra jednom od najjednostavnijih i

najkorištenijih trgovina za razmjenu kriptovaluta. Kada se Changelly koristi za razmjenu kriptovaluta, on se povezuje u stvarnom vremenu s najboljim i najprometnijim burzama kako bi se postigla što bolje cijena. (Khatwani, 2018.)

Korištenjem Changelly-a razmjena traje između 5 do 30 minuta. Za svaku transakciju naplaćuje se naknada koja iznosi 0.5%, što predstavlja donekle razumnu naknadu u usporedbi s rizikom koji oni preuzimaju u ime svih svojih korisnik. Korisnik također plaća naknadu za rudare koja se izravno odbija s njihovog računa. Sve što j potrebno za kupovanje putem Changelly trgovine je VISA/MasterCard (kreditna/debitna kartica) ili bilo koja kriptovaluta koju podržava Changelly te novčanik na koji će korisnik primati svoje nove jedinice/kovanice. (Khatwani, 2018.)

Najvažnije značajke Changelly trgovine:

- Mogućnost zamjene Bitcoina u bilo koju drugu kriptovalutu
- Tečajne naknade iznose 0,5%
- Podržava USD Tether (USDT)
- Moguće kupovanje kriptovaluta koristeći kreditnu/debitnu karticu
- Potrebna je samo e-mail adresa i iznos koji se želi promijeniti

Slika 19- Prikazuje službenu stranicu Changelly

Izvor: Autor

9.3 Kraken

Firma Kraken osnovana je 2011. godine, sa sjedištem u San Francisku. Jedan je od prvih servisa koji je prošao kriptografsku reviziju te je prvi postao partner s prvom kriptografskom bankom na svijetu. Također je i prvi servis za trgovanje Bitcoinom u svijetu. Kraken se smatra jednim od vodećih servisa/trgovina za razmjenu kriptovaluta. Omogućuje brzo izvršavanje zahtjeva, korisničku podršku, visoku razinu sigurnosti i još puno toga. Njegovo sjedište se nalazi u SAD-u, ali njegove usluge su dostupne i u Kanadi, Europi i Japanu.

Na Krakenu je moguće trgovati sa mnoštvom valuta, pa su tako neke od najpoznatijih Bitcoin, Ethereum, Monero, Ripple (XRP) i tako dalje. Valute je moguće kupovati klasičnim valutama kao što su američki dolari, euri, kanadskim dolarima, britanskim funtima, japanskim jenima. Osim kupovanja klasičnim valutama moguća je i zamjena jedne kriptovalute drugom. Zamjena se može raditi samo sa nekim kriptovalutama, uglavnom je moguće mijenjati Bitcoin i Ethereum za neku drugu kriptovalutu. (Khatwani, 2018.)

Sigurnost koju Kraken pruža je opravdana sigurnost. Stručnjaci za sigurnost Krakena imaju strog pristup kada je riječ o sigurnosti. Osim krađa koje se mogu dogoditi na mrežu, potrebna je i visoka profesionalnost. Potrebi su dobri odnosi s bankama, poštivanje zakonskih regulativa, održavanje financijske stabilnosti i slično. Potrebno je znati koje mjere oni provode, pa su tako neke od njih spomenute u tekstu koji slijedi. (Khatwani, 2018.)

Sigurnost financija

- Sva sredstva korisnika nalaze se na bankovnim računima koji su odvojeni o glavnog operacijskog računa, a sve naknade se održavaju na dnevnoj razini
- Ništa što korisnik posjeduje ne može se koristiti za neke financijske operacije, niti u bilo kojem smislu posuditi za neke druge radnje
- Cilj im je postići što više bankarskih partnerstva, tako da prilikom nekih problema, dnevne transakcije ne budu prekinute

Spremanje jedinica

- Svi novčanici su pod enkripcijom, odnosno svi novčanici su kriptirani
- Nove transakcije idu direktno u takozvane hladne novčanike, gdje su potpuno izolirane od online sustava
- Samo jedinice koje su potrebne za održavanje likvidnosti su spremljene online

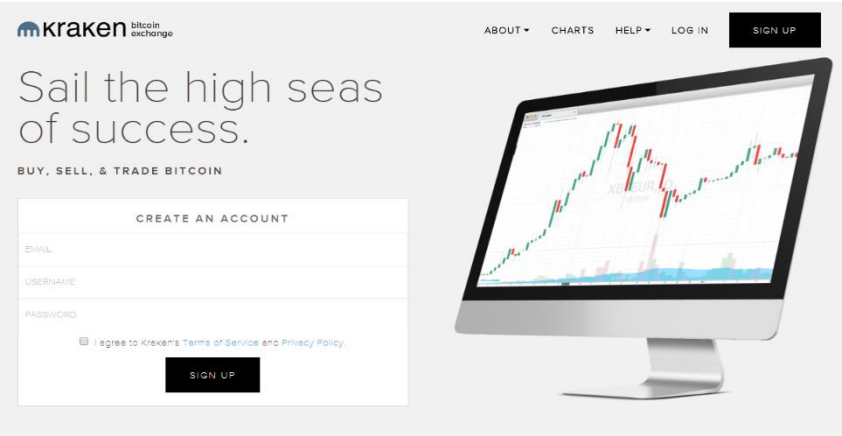
Sigurnost korisničkog računa

- Sve povjerljive informacije o korisničkim računima su kriptirane.
- Dvostruka autentikacija se nalazi pri logiranju za račun, trgovanju i slično
- Postoji i takozvani izolirani sustava za podizanje dokumenata potrebnih za verifikaciju
- *"Global settings lock"* dodatno osigurava korisnika od napadača - prekida petlje

