Analiza metoda pohrane kriptovaluta

Ladešić, Filip

SVEUČILIŠTE VERN'

Zagreb

Specijalistički diplomski stručni studij

IT menadžment

SPECIJALISTIČKI DIPLOMSKI STRUČNI RAD

ANALIZA METODA POHRANE KRIPTOVALUTA

Filip Ladešić

Zagreb, 2022.

SVEUČILIŠTE VERN'

Specijalistički diplomski stručni studij

IT menadžment

SPECIJALISTIČKI DIPLOMSKI STRUČNI RAD

ANALIZA METODA POHRANE KRIPTOVALUTA

Mentor: mr. sc. Kristian Saletović, v. pred.

Student: Filip Ladešić

Zagreb, listopad 2022.

SADRŽAJ

SAŽETAK

Napretkom financijskog sustava kreirane su digitalne valute pod nazivom kriptovalute. *Blockchain* tehnologija uz pomoć kriptografije svojim vlasnicima pruža visoku razinu sigurnosti, anonimnosti i mogućnosti zaobilaženja financijskih posrednika. Ubrzani porast zainteresiranih za ulaganje u kriptovalute nameće sa sobom pitanje sigurnosti metoda pomoću kojih se pohranjuju.

Ovaj diplomski rad obrađuje temu metoda pohrane kriptovaluta. U teorijskom dijelu razrađena je tema kriptovaluta, različitih vrsta i metoda stjecanja. U nastavku je utvrđeno da su kao metoda pohrane kreirani kripto novčanici koji se dijele na: web, mobilne, desktop, hardverske i papirnate novčanike. S ciljem utvrđivanja nedostataka kripto novčanika istraženi su aktualni hakerski napadi. U istraživačkom dijelu provedena je anketa nad korisnicima kriptovaluta s ciljem utvrđivanja najsigurnije metode pohrane kriptovaluta. Izvršena je analiza dobivenih odgovora s ciljem donošenja zaključaka i preporuka za poboljšanje postojećih metoda pohrane. Na temelju ostvarenih rezultata zaključeno je da se web novčanici smatraju najsigurnijima.

Ključne riječi: kriptovalute, blockchain, metode pohrane, kripto novčanik

ABSTRACT

Analysis of cryptocurrency storage methods

With the progress of the financial system, digital currencies called cryptocurrencies were created. Blockchain technology alongside cryptography provides its owners with a high level of security, anonymity and the ability to bypass financial intermediaries. The rapid increase in people interested in investing in cryptocurrencies brings with it the question of the security of the methods by which they are stored.

This thesis deals with the topic of cryptocurrency storage methods. In the theoretical part the topic of cryptocurrencies, different types and methods of acquisition is elaborated. In the following, it was determined that crypto wallets were created as a storage method and are divided into: web, mobile, desktop, hardware and paper wallets. In order to determine the shortcomings of crypto wallets, current hacker attacks were investigated. In the research part, a survey on cryptocurrency users was conducted with the aim of determining the safest method of storing cryptocurrencies. An analysis of the received responses was carried out with the aim of drawing conclusions and recommendations for improving existing storage methods. Based on the results, it was concluded that web wallets are considered the most secure.

Keywords: cryptocurrencies, blockchain, storage methods, crypto wallet

1. UVOD

Kriptovalute su tijekom 2021. godine doživjele novi rast vrijednosti na tržištu kapitala. Ova virtualna financijska sredstva doživljavaju sve veću popularnost zadnjih nekoliko godina. Razlozi tome su mnogi, ali univerzalno je što je ovakva valuta u pravilu neovisna, decentralizirana i ne ovisi o regulaciji financijskih institucija neke države. Također, volatilnost vrijednosti kriptovaluta dovodi do toga da zainteresirani ulaze u tržište kriptovaluta s ciljem brze, ali i dugoročne zarade. Prva povijesna kriptovaluta je bitcoin. Poslije bitcoina su se pojavile i druge: litecoin, dogecoin, ripple i ethereum itd.

Budući da se govori o financijskim sredstvima koja imaju karakteristike slične novčanim sredstvima, jako je važna sigurnost metode koja se koristi za pohranu kriptovaluta. Prije nego što se izvrši prijenos klasične valute s bankovnog računa, nužno je razmisliti o svim potezima kako bismo bili što sigurniji na Internetu. Svaki potez ostavlja trag pa su lako moguće krađe osobnih podataka uz krađu financijskih sredstava koja se drže na nekoj od metoda za pohranu kriptovaluta.

Sve to dovodi do pitanja koliko su korisnici kriptovaluta u Hrvatskoj upoznati s metodama pohrane. Kada se promatraju metode pohrane virtualnih financijskih sredstava odnosno oblike kripto novčanika možemo uzeti u obzir: mobilne novčanike, desktop novčanike, web novčanike te papirnate novčanike koji su fizički pohranjeni u obliku privatnih ključeva ispisanih na komadu papira. Naposljetku tu je i digitalni hardverski novčanik koji predstavlja prijenosni fizički novčanik.

Ovaj rad će istražiti koliko je ispitani uzorak korisnika kriptovaluta u Hrvatskoj upoznat s različitim metodama pohrane virtualnih financijskih sredstava te za koju od njih smatraju da je bolja i sigurnija za njih i zašto.

1.1. Problem istraživanja

Ovaj diplomski rad istražit će problematiku sigurne pohrane kriptovaluta. Brzi rast vrijednosti kriptovalute bitcoin koji je započeo u studenom 2017., a najveću vrijednost od 20.000 dolara dosegnuo u prosincu iste godine, privukao je mnogo potencijalnih korisnika. Neki od njih su oni koji su odlučili zaraditi trgovanjem na kratki rok, ali i oni koji su razmišljali o vrijednosti kriptovaluta na dulji rok u budućnosti. Sama popularnost i činjenica da sve više populacije prepoznaje i prihvaća kriptovalute kao sredstvo plaćanja sa sobom veže i problem sigurnosti pohrane tih sredstava.

Potencijalni rizici gubitka ovih virtualnih financijskih sredstava, krađe osobnih podataka, ali i dodatne štete koje mogu uslijediti prilikom neautoriziranog pristupa mogu biti velike i značajne za sve vlasnike kriptovaluta. Osobna računala i burze odnosno, mjenjačnice koje koriste vlasnici kriptovaluta su potencijalne mete hakerskih napada.

Ovdje se dolazi do glavnog cilja rada, a to je pronaći koja metoda pohrane kriptovaluta je najbolja i najsigurnija prema ispitanom uzorku korisnika kriptovaluta u Hrvatskoj. Metoda pohrane kriptovaluta ima mnogo. Njihova kvaliteta varira ovisno o samoj usluzi, neke su sigurnije, a neke manje sigurne. Određene metode zahtijevaju instalaciju aplikacija i mnoge sigurnosne mjere poput autorizacijskih kôdova, provjere osobnih podataka itd. Metode pohrane kriptovaluta sadrže sličnosti metodama pohrane novčanih sredstava - ovise o trećoj strani koja je odgovorna za pohranu sredstava ili pak o samim vlasnicima u slučaju fizičkog oblika pohrane.

1.2. Predmet istraživanja

U ovom radu provest će se istraživanje kojim se planira utvrditi najsigurnija odnosno najbolja metoda pohrane kriptovaluta za ispitani uzorak korisnika kriptovaluta u Hrvatskoj. Kako bi se utvrdilo koja od dostupnih metoda pohrane kriptovaluta je najbolja nužno je definirati razlike među metodama. Analizirat će se razlozi zbog kojih se korisnici kriptovaluta u Hrvatskoj odlučuju upravo za odabrane metode. Uz same metode pohrane istražit će se koje dobne skupine u istraživanom uzorku korisnika kriptovaluta u Hrvatskoj daju veću pozornosti kvaliteti usluge različitih metoda pohrane kriptovaluta.

U teorijskom dijelu će se obraditi tema kriptovaluta i pobliže predstaviti svaka od

raspoloživih metoda koje služe za pohranu kriptovaluta. Istraživački dio rada će povezati te dvije teme kroz provjeru stanja upotrebe metoda pohrane kriptovaluta na ispitanom uzorku korisnika kriptovaluta u Hrvatskoj.

1.3. Ciljevi istraživanja

Osnovni cilj ovog diplomskog rada je istražiti koja metoda pohrane kriptovaluta je najbolja za ispitani uzorak korisnika. U fokusu istraživanja su vlasnici kriptovaluta i njihova percepcija sigurnosti virtualnih financijskih sredstava. Istražit će se što ispitani uzorak korisnika kriptovaluta misli o dostupnim metodama pohrane, cijenama, kvaliteti usluge, dugotrajnosti korištene metode, rizicima te samoj razini sigurnosti.

Prvi cilj:

Utvrditi koja je od dostupnih metoda pohrane kriptovaluta najsigurnija za ispitani uzorak korisnika kriptovaluta u Hrvatskoj.

Drugi cilj:

Definirati ključne razlike među dostupnim metodama pohrane kriptovaluta. Definiranjem razlika ustanovit će se zašto ispitani uzorak korisnika kriptovaluta u Hrvatskoj koristi specifičnu metodu pohrane kriptovaluta.

Treći cilj:

Utvrditi koje dobne skupine među korisnicima kriptovaluta u Hrvatskoj daju veću pozornosti sigurnosti i pouzdanosti dostupnih metoda pohrane kriptovaluta. Nužno je razmotriti postoji li korelacija između dobnih skupina i sigurnosti kriptovaluta. Istražit će se pretpostavka da mlađa populacija pridaje manju pozornost kvaliteti usluge odnosno manje im je bitna pouzdanost određenih metoda pohrane kriptovaluta.

1.4. Istraživačka pitanja

IP1:

Kada govorimo o sigurnosti pohrane kriptovaluta odnosno virtualnih financijskih sredstava, koja se od dostupnih metoda za ispitani uzorak korisnika kriptovaluta u Hrvatskoj smatra sigurnijom te boljom od ostalih?

Odgovor na istraživačko pitanje će se dobiti provedbom ankete odnosno metodom komparacije dobivenih odgovora i primjenom statističke metode za analizu podataka.

Svrha ovog istraživačkog pitanja je utvrditi koja se metoda pohrane kriptovaluta smatra najsigurnijom za ispitani uzorak korisnika u Hrvatskoj.

IP2:

Zbog kojih razloga se korisnici kriptovaluta u Hrvatskoj odlučuju za određene metode pohrane kriptovaluta?

Odgovor na istraživačko pitanje će se dobiti metodom komparacije odgovara dobivenih putem ankete. Svrha ovog istraživačkog pitanja je utvrditi razloge odabira specifične metode pohrane kriptovaluta.

IP3:

Koje dobne skupine među korisnicima kriptovaluta u Hrvatskoj daju veću pozornost sigurnosti između različitih metoda pohrane kriptovaluta?

Odgovor na istraživačko pitanje će se dobiti putem ankete. Svrha ovog istraživačkog pitanja je utvrditi postoji li poveznica između metoda pohrane kriptovaluta i dobnih skupina njihovih korisnika u Hrvatskoj.

1.5. Metode istraživanja

Za potrebe izrade diplomskog rada provedeno je primarno i sekundarno istraživanje. Primarno istraživanje se temelji na istraživanju tržišta odnosno ispitivanju određenog uzorka populacije Hrvatske. Sekundarno istraživanje se postiže prikupljanjem i analizom znanstvene literature te drugih javno dostupnih stručnih izvora.

Metoda prikupljanja sekundarnih podataka

Za teorijski dio rada korištena je znanstvena literatura iz područja kriptovaluta i sigurnosti informacijskih sustava uz znanstvene i stručne članke koji se mogu pronaći u internetskim bazama podataka.

Metoda ankete

Za potrebe istraživanja kreiran je *online* anketni upitnik. Kako bi se dobili različiti odgovori i osigurao najbolji mogući zaključak, određeno je da se anketira najmanje 100 ispitanika. Obzirom da je raspon dobnih skupina ispitanog uzorka korisnika kriptovaluta putem *online* upitnika bio samo od 20-30 i 30-40 godina, anketni upitnik se dodatno proveo i fizičkim putem u Zagrebu s ciljem pronalaska starijih dobnih skupina 40-50 i 50+ godina. Upitnik istražuje koje metode pohrane kriptovaluta su

prihvatljivije, kvalitetnije, kakav im je odnos cijena/korist te koliko su sigurnije odnosno bolje za anketirani uzorak Hrvatske. Upitnik se sastoji od pitanja zatvorenog i otvorenog tipa. Pitanja se odnose na općenito znanje o kriptovalutama, njihovom načinu zarade, o metodama pohrane, što ispitanici znaju o određenim metodama, zašto su se za njih odlučili te koje primjedbe i želje za promjenama imaju u odnosu na odabrane metode. Podaci su prikupljeni putem *online* anketnog upitnika krajem 2021. godine i u prvoj polovici 2022.

Metoda deskripcije

Metodom deskripcije se opisalo sve trenutno raspoložive metode pohrane kriptovaluta.

Metoda komparacije

Metodom komparacije su se usporedile specifične metode pohrane kriptovaluta, konkretnije usporedile su se sličnosti i razlike između metoda. Naknadno se napravila usporedba mišljenja ispitanika za svaku metodu.

Statistička metoda

Statistička metoda se koristila za prikupljanje, analiziranje i obradu numeričkih podataka koji su se grafički prikazali i opisali. Za prikazivanje raspona zadovoljstva određenom metodom pohrane kriptovaluta, korištena je Likertova skala.

1.6. Struktura rada

Ovaj diplomski rad sastoji se od ukupno šest poglavlja u kojima je obrađena literatura te je predstavljeno provedeno empirijsko istraživanje. U uvodnom poglavlju opisana je tema ovoga rada, navedeno je područje i cilj diplomskog rada, metode i izvori prikupljanja podataka te struktura rada.

U drugom poglavlju fokus je stavljen na predstavljanje osnova kriptovaluta. Navedena je podjela kriptoimovine sa svojim definicijama, predstavljene su kriptovalute i javna knjiga. U nastavku će se navesti vrste kriptovaluta i na kraju su navedene metode stjecanja kako bi se dobio bolji uvid u tematiku.

U trećem djelu dan je detaljniji prikaz tame teme rada, odnosno metode pohrane kriptovaluta. Obrađeni su osnovni pojmovi novčanika, privatnog i javnog ključa te kriptografije. Analizirana je prikupljena literatura vezana uz kripto novčanike.

Predstavljene su vrste kripto novčanika uz brojne primjere.

U četvrtom poglavlju spomenuti su neki hakerskih napada na metode pohrane kriptovaluta. Cilj poglavlja je predstaviti nedostatke kripto novčanika odnosno načine na koje se propusti iskorištavaju te koje su posljedice nastale štete.

Peto poglavlje odnosi se na provedeno istraživanje s ciljem utvrđivanja koja je metoda pohrane kriptovaluta najbolja za istraživani uzorak. Uz same metode istraženo je i koje od metoda ispitanoj populaciji predstavljaju sigurnije i bolje rješenje za očuvanje svojih virtualnih financijskih sredstava. Predstavljena je metodologija istraživanja i prezentirani su prikupljeni podaci i rezultati. U nastavku su putem dubinske analize podataka doneseni zaključci na temu ovoga istraživanja.

U šestom poglavlju su izneseni prijedlozi poboljšanja postojećih metoda pohrane kriptovaluta na temelju prikupljenih podataka.

U posljednjem poglavlju navedena su zaključna razmatranja vezana za tematiku metoda pohrane kriptovaluta te su formulirani odgovori na istraživačka pitanja.

2. KRIPTOVALUTE

Početak 2009. godine je zabilježen kao početak transformacije financijskog sustava.[1] Ubrzani razvoj informacijske tehnologije doveo je do nastanka nove digitalne valute pod nazivom kriptovalute. Iako digitalni novac postoji već duže vrijeme kriptovalute su uvele nove modernije tehnologije poput javne knjige (eng. *blockchain)*. Najpoznatija kriptovaluta je Bitcoin.

U nastavku rada će biti opisana podjela kriptoimovine, spomenuti će se osnove kriptovaluta, javne knjige i načina njegova rada. U nastavku će se navesti vrste kriptovaluta i na kraju su navedene metode stjecanja kako bi se dobio bolji uvid u tematiku.

2.1. Općenito

Potrebno je promatrati širi aspekt s ciljem razumijevanja kriptovaluta. Aspekt se može predstaviti kao **kripto imovina** (eng. *crypto assets*) koja uključuje računalne programe za digitalni prikaz određene vrijednosti. Kripto imovina spada u nematerijalnu imovinu koja se pojavljuje samo u digitalnom obliku. Prijenos, izdavanje sredstava, prodaja odnosno transakcije i sami pristup su osigurani kriptografskom tehnologijom. Kripto imovina primjenjuje raznolike tehnološke komponente (glavna knjiga, specifične kriptografske tehnologije, protokol Peer-to-peer itd.).

U prvu kategoriju kripto imovine spadaju **digitalne valute središnje banke (**eng. *central bank digital currency*, CBDC). CBDC predstavlja digitalni oblik valute neke države. Digitalne valute su centralizirane odnosno njima upravlja monetarna vlast. Centralne banke država odobravaju digitalne valute. Većina rezervi koje banke drže su u digitalnom obliku. Druga podvrsta kripto imovine su tzv. ***Stablecoini.*** Vrijednosti *stablecoina* se veže uz vrijednost prave valute tzv. fiat neke države. Povezanost s nekom valutom npr. američkim dolarom smanjuje financijski rizik valute odnosno stablecoini nisu izloženi volatilnosti tržišta. Primjeri stablecoina su: Tether (USDT), USD Coin (USDC) itd. ***Kriptovalute*** spadaju pod treću značajnu kripto imovinu koja se temelji na kriptografiji s ciljem osiguranja sigurnosti transakcija i

[1] Time.com Bitcoin Price History: 2009 to 2022 Preuzeto s: https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-price-history/ (27.9.2022.)

pohrane kriptovaluta. Prva kriptovaluta, Bitcoin se svijetu predstavio 2008. godine. Godine nakon toga predstavljaju rast popularnosti i broja drugih kriptovaluta tzv. altcoina. Primjeri su Ethereum, Litecoin, Bitcoin Cash itd. Zadnja potkategorija su ***Kripto tokeni***. Kripto tokeni spadaju u digitalnu imovinu koja je izrađena na tuđoj glavnoj knjizi. Smatraju se oblikom financiranja projekta. Izdaju ih tvrtke ili manje zajednice. Široku popularnost su 2021. godine dosegli tzv. nezamjenjivi token (NTF).

Pojavom Bitcoina 2008. godine započela je transformacija financijskog sustava. **Kriptovalute** (eng. *cryptocurrency*) su digitalne valute bazirane na kriptografskoj tehnologiji. Mogu se prezentirati kao digitalni zapisi koji su pohranjeni u digitalnim bazama. Nisu izdane niti kontrolirane od strane bankarskih ustanova ili državnih institucija. Postoje samo u digitalnom obliku. Budući da su digitalne, vlasnicima pružaju brži proces prodaje i kupnje odnosno prijenos imovine. Tijekom zadnjih nekoliko godina sve češće se prihvaćaju kao sredstvo plaćanja. Pohranjuju se u digitalnim kripto novčanicima (eng. *crypto wallets)*. Funkcionalnost kriptovaluta se bazira na glavnoj knjizi tzv. *blockchainu*.

Prednosti kriptovaluta naspram tradicionalnih metoda plaćanja su:

- otporne su na inflaciju zbog ograničenih količina i pravila koja ograničavaju godišnju razinu izdanih kriptovaluta,
- nemogućnost manipulacije količinom izdanih kriptovaluta,
- složenost sigurnosnog sistema pruža visoku razinu zaštite od hakiranja,
- održavanje tj. vođenje novčanika se ne naplaćuje,
- transakcije se potvrđuju i trajno zapisuju u javnu knjigu koja je neizmjenjiva,
- javna knjiga dostupna je svima na uvid,
- transakcije se provode efikasnije bez nadzora vanjskih entiteta tj. posrednika,
- praktički su decentralizirani odnosno nisu pod kontrolom države i financijskih institucija,
- anonimnost, privatnost i sigurnost u smislu da kod procesa prijenosa sredstava nije potrebno dijeliti osobne informacije kao što su ime, prezime, adresa i slično.

Bez *blockchain* tehnologije ne bi postojala niti jedna kriptovaluta. Sve kriptovalute koriste vlastiti *blockchain* ili tuđi. Može se prevesti kao lanac blokova koji su povezani. ***Blockchain,*** javna tj. glavna knjiga ili lanac blokova je baza povezanih podataka koja sadrži sve kreirane transakcije na Internetu. Glavna značajka *blockchaina* je decentraliziranost odnosno zaobilaženje posrednika koji bi s njim upravljao. Uz to posebnost je trajna pohranjenost i dostupnost podataka svima, ali bez mogućnosti modificiranja i brisanja zapisa. *Blockchain* mrežu sačinjavaju umrežena računala koja provode proces verifikacije transakcija. Po završetku procesa prodaje nužno je da transakcija bude verificirana od strane rudara kako bi postala potvrđena. Verifikacijom se kreira zapis u *blockchainu*. Trajanje procesa verifikacije ovisi o vrsti kriptovalute. Potvrđivanje Bitcoin transakcija teoretski iznosi 10 minuta. Svaki blok ima vlastiti digitalni kod (eng. *hash*) koji se kronološki zapisuje u lanac. Pripajanjem bloka u lanac tj. *blockchain* on postaje javno dostupan. Njihovo povezivanje se temelji na kriptografiji kao metodi osiguranja sigurnosti i anonimnosti. Lanac blokova obuhvaća pregled svih transakcija. Svaki se blok sastoji od nekoliko elementa: verzije bloka (protokol koji treba slijediti za provjeru valjanosti bloka.), vrijednosti *hasha* za sve transakcije u postojećem bloku, *hash* vrijednosti roditeljskog odnosno prethodnog bloka, vremenske oznake zapisa, „*noncea“* (polje od 4 bajta čiji broj se može koristiti samo jednom u protokolima za provjeru autentičnosti i kriptografskim *hash* funkcijama) i podataka o transakciji.