Održavanje zakona

- Zakoni vezani za kriptovalute su još uvijek u nastajanju ali ih Kraken prati i nastoji biti u toku sa svim novitetima, kako bi njegovi korisnici bili što zadovoljniji
- Pridržavaju se svih zakona, predviđaju moguće promjene u zakonu
- Imaju pravne savjetnike, cijeli tim koji je odgovoran za sve promjene koje se događaju u pravnom svijetu

Slika 20- Prikaz stranice Kraken



Izvor: Autor

10. RIPPLE vs MONERO

U svijetu postoje stotine različitih kriptovaluta. Jedna od najpoznatijih je zasigurno Bitcoin. U proteklih nekoliko godina došlo je do pojave kriptovaluta koje se naprednije od Bitcoina, ali imaju i drugačiju arhitekturu i svrhu. Kriptovalute do nedavno nisu imale veliki utjecaj na poslovanje. Dolazi do promjena u svijetu kriptovaluta i one postaju tražene. Mnogi vlasnici firmi zainteresirani su za tehnologiju na kojoj se temelje nove kriptovalute. Dvije valute koje su u posljednje vrijeme postale popularnije nego inače su Monero (XMR) i Ripple (XRP). (Green, 2018.)

Monero i Ripple nedvojbeno predstavljaju dvije krajnosti ideološkog spektra kriptovaluta. Ripple je postao popularan među velikim tradicionalnim financijskim institucijama, dok je Monero zaokupio pažnju razvojnim zajednicama, u koje su upleteni politika i neki nelegalni motivi. Niti jedna valuta nije napravljena i namijenjena kako bi zadovoljila potrebe svih korisnika. Svaka valuta ima svoju svrhu i ciljano tržište. XMR i XRP su stekli zavidnu popularnost u kratko vrijeme, a njihove mogućnosti počeli su koristiti mnogi. (Green, 2018.)

10.1 Monero

Monero se može predstaviti kao kriptovaluta koja omogućuje potpunu privatnost korisnika. Njegova primanja i plaćanja su potpuno anonimna, a transakcije je nemoguće razlikovati. Osim toga, tradicionalno praćenje pasivne mreže neće otkriti aktivnosti trgovanja Monerom, zbog upotrebe I2P tehnologije "nevidljivog usmjeravanja". No Monero je selektivno transparentan, ako korisnik želi, svaka transakcija može biti vidljiva odabranim osobama, poput revizora, i to putem privatnog ključa za dijeljenje. Monero je dizajniran na takav način da velike organizacijene bi mogle dominirati stvaranjem novog novca. Iako je ovo dobro, oko 40 posto rudarskih aktivnosti na mreži Monero, provode tri igrača.

U vrijeme pisanja rada vrijednost Monero kriptovalute iznosi 108,80 Eura. Monero tehnologija se smatra složenom tehnologijom i ne preporuča se početnicima u kriptografskom svijetu. Međutim svaki iskusni korisnik je jednom bio početnik

10.2 Ripple

Ripple je i kriptovaluta (XRP) i mreža za transakcije. Koriste ga financijske institucije poput Santander Banke, Bank of America i švicarske UBS. Koriste ga kao način na koji se mogu održavati velike količine bilo koje valute i lako razmjenjivati i to na pouzdan način, dopuštajući da se novac prenosi preko međunarodnih granica bez ikakvih sankcija. Prava prednost Ripple-a za banke je likvidnost te brzina i niske naknade za transakcije. XRP - om se može brzo trgovati, ne može se rudariti odnosno stvaratelji valute imaju potpunu kontrolu nad 100 milijardi *tokena*.

Ripple nikad nije bio dizajniran kao metoda plaćanja za svakodnevne kupnje, umjesto toga okrenut je prema transakcijskim sustavima. Banke neće nikada koristit Monero za transakcije, kao što ni Ripple nikada neće biti korišten u zlonamjerne svrhe kao što je to slučaj sa Monerom.

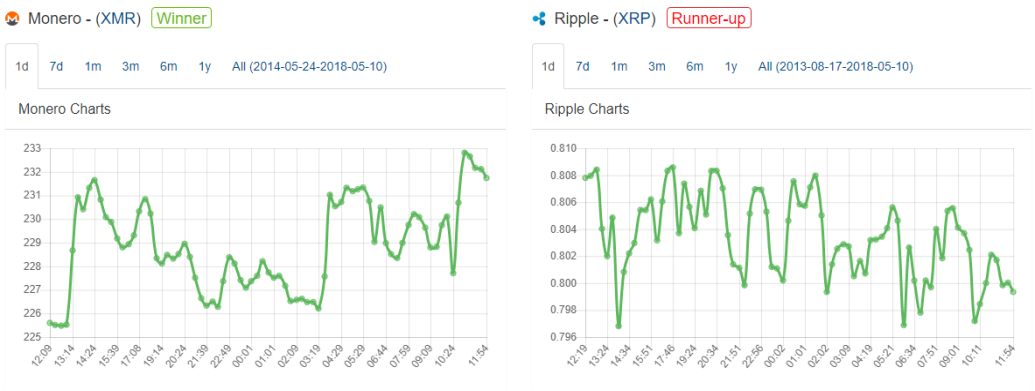
Kriptovalute i blockchain će promijeniti prirodu razmijene, trgovine, intelektualnog vlasništva. Za sada su ove tehnologije na pragu novih promjena. Koja će od njih prevladat odnosi o spletu okolnosti i nasumičnih događaja.