Postoji više vrsta *Blockchaina*. **Javni** na kojoj svi imaju uvid u transakcije i potpunu anonimnost i **privatni** kojoj mogu pristupiti samo verificirani sudionici. Manje poznati su **konzorcij** koji je zapravo djelomično decentralizirani *blockchain* poput -EWF (energija), R3 (banke), B3i (osiguranje) i **hibridni** koji je varijanta privatnog i javnog *blockchaina*. Tvrtke s ciljem poboljšanja svojeg poslovanja nastoje implementirati *blockchain* koji se osim u financijskoj industriji može standardizirati na području zdravstva, osiguranja, nekretnina, Internet stvari (eng. *Internet of things*) itd..

2.2. Vrste kriptovaluta

Danas se trguje s više od tisuću kriptovaluta. Do veljače 2022. je predstavljeno približno 18,000 kriptovaluta. Od toga trenutno je otprilike 10,000 aktivno[2].

[2]Explodingtopics.com. How Many Cryptocurrencies Are There In 2022?. Preuzeto s: https://explodingtopics.com/blog/number-

Svakodnevno se pojavljuju nove koje mogu imati preduvjete za uspješan rast, ali isto tako i za stagnaciju odnosno propadanje tj. nestajanje s tržišta. Kriptovalute se okvirno mogu podijeliti na dvije podvrste. To su Bitcoini i Altcoini. Među njih se može svrstati inicijalna ponuda virtualnih tokena (eng. *Initial Coin Offering*, ICO) koje se također može promatrati kao zasebne kripto tokene. Svaka kriptovaluta nije jednako stvorena i s istom svrhom. Altcoini predstavljaju sve kriptovalute koje nisu Bitcoin poput Ethereuma, Tethera, Bitcoin Cash, Solane itd. Razlika između Bitcoina i Altcoina se može promatrati u specifičnosti namjene, funkcionalnosti i načinu rada. Druga razlika kod Altcoina je u metodi odnosno kompleksnosti rudarenja. Za primjer se može uzeti kriptovaluta Litecoin koja je naprednija verzija Bitcoina u smislu brzine potvrđivanja transakcija tj. brzini rudarenja. ICO predstavlja način financiranja projekta prodajom kripto tokena. Svrha prodaje tokena je da osigura sredstva potrebna za napredak projekta. Iza ICO-a stoje privatne tvrtke koje koriste kriptovalute odnosno *blockchain* platformu za razvoj aplikacija.

Vrijednost ostalih kriptovaluta tj. Altcoina je najčešće vezana uz vrijednost Bitcoina čija je cijena općeniti pokazatelj kretanja na tržištu. Vrijednost se može analizirati na tečaju kriptovaluta. Pomoću njega se primjećuje da najčešće ako vrijednost Bitcoina poraste, ostale kriptovalute prate tu vrijednost te imaju uzlaznu putanju odnosno silaznu ako vrijednost Bitcoina opada. Vrijednosti na tržnicama kriptovaluta se ažuriraju iz minute u minutu na temelju ponude i potražnje odnosno broju transakcija kupnje i prodaje (eng. *buy* i *sale order*). Kriptovalute prate princip ponude i potražnje. Ako potražnja nadilazi ponudu, kriptovaluta dobiva na vrijednosti. Ako je većina kriptovalute izrudarena, stopa rudarenja usporava. Slika 2.1. prikazuje deset najbolje rangiranih kriptovaluta prema ukupnoj tržišnoj vrijednosti (eng. *Market Cap*). Ukupna tržišna vrijednost se dobiva množenjem trenutne vrijednosti valute s količinom jedinica valute koje su u opticaju. Na slici se može primijetiti da najveću vrijednost po jedinici kriptovalute na tržištu ima Bitcoin s 22.549,69 dolara. Ukupna tržišna vrijednost Bitcoina iznosi 431.684.685.197 dolara Slijedi ga Ethereum s iznosom od 1.229,47 dolara po jedinici valute odnosno ukupnom vrijednošću od 149.815.609.550 dolara Također se može primijetiti ranije navedena silazna putanja kriptovaluta koja

of-cryptocurrencies (24.03.2022.)

uglavnom prati vrijednost Bitcoina.

Slika 2.1. Vodećih deset kriptovaluta prema ukupnoj vrijednosti

#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$22,549.69	3.40%	24.61%	$431,684,685,197	$53,907,490,468 2,381,077 BTC	19,067,381 BTC	
2	Ethereum ETH	$1,229.47	0.57%	30.96%	$149,815,609,550	$35,411,440,081 28,640,664 ETH	121,170,403 ETH	
3	Tether USDT	$0.9989	0.02%	0.03%	$71,520,759,612	$84,188,433,246 84,280,684,849 USDT	71,599,130,291 USDT	
4	USD Coin USDC	$1.00	0.01%	0.03%	$54,049,334,738	$9,930,169,868 9,928,122,531 USDC	54,038,191,201 USDC	
5	BNB BNB	$223.28	0.39%	21.34%	$36,689,487,391	$2,072,610,603 9,223,612 BNB	163,276,975 BNB	
6	Binance USD BUSD	$0.9987	0.09%	0.23%	$17,577,211,591	$7,890,599,027 7,896,641,357 BUSD	17,590,671,571 BUSD	
7	Cardano ADA	$0.4918	5.71%	20.08%	$16,737,714,229	$2,305,557,515 4,647,424,953 ADA	33,739,028,516 ADA	
8	XRP XRP	$0.3182	1.38%	19.64%	$15,450,420,588	$2,080,341,498 6,509,218,244 XRP	48,343,101,197 XRP	
9	Solana SOL	$29.92	8.10%	23.46%	$10,306,221,761	$2,393,227,242 79,464,873 SOL	342,208,458 SOL	
10	Dogecoin DOGE	$0.05631	2.42%	29.66%	$7,500,443,540	$976,610,453 17,274,665,765 DOGE	132,670,764,300 DOGE	

Izvor: https://coinmarketcap.com (04.04.2022.)

Bitcoin je primjer prve izdane kriptovalute koja je ujedno najpoznatija i najkorištenija kriptovaluta. 2008. godine je objavljen znanstveni rad pod nazivom „Bitcoin: A Peer-to-peer Electronic Cash System“. Kroz rad su predstavljene značajke novog financijskog sustava, *blockchaina*, *Peer-to-peer* sustava, anonimnost vlasnika, decentralizirana kontrola nad valutom, omogućavanje slanja i primanja uplata bez posrednika, uvid u transakcije itd.. Rad je napisan pod pseudonimom Satoshi Nakamoto. 3. siječnja 2009. se uzima za dan kada je nastao bitcoin odnosno dan kada je izdan nakon što je izrudaren prvi block s nazivom „Genesis Block“. Skraćenica bitcoina je BTC. Bitcoin je podijeljen na manje dijelove, od kojih je najmanja jedinica nazvana “Satoshi” (1 satoshi = 0.00000001 BTC) po njegovom izumitelju.

Prema podacima koji prikazuju vrijednost bitcoina na 1. siječnja određene godine vrijednost jednog Bitcoina 2010. iznosila je 0.09 dolara. Osam godina kasnije tj. 2018. iznosila je 13,412.44 dolara [3]. 1. siječnja 2022. vrijednost je iznosila 47,743 dolara.

[3] in2013dollars.com. Bitcoin Historical Prices. Preuzeto s: https://www.in2013dollars.com/bitcoin-price (28.03.2022.)

Rudarenje Bitcoina je specifično zato što zahtjeva rudarenje s ASIC-om, a ne sa standardnim grafičkim karticama koje se koriste u stolnim računalima. ASIC računala su razvijena za jednu svrhu rudarenje Bitcoina. ASIC računala su skuplja, energetski zahtjevnija, ali donose neusporedivo veću brzinu rudarenja naspram standardnih GPU-ova koji nisu namijenjeni za rudarenje Bitcoina. Bitcoin ima ograničen broj jedinica koje se mogu izdati. Ograničen je na 21 milijun bitcoinova. Prema platformi Coindesk na početku 2022. godine iznos izrudarenih jedinica dosegnuo je 19 milijuna. Pretpostavlja se da će se zadnja jedinica izrudariti oko 2140 godine. Svakih četiri godina se smanjuje udio rudarenje Bitcoina. Događaj smanjena udjela rudarenja se naziva **halving**. Nakon izrudarenih 210.000 blokova bitcoina prepolovi se dobitak. Od početka se za svaki kreiran blok dobivalo 50 bitcoina dok je taj iznos u 2022. snižen na 6.25. Halving ujedno može predstavljati razlog rasta vrijednosti bitcoina.

Druga najpopularnija kriptovaluta je **Ether** (ETH). Ethereum je predstavio i osmislio ruski programer Vitalik Buterin 2013. godine, dok je Ethereum službeno pokrenut 30. srpnja 2015. Najveća vrijednost Ethera je bila dosegnuta u studenom 2021. godine u iznosu od 4.800 dolara. Tijekom 2022. godine vrijednost se smanjila odnosno fluktuira oko 3.000 dolara. **Ethereum** je zamišljen kao javna *blockchain* platforma koja bilo kome dozvoljava programiranje i korištenje decentraliziranih aplikacija koje se izvode pomoću *blockchain* tehnologije. Može se upotrijebiti kao platforma za specifične vrste aplikacija te nije uvjetovan da služi samo za izdavanje kriptovaluta. Bitcoin *blockchain* se koristi samo za potvrđivanje transakcija dok se kod Ethereuma promijenio način primjene tehnologije koji na Ethereumu može izvoditi programske kodove. Novitet Ethereuma su tzv. **pametni ugovori**.

Pametni ugovor (eng. *Smart contracts*) je računalni program koji služi za automatsko izvršavanje unaprijed određenih procesa. Izvršavaju se na javno decentraliziranoj *blockchain* mreži. S ciljem pisanja programskih kodova korišten je programski jezik Solidity. Ugovori se mogu koristiti za razmjenu novčanih sredstava, investiranje, kupnju nekretnina, logistiku, pisanje ugovora o radu itd. Cilj pametnih ugovora je ukloniti ulogu posrednika između dviju strana nalogodavca i nalogoprimca. Za primjer se može uzeti kupnja nekretnine koja može zahtijevati više posrednika poput financijske institucije, javnog bilježnika i agencije za nekretnine. Računalni kod se

automatizmom izvršava kada su unaprijed određeni uvjeti zadovoljeni. Automatizam računalnog programa predstavlja veliku prednost zato što spriječava manipuliranje ugovorom. Nedostatak pametnih ugovora je taj da nisu prilagodljivi odnosno dok se program izvodi nisu moguće promjene. Budući da se ugovor ne može mijenjati, pri izradi programa moraju se definirati svi potencijalni scenariji koji mogu utjecati na izvršavanje ugovora.

Treća značajna kriptovaluta je **Tether** (USDT koja pokriće ima u američkom dolaru. Tether je osnovan u srpnju 2014. s nazivom „RealCoin“ da bi promijenio naziv krajem 2014. Nema vlastitu *blockchain* mrežu već funkcionira putem Ethereuma. Tether spada u „**stablecoine**“ odnosno kriptovalute čija se vrijednost veže za vrijednost postojeće valute poput dolara, eura itd. Tether je primjer kriptovalute koja ne koristi *blockchain* tehnologiju te je centralizirana. Budući da nema vlastitu mrežu, Tether se ne može rudariti kao ostale kriptovalute. Tether se redovito koristi u trgovanju kriptovalutama zato što nudi stabilnu vrijednost kriptovalute. U opticaju je približno 75 milijardi Tether jedinica valute. Budući da je Tether vezan uz američki dolar to implicira da je i ukupna vrijednost svih jedinica 75 milijardi američkih dolara. Ovisno o ponudi i potražnji ukupna količina izdanih jedinica se može povećati. Tether ukupnu vrijednosti pohranjuje u rezervama s ciljem osiguranja sigurnosti i pouzdanosti valute. Svrha Tethera je da vlasnik drugih kriptovaluta u trenutku opadanja vrijednosti npr. Ethera može brzo i jednostavno prenijeti svoja sredstva u Tether. Isto tako je neusporedivo brže prebaciti Tether u Ether umjesto kupnje Ethera posredstvom banke ili kartične tvrtke, plaćanja proviziju trećoj strani i čekanja na potvrdu posrednika da je transakcija uspješna i realizirana.

2.3. Metode stjecanja kriptovaluta

Kriptovalute se tijekom zadnjih nekoliko godina sve češće koriste kao sredstvo plaćanja. Zahvaljujući sve većoj popularnosti, ali i općoj prihvaćenosti kao načinu razmjene proizvoda i usluga za virtualnu valutu, svakim danim se povećava broj populacije zainteresirane za kriptovalute. Zainteresirani za kriptovalute imaju na raspolaganju više metoda stjecanja. Okvirno bi ih vrijedilo podijeliti na dvije temeljne: **trgovanje** i **rudarenje**.

Trgovanje spada u učestaliju metodu kojom se stječu kriptovalute. Kupnja i prodaja

kriptovaluta nalikuje opće prihvaćenim transakcijama poput kupnje imovine, nekretnina, vrijednosnih papira, dionica i sl. Kupnja kriptovaluta se najčešće odvija na **specijaliziranim web stranicama i burzama** na kojima se provodi kupovina i prodaja kriptovaluta. Budući da vrijednost kriptovaluta određuje ponuda i potražnja za njima, ideja kupnje je kupiti po niskoj cijeni i prodati kada ona naraste. Proces čekanja dužeg perioda da cijena naraste na višu razinu koja je kupcu prihvatljiva da pokrene proces prodaje se zove *hold*. *Hold* uz potencijalnu višu vrijednost nakon određenog razdoblja donosi i beneficiju poreznog rasterećenja ovisno o državi u kojoj se transakcija ostvarila. Vlasnici u Sjedinjenim Američkim Državama ako svoje kriptovalute zadrže dulje od godinu dana, plaćaju manji porez pri prodaji. Zadržavanje kriptovaluta se može poistovjetiti s investiranjem u zlato. Osim stranica specijaliziranih za kupnju kriptovaluta, one se mogu kupiti direktno od **trgovaca** ili putem **specijaliziranih bankomata** po principu razmjene novčanih sredstava kupca za određeni iznos kriptovaluta. Kriptovalute se mogu steći prihvaćanjem **kao opcije plaćanja** kod prodaje proizvoda ili usluga. Dodatne metode koje se mogu okarakterizirati kao trgovanje su pregledavanje oglasa na web stranicama za čiji se trud naplaćuju male količine, primanje određenih iznosa u obliku donacija, programi preporučivanja (eng. *referral*) u kojemu se za svaku osobu koja se odluči registrirati na platformu nagrađuje itd.

Rudarenje (eng. *mining*) je vjerojatno najpoznatija metoda stjecanja kriptovaluta. Uslijed porasta popularnosti kriptovaluta, mnogi su se s njom počeli baviti. Rudarenje je automatizirani proces potvrde transakcija *blockchaina* odnosno proces dodavanja blokova na blokovni lanac. Ovisno o vrsti kriptovalute, svakih 10 minuta do jednog sata transakcija postaje potvrđena. *Blockchain* mrežu čine međusobno povezana računala. U tom kontekstu sva međusobno povezana računala se nazivaju **rudarima** (eng. *crypto miners*). Rudari se mogu podijeliti na **samostalne** (eng. *solo mining*) i **grupne** (eng. *pool mining*). U slučaju da se prestanu baviti rudarenjem, *blockchain* mreža ne bi funkcionirala. Za proces je potrebna računalna oprema koja troši svoje resurse, procesorsku ili grafičku snagu kako bi ono izvršavalo kriptografski algoritam koji služi za potvrđivanje transakcija. Kao nagradu za obavljeni posao, rudarima se dodjeljuje određeni iznos kriptovalute. Što više pojedinci ulože u snagu svojih računala, veća je zarada od potvrđivanja transakcija. Isplativost rudarenja ovisi o cijeni, snazi i brzini

grafičke kartice (eng. *Graphics processing unit*), maksimalnoj potrošnji energije cijelog hardvera, postojećoj cijeni električne energije te trenutnoj vrijednosti iznosa kriptovalute koja se zaradi nakon uspješnog procesa rudarenja tzv. MH/s (eng. *MegaHashes per Second*). Nameće se problem potrošene električne energije koja ne smije biti veća od nagrade tj. zarade. Rudarenje Bitcoina više nije isplativo s većinom standardnih grafičkih kartica, te je potrebna nabava specijaliziranog računala. Postoje posebna ASIC računala (eng. *Application-Specific Integrated Circuit*) namijenjena samo za efikasno rudarenje Bitcoina. Trenutno je najpopularnija kriptovaluta za rudarenje Ether. Slika 2.2. prikazuje računalo za samostalno rudarenje (eng. *mining rig*) dok je s desna ASIC.

Slika 2.2. Računala za rudarenje

Izvor: https://outletcryptomarket.com/product/8-gpu-nvidia-rtx-3080-complete-mining-rig/ (04.04.2022.) i https://www.coindesk.com/markets/2018/05/01/crypto-needs-more-than-code-to-beat-the-asic-mining-threat/ (04.04.2022.)

Budući da samostalno rudarenje može istiskivati velike troškove nabave i potrošnje električne energije, postoji opcija **rudarenja putem oblaka** (eng. *cloud mining*). Osoba unajmljuje opremu koja se ne nalazi u njegovom vlastitom prostoru. Za to se plaća mjesečna cijena korištenja. Iznosi mogu varirati od 500 američkih dolara do nekoliko tisuća ovisno o snazi računala.

3. METODE POHRANE KRIPTOVALUTA

Korištenje i slanje kriptovaluta zahtjeva da korisnik primjenjuje neku od metoda pohrane kriptovaluta. U ovom poglavlju obradit će se tema kripto novčanika te će se analizirati svaki od njih: web, desktop, mobilni, hardverski i papirnati novčanici.

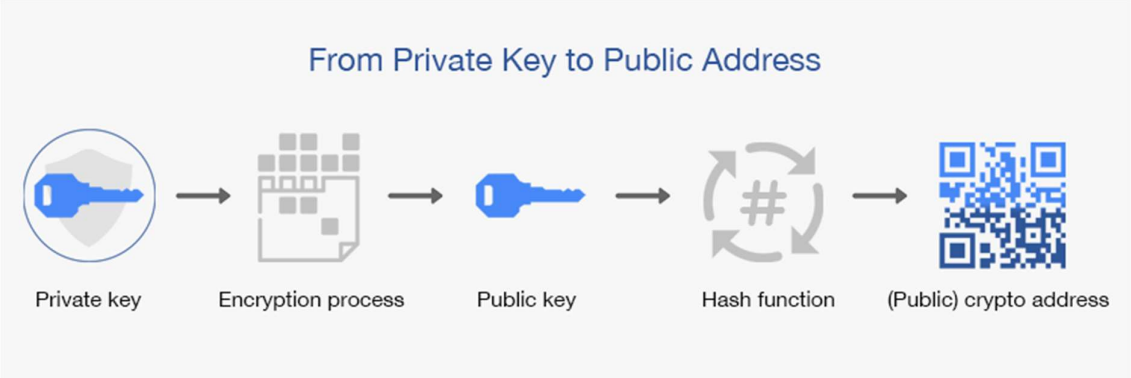
3.1. Općenito

Po uzoru na novčana sredstva koja se drže u financijskim institucijama ili u novčanicima građana, na sličan se način mogu pohranjivati kriptovalute. Metode pohrane kriptovaluta se jednostavnije mogu smatrati kripto novčanicima budući da se u njih pohranjuju. Novčanik se može opisati kao softver koji komunicira s lancem blokova (eng. *blockchain*). Postoji samo u digitalnom obliku. Kripto novčanik (eng. *crypto wallet*) se sastoji od adrese novčanika, javnog i privatnog ključa. Privatni i javni ključevi koriste kriptografske metode s ciljem kreiranja novčanika. Javna adresa se može dijeliti, dok se privatni ključ ne smije otkrivati te mora ostati poznat samo vlasniku novčanika.

Kod instalacije na osobno računalo ili mobilni telefon odnosno prilikom inicijalnog otvaranja novčanika putem internetskog preglednika generiraju se adrese i ključevi novčanika. Adresa i javni ključ nisu isti pojmovi, ali su matematički povezani. Adresa je *hashirana* verzija javnog ključa. *Hash* je matematička funkcija koja pretvara ulaz proizvoljne duljine u šifrirani izlaz fiksne duljine. Svaki javni ključ dugačak je 256 bita dok je konačni hash tj. adresa dugačka 160 bita. U kriptografiji javni ključ je brojčana vrijednost, koja se koristi za šifriranje podataka s ciljem osiguranja provjere autentičnosti adrese primatelja. Javni ključ se matematički izračunava iz privatnog ključa korištenjem množenja eliptičke krivulje, formulom K= k * G u kojoj k predstavlja privatni ključ, a G konstantnu točku koja se zove generatorska točka. K je rezultat odnosno javni ključ. Javni ključevi se koriste za primanje kriptovaluta. Prilikom otvaranja novčanika tj. generiranja ključeva koristi se kriptografski algoritam građen na temelju asimetričnog kriptiranja pod nazivom algoritam digitalnog potpisa eliptične krivulje (eng. *elliptic curve digital signature algorithm*)[4]. Kriptografija eliptičke krivulje spada u segment asimetrične kriptografije.

[4] oreilly. Mastering Bitcoin. Preuzeto s: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ (04.04.2022.)

Slika 3.1. Proces dobivanja javnog ključa iz privatnog i javne adrese novčanika iz javnog ključa



Izvor: https://www.bitira.com/public-key-vs-private-key-what-are-the-key-differences/ (04.04.2022.)

Privatni ključ (eng. *Private Key*) je šifrirani numerički broj koji služi za dokazivanje vlasništva nad kriptovalutama koje se nalaze u novčaniku. Povezan je s javnim ključem. U kriptografiji svi podaci koji su kodirani javnim ključem mogu se dešifrirati samo odgovarajućim privatnim ključem. Služi za slanje kriptovaluta tj. autorizaciju prijenosa. Proces se još zove potpisivanje transakcije. Privatni ključ se prikazuje kao nasumično generiran 256 bitni broj. Kada se 256 binarnih znamenki prikaže kao 64 heksadecimalne znamenke odnosno svaka 4 bita, dobiva se ključ koji se sastoji od 64 broja. Primjer privatnog ključa:

5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF[5]

Privatni ključ je poznat samo vlasniku novčanika te se on mora čuvati u tajnosti. U slučaju da vlasnik zaboravi lozinku te izgubi privatni ključ, novčanik i sredstva nije moguće vratiti. Nadalje ako haker ukrade privatni ključ, tada on ima kontrolu nad novčanikom i može prenijeti kriptovalute. U svrhu osiguranja povrata novčanika nužno je napraviti kopiju fraze za oporavak i privatnog ključa (ako je to moguće) te ih pohraniti na sigurno mjesto.

Upotreba dva ključa novčanika naziva se asimetrična kriptografija. Asimetrična kriptografija koristi privatni i javni ključ s ciljem šifriranja odnosno dešifriranja podataka. Proces asimetrične enkripcije čine novčanici pošiljatelja i primatelja. Pošiljatelj na adresu novčanika primatelja šalje transakciju te se pomoću javnog ključa primatelja ta

[5] Tokenexus.com Bitcoin Private Keys: Everything You Need To Know. Preuzeto s: https://www.tokenexus.com/bitcoin-private-keys-everything-you-need-to-know/ (15.03.2022.)

adresa šifrira algoritmom asimetrične enkripcije. Šifrirani podaci se šalju primatelju transakcije pomoću privatnog ključa koji potpisuje transakciju te koji dešifrira podatke. Nakon toga zapis se šalje u *blockchain* na potvrdu od strane drugih korisnika. Pošiljateljev kriptografski potpis osigurava da nitko drugi izvan transakcije ne može kompromitirati njezin sadržaj. Rudari kriptovaluta provjeravaju sadržaj transakcije koja se dešifrira uporabom javnog ključa pošiljatelja. Sve provedene transakcije koje su zapisane u *blockchainu* se kriptografijom osiguravaju da se ne mogu ukloniti odnosno korigirati. Svaka transakcija koju vlasnik kriptovaluta kreira, stvara zapis na *blockchainu*. Zapisane transakcije zauvijek ostaju pohranjene. Kako bi sve transakcije bile provedene, zahtijevaju da se u *blockchainu* autentificira potpis. Potpis se dobiva samo s važećim ključevima. Kriptografski potpis se opisuje kao proces koji omogućuje vlasniku da dokaže vlasništvo nad novčanikom. Kod potpisivanja transakcije odgovarajućim privatnim ključem, mreža bilježi transakciju koja prepoznaje da potpis odgovara transakciji koja se izvršava. *Blockchain* prepoznaje potpis transakcije, ali ne može vidjeti privatni ključ koji se koristi kod potpisivanja.

Vlasnik kriptovaluta nije ograničen na jedan novčanik već ima mogućnost raspodjele sredstava na više različitih novčanika. Novčanici dolaze u različitim oblicima namijenjenima za različite uređaje. Metode pohrane kriptovaluta odnosno novčanici se dijele na dvije vrste: **vruće** i **hladne**.

3.2. Vrući novčanik

Vrući novčanik (eng. *Hot wallet*) je novčanik koji je povezan na mrežu odnosno internet. Za pristupanje kriptovalutama, pokretanje i završavanje transakcije potrebna je stabilna internetska veza. Vrući novčanik prikladniji je za češći pristup kriptovalutama odnosno za vlasnike koji češće trguju. Svrha je pružiti vlasniku brz i neposredan pristup njegovom novčaniku. Uporaba je moguća uz preduvjet preuzimanja aplikacije na računalo i pametni telefon ili pristupanjem putem internetskog preglednika. Kontrola nad privatnim ključevima novčanika se može podijeliti na skrbničke ili neskrbničke novčanike (eng. *Custodial* i *Non-Custodial Wallets*). Osnovna razlika između skrbničkih i neskrbničkih je u tome što kod je skrbničkih privatni ključ novčanika nepoznat vlasniku i ključem upravlja treća strana. Kod neskrbničkog, korisnici su odgovorni i imaju potpunu kontrolu nad privatnim

ključem. Vrući novčanici nude manju sigurnost naspram hladnih. Izlaganjem internetu, sigurnost novčanika je narušena. Posrednici nude visoku razinu sigurnosti vlasnicima korištenjem sigurnosnih fraza, PIN-ova i dvofaktorskom provjerom autentičnosti. Međutim, sve navedeno nije dovoljno u sprečavanju hakiranja i krađe kriptovaluta. Hakeri najčešće ciljaju na poznatije davatelje usluge koji brinu o većoj količini vrijednosti kriptovaluta svojih korisnika. Korištenje vrućih novčanika u smislu preuzimanja se ne naplaćuje, ali posrednici naplaćuju naknade za provođenje transakcija. Većina ih ima širok spektar podržanih kriptovaluta dok ostali podržavaju uži, najčešće najpopularnije kriptovalute poput Bitcoina, Ethera i Tethera. Vrući novčanici se mogu podijeliti na tri kategorije: **web**, **desktop** i **mobilne novčanike**.

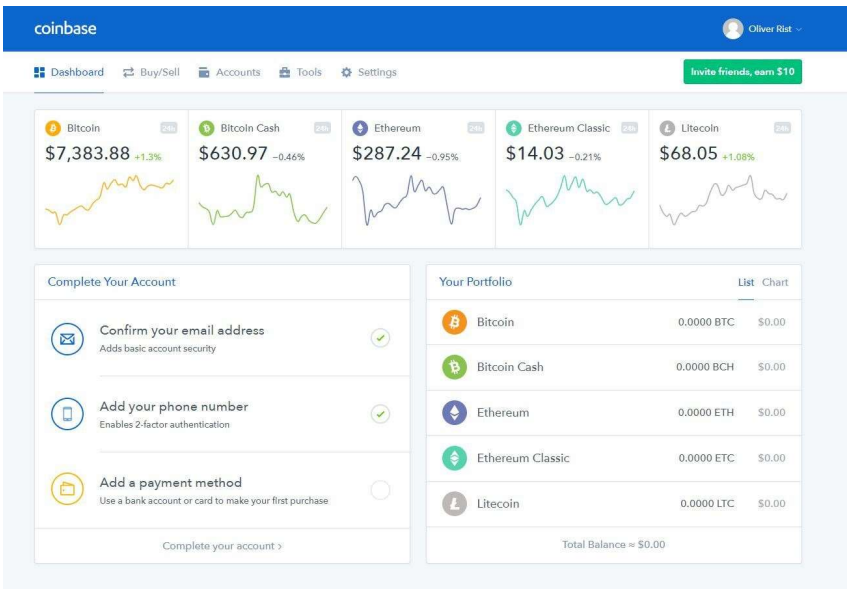
Web novčanici spadaju u kategoriju vrućih novčanika koji su dostupni isključivo putem internetskog preglednika. Omogućuju pristup kriptovalutama na bilo kojem uređaju i na svim poznatim preglednicima poput Google Chroma, Microsoft Edgea, Mozzila Firefoxa itd.. Za korištenje nije potrebno prethodno preuzimanje programa odnosno instalacija. Registracija je potrebna kao preduvjet pristupanju jednoj od platformi. Među poznatije *web* novčanike spadaju Coinbase, Binance, Blockchain wallet i Kraken itd.. Prednost im je da vlasnici mogu pristupiti s bilo kojeg uređaja s preduvjetom da imaju pristup internetu. Nedostatak je da su treće strane odnosno posrednici koji pružaju uslugu odgovorni za sigurnost i zaštitu privatnih ključeva novčanika njihovih korisnika. Budući da je treća strana posrednik, ona ima uvid u sve transakcije novčanika svojih korisnika. Posrednici pohranjuju privatne ključeve na vlastitim serverima. Privatne ključeve korisnici u većini slučajeva ne mogu saznati. Sigurnost *web* novčanika predstavlja veliku važnost. Podložni su većem riziku hakiranja, krađe podataka korisnika platforme, krađe korisničkih lozinki itd.

Različiti vrući novčanici konkretnije *web* nose različite sigurnosne rizike. Najmanje sigurni su novčanici koji se nalaze na „**mjenjačnicama**“ (eng. *exchange*) stranicama koje su namijenjene za trgovinu kriptovaluta. *Exchange stranice* odražavaju trenutne tržišne cijene kriptovaluta koje nude. Mogu poslužiti kao novčanik zato što imaju sve njegove karakteristike. Potreban je registrirani profil, potvrda autentifikacije korisnika, generirana javna adresa te naposljetku novčanik koji može pohranjivati kriptovalute ili uplaćene iznose u fiat valutama poput dolara. Vlasnici kriptovaluta koji imaju veću

koncentraciju trgovanja na *exchange* stranicama znaju svoja sredstva ostaviti tamo gdje su ih i kupili. U slučaju da vrijednost određene kriptovalute počne padati, vlasnik može lakše i brže prodati ili zamijeniti za drugu valutu. *Exchange* stranice su značajna meta za hakere zato što pohranjuju velike vrijednosti.

Jedan od najpoznatijih *web* novčanika je **Coinbase.** Pripada i poznatijim *exchange* stranicama u SAD-u. Coinbase je besplatni vrući novčanik koji broji bazu od otprilike 56 milijuna korisnika od kojih 6.1 milijuna su aktivni korisnici koji izvršavaju minimalno jednu transakciju mjesečno[6]. Svoju bazu korisnika grade atraktivnim i intuitivnim dizajnom koji je početnicima jednostavan za korištenje. Budući da se govori o *web* novčaniku, vlasnik novčanika nema potpunu kontrolu nad svojim novčanikom odnosno privatni ključ nije vidljiv vlasniku. Za sigurnost novčanika vodi njegov izdavatelj odnosno Coinbase. Svojim korisnicima u cilju osiguranja sredstava, nude opciju uključivanja dvofaktorske provjere autentičnosti iliti 2FA kao dodatnu razinu sigurnosnog sloja uz korisničko ime i lozinku. 2FA dodaje dodatnu zaštitu s ciljem sprječavanja neautoriziranih upada.

Slika 3.2. Izgled Coinbase portfolio stranice



Izvor: https://www.pcmag.com/reviews/coinbase-wallet (04.04.2022.)

14. travnja 2021. izvršen je proces inicijalne javne ponude dionica na američkoj burzi.

[6] Backlinko.com Coinbase Usage and Trading Statistics (2022). Preuzeto s: https://backlinko.com/coinbase-users (15.03.2022.)

Kako bi se korisnicima olakšala trgovina kriptovalutama Coinbase ima vlastitu debitnu karticu. Također po uzoru na sve veće i poznatije davatelj usluge usluge imaju mobilnu aplikaciju koja se može preuzeti na Android ili iOS uređajima. Naplaćuju naknade pri kupovini, prodaji ili zamjeni kriptovalute. Naknade se izračunavaju u trenutku provođenja transakcije na koju utječe kombinacija čimbenika. Čimbenike uključuje način plaćanja, veličina narudžbe i tržišni uvjeti kao što su volatilnost i likvidnost odabranih kriptovaluta. Naknade variraju između 0,5% - 4,5% ovisno o navedenim čimbenicima.

Desktop novčanici su programi koji su namijenjeni za instalaciju na prijenosna i klasična stolna računala. Navedena funkcionalnost im omogućuje pristup kriptovalutama u slučajevima kada računalo vlasnika kriptovaluta nije povezano na mrežu odnosno Internet. Instalacijom na računalo vlasnik kriptovaluta stječe potpunu kontrolu nad svojim novčanikom. *Desktop* novčanici omogućuju vlasniku generiranje javne adrese za slanje i primanje kriptovaluta. Dodatna funkcionalnost koju nemaju ostali korisnici drugih vrućih novčanika je kontrola nad privatnim ključem. Budući da vlasnik pohranjuje svoj novčanik na računalu koje je u njegovom vlasništvu on postaje odgovorna osoba za sigurnost svojih kriptovaluta. Kod *desktop* novčanika ključno je kreiranje *backupa* odnosno sigurnosne kopije novčanika. Uz to bitna je pohrana privatnog ključa zato što u slučaju kvara diska na kojemu je novčanik, vlasnik gubi svoje kriptovalute. Nadalje preporuka je zaštititi računala antivirusnim programom kako ne bi došlo do otuđenja sredstava od strane hakera. Činjenica je da danas većina računala već koristi antivirusne programe koji nisu u potpunosti zaštićeni, preporučljivo je desktop novčanike instalirati na odvojenom računalu koje se koristi samo za svrhu kontrole nad novčanikom. Dostupni su za različite operacijske sustave: Windows, Mac OS i Linux. Među poznate *desktop* novčanike spadaju Bitcoin Core, Armory, Hive, Electrum, Exodus itd. Neki imaju bolje sigurnosne funkcionalnosti poput programa Armory koji je namijenjen za izvanmrežno potpisivanje transakcija.

Primjer popularnog *desktop* novčanika je **Exodus**. Exodus je besplatni novčanik osnovan 2015. godine od strane istoimene kompanije. Kompatibilan je za rad na Windows, OS X i Linux operativnim sustavima. Uz instalaciju na stolno računalo, dostupna je mobilna aplikacija za Android i iOS uređaje. Exodus podržava pohranu

više od 150 kriptovaluta. Posjeduje dobro dizajnirano i jednostavno grafičko korisničko sučelje (eng. *Graphical user interface* - *GUI*) koje nudi detaljan prikaz podataka portfelja vlasnika. Kriptovalute se mogu filtrirati po ukupnoj vrijednosti u portfelju te je ponuđen grafički dijagram trenda vrijednosti.

Slika 3.3. Izgled grafičkog sučelja Exodus desktop novčanika

Izvor: https://masterthecrypto.com/exodus/ (04.04.2022.)

Korisne podatke čine: 24-satna promjena vrijednosti portfelja, ukupna vrijednost imovine u odabranoj valuti, najvišu vrijednost portfelja, starost portfelja, najbolju vrijednost u posljednja 24 sata te najlošiju u posljednja 24 sata. Detaljni prikaz informacija vlasnicima omogućuje efikasno, pojednostavljeno i lakše upravljanje nad portfeljem i praćenje vrijednosti cijelog novčanika. Korisna funkcionalnost je integrirano povezivanje s Trezor hardverskim novčanicima. Za korištenje nije potrebna registracija odnosno izrada korisničkog profila. Korisnike se ne traže identifikacijski podaci te njihovi osobni podaci i privatni ključevi ostaju u potpunosti privatni. Svi podaci se pohranjuju i šifriraju na disku korisnika odnosno vlasnika novčanika. Budući da se radi o *desktop* novčaniku, korisnici imaju pristup privatnom ključu koji se nikada ne dijeli s Exodus-ovim davateljem usluge. Korisnicima je omogućena izrada sigurnosne

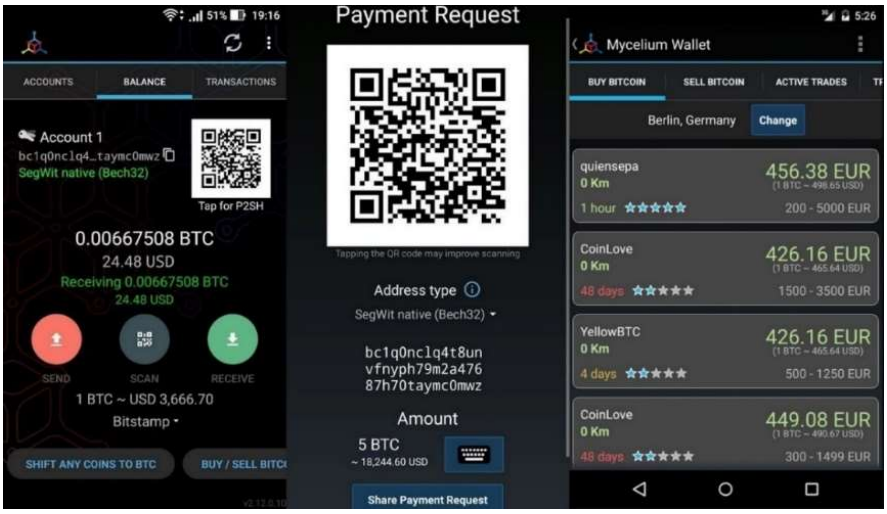
kopije novčanika korištenjem fraze za oporavak koja sadrži 12 riječi. Iako je preuzimanje i postavljanje novčanika besplatno, kao i svaki drugi vrući novčanik, Exodus naplaćuje mrežnu naknadu samo za slanje sredstava bez naknade za primanje.

U treću vrstu pripadaju **mobilni novčanici.** Mobilni novčanici su aplikacije koje su prilagođene za rad na pametnim telefonima. Najpopularniji su na Androidu i Apple iOS mobilnim operacijskim sustavima. Zahtijevaju instalaciju aplikacije koja služi kao novčanik i povezanost na mrežu odnosno Internet za provođenje transakcija. Mobilni novčanik mora sadržavati iste funkcije kao *web* novčanik. Dodatne funkcije se mogu pojavljivati u obliku upotrebe funkcija koje imaju pametni telefoni. Jedna od tih funkcija je mogućnost korištenja QR kodova za plaćanje transakcija. Vlasnik ima mogućnost skeniranja QR koda i jednostavnijeg izravnog pružanja putem mobitela, bez pristupanju novčaniku i popunjavanja klasične forme kod transakcija. Mnogi mobilni novčanici pružaju jednostavnije i brže plaćanje u fizičkim trgovinama putem komunikacija bliskog polja iliti NFC (eng. *Near-field communication*). Uporabom NFC-a, novčanik će iskoristiti mogućnosti pametnih telefona te omogućiti plaćanje dodirom uređaja s čitačem bez unosa bilo kakvih informacija. Prilikom plaćanja iznos vrijednosti proizvoda će se automatski oduzeti s mobilnog novčanika ako vlasnik ima raspoloživ određeni iznos. Budući da se mobilni novčanici instaliraju kao aplikacija na pametnim telefonima, neki novčanici imaju mogućnost pohrane privatnih ključeva. Primjeri mobilnih novčanika su: Mycelium, Bitcoin wallet, Blockchain, HiveWallet itd. Većina poznatijih *web* novčanika ima svoju mobilnu verziju.

Aplikacija **Mycelium** spada među najbolje mobilne novčanike za korisnike. Kompanija Mycelium je osnovana 2008. godine. U svom asortimanu imaju mnogobrojne vrste proizvoda: Mycelium novčanik, Mycelium Entropy generator hardverskog papirnog novčanika, Mycelium karticu koja pruža softversku kompatibilnost s *Blockchainom* za plaćanje računa, dopune računa i druge financijske operacije. Proizvođač nudi i Mycelium Swish sustav za poboljšanje korisničkog iskustva naručivanja usluga. SWISH sustav uključuje fleksibilni softver za upravitelje restorana, aplikaciju za konobare i web aplikaciju za kupce. Kupci skeniranjem QR koda na oglasnim pločama restorana mogu dobiti sve potrebne informacije o narudžbi, naručiti hranu te platiti

narudžbu kriptovalutama.

Slika 3.4. Izgled sučelja Mycelium aplikacije



Izvor: https://play.google.com/store/apps/details?id=com.mycelium.wallet&hl=en&gl=US (04.04.2022.)