10.3 Grafička prikaz (statistika)

Na grafu ispod ovog teksta grafički je prikaz i usporedba Monero i Ripple kriptovaluta. Prikaz se odnosi na trenutno stanje na tržištu na dan pisanja rada. Potrebno je napomenuti da se stanje i vrijednosti mijenjaju iz minute u minutu. Prikazane su dvije slike, od kojih prva prikazuje stanje i promjene koje su se događale unutar 24 sata, dok druga slika prikazuje promjene koje su nastale unutar jedne godine. Iz prve slike je moguće zaključiti da je Monero unutar zadnjih sat vremena statistički gledano bio u prednosti u odnosu na Ripple odnosno XRP. XRP je ima nešto dublje padove cijene i nagle poraste, što bi se dalo zaključiti da je nešto nestabilniji u zadnjih sat vremena nego je to XMR. Dok na drugoj slici možemo vidjeti promjene nastale unutar zadnjih godinu dana. U ovom slučaju može se reći da pobjedu odnosi Ripple odnosno XRP. XRP je imao dosta naglu i brzu uzlaznu putanju nakon koje je slijedio isto takav i pad, te se u zadnjih nekoliko mjeseci drži oko istih brojki. Monero to jest XMR je

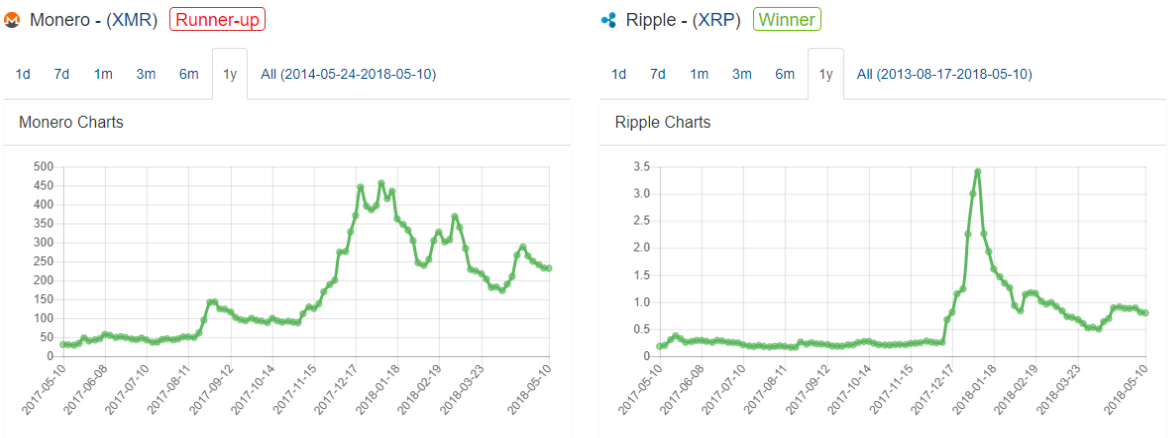
imao nešto sporiju uzlaznu putanju, ali i više uzlazno silaznih kretnji. Stabilnost kriptovaluta općenito je duboka i kontroverzna tema koja zahtjeva dublje i detaljnije istraživanje.

Slika 21- Prikaz grafova XRP i XMR unutar 24 sata



Izvor: Autor

Slika 22- Prikaz grafova XRP i XMR unutar jedne godine



Izvor: Autor

11. POREZI NA KRIPTOVALUTE U HRVATSKOJ

Od 14. srpnja 2017. godine razriješeno je pitanje vezano za porez na dobit od kriptovaluta u Republici Hrvatskoj. Prema mišljenju porezne uprave dohodak ostvaren trgovanjem kriptovalutama mora se oporezivati po osnovi kapitalnih dobitaka.

Profit koji se dobije vezan uz kriptovalute mora se prijaviti. Profitom se smatraju novci koji su primljeni na račun neke banke i to na temelju isplate novca sa neke burze ili trgovine za razmjenu. Porez se odnosi na profit. Ukoliko se radi o gubitku porez se ne računa, i nije potrebno prijavljivati gubitak.

Porezna uprava je definirala da je porezni obveznik dužan prijaviti sve svoje porezne obveze najkasnije do drugog mjeseca u godini, i to za dobitke stečene u prošloj godini. Porez se obračunava po stopi od 12% te se uvećava za prirez općine i grada samog podnositelja prijave poreza. (Rogina, 2018.)

Porez koji se uplati smatra se konačnim rješenjem. Što bi značilo da se porez uplaćen na osnovu dobiti iz kriptovaluta ne zbraja s drugim dohocima kao što su na primjer ugovor o djelu i slično. Bolje rečeno, profit stečen zaradom iz kriptovaluta ne može korisnika prebacit na višu razinu porezne stope. Nakon plaćenih 12% na dobit, građanin RH odradio je svoju građansku dužnost. Ukoliko se radi o zaradi koja je manja od 112 kuna godišnje nije potrebno obračunavati niti plaćati porez. (Rogina, 2018.)

Što je potrebno za prijavu poreza?

- Obrazac JOPPD - izvješće o porezu i prirezu na dobit, pravovaljano ispunjeno
- Izračun poreza - prema first in - first out načelu, potrebno čuvati sve poruke
- Bankovna uplatnica - uplatnica s pravilno unesenim iznosom, brojem računa i pozivom na broj
- Obrazac RPO - ukoliko je novac pristigao sa inozemne mjenjačnice/burze