Mycelium novčanik ima jednostavno sučelje koje ima funkcionalnost kupovanja i prodaje kriptovaluta izravno iz aplikacije. Također omogućuje kupnju s *fiat* valutom. Jedna od najvažnijih značajki je da vlasnik ima pristup privatnom ključu. Sve transakcije i podaci su šifrirani. Po uzoru na *web* i *desktop* novčanike u slučaju gubitka ili krađe računa, pomoću sigurnosnih fraza koje čine 12 riječi se može napraviti povrat sredstava. Novčanik je zaštićen PIN-om od četiri broja kako bi se osigurala zaštita u slučaju krađe ili gubitka mobilnog uređaja. Prednost Mycelium novčanika je u otvorenom kodu kojega svatko može pročitati i provjeriti postoje li greške i propusti u kodu. Novčanik omogućuje vlasnicima da uklone svoj privatni ključ s uređaja kako bi zaključali svoj fond zbog čega novčanik postaje nedostupan. Kada se vlasnik odluči vratiti pristup svom novčaniku funkcijom „uvezi“ može uvesti svoj privatni ključ natrag u mobilni uređaj. Kompanija MyCelium ima pristup samo najosnovnijim informacijama kao što su povijest trgovanja, vremenske oznake transakcija i javne adrese. Novčanik podržava QR kod i nudi kompatibilnost s hardverskim novčanicima iz Ledgera i Trezora. Besplatan je za korištenje, ali postoje naknade za transakcije koje ovise o iznosu koji se provodi. Mogu varirati od 0,25 do 8 dolara[7]. Nedostatak Mycelium novčanika je u broju podržanih kriptovaluta. Mycelium podržava: Bitcoin, Ethereum,

[7] Cryptonewsz.com Mycelium Wallet Review 2022 Preuzeto s: https://www.cryptonewsz.com/crypto-wallet/mycelium-wallet-review/ (15.03.2022.)

Tether USD , USD coin i Binance USD.

3.3. Hladni novčanik

Hladni novčanik (eng. *Cold wallet*) je novčanik koji nije spojen na mrežu odnosno Internet. Smatra se najsigurnijom metodom pohrane kriptovaluta. Glavna svrha je dugotrajna pohrana. Uglavnom je namijenjen vlasnicima većih iznosa vrijednosti kriptovaluta. Uz izvanmrežnu pohranu koja smanjuje potencijalnu izloženost hakerskim napadima, enkripcija pomaže u osiguranju najveće moguće razine sigurnosti ove metode. Glavno pravilo hladnih novčanika je osiguranje potpune izolacije između privatnih ključeva novčanika i računala odnosno pametnih telefona. To podrazumijeva da su privatni ključevi isključivo u vlasništvu i pod kontrolom vlasnika.

Postoje dvije vrste hladnih novčanika: **hardverski** i **papirnati**. Hladni novčanik koji funkcionira izvan mreže zahtijeva zapisivanje privatne adrese na komad papira ili kupnju fizičkog uređaja koji služi za pohranu kriptovaluta. **Hardverski novčanici** su prijenosni uređaji, dimenzija poput USB prijenosne memorije. Njihova glavna značajka je visoka razina sigurnosti dok je nedostatak naspram vrućih novčanika cijena odnosno zahtijevaju kupnju uređaja. Dizajnirani su tako da sve što vlasnici trebaju učiniti je povezati uređaj na računalo ili pametni telefon, otključati novčanik lozinkom, poslati određeni iznos i naposljetku potvrditi transakciju. Najčešće imaju zaslon koji korisnicima omogućava učinkovit rad s aplikacijama povezanim na računala ili pametne telefone. Hardverski novčanici ne izlažu privatne ključeve internetu. Najpopularniji od njih osiguravaju sigurnost generiranjem sigurnog pojma odnosno „sjeme za oporavak“ (eng. *recovery seed*.). Pojmovi su u osnovi niz riječi koje je generirao novčanik prilikom inicijalnog postavljanja te one služe za povrat vlasništva u slučaju gubitka ili krađe. Iako su pouzdani i sigurni nisu otporni na hakiranja. Napadi najčešće zahtijevaju fizički pristup uređaju s ciljem krađe PIN broja. Posjedovanjem hladnog novčanika vlasnik stječe privatni ključ kojeg je nužno čuvati na sigurnom mjestu. Hladni novčanici pružaju visoku razinu zaštite te je njihov privatni ključ zaštićen na certificiranom čipu unutar uređaja.

Prema istraživanju provedenog na *web* stranici *blockgeeks*, 2022. godine

najpopularniji proizvođač **hardverskih novčanika** je francuski startup **Ledger[8].** U svojoj ponudi imaju dva modela: Nano S i Nano X. 2016. godine je lansiran Ledger Nano S, prvi Ledger novčanik za hladnu pohranu kriptovaluta. Njegove dimenzije dopuštaju praktično korištenje zahvaljujući elegantnom dizajnu nalik USB prijenosnoj memoriji. Novčanik podržava više od tisuću kriptovaluta. Spajanje na računalo omogućava usb micro b priključak. Uređaj je lansiran s početnom cijenom od 79 dolara. Po završetku instalacije odgovarajućeg softvera, određuje se PIN broj te se generiraju pojmovi čija je svrha oporavak računa. Pojmovi sačinjavaju 24 riječi. Po završetku postavljanja uređaja, Ledger novčanik je spreman za primanje kriptovaluta.

Slika 3.5. Izgled Ledger hardverskog novčanika

Izvor: https://shop.ledger.com/products/ledger-nano-s (04.04.2022.)

Ledger Nano X spada u drugu generaciju Ledger novčanika. Na tržište je predstavljen 2019. godine te je istih dimenzija na prethodnu generaciju. Predstavljen je s cijenom od 150 dolara. Glavne prepoznatljive značajke poput prenosivog i manjeg dizajna uređaja, visoka sigurnost novčanika, usb povezivost su ostale nepromijenjene. Nano X uključuje važne nadogradnje kao što su LED zaslon za lakšu i praktičniju navigaciju po izborniku, USB Type-C priključak za punjenje, bateriju od 100 mAH i Bluetooth funkcionalnost. Kod jeftinijeg Nano S modela se može instalirati tri aplikacije dok je broj na jačem modelu proširen na 100 aplikacija. Nalik prethodniku podržava više od tisuću kriptovaluta. Uz novi uređaj razvijen je vlastiti softver Ledger Live koji predstavlja softversko sučelje hardverskog novčanika namijenjen Ledger korisnicima. Aplikacija omogućuje upravljanje uređajem i novčanikom.

[8] Blockgeeks.com. Best Hardware Wallets in 2022: Blockgeeks Crypto Awards. Preuzeto s: https://blockgeeks.com/guides/best-hardware-wallets-comparative-list-blockgeeks/ (15.3.2022.)

Drugi popularan model hardverskog novčanika pripada kompaniji **Trezor**. U svojem asortimanu imaju dva modela: Trezor One i Trezor Model T. Poput proizvoda kompanije Ledger koji proizvode fizičke uređaje Trezorovi se također spajaju USB kablom na računalo. Skuplji Model T ima zaslon osjetljiv na dodir koji ga čini jednostavnim za korištenje za razliku jeftinijeg modela. Trezor One model zahtijeva korištenje kombinacijom s mobilnim uređajem ili računalom. Oba modela mogu pohraniti više od tisuću kriptovaluta čija sigurnost je osigurana s nekoliko enkripcija. Poput Ledgera, razvijena je desktop aplikacija, ali i *web* aplikacija pomoću koje vlasnici mogu pristupiti upravljanju računom. Trezor uređaji imaju razliku kod sigurnosnih pojmova koji kod Trezor One čine 12 tj. 24 riječi u slučaju naprednijeg uređaja**.** Cijena osnovnog Trezor One modela iznosi 80 dolara dok kompletniji Model T 250 dolara. Razlika kod Trezor modela hladnih novčanika u usporedbi s Ledger uređajima je u softveru koji je naspram Ledgera otvorenog koda (eng. *open source*). Trezorov *firmware* i aplikacije su javno dostupni i omogućavaju kodiranje od strane zajednice. To omogućuje brže otkrivanje potencijalnih grešaka u implementaciji te omogućuje zajednici i kompaniji da razviju prikladne ispravke softvera.

Među prva tri najpopularnija hardverska novčanika još spada **KeepKey** novčanik Švicarske kompanije ShapeShift. Za razliku od Ledger i Trezor uređaja dimenzija KeepKey uređaja je izraženija. To je omogućilo implementaciju većeg zaslona koji omogućuje čitanje dugih kripto adresa. Način funkcioniranja je nalik Ledgeru i Trezoru. Podržava više od 40 najpopularnijih kriptovaluta. S ciljem pridobivanja većeg broja korisnika preporučena cijena ovog uređaja je najniža između prve tri kompanije te iznosi 50 dolara.

Slika 3.6. Dizajn različitih modela hardverskih novčanika

Izvor: https://captainaltcoin.com/trezor-vs-ledger-nano-s-vs-keepkey/ (04.04.2022.)

Drugoj vrsti hladnih novčanika pripadaju **papirnati novčanici** (eng. *Paper wallets*). Papirnati novčanici pohranjuju kriptovalute u fizičkom obliku koji nije temeljen na hardveru. Smatraju se sigurnijom metodom pohrane od hardverskih novčanika zato što za razliku od hardverskih poput Ledgera nemaju rizik od kvara te brigu za dugotrajnost baterije. Za osiguranje pristupačnosti novčaniku, vlasniku kriptovaluta se preporučuje odvajanje privatnog ključa od hardverskog novčanika. Vlasnicima kriptovaluta pri izradi papirnatog novčanika, dostupne su web stranice poput *WalletGenerator.net*, *Bitaddress.org*, *MyEtherWallet.com* i ostale specijalizirane za ovakvu vrstu usluge. Kod generiranja sustav odredi javnu adresu i privatni ključ, koja naposljetku ostaje korisniku kao opcija printanja ili prepisivanja na list papira.

Slika 3.7. Izgled papirnatog novčanika generiranog za vlasnike Ether kriptovalute

Izvor: https://blockgeeks.com/guides/paper-wallet-guide/ (05.04.2022.)

Određene web stranice namijenjene generiranju papirnatih novčanika posjeduju funkciju ispisa QR-a koda koji omogućuje jednostavniji pristup. Generiranje papirnatog novčanika ne predstavlja trošak vlasniku, ali posjeduje neke od bitnih nedostataka s kojima se vlasnici moraju suočiti. Ako vlasnik izgubi pristup papiru na koji je prepisao svoj privatni ključ, a dogodilo se otuđenje novčanika, u potpunosti se gubi pristup kriptovalutama. Kod generiranja papirnatog novčanika, mnoge *web* stranice omogućuju spremanje papirnatog novčanika u obliku tekstualne datoteke ili slikovnog formata koji predstavlja dodatni rizik za vlasnike ako je računalo na koje je spremljena datoteka spojeno na Internet. Preporuka je da se privatni ključ papirnatog novčanika uvijek drži izvan mreže. Dodatni problemi se manifestiraju u problemu papira kao fizičkog materijala za ispis. Papir se može lako oštetiti, zapaliti ako nije spremljen na

sigurno mjesto poput sefa, kopirati odnosno fotografirati. Uz to postoji ljudska pogreška u obliku zaboravljanja lokacije na koju je on pohranjen. S ciljem zadržavanja veće sigurnosti papirnatih novčanika preporučljivo je stvaranje kopija i pohrana na više sigurnih lokacija. Dodatna mogućnost je graviranje na komad metala ili druge čvrste materijale.

Kod hladnih novčanika se može koristiti računalo koje nije spojeno na mrežu kao novčanik. Izvanmrežno potpisivanje transakcija uključuje dva računala koja dijele neke dijelove istog novčanika. Prvo mora biti isključeno s mreže zato što je to računalo na kojem se nalazi novčanik i služi za potpisivati transakcije. Drugo računalo je spojeno na mrežu i ima samo novčanik za praćenje koji služi jedino za kreiranje nepotpisane transakcije. Za ovaj tip potpisivanja transakcija postoji program **Armory**. Nakon instalacije Armory programa na izvanmrežnom računalu, stvara se novi novčanik. Po završetku se odabire lozinka i generira sigurna kopija. Pravilo Armory novčanika je da će računalo spojeno na mrežu generirati identične adrese kao i izvanmrežno računalo, ali računalo spojeno na mrežu ne može trošiti sredstva koja se nalaze na izvanmrežnom računalu. Nove transakcije se kreiraju na računalu spojenom na mrežu i pospremaju na USB prijenosnu memoriju. Transakcije se autentificiraju na izvanmrežnom računalu. Po završetku procesa, potpisana transakcija se šalje na računalo koje je spojeno na mrežu. Armory podržava samo Bitcoin kriptovalutu.

4. SIGURNOSNI PROBLEMI METODA POHRANE KRIPTOVALUTA

Nakon što su u prošlom poglavlju predstavljene metode pohrane kriptovaluta u ovom poglavlju istaknut će se neki od hakerskih napada. Napadi su bili usmjereni na metode pohrane kriptovaluta s ciljem otuđenja financijskih sredstava. 2018. godine je provedeno istraživanje koje pokazuje da je ukradeno više od 1,5 milijardi dolara[9]. Hakerski napadi i prijevare su česti, a za posljedicu znaju imati milijunske štete. U nastavku predstavit će se neki od njih.

4.1. Lažni hladni novčanici

U prethodnom poglavlju su predstavljeni hladni novčanici kao jedna od najsigurnijih metoda pohrane kriptovaluta. Iako najsigurniji, njihova pouzdanost se može iskoristiti u kriminalne svrhe. U srpnju 2020. otkriveno je da postoji sigurnosni propust na web stranici Ledger kompanije koja se bavi prodajom fizičkih novčanika za pohranu kriptovaluta. Propust seže nekoliko mjeseci unatrag u kojem razdoblju je treća neovlaštena strana prisvojila osobne podatke korisnika Ledger novčanika. Među tim podacima nalazili su se podaci o narudžbi i kontaktu vlasnika kao što su: ime i prezime, poštanska adresa, adresa e-pošte i telefonski broj. U ovom hakerskom napadu nešto više od milijun adresa e-pošte je ukradeno iz baze pretplatnika. Od toga 272 853 kupaca fizičkog uređaja izgubilo je osjetljivije podatke[10]. Kompanija Ledger je spoznajom za sigurnosni propust u svojim sustavima brzo reagirala ispravljanjem, ali se ispostavilo da hakerskom napadu nije bio kraj odnosno imao je skrivenu svrhu.

Objavljivanje kontaktnih podataka predstavlja značajan rizik jer omogućuje *phishing* napade protiv vlasnika Ledger uređaja. *Phishing* ili krađa identiteta predstavlja radnju koja započinje sa slanjem e-pošte osmišljene kako bi privukla žrtvu. Obavijest je kreirana na način kao da dolazi od pouzdanog pošiljatelja odnosno prodavača. Cilj je otuđiti osjetljive podatke kao što su podaci o bankovnim i kreditnim karticama. Ponekad se žrtvu nagovara na instalaciju zlonamjernog softvera koji ima daljnje ciljeve

---

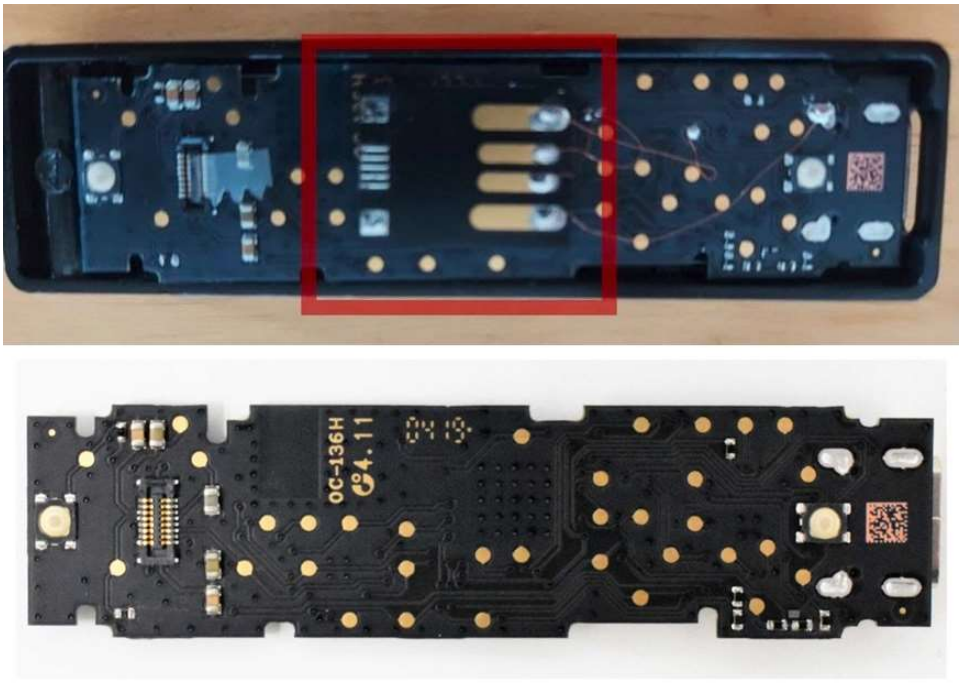
[9] Ledger. Preuzeto s: https://www.ledger.com/my-crypto-got-hacked-true-stories-about-security-breaches-leading-to-devastating-losses-and-how-these-can-be-prevented (15.3.2022.)

[10] Lawrence A. (16.6.2021). Criminals are mailing altered Ledger devices to steal cryptocurrency. *bleepingcomputer.com* Preuzeto s: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency/ (15.3.2022.)

krađe podataka. Od listopada 2020. korisnici Ledgera su žrtve phishing e-pošte u kojima se pretvaraju da obavještavaju korisnike o hakerskom napadu. Korisnici su upućeni na preuzimanje najnovije verzije Ledger Livea, aplikacije koju koriste Ledger korisnici s ciljem osiguranja novčanika novim sigurnosnim PIN brojem. Nakon preuzimanja i instalacije lažne aplikacije Ledger Live, od žrtvi se tražio unos tajne fraze i šifre za oporavak. To su informacije koje su se po izvršenju procesa slale napadačima, koji su ih upotrijebili za krađu sredstava.

Pojedinci koji su posumnjali u autentičnost *Phishing* obavijesti tj. kupci fizičkog novčanika Ledger su bili žrtve drugačijeg oblika prevare. Prevara je bila u obavijesti da Ledger želi dodatno osigurati svoje klijente koji su bili izloženi nedavnom proboju podataka šaljući im lažne uređaje. Uređaji koje su žrtve zaprimile su se nalazili u autentičnom pakiranju kojega se zaprimi pri svakoj kupnji Ledger uređaja. Razlog slanja novog uređaja je bilo sigurnosno poboljšanje fizičkog uređaja nakon krađe podataka iz srpnja 2020. Paket je sadržavao Ledger Nano X koji je izvana izgledao kao originalni Nano X. Žrtve kojima je zaprimljeni paket bio sumnjiv su se odlučile na otvaranje uređaja.

Slika 4.1. Izgled lažnog uređaja te sliku originalnog bez modifikacije.



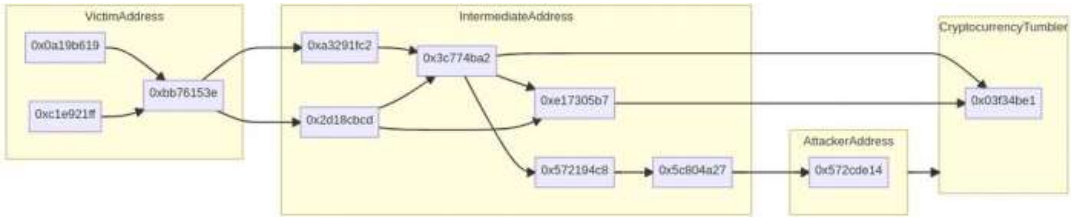
Izvor: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency/ (04.04.2022.)

Lažni uređaj je na sebi imao modifikaciju koja se sastojala od *flash* pogona spojenog na USB konektor. Upute su navodile da se novi Ledger spoji na računalo i pokrene priložena aplikacija. Pri inicijalnom pokretanju aplikacije je bilo nužno unijeti frazu za oporavak kako bi se povezao novčanik na novi Ledger uređaj. Nakon unosa fraze za oporavak, ona bi se automatizmom proslijedila napadačima, koji su ju iskoristili kako bi preusmjerili iznos s novčanika žrtve na vlastiti i tako otuđili sredstva.

4.2. Lažni vrući novčanici

Posljednjih nekoliko godina sve su učestalije prevare u obliku oglasa koji se nalaze na tražilici Google. Putem tražilice se promoviraju lažni novčanici za kriptovalute. Hakeri kreiraju lažne web stranice i aplikacije za pohranu kriptovaluta dizajnirane da nalikuju službenim. Neke od njih uključuju aplikacije iz MetaMask, Phatnom, imToken, Bitpie i Trust Wallet. Oglasi promoviraju web stranice s teško uočljivim razlikama u usporedbi sa službenim stranicama. Jedina razlika između legitimne i lažne web stranice je u drugačijim nazivima domena. Razlog zašto žrtve ne uoče razliku je u tome što se lažne web stranice najčešće pojavljuju vrlo visoko u rezultatima pretraživanja i nalikuju legitimnim verzijama. Za primjer se može uzeti stranica phantom.com. Phantom novčanik je proširenje za internetske preglednike koji nudi siguran način interakcije s više *blockchain* mreža u Solana lancu blokova. Solana je javna decentralizirana platforma koja koristi svoju valutu SOL kao sredstvo za provođenje transakcija. Hakeri su s ciljem obmane zakupili domene sa sličnim nazivima službene stranice poput “pnantom.com”, "phanton.app" ili slično. Naziv domene je jedina uočljiva razlika zato što dizajn lažne stranice kopira dizajn legitimne u njenoj cijelosti. Putem lažnih stranica žrtve su upućene na kreiranje novog novčanika, upisivanje fraze za oporavak te lozinke za pristup računu. Nakon toga se preusmjeravaju na preuzimanje službene aplikacije ili proširenja za internetski preglednik. Žrtve su upisivanjem svoje fraze za oporavak dopustile hakerima da se prijave u njihove račune te tako prenesu raspoložive iznose na druge račune. Cilj je bio prikrivanje traga.

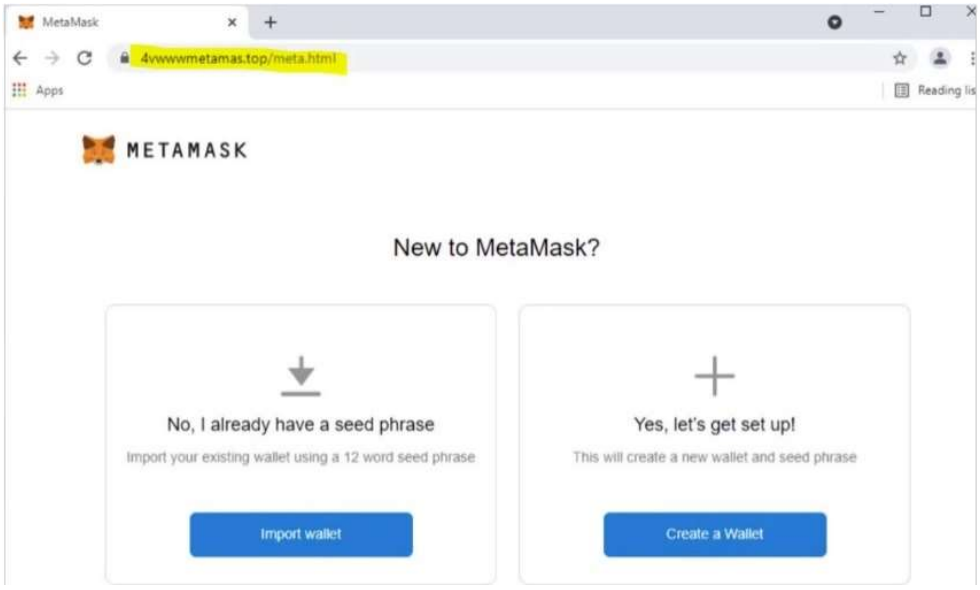
Slika 4.2. Tok prebacivanja kriptovaluta s jednog računa na drugi



Izvor: https://news.trendmicro.com/2022/01/20/watch-out-for-fake-crypto-wallet-apps-4-3m-stolen-metamask-imtoken-bitpie-trust-wallet-and-more/ (04.04.2022.)

Metamask je dodatni primjer koji je bio na meti hakera. MetaMask je vrući novčanik za kriptovalute koji se koristi za interakciju s Ethereum *blockchainom*. Omogućuje korisnicima pristup Ethereum novčaniku putem proširenja preglednika ili mobilne aplikacije za android i Apple uređaje. Tijekom 2021. pojavili su se reklamni oglasi koji su oponašali MetaMask novčanik. Hakeri su se odlučili implementirati funkciju "Uvedi novčanik", koja predstavlja krađu fraze za oporavak žrtve.

Slika 4.3. Lažna stranica "metamas"



Izvor: https://www.bleepingcomputer.com/news/security/metamask-phishing-steals-cryptocurrency-wallets-via-google-ads/ (04.04.2022.)

Nakon što je hakerima osiguran pristup novčaniku žrtve, haker može raspoložive kriptovalute prenijeti na više novčanika za jednokratnu upotrebu kako bi prikrio trag. Nakon višestrukih prijenosa, sredstva se podijele između nekoliko novčanika kako bi se dodatno izgubio svaki trag izvornog iznosa.

Trend Micro, kompanija koja pruža usluge u kibernetičkoj sigurnosti, tijekom 2021. je provela istraživanje tržišta na temu lažnih novčanika, proširenja za internetske preglednike i aplikacija za pohranu kriptovaluta. Otkriveno je da je otprilike 4,3 milijuna dolara ukradeno putem lažnih novčanika[11]. Budući da hakeri koriste više novčanika i razne metode kako bi sakrili trag, vrijednost ukradenih kriptovaluta prema procjenama nadilazi 4,3 milijuna dolara. Uz ukradeni iznos otkriveno je približno 250 lažnih aplikacija za kripto novčanike.

4.3. Napad prašine

Napad zaprašivanja ili prašine (eng. *dusting attack*) pripada u jednu od zlonamjernih aktivnosti koje hakeri provode kako bi otuđili podatke vlasnika kriptovaluta. Prašina se u svijetu kriptovaluta odnosi na najmanju količinu određene valute koja se može poslati na druge adrese novčanika za pohranu kriptovaluta. Najmanja vrijednost kod primjera kriptovalute Bitcoin iznosi 0,00000001 BTC iliti takozvani 1 Satoshi. Iznosi od nekoliko stotina Satoshija najčešće ostanu na računima kupaca ili prodavača nakon izvršenja transakcije pri trgovanju s kriptovalutama. Srž prašine je u iznosu koji je toliko mali da je manji od većine transakcijskih naknada pa je i s time neprimjetan većini korisnika.

Napad se izvršava tako da žrtva zaprimi teško uočljive jedinice kriptovaluta u novčanik s ciljem krađe njihovih osobnih podataka. Ovakav priljev u novčanik žrtve hakeru može omogućiti pristup osobnim informacijama putem zlonamjernih programa. Ako žrtva potroši zaražene jedinice, haker može iskoristiti zlonamjerni program za analizu transakcije koji otkriva povijest transakcija novčanika. Nakon toga se provodi analiza različitih adresa kako bi se identificirale koje od njih pripadaju istom novčaniku žrtve. Cilj je povezati adrese s novčanicima odnosno s njihovim vlasnicima. Ako uspiju u povezivanju, hakeri mogu iskoristiti dobivene informacije u daljnjim napadima poput *phishing*a ili *ransomware* odnosno iznude.

Kako bi se spriječilo slanje teško uočljivih jedinica neke kriptovalute predstavljena je granica prašine (eng. *dust threshold*). Ona predstavlja prašinu koja je preostala te nije dovoljna za dovršetak druge valjane transakcije. Većina vrućih novčanika ima

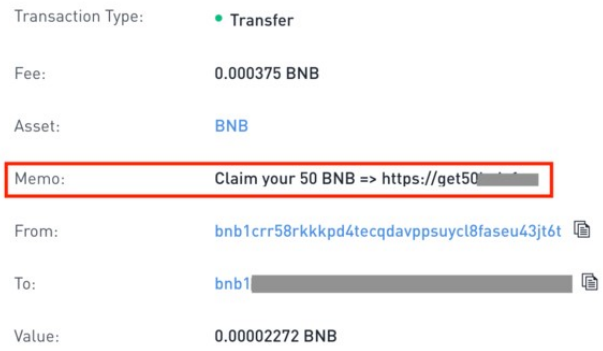
[11]Trendmicro.com. Watch Out for Fake Crypto Wallet Apps, $4.3M Stolen — MetaMask, imToken, Bitpie, Trust Wallet, and More!. Preuzeto s https://news.trendmicro.com/2022/01/20/watch-out-for-fake-crypto-wallet-apps-4-3m-stolen-metamask-imtoken-bitpie-trust-wallet-and-more/ (04.04.2022.)

ograničenje transakcije u vrijednosti od 546 satoshija (0,00000546 BTC). Iznos od 546 satoshija znači da će svaka transakcija manja ili ista kao 546 satoshija smatrati neželjenom te neće završiti provjeru autentičnosti. S ciljem izbjegavanja granice prašine mnogi hakerski napadi sačinjavaju veće iznose kako bi transakcija bila uspješna.

Prvi zabilježeni napad prašine se dogodio na korisnicima kriptovalute Litecoin 2018. godine. Davatelj usluge vrućeg novčanika Samourai Wallet, obavijestio je svoje korisnike da bi mogli biti izloženi napadima zaprašivanja ako zaprime male količine Bitcoina ili drugih Altcoina[12]. Budući da su primljene jedinice "zaražene" Samourai je uveo funkciju "Ne troši" koja omogućuje korisniku da odabere transakciju odnosno sumnjiv iznos koji je zaprimio na svoj novčanik. Uz to implementirana je funkcija prijavljivanja sumnjivih transakcija. Glassnode, davatelj usluge *blockchaina* i obavještajnih podataka koji razvija alate za dionike koji posjeduju digitalnu imovinu, 15. kolovoza 2019. godine putem društvenih mreža je otkrio da su 294.582 adrese novčanika zahvaćene napadima zaprašivanja[13]. Sličan napad dogodio se u listopadu 2020. kada su hakeri proveli novu vrstu napada zaprašivanja na Binance Chain (BC)[14]. Poslali su male količine kriptovalute Binance Coina (BNB) na veću količinu adresa, ostavljajući komentar unutar transakcije koji je bio poveznica na zlonamjernu web stranicu. Poveznica je obećavala žrtvama određeni iznos pod izlikom osvojene nagrade.

[12] Twitter.com. Preuzeto s: https://twitter.com/samouraiwallet/status/1055345822076936192 (04.04.2022.)
[13] Twitter.com. Preuzeto s: https://twitter.com/glassnode/status/1162024332740235264 (04.04.2022.)
[14] Twitter.com. Preuzeto s: https://twitter.com/binance/status/1318899571855138817?lang=en (04.04.2022.)

Slika 4.4. Komentar s poveznicom unutar izvršene transakcije



Izvor: https://academy.binance.com/en/articles/what-is-a-dusting-attack (04.04.2022.)

Kod napada zaprašivanja važno je naglasiti da napad ne prenosi prava nad novčanikom žrtve odnosno ne prenosi kontrolu nad njihovom imovinom. Nove mjere koje implementiraju brojne kompanije koje pružaju usluge pohrane kriptovaluta značajno su smanjile mogućnost zaprašivanja. Svrha ove vrste napada je deanonimizirati žrtvu kako bi se prikupilo dovoljno informacija za daljnje napade.

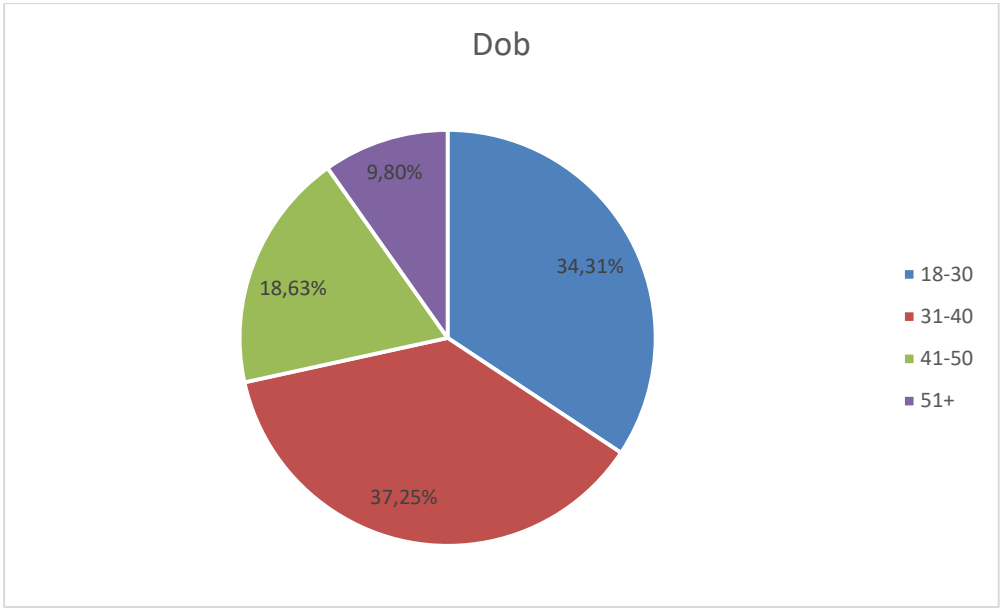
5. ISTRAŽIVANJE O METODAMA POHRANE KRIPTOVALUTA

U ovom poglavlju bit će prikazano istraživanje na temu metoda pohrane kriptovaluta. Cilj istraživanja je bio prikupiti dovoljan broj odgovora kako bi se utvrdilo koje metode pohrane vlasnici koriste, koje smatraju sigurnijima i zašto, te imaju li dodatnih primjedbi i prijedloga. U prvom potpoglavlju će se grafički prikazati rezultati i opisno interpretirati njihovo značenje. U drugom potpoglavlju će se na temelju prikupljenih podataka i pomoću dubinske analize donijeti zaključci s ciljem dobivanja odgovora na istraživačka pitanja. Upitnik se sastoji od 20 pitanja, od čega petnaest zatvorenog i pet otvorenog tipa. Prva dva pitanja postavljena su u svrhu dobivanja boljeg uvida u ispitanike (spol i dob). Anketni upitnik su ispunila 102 ispitanika. Ispitanicima se pristupilo objavljujući anketu na forumima koji su namijenjeni internetskim tehnologijama. Rezultati istraživanja prikazani su u nastavku.

5.1. Prikaz i interpretacija rezultata istraživanja

Prvo pitanje se odnosilo na spol ispitanika. Ponuđeni su odgovori „muško“ i „žensko“. Anketu koju su ispunila 102 ispitanika od toga 88 muškaraca (86,27%) i 14 žena (13,73%).

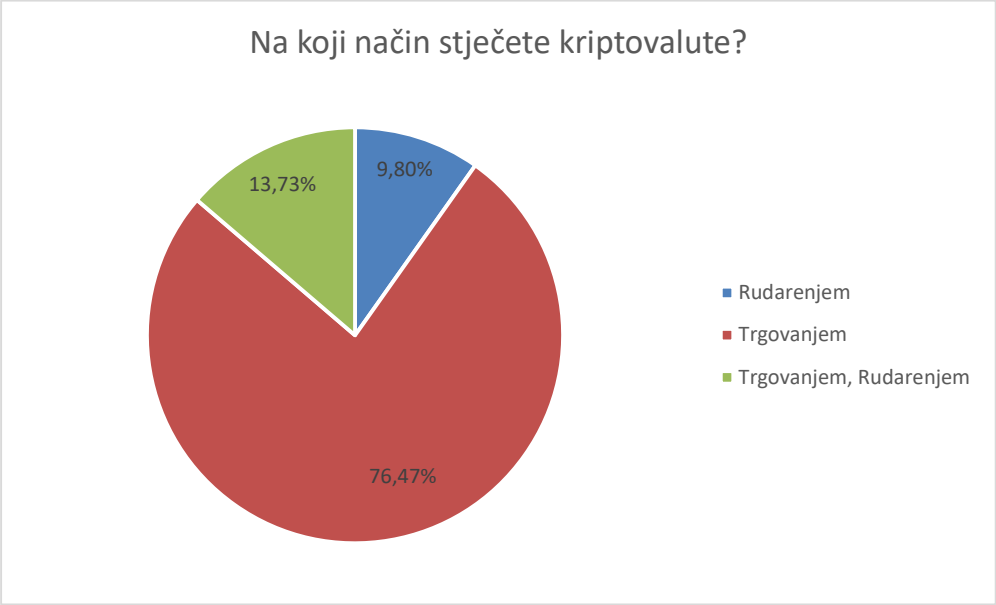
Slika 5.1 Dob ispitanika



Izvor: Rad autora

Drugim se pitanjem željela saznati dob ispitanika. Dob ispitanika razvrstana je u četiri skupine: od 18 do 30, od 31 do 40, od 41 do 50 i 51 ili više godina. Analiza starosti ispitanika je važna kako bi se utvrdilo koje dobne skupine daju veću pozornost sigurnosti metoda pohrane kriptovaluta. Obradom podataka dolazimo do informacije da su u anketiranom uzorku prve dvije skupine prema dobi podjednako bile zastupljene. S dobi od 18 do 30 godina je bilo ukupno 35 ispitanika (34,31%), a 38 ispitanika (37,25%) je bilo u dobi od 31 do 40 godina. 19 ispitanika (18,63%) je bilo u dobi od 41 do 50 godina. Najmanji broj je bio u dobi od 51 ili više s 10 ispitanika (9,80%) koji su bili dovoljni kako bi se stekao adekvatan broj iz svih dobnih skupina.

Slika 5.2. Način na koji ispitanici stječu kriptovalute

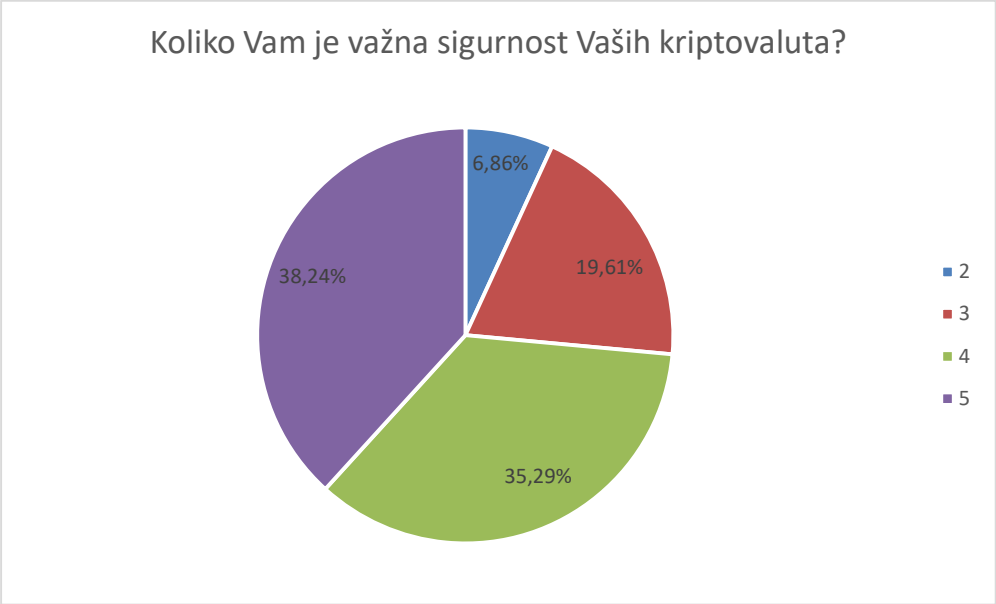


Izvor: Rad autora

S trećim pitanjem se željelo provjeriti na koji način ispitanici stječu kriptovalute. Ponuđen je višestruki odabir: „rudarenjem“, trgovanjem“ ili kombinirano „trgovanjem i rudarenjem“. Kod odabira „trgovanjem“ podrazumijevali su se svi načini koji ne spadaju pod rudarenje: kupnja, prihvaćanje kriptovaluta kao način plaćanja, donacije, programi preporučivanja, gledanje oglasa itd. Rudarenje je podrazumijevalo samostalno rudarenje ili zakup računala za rudarenje kriptovaluta. Pomoću ovoga pitanja željela se dobiti informacija o podjeli ispitanih odnosno koji uzorak koristi kombinirani način stjecanja koji će kasnije u istraživanju dati detaljniju informaciju o

metodi pohrane koju koriste. Pomoću pitanja u nastavku će se dodatno provjeriti koje davatelje usluge kripto novčanika koriste određene skupine ispitanika prema načinu stjecanja. Od 102 ispitanika, 10 (9,80%) ih stječe kriptovalute samo rudarenjem što predstavlja zadovoljavajući i očekivani broj budući da rudarenje zahtjeva određene dodatne angažmane. 14 ispitanika (13,73%) stječe kriptovalute na oba načina trgovanjem i rudarenjem. Najviše ispitanika stječe kriptovalute trgovanjem s 78 odgovora (76,47%) što nije neočekivano zbog relativno jednostavnog procesa stjecanja.

Slika 5.3. Važnost sigurnosti kriptovaluta

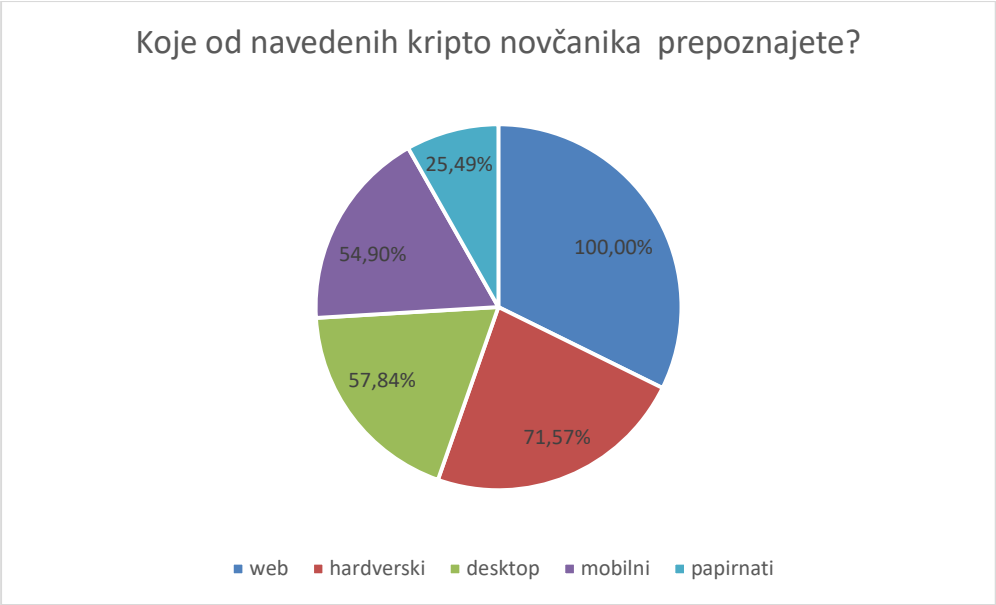


Izvor: Rad autora

Iduće pitanje u anketi je postavljeno s ciljem utvrđivanja važnosti sigurnosti kriptovaluta. Ispitanici su u skali od 1 do 5 tj. nimalo važna do vrlo važna, mogli označiti važnost koju daju sigurnosti svojih kriptovaluta. Sigurnost kriptovaluta je „vrlo važna“ za 39 ispitanih (38,24%) dok je „važna“ za njih 36 (35,29%). S „relativno važna“ odnosno ocjenom 3 odgovorilo je 20 ispitanika (19,61%). 7 ispitanika (6,86%) je odgovorilo da im je sigurnost kriptovaluta „dovoljno važna“. Potrebno je napomenuti da odabir „nimalo važna“ nije dobila odgovore. Analizirajući rezultate dolazi se do zaključka da je većini ispitanika sigurnost kriptovaluta poprilično važna s ukupno 75 tj.