12. RUDARENJE MONERA

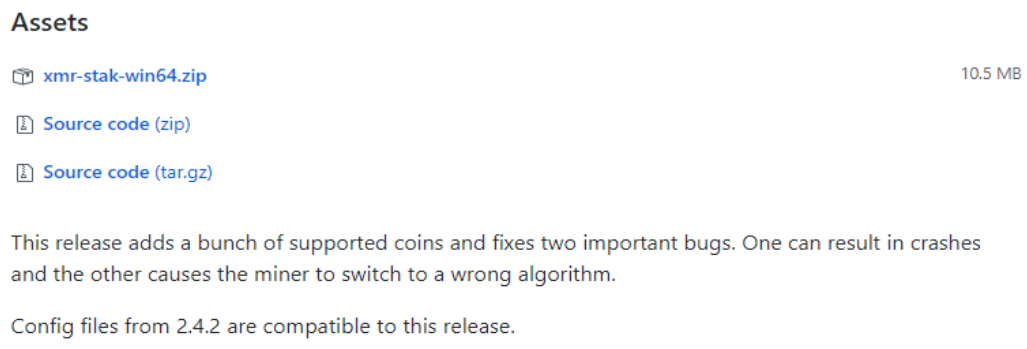
Kao što je već spomenuto u radu Monero je kriptovaluta usmjerena na privatnost te se nalazi u prvih 10 kriptovaluta na tržištu. Rudarenje Monera može biti profitabilan poduhvat iz razloga što Monero ima kriptografski algoritam koji je otporan na SIC rudarenje. To bi značilo da svatko s CPU-om [3]i GPU-om [4]može rudariti Monero. Kroz ovo poglavlje biti će prikazano koje programe je potrebno imati i kako postaviti te programe da bi rudarenje Monera bilo moguće.

12.1 Rudarenje Monera GPU

XMR Stak je nedavno izašao s novim ažuriranjima koja omogućuju korisnicima jednostavno preuzimanje jednog instalatora na *hardware* koji se namjerava koristiti. XMR Stak je jednostavan alat za korištenje te je i iz tog razloga prikazan u ovom radu. Potrebno je napomenuti da neki anti virusi mogu XMR Stak prepoznati kao zlonamjernu datoteku , iako on to nije, pa je potrebno provjeriti od kuda se preuzimaju datoteke.

Najnovija verzija XMR Stak vrlo je jednostavna za postavljanje. Dostupne su verzije za Windows, Linux i MacOS operativne sustave. Datoteku je potrebno preuzeti, raspakirati te pokrenuti izvršnu datoteku (.exe).

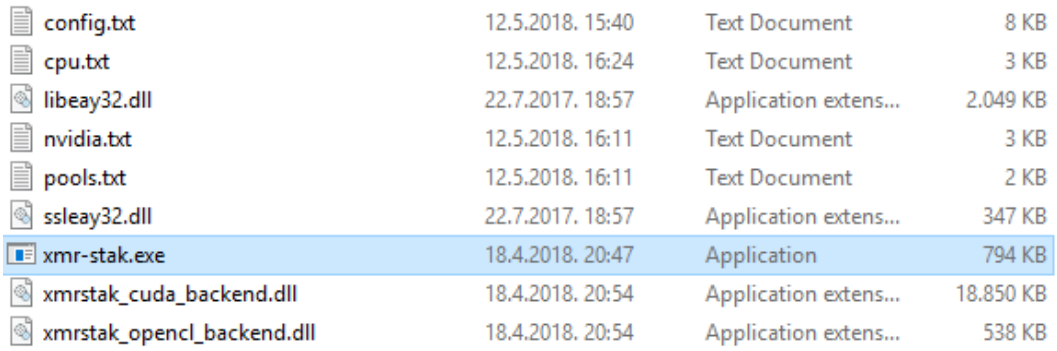
Slika 23- Prikaz XMR Stak paketa kojeg je potrebno preuzeti



Izvor: Autor

[3] Central Processing Unit – glavni čip računala
[4] Graphics processing unit – procesor za prikazivanje računalne grafike

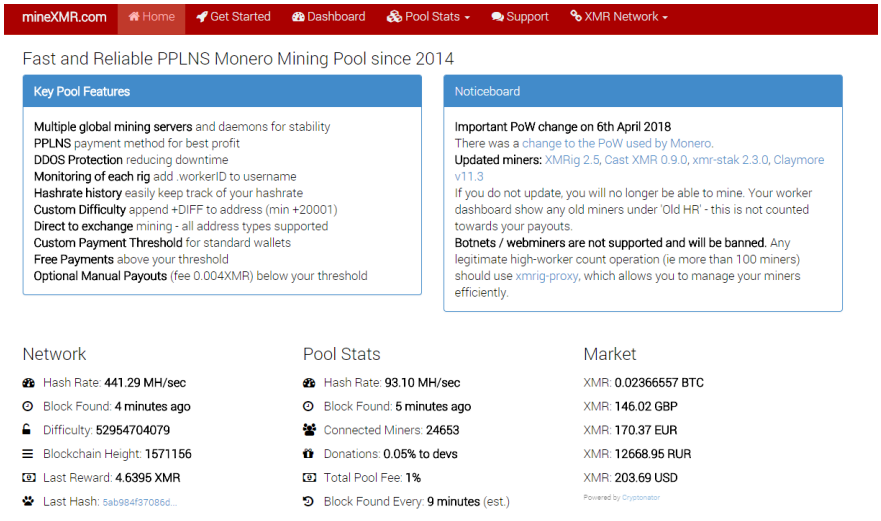
Slika 24- Prikaz izvršne datoteke



Izvor: Autor

Također prije samog rudarenja, kako bi rudarenje bilo moguće, potrebno je izabrati „bazen“ kroz koji će se ono odvijati. Dobar odabir rudarskog bazena može uvelike utjecati na dobit ili gubitak u rudarenju Monera. Svaki rudarski bazen ima neku naknadu koja se odbija automatski prilikom rudarenja. Odabrani poslužitelj zove se MineXMR, ima najnižu naknadu, te je lociran u Njemačkoj (vrlo je bitna blizina servera). Slika ispod prikazuje detalje koji se unose kroz ovaj softver.