73,5% (ocjene 4 i 5). S ciljem dobivanja izraženijeg zaključka o podjeli ispitanika koji su odgovorili na ovo pitanje s 4 i 5, u potpoglavlju 5.2. je provedena dubinska analiza podataka.

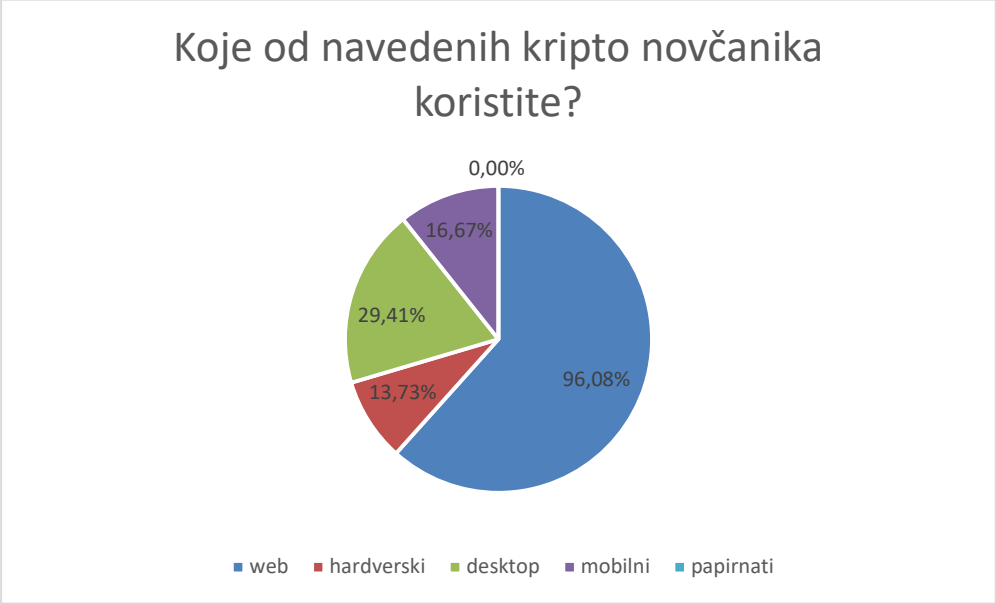
Slika 5.4. Prepoznati kripto novčanici



Izvor: Rad autora

S petim pitanjem se željelo provjeriti koliko su ispitanici upoznati s metodama pohrane kriptovaluta odnosno kripto novčanicima. U ovom pitanju navedeno je svih pet vrsta kripto novčanika koje su ispitanici mogli odabrati uz mogućnost višestrukog odabira: mobilni novčanik, desktop novčanik, web novčanik, papirnati novčanik i hardverski novčanik. U anketiranom uzorku svih 102 ispitanika (100%) su izjavili da su prepoznali web novčanik. Činjenica da su svi ispitanici prepoznali web novčanik nije nelogična budući da se većina bavi trgovanjem kao načinom stjecanja kriptovaluta. Hardverski novčanik je pozicioniran na drugom mjestu s 73 odgovora (71,57%). Nakon hardverskog slijedi desktop novčanik s 59 odgovora (57,84%) kojemu je najbliže bio mobilni novčanik s 56 odgovora (54,90%). Unutar anketiranog uzorka najmanje je bio prepoznat papirnati novčanik s 26 odgovora (25,49%).

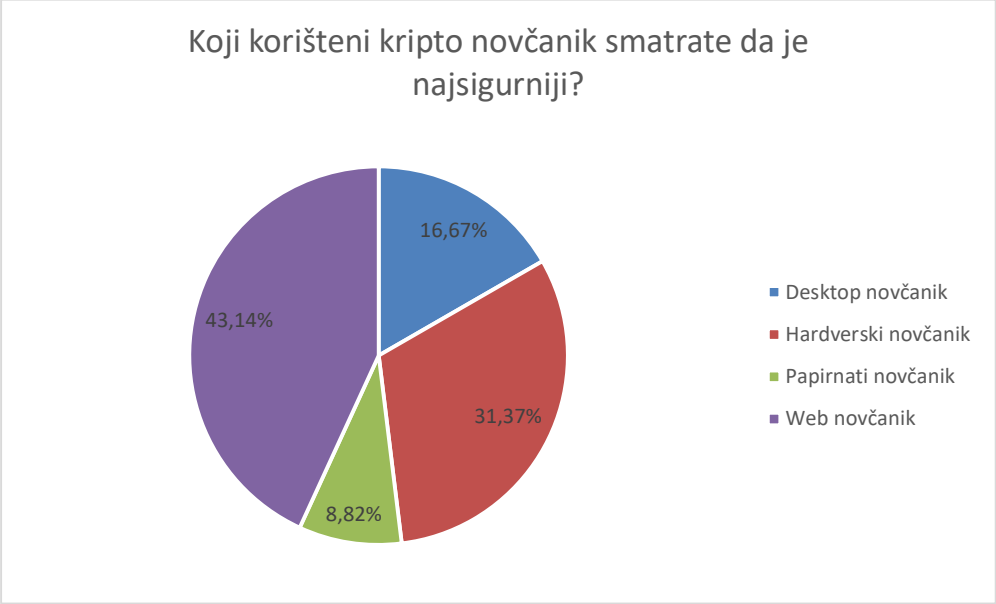
Slika 5.5. Korišteni kripto novčanici



Izvor: Rad autora

Nakon novčanika koji su prepoznati od strane ispitanika, ispitanici su trebali odgovoriti na pitanje koji od kripto novčanika koriste. Odgovori su bili višestrukog odabira kako bi ispitanici mogli odabrati one novčanike koje koriste. Ovo pitanje je pružilo uvid u omjer između novčanika koji su ispitanici izjavili da su prepoznali i koristili. S grafa se može vidjeti da je najkorišteniji kripto novčanik na anketiranom uzorku bio web novčanik s 98 odgovora (96,08%). Dobiveni podatak nije neuobičajen budući da su svi ispitanici prepoznali web novčanik kao metodu pohrane. Dodatno većina ispitanika stječe kriptovalute trgovanjem. Slijedi ga desktop novčanik na drugom mjestu s 30 odgovora (29,41%). Podjednako je bio zastupljen mobilni novčanik s 17 odgovora (16,67%) i hardverski novčanik s 14 odgovora (13,73%). Uvidom u prošli graf može se vidjeti da 26 ispitanika koji su izjavili da su upoznati s papirnatim novčanikom kao metodom pohrane, dotičnoga nisu koristili. Ovim odgovorom je vidljivo da papirnati novčanici nisu dovoljno promovirani i naglašavani kao sigurna metoda pohrane kriptovaluta.

Slika 5.6. Omjer sigurnosti kripto novčanika



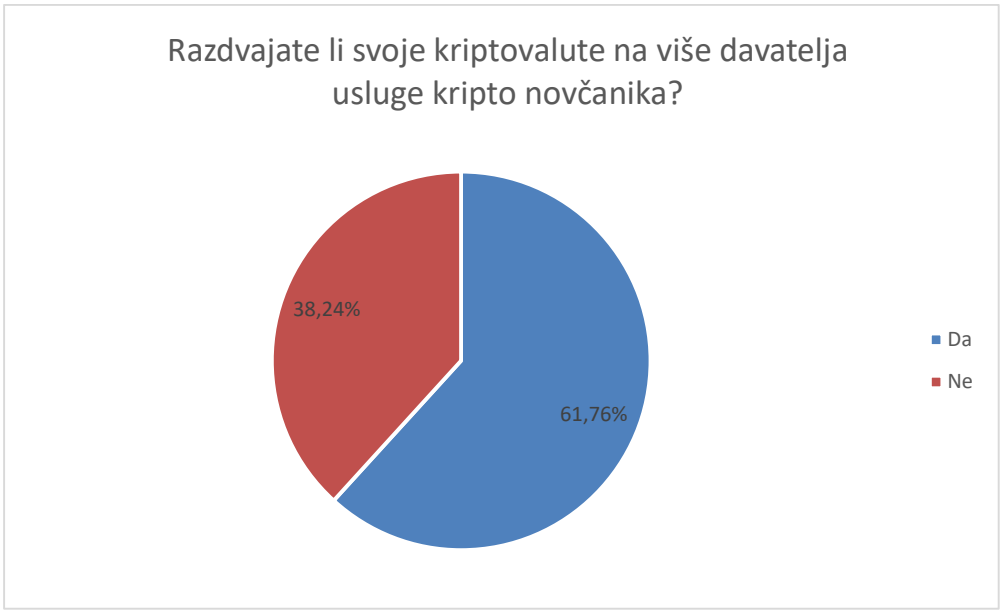
Izvor: Rad autora

S ciljem provjere oscilacija između poznatih i korištenih novčanika, postavljeno je pitanje koje traži da se s popisa novčanika odabere samo jedan za kojega se smatra da je najsigurniji. Svrha pitanje je bila pronaći najsigurniji novčanik prema ispitanicima, ali i ustanoviti koliki je broj odgovora koji se razlikuju. Ovo pitanje će pružiti bolji uvid u skupine ispitanih ovisno o načinu stjecanja kriptovaluta. Najpouzdaniji ili bolje rečeno najsigurniji kripto novčanik prema dobivenim podacima je web novčanik s 44 odgovora (43,14%). Pretpostavka je da ispitanici svoje povjerenje pružaju davateljima usluge web novčanika koji putem marketinških kampanja najčešće reklamiraju visoku sigurnost kriptovaluta. Drugi najsigurniji novčanik prema ispitanicima je hardverski novčanik s 32 odgovora (31,37%). Desktop novčanik je dobio 17 odgovora (16,67%) te je pozicioniran na treće mjesto prema sigurnosti. Odgovor „papirnati novčanik“ se spominje ukupno 9 puta (8,82%). Iako je papirnati novčanik u praksi jedan od najsigurnijih kripto novčanika, činjenica da ga je prepoznalo samo 26 ispitanika od kojih ga nijedan ne koristi i da njegova sigurnost ovisi o ljudskom faktoru, nije neobično da nije ostvario veću pouzdanost od strane ispitanih. Iako je veliki broj ispitanika izjavio da prepoznaje mobilni novčanik, ispitanici se nisu pouzdali u njegovu sigurnost budući da nije označen u nijednom odgovoru. Pretpostavka je nedovoljno poznavanje

mobilnog novčanika koji koristi identične funkcionalnosti kao web novčanik.

Ako su ispitanici odgovorili da se kripto novčanik kojega koristite razlikuje od onoga za kojega smatraju da je najsigurniji, upitani su zašto ne koriste sigurniju metodu pohrane. Analizom je utvrđeno 31 odgovor u kojem se koristeni i najsigurniji novčanik razlikuju. Odgovori su najčešće podrazumijevali odgovore iz prethodnog pitanja da su najsigurniji hardverski i papirnati novčanici. Obradom podataka u nastavku su prikazani najčešći odgovori zašto pojedini ispitanici ne koriste sigurniji kripto novčanik. Najčešći prigovori za nekorištenje hardverskih novčanika su bili: cijena, gubitak uređaja, nepraktičnost fizičkog uređaja, dugovječnost baterije, činjenica da ispitanici preferiraju digitalni oblik novčanika i jednostavnije korištenje putem web sučelja. Za papirnate novčanike se podrazumijevala činjenica dugovječnosti papira kao materijala za ispis, zaboravljena lokacija pohrane, gubitak ili otuđenje i cijena u slučaju ispisivanja podataka na metale s ciljem očuvanja dugovječnosti itd. Pomoću ovog pitanja dolazimo do informacije da 69,60% ispitanih koristi novčanik koji istovremeno smatraju najsigurnijim.

Slika 5.7. Omjer razdvajanja kriptovaluta

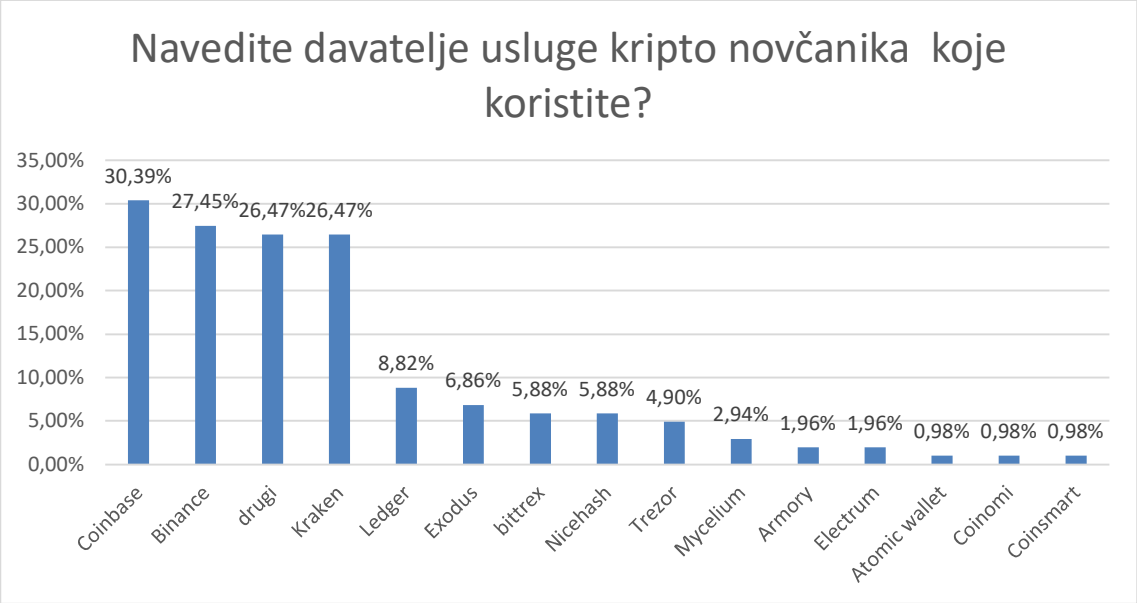


Izvor: Rad autora

Iduće pitanje utvrđuje razdvajaju li ispitanici svoje kriptovalute na više kripto

novčanika. Budući da je pitanje povezano sa sigurnošću kriptovaluta ono predstavlja veliku važnost za daljnju analizu podataka. Ponuđeni odgovori su „da“ i „ne“. Od ukupnog uzorka 63 ispitanih (61,76%) razdvaja svoje kriptovalute dok preostalih 39 (38,24) ne.

Slika 5.8. Davatelji usluge kripto novčanika

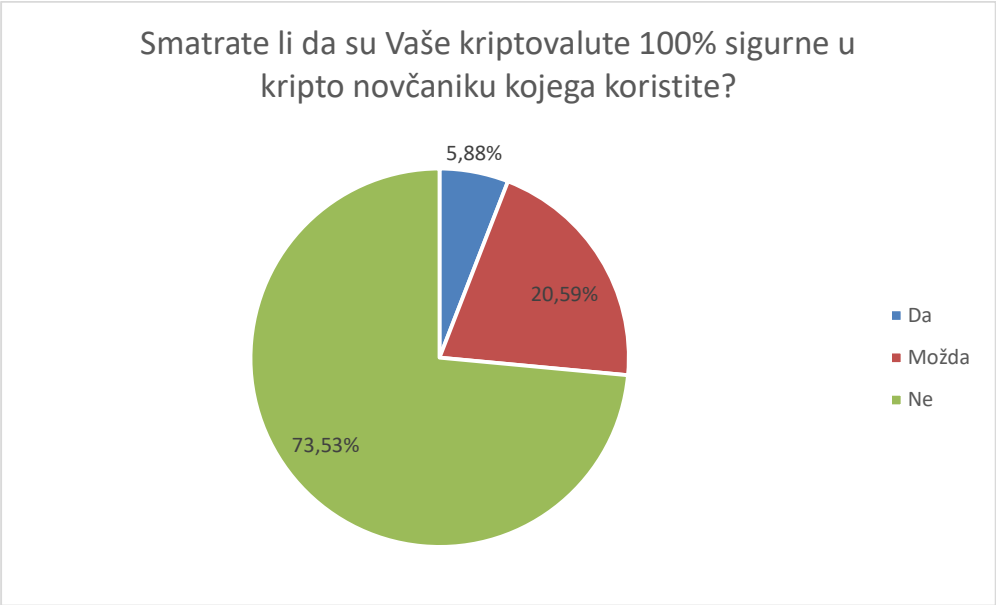


Izvor: Rad autora

Nakon pitanja s poznavanjem i korištenjem kripto novčanika, dolazi se do pitanja koji nudi slobodan unos odgovora. Od ispitanika se traži da navedu davatelje usluge kripto novčanika koje koriste. Svrha pitanja je utvrditi najkorištenijeg davatelja usluge unutar ispitivanog uzorka. Analizirajući odgovore, odgovori su podijeljeni u nekoliko skupina. S priloženog grafa se može razaznati da s 30,39% prevladava davatelj usluge web novčanika Coinbase. Drugi najkorišteniji davatelj usluge je bio Binance s 27,45%. Ostali davatelji usluge kripto novčanika u koje mogu spadati sve vrste kripto novčanika su korišteni od strane 26,67% ispitanih. Neki od njih su: Ambire wallet, MyEther wallet, BitGo, Jaxx, Omniwallet, Metamask, Trust Wallet, Block.io wallet itd. Uzorak od 26,47% ispitanih koristi Kraken. Iako je Coinbase bio najkorišteniji može se zaključiti da je prvih četiri odgovora tj. davatelja usluge bilo podjednako korišteno. Ovaj rezultat

nije neočekivan budući da su prema drugim istraživanjima navedeni davatelji usluge u vrhu prema broju korisnika. Uz to može se zaključiti da većina ispitanika osim najpopularnijih davatelja usluge koristi i manje poznate. Pretpostavka za navedeno su manje poznate kriptovalute odnosno kripto tokeni koji uglavnom koriste vlastite kripto novčanike kao jedina metoda pohrane. Kao predstavnika hardverskih novčanika, Ledger koristi 8,82% dok Trezor 4,90% ispitanih. Ostali davatelji usluge koji nisu bili svrstani unutar „drugi“ su korišteni kod uzorka manjim od 10% ispitanih.

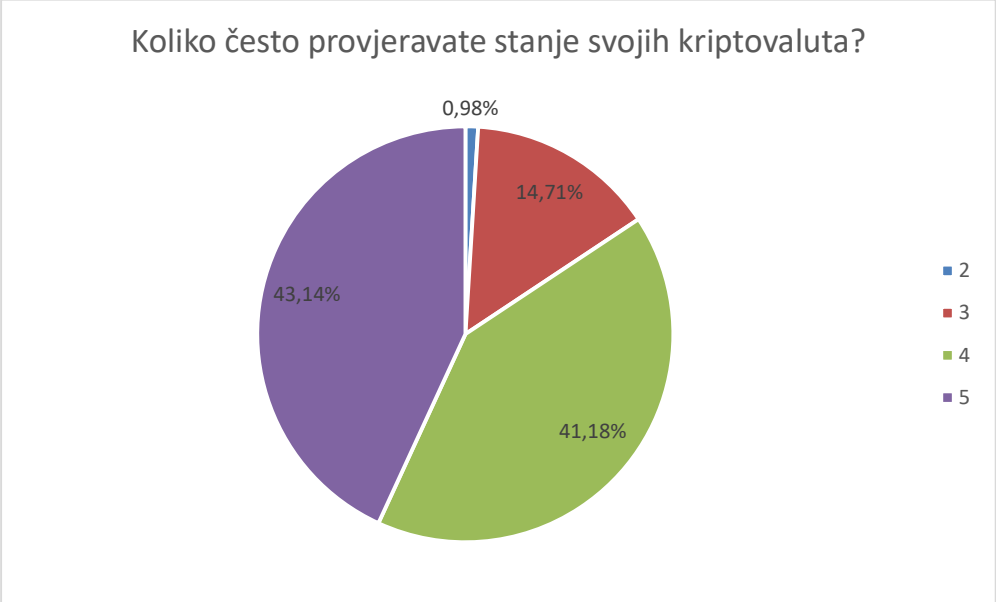
Slika 5.9. Sigurnost kripto novčanika



Izvor: Rad autora

Iduće pitanje traži od ispitanih mišljenje smatraju li da su njihove kriptovalute 100% sigurne u kripto novčanicima koje koristite. 75 ispitanika (73,58%) je odgovorilo da smatra da njihove kriptovalute nisu 100% sigurne. Odgovori ispitanih predstavljaju logičan zaključak zato što ni jedna od vrsta kripto novčanika, ali ni davatelja usluge ne može osigurati 100% sigurnost. Ljudske greške uključuju značajan faktor koji može utjecati na sigurnost. 21 ispitanika (20,59%) je izjavilo „možda“. Preostalih 6 ispitanika (5,88%) je izjavilo da smatraju da su njihove kriptovalute u potpunosti sigurne.

Slika 5.10. Učestalost provjere stanja kriptovaluta



Izvor: Rad autora

Svrha sljedećeg pitanja je utvrditi koliko često ispitanici provjeravaju stanje svojih kriptovaluta. Odgovori su bili mogući u rasponu od 1 do 5. Odgovor 1 predstavlja nikada, 2 rijetko, 3 ponekad, 4 relativno često i 5 vrlo često. Budući da je ovo pitanje povezano sa sigurnošću kripto novčanika ono predstavlja veliku važnost za daljnje zaključke. S grafa se može vidjeti da najviše ispitanika, njih 44 (43,14%) vrlo često provjerava svoje kripto novčanike. Slijedi ga „relativno često“ s 42 odgovora (41,18%). Kada se odgovori promatraju kombinirano (vrlo često i relativno često) slijedi činjenica koja ne odudara od odgovora dobivenih u četvrtom pitanju u kojemu je većina ispitanika izjavila da im je sigurnost kriptovaluta poprilično važna. Ponekad stanje provjerava 15 ispitanika (14,71%). Najmanje je bio odabran „rijetko“ s jednim odgovorom. „Nikada“ nije dobio odgovor što predstavlja zadovoljavajuću informaciju. Zaključak ovog pitanja se može interpretirati u činjenici da kombinirano 86 ispitanika često provjerava svoje kripto novčanike.

Slika 5.11. Važnost jednostavnosti korištenja kripto novčanikom

Izvor: Rad autora

Iz prijašnja dva pitanja se može vidjeti da većina ispitanika ne smatra da su njihove kriptovaluta 100% sigurne te redovito pregledavaju stanje kriptovaluta. Svrha ovoga pitanja je bila utvrditi koliko je važna jednostavnost korištenja novčanikom za ispitanike. Jednostavno korištenje podrazumijeva pregledno grafičko sučelje i intuitivne funkcionalnosti. U rasponu od 1 do 5 odnosno od „nije bitno“ do „jako bitno“ ispitanici su mogli pružiti odgovore na pitanje. S „nije bitno“ je odgovorilo 13 ispitanika (12,75%). 43 ispitanika (42,16%) su odgovorili da im jednostavnost korištenja novčanikom predstavlja malu značajnost tj. odgovor „ uglavnom bitno“. S „bitno“ je odgovorilo 36 ispitanika (35,29%). 9 ispitanika je izjavilo da je jednostavnost relativno bitna odnosno ocjena 4. Samo jedan ispitanik je odgovorio da jednostavnost korištenja jako bitna. Kombinirano 54,91% ispitanika jednostavnost korištenja ne predstavlja nužnost za odabir novčanika.

Iduća tri pitanja u anketi postavljena su u svrhu dobivanja informacija o zadovoljstvu korištenja kripto novčanika kojega su ispitanici naveli.

Četrnaesto pitanje od ispitanika je zahtijevalo da obrazlože zašto koriste odabrane novčanike. Ispitanici su imali omogućen slobodan unos odgovora. U nastavku su

navedeni neki od odgovora:

- „Dobio sam preporuku pa sam odlučio isprobati ovaj novčanik.“
- „Istražio sam ponudu web novčanika. Nakon analize nekoliko članaka odlučio sam se za korištenje Coinbase novčanika.“
- „U nekom od izdanja BUG časopisa sam pročitao listu poznatih crypto novčanika. Između nekoliko njih sam se odlučio za njih dva koja najbolje odgovaraju mojim potrebama. Koristim Kraken za pristupanje putem browsera, dok Trezor za vanjsku pohranu kriptovaluta.“
- „Na preporuku kolega s posla sam se odlučio za rudarenje putem Nicehash programa koji uz mogućnost rudarenja ima mogućnost pohrane kriptovaluta u svojem novčaniku.“
- „Dobar dizajn kojega prati korisno i jednostavni GUI na mobitelu koje mi omogućava jednostavni pregled stanja kriptovaluta i njihovih kretanja u cijeni.“
- „Koristim Ledger novčanik kojega sam kupio na popustu budući da nemam povjerenja u korporacije koje bez moga znanja mogu imati uvid i pristup mojem novčaniku. Nadam se da će me uređaj dugo služiti u idućim godinama. Sviđa mi se što je prijenosan, lagan i može se spremiti u svaki džep.“
- „Visoka sigurnost, veliki broj kriptovaluta, ugrađena baterija, bluetooth.“
- „Jednostavan za korištenje.“
- „Brzo i jednostavno sam podesio račun, postavke, sigurnosne značajke.“

Iduće pitanje od ispitanika tražilo je da navedu nedostatke kod korištenih novčanika. Ispitanici su imali omogućen slobodan unos odgovora. U nastavku su prepisani i parafrazirani neki od odgovora:

- „Bilo mi je nužno kupiti hladni novčanik pa ne znam jesam li kupio odgovarajući za moje potrebe budući da sam ga skupo platio.“
- „Na mobilnoj verziji je čudno i neorganizirano sučelje koje zamara otvaranjem dodatnih menija i pod menija.“
- „Pročitala sam da su imali propust i gubitak osobnih podataka pa me brinu

potencijalni novi propusti koji mogu ovaj put i mene zadesiti.“

- „Koristio sam desktop novčanik na kojemu mi je bilo spremljeno oko 10 000$. Hard disk mi se počeo kvariti pa sam se zabrinuo za uložene kriptovalute koje sam morao prebaciti i raspodijeliti zbog sigurnosti na Binance, Kraken i Coinbase.“
- „Brine me sigurnost kriptovaluta. Zbog toga kombiniram Ledger i Binance.“
- „Ne volim transakcijske naknade.“
- „Koristim Electrum. Ne sviđa mi se što novčanik nema korisničku podrške putem chat bota ili emaila. Uz to podržava samo bitcoin.“
- „Loše organizirani meniji koji ponekad zbunjuju. Podržava samo najpopularnije kriptovalute.“
- „Nedostatak dvije faktorske autentifikacije“
- „Zamijenio sam mobitel na Iphone 12 da bi shvatio da iOS ne podržava moj novčanik.“

Sljedeće pitanje pruža mogućnost ispitanicima da se izjasne koje nedostatke bi promijenili kod korištenog kripto novčanika. Ako su imali ideje, primjedbe ili želje omogućen im je slobodan unos**.** U nastavku su prepisani i parafrazirani neki od odgovora:

- „Bolja sigurnost kriptovaluta. Želim uvođenje 2FA.“
- „Bolji dizajn mobilne aplikacije koji je jako zbunjujući.“
- „Samostalna zamjena baterije u Ledger uređaju budući da ga ne želim bacati u smeće kada bateriji prođe rok trajanja.“
- „Volio bih imati mogućnost prikaza ukupne svote koju sam potrošio na sve transakcijske naknade te koliko je uopće bilo transakcija u godini dana.“
- „Bolja korisnička podrška od strane davatelja usluge. Imao sam slučaj u kojemu sam zaboravio lozinku novčanika, a šifra za oporavak novčanika koja je došla na mail adresu nije funkcionirala. Cijeli proces je trajao nekoliko dana, što je u međuvremenu dovelo do većih promjena u vrijednosti mojega novčanika pa

nisam uspio prodati odnosno kupiti na vrijeme.“

- „Koristim Ledger kojemu će prije ili kasnije riknuti baterija. Volio bih da već postojeći kupci imaju barem 20% popusta na novi uređaj. Kako bi bili u doticaju s ekološkim promjenama bilo bi super da pri vračanju uređaja kupac ostvari još veći popust.“

Slika 5.12. Omjer spremnosti za plaćanje usluge 100% sigurnosti kriptovaluta

Izvor: Rad autora

Sedamnaesto pitanje je glasilo: „Biste li plaćali pretplatu na uslugu koja promovira 100% sigurnost kriptovaluta?“. Svrha ovoga pitanja je bila provjera jesu li ispitanici spremni plaćati mjesečnu pretplatu na uslugu koja bi nudila zaštitu od svih potencijalnih hakerskih napada. Mogući odgovori su bili „da“, „ne“ i „možda“. Ovo pitanje je važno za dubinsku analizu podataka s ciljem utvrđivanja koje skupine ispitanika su odlučnije za korištenje usluge. 27 ispitanika (26,47%) je odgovorilo da ne bi plaćali uslugu. S „možda“ su odgovorila 42 ispitanika (41,18%). Preostalih 33 ispitanika (32,35%) su odgovorili da bi plaćali uslugu kompletne zaštite kriptovaluta. Kombinirano „možda“ i „da“ tj. 75 ispitanika su upućeni na sljedeće pitanje.

Slika 5.13. Raspon vrijednosti usluge 100% sigurnosti kriptovaluta

Izvor: Rad autora

Kao nastavak na prethodno pitanje, ako su ispitanici na prethodno pitanje odgovorili s „da“ ili „možda“, pozvani su da odgovore na dodatno pitanje. Od ispitanika se tražilo da odluče u kojem rasponu bi bili spremni platiti uslugu 100% učinkovite sigurnosti njihovih novčanika odnosno kriptovaluta. Mogući rasponi su bili: od 5 do 10 dolara, od 11 do 25 dolara, od 26 do 50 dolara i više od 50 dolara. Većina ispitanika 41 (54.67%) je spremna platiti uslugu u rasponu od 5 do 10 dolara. Drugi vrijednosni raspon 11 do 25 dolara je prihvatljiv za 29 ispitanika (38,67%). Raspon od 26 do 50 dolara je razuman za samo 4 ispitanika (5,33%). Jedan ispitanik je odgovorio da je spreman plaćati više od 50 dolara za 100% sigurnost kriptovaluta. Iz utvrđenog se može vidjeti da zadnja dva vrijednosna raspona ne bi ostvarili značajniju količinu pretplatnika. Pretpostavka je da je većina korisnika naviknuta na besplatno korištenje novčanicima i jedino na plaćanje transakcijskih naknada. Ovo pitanje je važno kod dubinske analize podataka kako bi se utvrdilo koje dobne skupine su spremnije platiti više za bolju sigurnost kriptovaluta. Također se postavlja pitanje jesu li ispitanici koji stječu kriptovalute rudarenjem spremni plaćati uslugu i u kojem rasponu budući da pretežito takvi ispitanici imaju mogućnost vlastite odgovornosti nad kriptovalutama pomoću

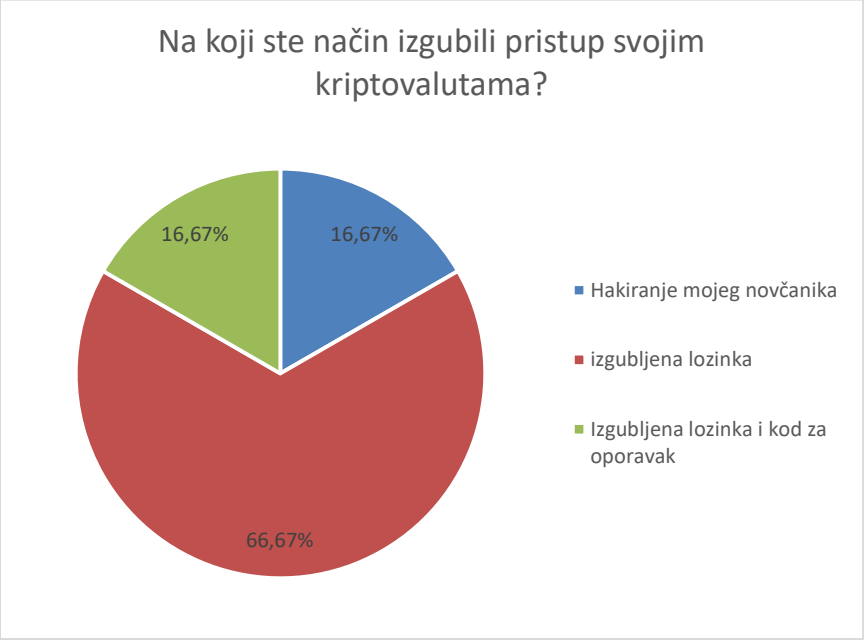
hladnih novčanika.

Slika 5.14. Omjer izgubljenih pristupa kripto novčaniku

Izvor: Rad autora

Sljedeće pitanje je tražilo od ispitanika informaciju jesu li ikada izgubili pristup svojim kripto novčanicima. Ponuđeni odgovori su „da“ i „ne“. Iz prikazanog grafa se vidi da većina ispitanika odnosno 88,24% nije izgubila pristup novčaniku. 12 ispitanika su na određeni način koji je utvrđen idućim pitanjem izgubili pristup novčaniku. Pitanje će služiti u dubinskoj analizi s ciljem provjere jesu li ispitanici koji su odgovorili da im je sigurnost kriptovaluta „izrazito“ ili „vrlo važna“ ikada izgubili pristup svojem novčaniku i na koji način.

Slika 5.15. Način gubitka pristupa kriptovalutama



Izvor: Rad autora

Svrha zadnjeg pitanja je provjera razloga gubitka novčanika. Ako su ispitanici na prethodno pitanje odgovorili s „da“, pozvani su da odgovore na koji način su izgubili pristup. Od ponuđenih odgovora su mogli odabrati između : „hakiranje novčanika“, „hakiranje davatelja usluge“, „izgubljena lozinka“, „izgubljena lozinka i kod za oporavak“ ili „nešto drugo“. Ovo pitanje će poslužiti u dubinskoj analizi s ciljem provjere koje dobne skupine i kod kojih kripto novčanika je izgubljen pristup. Od 102 odgovora samo 12 ispitanih su izgubili pristup novčaniku. 8 ispitanih (66,67%) je izgubilo lozinku novčanika, dvoje (16,67%) su izgubili lozinku i kod za oporavak što predstavlja potpuni gubitak novčanika i svih kriptovaluta. Dvoje ispitanika (16,67%) je pretrpjelo hakerski napad koji je bio usmjeren na njihove novčanike.

5.2. Zaključak istraživanja

Na temelju rezultata iz provedenog istraživanja u kojemu je anketirano 102 ispitanika u nastavku su doneseni neki od zaključaka korištenjem dubinske analize podataka.

Unutar promatranog uzorka dobna skupina od 31 do 40 godina je ponudila najviše odabira opcija „vrlo važno“ i „važno“ kod pitanja važnosti sigurnosti kriptovaluta. Ova

dobna skupina se najviše bavila trgovanjem kriptovaluta, 34 ispitanika, dok se rudarenjem bavilo njih 12. Ispitanici koji su se samo bavili trgovanjem najviše su koristili web novčanik. Pretežito su koristili manje poznate davatelje usluge web novčanika s pretpostavkom da su većina bili novčanici kripto tokena. Ostali poznatiji korišteni davatelji usluge su bili Coinbase, Kraken i Binance. Promatrana dobna skupina izjavila je da smatra hardverski novčanik najsigurnijim kripto novčanikom. Slijedi ga web novčanik. Većina ispitanika ove skupine smatra da njihove kriptovalute nisu sigurne. Redovito provjeravaju stanje svojih kriptovalute te ih većina razdvaja na nekoliko davatelja usluge. Jednostavnost korištenja kripto novčanikom im je manje bitna. 16 ispitanika je odgovorilo da bi koristili uslugu 100% zaštite kriptovaluta od koje bi većina platila iznos u rasponu od 11 do 25 dolara. Većina ispitanika koji nisu bili sigurni u vjerojatnost pretplate na uslugu bi plaćali u rasponu od 5 do 10 dolara. 89% ispitanika nije izgubilo pristup svojim novčanicima. Samo su četiri ispitanika izgubila pristup svojim kriptovalutama tako da su izgubili lozinku od kojih je jedan izgubio lozinku i kod za oporavak. Iz priloženog se može zaključiti da je dobna skupina od 31 do 40 godina adekvatno educirana o kriptovalutama i metodama pohrane. Svjesni su potencijalnih rizika gubitka svojih sredstava te se na odgovarajući način štite od gubitka kriptovaluta.

Kada se promatraju ispitanici iz najstarije skupine prema dobi tj. više od 50 godina, većina ispitanika je izjavila da im je sigurnost kriptovaluta jako važna. Svi ispitanici iz skupine su se bavili trgovanjem kriptovaluta kao načinom stjecanja. Najviše se koristi web novčanik koji je istovremeno smatran i najsigurnijim. Najkorišteniji davatelj usluge bio je Coinbase. Najčešći razlog korištenja ovog davatelja usluge je jednostavnost, dobar dizajn i preporuke poznanika i zajednice. Većina ispitanika ne razdvaja svoje kriptovaluta te pretežito smatraju da su sigurne iako često provjeravaju stanje novčanika. Analizom odgovora je uočeno da unutar ove dobne skupine nisu sigurni bi li plaćali uslugu zaštite kripto novčanika. Ako bi se odlučili na uslugu plaćanja, preferirali bi najjeftiniju opciju. Jedan ispitanik je izgubio lozinku za pristup novčaniku. Može se primijetiti da se odgovori starije dobne skupine ne razlikuju mnogo od prethodno analizirane skupine. Utvrđena je specifična situacija u kojoj ispitanici ne iskazuju interes za plaćanje dodatnih troškova na uslugu za koju vjerojatno smatraju da im nije potrebna. Posljedica toga se vidi u odabiru najnižeg vrijednosnog raspona

usluge. Uz to može se zaključiti da je starija dobna skupina također poprilično educirana.

Skupina ispitivanih koji su izjavili da stječu kriptovalute rudarenjem smatra da je sigurnost kripto novčanika izrazito važna budući da se prema izjavama ne pouzdaju u davatelje usluge. Svi ispitanici se odlučuju na razdvajanje kriptovaluta ponajviše na web i desktop novčanik te hardverski novčanik za dodatno osiguranje sigurnosti. Među korištenim davateljima usluge se pronašao Coinbase kao web, Exodus kao desktop i kombinacija Ledger i Trezor kao hardverski novčanik. Budući da se bave rudarenjem podatak o stanju kriptovaluta im je uvijek dostupan te je provjera stanja uhodana radnja. Programi koji se koriste za rudarenje imaju rudimentaran dizajn pa se s time potvrđuje podatak da im jednostavnost korištenja kripto novčanicima nije važna. Iako polovica ispitanih koristi hardverski novčanik u cilju povećanja sigurnosti kriptovaluta, izjavili su da bi plaćali dodatnu uslugu zaštite kriptovaluta. Vrijednosni raspon koji je za njih bio najisplativiji je 5 do 10 dolara. Pretpostavka za to je razlog već investiranih novčanih sredstava u hardverski novčanik. Većina nije izgubila pristup novčaniku. Iz promatranog je nesporno da osobe koje rudare kriptovalute ulažu veće napore u očuvanje sigurnosti. Vidljivo je da su spremni izdvojiti određeni iznos za dodatnu razinu sigurnosti.

Ako se promatraju ispitanici koji su izjavili da im je sigurnost kriptovaluta izrazito važna prema analiziranim podacima utvrđeno je devet izgubljenih pristupa novčaniku. Ovaj podatak iako nije brojčano značajan stvara zabrinutost u neznanje i lakovjernost ispitanih. Od devet ispitanih osam je izgubilo lozinku što predstavlja neodgovornost vlasnika.

6. PRIJEDLOG POBOLJŠANJA METODA POHRANE KRIPTOVALUTA

U ovom radu su analizirane dostupne metode pohrane kriptovaluta. Analizom dobivenih odgovora iz provedene ankete prikupljene su informacije o potrebama i željama vlasnika novčanika. Sigurnost kriptovaluta predstavlja visoku važnost za vlasnike. Napadi na kriptovalute odnosno kripto novčanike su i dalje aktualni za razliku od napada na digitalne valute koje se nalaze u bankarskim institucijama. Sve češći hakerski napadi zahtijevaju pojačanu zaštitu ove digitalne valute. Osim hakerskih napada sve su češći slučajevi eksploatiranja ljudske nebrige, neznanja, neinformiranosti i lakovjernosti.

S ciljem smanjenja broja izgubljenih kriptovaluta odnosno pristupa kripto novčanicima, vlasnicima se predlaže edukacija na temu sigurnosti. Po završetku registracije u kripto novčanik predlaže se da davatelji usluge pošalju novim korisnicima kratke video zapise, ali i tekstualne edukacijske materijale putem e-pošte. Korisnici bi trebali biti upućeni na provjeru autentičnosti web stranice na koju se prijavljuju budući da su lažne stranice sve češće, a sadrže sličan dizajn i URL adresu. Uz to predlaže se redovito informiranje vlasnika o unošenju kompleksnijih lozinki za prijavu, redovitu provjeru stanja novčanika, provjeru adresa pri slanju kriptovaluta, sigurnosnu pohranu fraze za oporavak itd. Kao dodatna razina sigurnosti davateljima usluge se predlaže integriranje sigurnosne značajke kod koje bi korisnici češće bili prisiljeni mijenjati lozinku (svakih tri ili šest mjeseci). Postotak otuđenih kriptovaluta bi se trebao smanjiti pri redovitoj promijeni i unošenjem složenije lozinke.