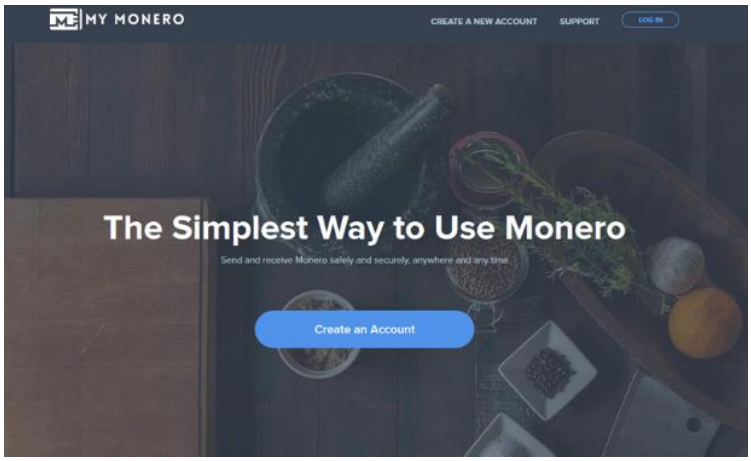
Slika 25- Prikaz detalja MineXMR



Izvor: Autor

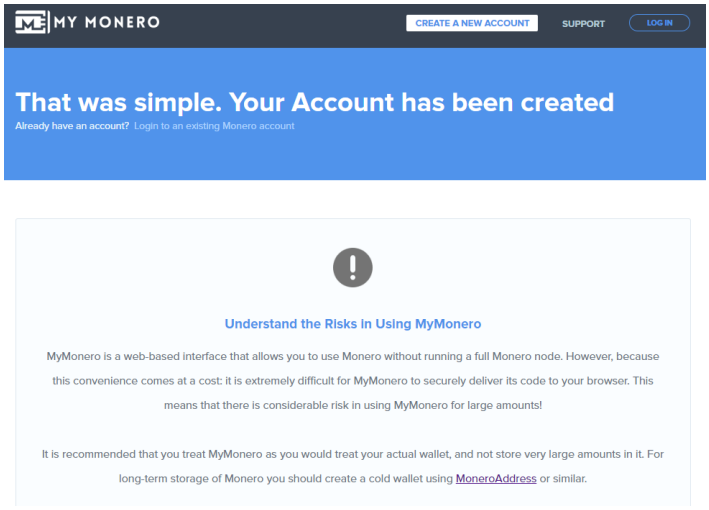
Nadalje, potrebno je imati novčanik koji će biti spojen sa *software* te će se tako sve rudarene jedinice moći spremati na njega. Za ovaj primjer odabran je Monero novčanik MyMonero koji je ranije opisan u radu. Ne zahtjeva registraciju, već je dovoljno kliknuti na dugme koje upućuje na kreiranje novog računa. Nakon toga se dobiva šifra od 13 nasumičnih riječi koja kasnije služi za ulaza u račun. Šifru je potrebno dobro spremiti i čuvati.

Slika 26- Prikaz početne stranice za kreiranje računa za MyMonero novčanik



Izvor: Autor

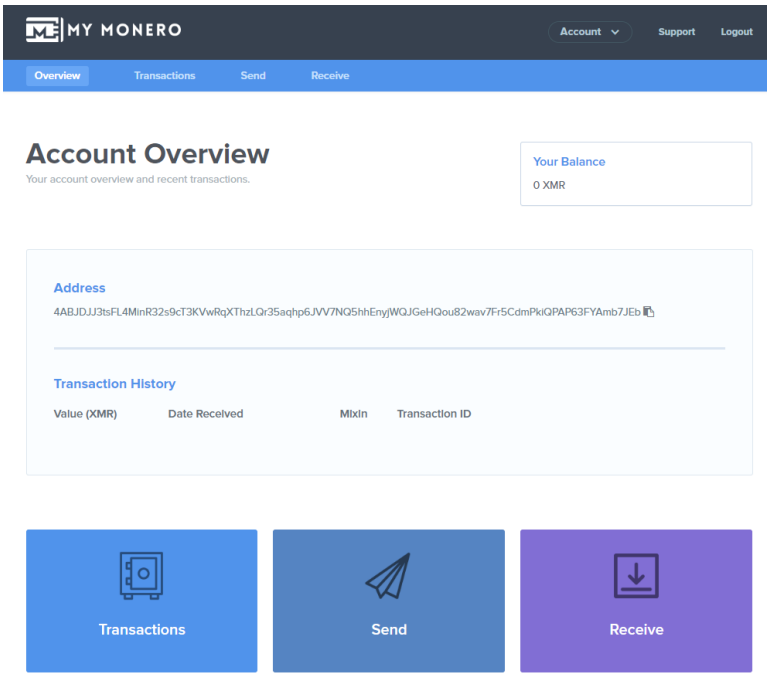
Slika 27- Prikaz izrađenog računa na MyMonero novčaniku



Izvor: Autor

Kada korisnik kreira račun na MyMonero novčaniku, ima sljedeće opcije: može pregledati sve transakcije koje su se dogodile od početka izrade računa pa do kraja, može pregledati sve poslane transakcije koje su se dogodile, može pregledati sve primljene transakcije, vidi trenutno stanje XMR-a na svom računu kao i adresu njegovog računa. Slika ispod prikazuje sve prethodno spomenuto.

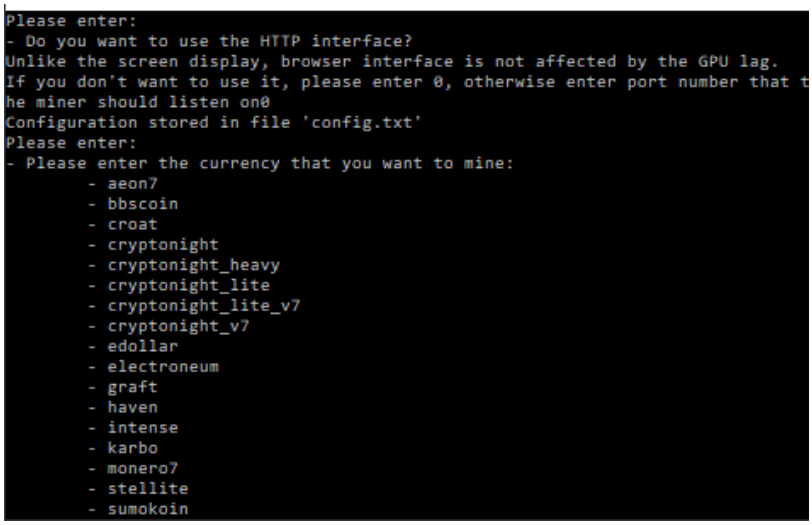
Slika 28- Prikaz MyMoner računa



Izvor: Autor

Nakon svih odrađenih postavki, potrebno je pokrenuti izvršnu datoteku. Datoteka se otvara, dolazi pitanje da li se želi koristiti http korisničko sučelje, odgovor je ne, odnosno nula 0. Nakon toga dobiva se popis koji nudi izbor kriptovaluta koje je moguće izabrati i rudariti preko ovog *softwarea*. Odabire se i upisuje –monero7 te potvrđuje enterom. Slika ispod prikazuje prethodno napisano.

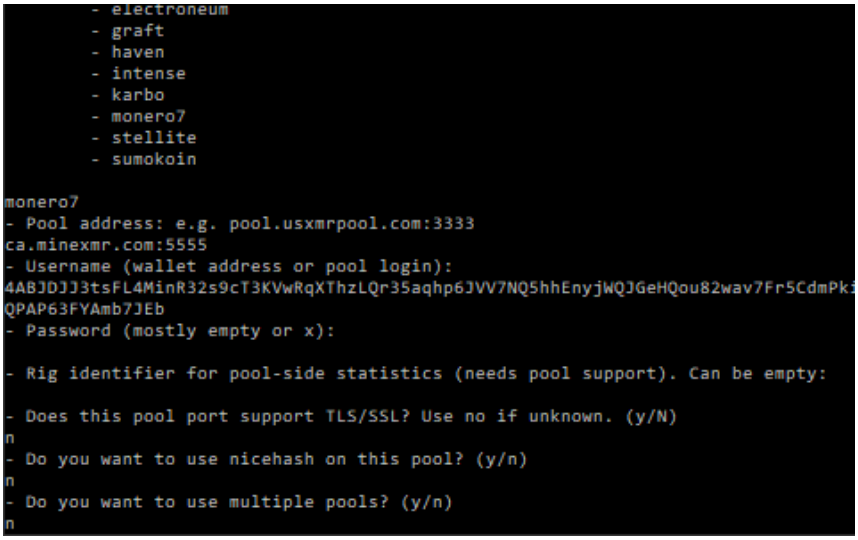
Slika 29- Prikaz rudarenja Monera 1



Izvor: Autor

Nakon odabira valute koja se rudari, potrebno je upisati adresu novčanika koja je prethodno kreirana izradom samog novčanika.. Odgovara se na pitanja kao što su: da li se želi koristiti neko mjesto trgovanja, da li se želi koristiti više bazena te su odgovori u ovom slučaju na sva pitanja negativni.. Sada će se aplikacija pokrenuti na temelju instaliranih GPU-ova.

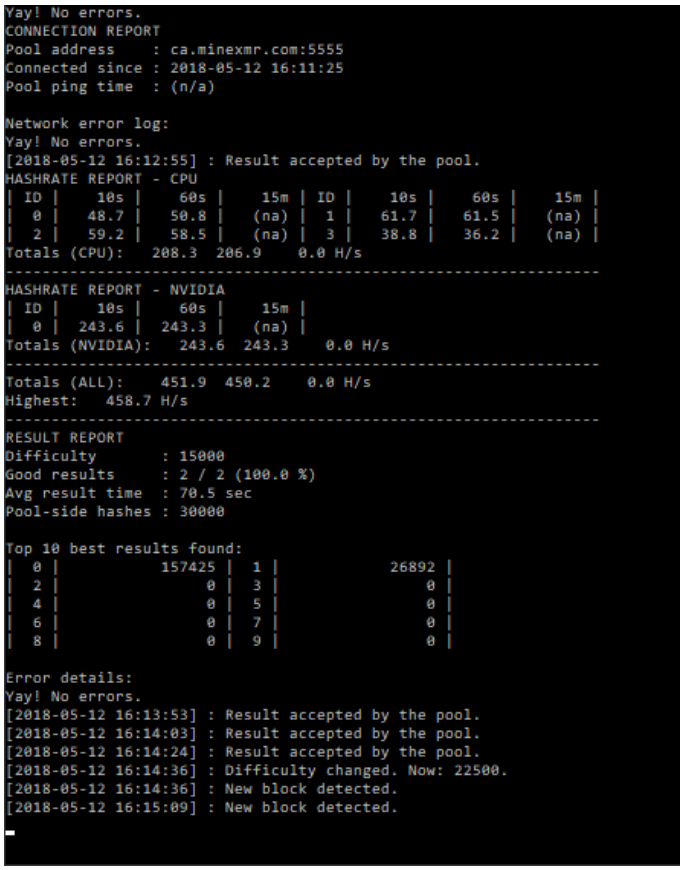
Slika 30- Pikaz rudarenja Monera 2



Izvor: Autor

Za dodatne informacije moguće je koristiti kratice kao što su „h“ za *hashrate*, „r“ za rezultate *hashova* ili „c“ za provjeru veze s bazenom. Podaci ispisane nekom od kratica uvelike mogu pomoći u daljnjim analizama ili poboljšanjima rada. Potrebno je napomenuti da iako ne zahtjeva jako snažna računala kao što je to slučaj kod nekih drugih kriptovaluta, rudarenje Monera može uvelike usporiti računalo.