Davatelji usluge kripto novčanika trebali bi na svojim web stranicama češće i u značajnijem opsegu obavještavati svoje korisnike o sigurnosnim aspektima kripto novčanika. Kod prijave u web novčanik preporučljivo bi bilo vlasnicima generirati skočni prozor (eng. *pop-up window*) koji bi ih obavijestio o neuključenim sigurnosnim postavkama. Većina web novčanika sadrži već uobičajenu 2-faktorsku autentifikaciju koja u proces prijave uvodi dodatnu sigurnosnu razinu. U budućnosti se pretpostavlja da će se koristiti biometrijske karakteristike čovjeka poput otiska prsta ili skena oka za pristupanje kripto novčanicima. Budući da danas većina korisnika prijenosnih i stolnih računala te mobilnih uređaja ima web kameru, kao dodatna razina zaštite moglo bi se

implementirati skeniranje lica vlasnika kao način prijave u novčanik.

Kao dodatna sigurnosna značajka za sve kripto novčanike predlaže se uvođenje opcije pri kojoj bi vlasnici pri svakom pristupanju novčaniku morali unijeti sve svoje pristupne podatke (korisničko ime, lozinka i dodatna metoda – npr. otisak prsta). Ova opcija bi bila neobvezujuća i preporučljiva korisnicima koji žele dodatno osigurati svoje kripto novčanike.

Kod hardverskih novčanika proizvođačima se predlaže implementacija popusta pri kupnji novog uređaja za postojeće kupce. Utvrđeno je da se kod Ledger novčanika vlasnici brinu za dugotrajnost baterije i ponavljanje kupnje istog uređaja po standardnim cijenama. Ako bi postojeći kupci ostvarili popust pri kupnji novog uređaja veća je vjerojatnost da bi ih privukli na kupnju. Dodatna mogućnost je vraćanje starih uređaja pri čemu bi proizvođači ostvarili pozitivni dojam od strane javnosti zbog brige o okolišu i zagađenju. Proizvođači bi trebali razmisliti o opciji zamijene baterije od strane kupaca. Kao dodatna sigurnosna zaštita predlaže se primjena skenera otiska prsta koji bi bio integriran u hardverski novčanik.

Iz analiziranih odgovora dobivenih putem istraživanja činjenica je da je određenom postotku vlasnika kripto novčanika dizajn i navigacija unutar aplikacije relativno važna. Utvrđeno je da dobro osmišljen dizajn kod mobilnih novčanika može pomoći u zadržavanju korisnika. Predlaže se da osobe koje projektiraju dizajn sučelja optimiziraju navigaciju na praktičan način. Pod ovime se smatra da korisnici sa što manje koraka dođu do željene funkcionalnosti.

Za korisnike desktop novčanika se predlaže redovito ažuriranje aplikacije. Važno je spomenuti i antivirusne aplikacije koje bi isto tako trebalo obnavljati i češće koristiti u cilju smanjenja rizika od potencijalnih trojanskih hakerskih napada koji oponašaju službene aplikacije. Ako se kriptovalute pohranjuju na računalo predlaže se povremena provjera ispravnosti diska na kojega se pohranjuju.

7. ZAKLJUČAK

Ovaj diplomski rad objašnjava pojam i metode pohrane kriptovaluta. Cilj rada bio je istražiti kriptovalute i metode pomoću kojih se pohranjuju. S ciljem dobivanja potrebnih informacija o metodama pohrane kriptovaluta istražena je literatura na ovu temu. Za potrebe istraživanja provedena je anketa.

Ubrzani razvoj globalizacije 2008. godine doveo je do zaokreta na financijskom tržištu. Kreirana je prva kriptovaluta pod nazivom Bitcoin. Bio je to prvi pokušaj predstavljanja digitalne valute koja je u kompletnosti decentralizirana od strane državnih institucija. Ova vrsta digitalne valute zahtijeva korištenje napredne kriptografske tehnologije koja je bazirana na *blockchainu* tj. lancu blokova. Lanac blokova sadrži sve kreirane transakcije koje se dugoročno pohranjuju na mrežu. Transakcije su vidljive svim korisnicima koji su zaslužni za verifikaciju zapisa. Lanac blokova osigurava visoku razinu sigurnosti i anonimnosti svih sudionika. U nastavku drugog poglavlja su predstavljene najpopularnije kriptovalute i metode stjecanja.

Za analizu dobivenih informacija iz provedenog istraživanja bilo je potrebno utvrditi dostupne metode pohrane kriptovaluta. Utvrđeno je da su metode pohrane podijeljene na dvije temeljne vrste: vruće i hladne kripto novčanike. Iz prikupljene i istraživane literature dolazi se do zaključka da su hladni novčanici sigurniji za vlasnike kriptovaluta. Njihova osnovna značajka izvanmrežne pohrane predstavlja ključnu prednost nad vrućim novčanicima.

Sve veći porast broja vlasnika kriptovaluta nameće problematiku sigurnosti kripto novčanika. Posljedično se stvara prilika za kriminalnim radnjama koje mogu imati znatnu financijsku štetu. Iz prakse je vidljivo da ljudski faktor utječe na sigurnost kripto valuta kroz obmanu vlasnika i hakerske napade na davatelje usluge web novčanika.

U istraživačkom dijelu rada postavljena su pitanja čija je svrha bila dobiti uvid u mišljenja vlasnika kriptovaluta. Tema ankete su bile metode pohrane odnosno kripto novčanici. Ispitanici su putem ankete iskazali da su za njih najkorištenije metode pohrane bili web novčanici. Većina ispitanika se bavila trgovanjem kriptovaluta. Bili su zabrinuti za stanje sigurnosti, redovito su provjeravali stanje novčanika te su svoje kriptovalute razdvajali na nekoliko davatelja usluge kripto novčanika.

U posljednjem poglavlju istraživačkog dijela izrađen je prijedlog poboljšanja metoda pohrane kriptovaluta. U nastavku su izneseni zaključci na temelju svih prikupljenih i analiziranih informacija.

IP1:

Kada govorimo o sigurnosti pohrane kriptovaluta odnosno virtualnih financijskih sredstava, koja se od dostupnih metoda za ispitani uzorak korisnika kriptovaluta u Hrvatskoj smatra sigurnijom te boljom od ostalih?

Provedeno istraživanje je pokazalo da su svi ispitanici upoznati s web novčanikom kojega istovremeno koristi njih 98. Iz analiziranih odgovora dolazimo do pitanja u kojemu je 44 ispitanika izjavilo da smatra da je web novčanik najsigurniji. Najzastupljeniji davatelji usluge među 44 ispitanika su bili Coinbase i Binance. Ispitanici su pretežito navodili visoku sigurnost, dobro razvijenu mobilnu aplikaciju, jednostavan dizajn, visoku količinu podržanih kriptovaluta kao razloge korištenja. Prema odgovorima dolazi se do zaključka da brojni ispitanici smatraju da davatelji usluge web novčanika ulažu velike napore i financijska sredstva u svrhu poboljšanja i očuvanja stanja sigurnosti kriptovaluta svojih korisnika. Iako je web novčanik statistički gledano bio najbrojniji među odgovorima prema sigurnosti važno je spomenuti podatak da su brojni ispitanici istovremeno koristili desktop i hardverski novčanik.

IP2:

Zbog kojih razloga se korisnici kriptovaluta u Hrvatskoj odlučuju za određene metode pohrane kriptovaluta?

Analizirajući dobivene odgovore u četrnaestom pitanju neki od razloga zašto većina ispitanika koristi web novčanik je bila jednostavnost korištenja, popularnost i preporuke ostalih korisnika. Kao dodatna prednost navodi se pristupačnost novčaniku. Većina poznatijih web novčanika posjeduje vlastitu mobilnu aplikaciju što im omogućava veću zastupljenost budući da je za njihovo korištenje potrebna samo internetska povezanost koja je u današnje vrijeme uvijek dostupna. Korištenje mobilnim novčanicima je bila manje zastupljena zbog nedovoljne informiranosti odnosno zato što su njihove funkcionalnosti pretežito identične web novčanicima. Hardverski novčanici se koriste zbog velikog broja podržanih kriptovaluta, značajnih

sigurnosnih aspekata među kojima je izvanmrežna pohrana koju ispitanici zahtijevaju i činjenica da ne ovise o trećoj strani odnosno davatelju usluge.

IP3:

Koje dobne skupine među korisnicima kriptovaluta u Hrvatskoj daju veću pozornost sigurnosti između različitih metoda pohrane kriptovaluta?

Dubinskom analizom podataka utvrđeno da je dobnim skupinama od 18 do 30 i 31 do 40 godina sigurnost kriptovaluta vrlo važna. Ako bi se promatrale skupno ocjene „vrlo važna“ i „važna“ prema skali važnost tada prevladavaju ispitanici iz skupine od 31 do 40 godina s 40,12%. Dobna skupina od 31 do 40 godina smatra da su približno podjednako sigurni hardverski i web novčanici. Većina ispitanika redovito pregledava stanje svojih kriptovaluta, razdvaja ih na više davatelja usluge te 90% unutar skupine nije izgubilo pristup kripto novčaniku. Izjavili su da bi bili spremni plaćati uslugu 100% sigurnosti kriptovaluta po cijeni od 10 do 25 dolara.

Iz svih prikupljenih informacija može se zaključiti da je sigurnost kriptovaluta i metoda pohrane izrazito važna za vlasnike. Istovremeno najpoznatijom i najsigurnijom metodom pohrane se smatra web novčanik. Analizom literature se može doći do zaključka da web novčanik nije najsigurnija metoda pohrane. Hladni novčanici se zahvaljujući izvan mrežnoj pohrani generalno smatraju najboljom metodom pohrane kriptovalute. Trgovanje prevladava kao način stjecanja kriptovaluta. Vlasnici kriptovaluta razdvajaju kriptovalute na nekoliko davatelja usluge. Preferiraju dobro dizajnirane i osmišljene kripto novčanike koji im pružaju sve potrebne funkcionalnosti uz visoku razinu sigurnosti. Ako bi bila osmišljena usluga koja štiti kripto novčanike od hakerskih napada, vlasnici bi bili spremni platiti takvu uslugu u nižim iznosima.

Ovaj diplomski rad je namijenjen svim postojećim i novim korisnicima kriptovaluta koji u zbirnom radu nastoje provjeriti dostupne i čim sigurnije metode pohrane kriptovaluta, njihove karakteristike i razinu sigurnosti. Uz teoriju moguća je provjera stanja korištenja određenih kripto novčanika na anketiranom uzorku. Daljnji razvitak istraživanja ove teme može se ostvariti putem evaluacije odgovora značajnijeg uzorka pomoću kojega se mogu steći složeniji odgovori i ravnopravno raspoređene dobne skupine. Zbog ubrzanog napretka tehnologija nužno je kroz slijedećih godinu-dvije provesti ponovljeno istraživanje novije literature na temu kripto novčanika i njihove

sigurnosti.

LITERATURA

a) Knjige

1. Karame G., Audroulaki E. (2016). *Bitcoin and Blockchain Security*. London: Artech House.
2. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press.
3. Rosenberg W. (2017). *A Quick Guide to Bitcoin Security: Securing your Bitcoins from Theft, Hacking and Accidental Loss.* CreateSpace Independent Publishing Platform; Bitcoin Security edition.
4. Shrivastava G., Le D., Sharma K. (2020). *Cryptocurrencies and Blockchain Technology Applications*. Beverly: Scrivener Publishing
5. Antonopoulos A. (25.7.2017.) *Mastering Bitcoin*. Oreilly.
6. (2019). *Transacting in Crypto-assets: Management Considerations and Controls for Small and Medium-sized Enterprises*. Canada: Chartered Professional Accountants of Canada. Preuzeto s: https://www. cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/transacting-in-crypto-assets-for-smes (22.5.2021.)

b) Članci

7. Bartolucci S., Kirilenko A. (2020). A model of the optimal selection of crypto assets. *Royal Society Open Science.* Preuzeto s: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7481708/# (27.4.2021.)
8. Dika A. (2017). Ethereum Smart Contracts: Security Vulnerabilities and Security Tools. *Norwegian University of Science and Technology.* Preuzeto s: https://www.researchgate.net/publication/333590995_Security_Vulnerabilities_in_Ethereum_Smart_Contracts/link/5dd2a955299bf1b74b4ca6b9/download (26.4.2021.)

9. Vyas C., Lunagaria M. (2014). Security Concerns and Issues for Bitcoin. *International Journal of Computer Applications*. No. 2. Preuzeto s: https://www.ijcaonline.org/proceedings/ncwbcb/number2/16513-1414 (26.4.2021.)

10. Zimonja O., Vujić D. (2020). Kriptovalute - izazovi aktuelnog globalnog trenda za kriminalističku praksu. *Kriminalistička teorija i praksa*, Vol. 7. No. 2/2020. 55-71. Preuzeto s: https://hrcak.srce.hr/252827 (26.4.2021.)

c) Internetski izvori

11. Skalkotos D. (2019). How to properly safeguard massive amounts of cryptocurrency assets. *Securityinfowatch.com*. Preuzeto s: https://www.securityinfowatch.com/cybersecurity/information-security/managed-network-security/article/21078831/how-to-properly-safeguard-massive-amounts-of-cryptocurrency-assets (26.4.2021.)

12. (2021). Securing your wallet. *bitcoin.org* Preuzeto s: https://bitcoin.org/en/secure-your-wallet#online (26.4.2021.)

13. (2021). How To Store Cryptocurrency Safely in 2021. *cryptonews.com.* Preuzeto s: https://cryptonews.com/guides/how-to-store-cryptocurrency-safely.htm (26.4.2021.)

14. (14.2.2021). World Most Popular Hardware Wallet-Ledger Nano S and Nano X. Ox-currencies.com/. Preuzeto s: https://ox-currencies.com/world-most-popular-hardware-wallet-ledger-nano-s-and-nano-x/ (26.4.2021.)

15. Security First. Always. *Crypto.com.* Preuzeto s: https://crypto.com/security (26.4.2021.)

16. *https://ec.europa.eu/croatia/cryptocurrencies_and_blockchain_all_you_need_to_know_hr*

17. Lawrence A. (16.6.2021). Criminals are mailing altered Ledger devices to steal cryptocurrency. *bleepingcomputer.com* Preuzeto s: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency/ (27.7.2021.)

18. Lawrence A. (7.12.2021). Twitter bots pose as support staff to steal your crypto-currency. *bleepingcomputer.com* Preuzeto s: https://www.bleepingcomputer.com/news/security/twitter-bots-pose-as-support-staff-to-steal-your-cryptocurrency/ (10.12.2021.)

19. Lawrence A. (4.11.2021). Crypto investors lose $500,000 to Google Ads pushing fake wallets. *bleepingcomputer.com* Preuzeto s: https://www.bleepingcomputer.com/news/security/crypto-investors-lose-500-000-to-google-ads-pushing-fake-wallets/ (5.12.2021.)

20. Lawrence A. (21.12.2020). Physical addresses of 270K Ledger owners leaked on hacker forum. *bleepingcomputer.com* Preuzeto s: https://www.bleepingcomputer.com/news/security/physical-addresses-of-270k-ledger-owners-leaked-on-hacker-forum/ (5.12.2021.)

21. Chang E. (9.2.2021). 10 Ways to Keep Your Cryptocurrency *Safe. money.usnews.com* Preuzeto s: https://money.usnews.com/investing/cryptocurrency/slideshows/ways-to-keep-your-cryptocurrency-safe (10.12.2021.)

22. Frankenfield J. (8.8.2021). Bitcoin wallet. *Investopedia.com*. Preuzeto s: https://www.investopedia.com/terms/b/bitcoin-wallet.asp (12.12.2021.)

23. Eddu O (9.2.2021). Crypto Dusting Attacks and Clever Ways to Prevent It. *ox-currencies*. Preuzeto s: https://ox-currencies.com/crypto-dusting-attacks-and-clever-ways-to-prevent-it/ (15.12.2021.)

24. (28.11.2018). What Is a Dusting Attack?. *academy.binance.* Preuzeto s: https://academy.binance.com/en/articles/what-is-a-dusting-attack (15.12.2021.)

25. Eddu O. (17.12.2020). Best Hot and Cold Bitcoin Wallets. *ox-currencies*. Preuzeto s: https://ox-currencies.com/best-hot-and-cold-bitcoin-wallets/ (15.12.2021.)

26. (29.7.2020). Addressing the july 2020 e-commerce and marketing data breach — a message from ledger's leadership. *ledger*. Preuzeto s: https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach (15.4.2022.)

27. Arunović D. (24.2.2018). Što je u stvari blockchain i kako radi?. *Bug.* Preuzeto s: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011

(13.4.2022.)

28. Dean B. (15.4.2021). Coinbase Usage and Trading Statistics (2022). *backlinko.* Preuzeto s: https://backlinko.com/coinbase-users (13.4.2022.)
29. Dossett J. (20.3.2022). Best Bitcoin and Crypto Wallets for July 2022. *cnet.* Preuzeto s: https://www.cnet.com/personal-finance/crypto/the-best-bitcoin-and-crypto-wallets/ (13.4.2022.)
30. (30.4.2022). Understanding the value of a cryptocurrency. *analyticsinsight*. Preuzeto s: https://www.analyticsinsight.net/understanding-the-value-of-a-cryptocurrency/ (5.5.2022.)
31. Kladarić M. (05.4.2018). 15 načina kako da dođete do svog prvog bitcoina. *crobitcoin*. Preuzeto s: https://crobitcoin.com/15-nacina-kako-da-dodete-do-svog-prvog-bitcoina/ (5.5.2022.)
32. Bitcoin novčanici wallets. *crobitcoin*. Preuzeto s: https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/ (5.5.2022.)
33. (30.4.2022). Bitcoin novčanici – odaberite najbolji za jednostavno korištenje i kriptosigurnost. *kriptomat*. Preuzeto s: https://kriptomat.io/hr/kriptovalute/bitcoin/sto-je-bitcoin-novcanik/ (5.5.2022.)
34. (2.2021.) *Gocardless*. Preuzeto s: https://gocardless.com/guides/posts/what-are-cryptoassets/ (5.5.2022.)
35. (2.7.2021). Kriptovalute u turističkoj, event i kongresnoj industriji. *Meetinzagreb*. Preuzeto s: https://www.meetinzagreb.hr/novosti/kriptovalute-u-turistickoj-event-i-kongresnoj-industriji (5.5.2022.)
36. Viktor F. (02.10.2020). Bitcoin Private Keys: Everything You Need To Know. *crobitcoin*. Preuzeto s: https://www.tokenexus.com/bitcoin-private-keys-everything-you-need-to-know/ (5.5.2022.)

POPIS SLIKA

SLIKE

PRILOZI

Pitanja za anketu

1. Označite Vaš spol
2. Označite Vašu dob
3. Na koji način stječete kriptovalute?
4. Koliko Vam je važna sigurnost vaših kriptovaluta?
5. Koje od navedenih kripto novčanika prepoznajete?
6. Koje od navedenih kripto novčanika koristite?
7. Koji korišteni kripto novčanik smatrate da je najsigurniji?
8. Ako se kripto novčanik kojega koristite razlikuje od onoga za kojega smatrate da je najsigurniji, zašto ne koristite sigurniju metodu pohrane?
9. Razdvajate li svoje kriptovalute na više davatelja usluge kripto novčanika?
10. Navedite davatelje usluge kripto novčanika koje koristite?
11. Smatrate li da su Vaše kriptovalute 100% sigurne u kripto novčaniku kojega koristite?
12. Koliko često provjeravate stanje svojih kriptovaluta?
13. Koliko Vam je važna jednostavnost korištenja kripto novčanika?
14. Zašto koristite odabrane kripto novčanike?
15. Što Vam se ne sviđa kod kripto novčanika kojega koristite?
16. Što bi promijenili na postojećom kripto novčaniku kojega koristite?
17. Biste li plaćali pretplatu na uslugu koja promovira 100% sigurnost kriptovaluta?
18. Ako ste na prethodno pitanje odgovorili s „Da“ ili „Možda“, u kojem rasponu ste spremni platiti za tu uslugu ?
19. Jeste li ikada izgubili pristup kripto novčanika?
20. Ako ste na prethodno pitanje odgovorili s „Da“, na koji ste način izgubili pristup?

ŽIVOTOPIS

OSOBNI PODACI

Ime i prezime: Filip Ladešić
Datum rođenja: 12.01.1995.
Adresa: Klaićeva 72, 10 000 Zagreb, Hrvatska
Mobitel: +385 98 638511
E-mail: filip.ladesic@gmail.com

OBRAZOVANJE

- 2020.- 2022. (očekivano)

VERN' Zagreb; Diplomski stručni studij
Smjer: IT Menadžment

- 2017. - 2019.

VERN' Zagreb; Preddiplomski stručni studij
Smjer: Ekonomija poduzetništva

RADNO ISKUSTVO

- srpanj 2021. -

Hrvatska turistička zajednica
Odjel za eVisitor i aplikativna rješenja

VJEŠTINE

- Strani jezici: Engleski jezik: certifikat Business English Certificate Vantage - B2
- Računalne vještine: Microsoft Office paket, Adobe Photoshop, Sony Vegas
- Komunikacijske i organizacijske vještine: Iskustvo u grupnim zadacima i rad na projektima u timu, dobre prezentacijske vještine, organiziranost
- Vozačka dozvola: B

HOBI I INTERESI

Nove tehnologije i njihova primjena u poslovnom svijetu, sport