Slika 31- Prikazuje rudarenje Monera 3



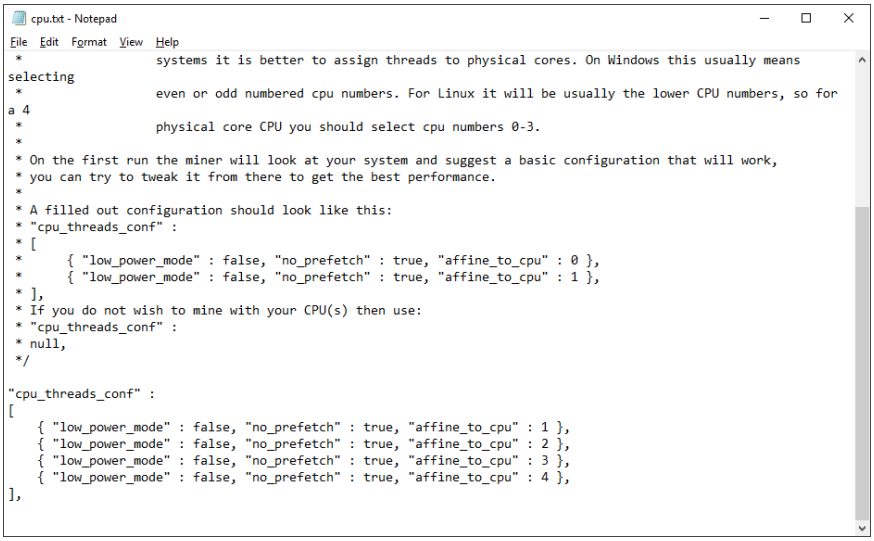
Izvor: Autor

12.2 Rudarenje Monera CPU

Ukoliko se želi rudariti Monero s CPU-om potrebno je postaviti konfiguracijsku datoteku prije nego se započne sa radom. Potrebno je otvoriti tekstualnu datoteku i u njoj promijeniti postavke. Određuje se rad jezgri na računalu koje će biti korištene za rudarenje. Ukoliko je računalo sa 4 jezgre kao u ovom slučaju, moguće je iskoristiti sve četiri jezgre za rada ili ostaviti jednu slobodnu, ako korisnik koristi to računalo i za ostale potrebe. Nakon

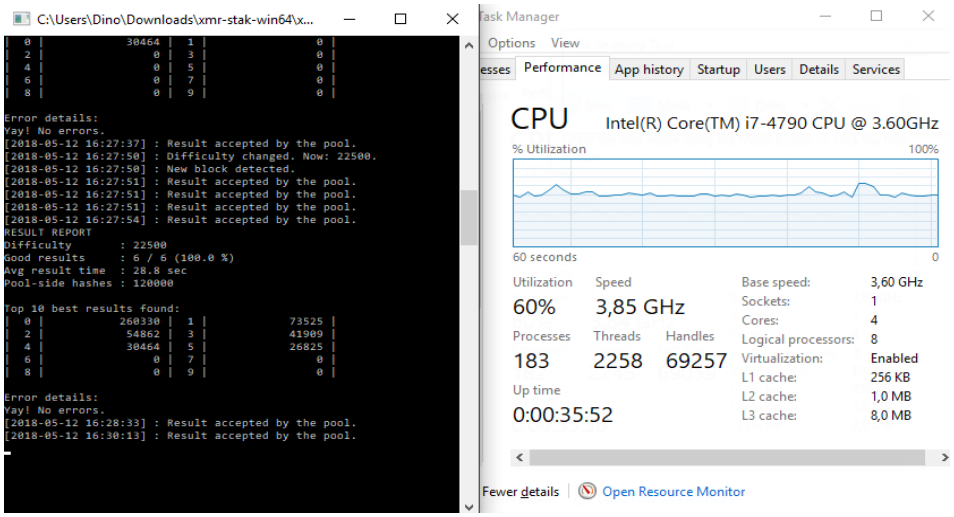
postavljenih novih promjena potrebno je ponovo pokrenuti aplikaciju te zamijetiti povećanje *hashrata* jer je u isto vrijeme korišten GPU I CPU za rudarenja.

Slika 32- Prikazuje tekstualnu datoteku s postavkama za CPU rudarenje



Izvor: Autor

Slika 33- Prikazuje rudarenje s CPU-om



Izvor: Autor

Također se ova promjena ubrzanja rada može vidjeti i kroz upravitelj zadataka koji očitava rad CPU-a. Rudarenje GPU-om I CPU-om postavljeno je te se dodatne promjene mogu doraditi unutar tekstualne datoteke ili promjenom računala, nadogradnjom i slično.

13. ZAKLJUČAK

Kriptovalute su nova tema koja je postala popularna u zadnjih 3 do 5 godina. Kriptovalute i njihova primjena su budućnost razmjene, transakcije, trgovine, povećanja sigurnosti i privatnosti. Na samom početku postojalo je tek nekoliko kriptovaluta, prva kriptovaluta na tržištu bila je Bitcoin. U vrijeme pisanja rada broj kriptovaluta na tržištu iznosio je 1600. Iako postoji niz kriptovaluta koje imaju različitu svrhu, samo neke od njih su se uspjele probiti na sam vrh, pa su tako neke od njih Bitcoin, Ethereum, XRP i Monero. U radu su opisane dvije kriptovalute koje spadaju u taj vrh XRP i Monero. Svaka valuta sa sobom nosi prednosti koje pruža, kao na primjer povećanu sigurnost, brže transakcije, fleksibilnost, dok s druge strane dolazi i do mogućih rizika vezanih uz njihovu povjerljivost i pouzdanost. XRP i XMR dvije su kriptovalute koje imaju različitu svrhu i različitu mogućnost upotrebe. Pa tako XRP (Ripple) služi za ubrzavanje razmjene vrijednosti, dok je Monero usmjeren na sigurnost i zaštitu. Statistički podaci pokazuju nagli porast vrijednosti ovih valuta u zadnjih godinu dana. Vrijednost XRP valute porasla je za 89% u odnosu na prošlu godinu, dok je vrijednost XMR valute porasla za 21%. Promjene na tržištu kriptovaluta se događaju u izuzetno kratkom vremenskom razmaku te ovise o vijestima i događajima u svijetu, što ovo trgovanje čini nestabilnim. Smatra se da je ovo tek početak kriptovaluta i onoga što dolazi s njima. Koja će od njih zavladati ovisi o nizu događaja, politici, nestabilnosti tržišta u svijetu, ali i o burzama. Iako su nastale prije nekoliko godina, kriptovalute su u kratkom periodu zaintrigirale veliki broj korisnika, smatra se da će se ta praksa nastaviti i u budućnosti te da će njihova upotreba u rasponu od 2 do 3 godine postati globalna, a njihova vrijednost se povećati za 50 do 70 posto.

POPIS I OBJAŠNJENJE KORIŠTENIH KRATICA I INFORMATIČKIH POJMOVA

CPU - Central Processing Unit – glavni čip računala

GPU - Graphics processing unit – procesor za prikazivanje računalne grafike

HARDWARE – Fizički opipljiv dio računala

IP - Internet Protocol, jedinstvena brojčana oznaka računala

LEDGER - Glavna knjiga, vrsta novčanika za pohranu jedinica

USB- Universal Serial Bus, tehničko rješenje za komunikaciju računala s vanjskim uređajima

SOFTWARE – Računalni program napisan tako da je njegov sadržaj jednostavno prilagoditi

XMR - Jedna od vodećih kriptovaluta na tržištu

XRP - Jedna od vodećih kriptovaluta na tržištu

POPIS LITERATURE

1. Buntinx, J., The Best Monero Wallets of 2018, 2018., https://themerkle.com/the-best-monero-wallets-of-2018 (26.4.2018.)
2. Cohen, D., Schwartz, D., Britto, A., The XRP Ledger Consensus Process, 2017., https://ripple.com/build/xrp-ledger-consensus-process/ (18.4.2018.)
3. Green, J., Ripple & Monero: Two cryptocurrencies to watch, 2018., http://techwireasia.com/2018/01/ripple-monero-two-cryptocurrencies-watch/ (05.5.2018.)
4. Khatwani, S., 7 Best Cryptocurrency Exchanges In The World To Buy Any Altcoins, 2018, https://coinsutra.com/best-cryptocurrency-exchanges/ (26.4.2018.)
5. Lutpin, The basics of Monero [XMR], 2017., https://www.crypto-news.net/the-basics-of-monero-xmr (23.4.2018.)
6. Mangal, A., What is Monero? An In – Depth Guide, 2017., https://coincentral.com/what-is-monero/ (23.4.2018.)
7. Nel , L., Best Ripple Wallets 2018: Hardware vs Mobile vs Software vs Paper, 2018., https://blockonomi.com/best-ripple-wallets/ (20.4.2018.)
8. Rogina, N., Porezi na kriptovalute u Hrvatskoj, 2018., https://www.kriptovaluta.hr/vijesti/porez-na-kriptovalute-hrvatska (30.4.2018.)

KNJIGE

1. Narayanan A., et al., Bitcoin and cryptocurrency technologies, Princeton and Oxford, New Yersey, 2017.

POPIS SLIKA

Slika 1 - Prikaz ralike između BTC, ETH i XRP 7
Slika 2 – Prikaz sudionika u XRP Ladger protokolu 8
Slika 3- Prikazuje validatore koji predlažu transakcijski skup 9
Slika 4– Prikaz kako se čvorovi slažu u skupu transakcija 10
Slika 5- Prikazuje mrežni čvor koji izračunava valjanost Ledgera 11
Slika 6- Prikaz provjere Ledger-a (kada glavni izračuna isti rezultat) 11
Slika 7- Prikaz kada mreže prepoznaje novi validirani Ledger 12
Slika 8- Prikaz Adrese novčanika 15
Slika 9- Prikaz "Minialist Ripple Client" 18
Slika 10- Prikazuje grafove vrijednosti valute 20
Slika 11- Prikaz grafa Monero kriptovalute 21
Slika 12- Prikaz normalne transakcije 23
Slika 13- Prikaz "Ring Signature" transakcija 23
Slika 14- Prikaz kreiranja računa na MyMonero 26
Slika 15- Prikaz stranice za preuzimanje potrebne vrste Monero GUI novčanika 27
Slika 16- Prikaz Monerujo stranice za preuzianje aplikacije 28
Slika 17- Prikaz stranice Binance trgovine 32
Slika 18- Prikazuje popuste BNB 33
Slika 19- Prikazuje službenu stranicu Changelly 34
Slika 20- Prikaz stranice Kraken 36
Slika 21- Prikaz grafova XRP i XMR unutar 24 sata 39
Slika 22- Prikaz grafova XRP i XMR unutar jedne godine 39
Slika 23- Prikaz XMR Stak paketa kojeg je potrebno preuzeti 41
Slika 24- Prikaz izvršne datoteke 42
Slika 25- Prikaz detalja MineXMR 42
Slika 26- Prikaz početne stranice za kreiranje računa za MyMonero novčanik 43
Slika 27- Prikaz izrađenog računa na MyMonero novčaniku 43
Slika 28- Prikaz MyMoner računa 44
Slika 29- Prikaz rudarenja Monera 1 45
Slika 30- Pikaz rudarenja Monera 2 45
Slika 31- Prikazuje rudarenje Monera 3 46

Slika 32- Prikazuje tekstualnu datoteku s postavkama za CPU rudarenje 47
Slika 33- Prikazuje rudarenje s CPU-om.....47